Universidad de Antioquia
Facultad de Ciencias Exactas y Naturales
Programa de pregado de Matemáticas

Trabajo de grado

sobre la conjetura del divisor de cero y la conjetura de intersección de Peskine-Szpiro

Juan Camilo Sierra Rangel

Asesor: Pedro Hernandez Rizzo
Profesor Instituto de Matemáticas
Universidad de Antioquia

Medellín

2 0 2 2

Índice

Agradecimientos

A mis padres Eduith Sierra y Gloria Rangel por sus esfuerzos y sacrificios en beneficio a la educación a sus hijos.

A mis amigos por su apoyo en todo el transcurso de mi vida académica. En particular, a Mateo Restrepo por toda su motivación y colaboración.

A mi asesor Pedro Hernandez Rizzo por la paciencia y la ayuda brindada durante sus cursos y el desarrollo de este trabajo de grado.

A la Universidad de Antioquia por brindarme un espacio para mi formación académica, profesional y personal.

1. Introducción

El estudio de las propiedades homológicas de algunos objetos pertenecientes al área del algebra conmutativa han conducido a proponer numerosas conjeturas con el transcurso de los años. Ejemplos ilustres de estas formulaciones son las llamadas *Conjeturas Homológicas*. Dicho término hace referencia a un cierto conjunto de conjeturas relacionadas sobre propiedades homológicas en anillos conmutativos.

En 1975 el matemático Mel Hochster en su monografía *Topics in the homological theory of modules over commutative rings* (ver [HO]) propone una serie de conjeturas en donde extiende la lista de problemas abiertos que se conocían hasta entonces y resuelve varios de ellos. En particular, es mencionado el problema conocido como *The Canonical Element Conjecture*, donde Hochster introdujo un número de formas equivalentes de esta conjetura y las probó para un caso muy particular conocido como "the equicharacteristic case". Una de las formas tempranas de la conjetura, conocida por *la conjetura del sumando directo*, fue demostrada por Hochster una década antes bajo las mismas hipótesis que propuso. En 1973 los matemáticos C. Peskine y L. Szpiro en su artículo *dimensión projective finie et cohomologie locale* (ver [PE]) probaron el problema conocido como *teorema de interseccion* formulado años antes por el matemático Jean Pierre Serre para los siguientes casos:

1. Anillos con característica prima.
2. Anillos que son esencialmente de tipo finito sobre un campo de característica cero.
3. Anillos ind- étale sobre un anillo local de la forma mencionada en el numeral anterior.

Muchas de las conjeturas homológicas surgieron de los intentos de Serre por definir una noción adecuada de multiplicidad de intersección para variedades algebraicas de dimensión mayor que uno. En particular, si R es un anillo local regular y si M y N son R-módulos finitamente generados tales que $M \otimes_R N$ tiene una longitud finita, Serre define la multiplicidad de intersección de M y N como:

$$\chi(M, N) = \sum_{i=0}^{\infty} (-1)^i l(Tor_i^R(M, N)).$$

Conjeturando que esta noción satisface las siguientes propiedades:

Conjetura (de Multiplicidad de Serre). Para M y N son R-módulos finitamente generados tales que $M \otimes_R N$ tiene una longitud finita se cumple que:

1. $dim(M) + dim(N) \leq dim(R)$.
2. $\chi(M, N) \geq 0$.
3. $\chi(M, N) > 0$ si y solo si $dim(M) + dim(N) = dim(R)$.

Como cada módulo finitamente generado sobre un anillo local regular tiene dimensión proyectiva finita, es natural conjeturar que las mismas afirmaciones se sostienen sobre un anillo local Noetheriano arbitrario si uno de los módulos, digamos M, tiene una dimensión proyectiva finita. Con esto en mente, un resultado estrechamente relacionado, formulado por Peskine y Szpiro, es el siguiente:

Teorema de la intersección. Sean R un anillo local noetheriano y M un R-módulo finitamente generado no-cero de dimensión proyectiva finita. Entonces para cada R-módulo N finitamente generado tal que $M \otimes_R N$ tiene longitud finita, se tiene que:

$$dim(N) \leq d.h_R(M).$$

Peskine y Szpiro, a partir de las técnicas aplicadas para el caso de característica prima, presentaron una prueba del caso (2) a través de un proceso que hoy es conocido como *reducción a la característica p*. Este procedimiento fue refinado más tarde por Hochster para dar una prueba del Teorema de Intersección para todos los anillos locales Noetherianos equicaracterísticos y el caso característico mixto fue probado por el matemático Paul Roberts usando diferentes métodos.

En 1980, los matemáticos G. Evans y P. Griffith dieron una respuesta afirmativa al problema de la sizigia para anillos locales equicaracterísticos. En el transcurso de su prueba, establecieron implícitamente un resultado para complejos libres finitos, el cual Hochster trataba explícitamente en su artículo. Se refirió al nuevo resultado como el "nuevo teorema de intersección mejorado" (en adelante, INIT). Por supuesto INIT sigue siendo una conjetura en el caso de característica mixta. En el mismo artículo Hochster señaló que el INIT fue una consecuencia de la conjetura del elemento canónico y más tarde el matemático S. P. Dutta en su trabajo *On the canonical element conjecture*, mostró que las dos conjeturas son equivalentes. A lo largo de los años se han probado varios casos especiales de la conjetura del elemento canónico y se han introducido nuevas formas equivalentes.

El teorema de la intersección ha atraído mucho interés, en parte porque implica otras dos conjeturas que estaban abiertas en el momento en que se formuló por primera vez. Una de estas conjeturas es la conocida como *Zero Divisor Conjecture* o conjetura del divisor de cero.

Conjetura del divisor de cero. Sea M un R-módulo finitamente generado, con R un anillo conmutativo Noetheriano. Si $M \neq (0)$ tiene dimensión proyectiva finita y $r \in R$ no es un divisor de cero en M, entonces r no es un divisor de cero en R.

El objetivo de este trabajo será establecer la equivalencia que existe entre la famosa conjetura llamada teorema de intersección Peskine-Szpiro y la conjetura del divisor de cero.

2. Preliminares

Antes de enunciar y describir las 4 conjeturas relacionandas con los conceptos de *dimensión homológica*, *profundidad*, *dimensión de Krull*, necesitaremos desarrollar un poco la teoría que hay detrás de la estructura conocida como *Módulo*. En los siguientes capítulos nos ocuparemos de dar una introducción a los conceptos fundamentales para dar construcción a la teoría de *Módulos noetherianos finitamente generados bajo anillos locales*, en donde nos enfocaremos en sus propiedades homológicas.

2.1. Anillos e Ideales

Un *módulo* sobre un *anillo* es una generalización de los espacios vectoriales, donde los elementos que operan sobre el módulo son tomados de un *anillo* dado. En álgebra conmutativa, tanto los anillos como los anillos de cociente son módulos, por lo que muchas propiedades notables de la teoría de módulos son heredadas en la estructura de anillo. Comenzaremos entonces con la descripción y el desarrollo de la noción algebraica de estos objetos matemáticos.

Definición 2.1. *(Anillo). Un anillo conmutativo con unidad es un terna* $(R, +, \cdot)$*, donde* R *es un conjunto no vacío tal que:*

- R *es un grupo abeliano respecto el operación binaria (+).*
- *La operación binaria* $(\cdot)$ *es asociativa,* $(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$*, y distributiva respecto a (+):* $(x \cdot (y + z) = x \cdot y + x \cdot x;\ (y + z) \cdot x = y \cdot x + z \cdot y)$*, para todo* $x, y, z \in R$*.*
- *La operación binaria* $(\cdot)$ *es conmutativa* $(x \cdot y = y \cdot x)$*, para todo* $x, y \in R$*.*
- *Existe un único elemento denotado por* $1 \in R$ *tal que* $x \cdot 1 = 1 \cdot x = x$*, para todos los elementos en* R*. Dicho elemento es llamado elemento identidad.*

Ejemplo 2.2. *El conjunto de enteros* $\mathbb{Z}$ *con las operaciones usuales de suma y producto tiene estructura de anillo.*

Ejemplo 2.3. *El conjunto de polinomios bajo la indeterninante* x *con coeficientes en el conjunto de los reales* $\mathbb{R}$ *denotado por* $\mathbb{R}[x]$ *tiene estructura de anillo.*

Definición 2.4. *Un subcojunto* S *de* R *es llamado subanillo de* R *si es cerrado bajo las operaciones* $(+)$, $(\cdot)$ *y contiene el elemento identidad* $(1 \in S)$*.*

De ahora en adelante abreviaremos la operación de multiplicaión sobre un anillo, $x \cdot y$ como xy.

Definición 2.5. *(Ideal). Un ideal* I *de un anillo* R *es un subconjunto de* R*, tal que es un subgrupo de* $(R, +)$ *y, para cada* $x \in A$ *y* $w \in I$*, se tiene* $xw \in I$*, conocida como propiedad de* absorción*.*

Definición 2.6. *(Anillo de cociente) Dado un anillo* R *y un ideal* I*, el conjunto de las clases de equivalencia definidas por la relación de equivalencia* $a \sim b$ *si y solo si* $a - b \in I$ *denotado por* R/I *se conoce como anillo cociente. Es fácil ver que este conjunto tiene estructura de anillo con suma definida por:* $[a] + [b] := (a + I) + (b + I) = (a + b) + I$*; y multiplicación definida por:* $[a][b] := (a + I)(b + I) := ab + I$*.*

Definición 2.7. *(Homomorfismo de anillos). Un homomorfismo de anillos es una función ϕ del anillo A sobre el anillo B tal que:*

- *ϕ es un homomorfismo de grupos abelianos. ($\phi(x+y) = \phi(x) + \phi(y)$).*
- *$\phi(x \cdot y) = \phi(x) \cdot \phi(y)$, para todo elemento x, y en el anillo A.*
- *$\phi(1) = 1$.*

Una hecho importante que es comunmente usado en demostraciones de propiedades algebraicas de la estructura de anillos, es la correspondencia única que existe entre los ideales del anillo cociente R/I y los ideales que contienen a I. Este hecho es consecuencia de la siguiente propiedad: La imagen inversa de un ideal en un homomorfismo de anillos es un ideal; esta propiedad aplicada al homomorfismo de proyección (sobreyector): $\phi : I \to R/I$, $x \mapsto [x]$, da como resultado la siguiente proposición.

Proposición 2.8. *Existe una correspondencia uno a uno entre los ideales J de un anillo R que contienen al ideal I y los ideales $\overline{J}$ de R/I, dado por $J = \phi^{-1}(\overline{J})$. Donde ϕ es el homomorfismo de proyección (canónico) entre los anillos R y R/I.*

$$\{\textit{Ideales de } R/I\} \overset{1:1}{\longleftrightarrow} \{\textit{Ideales } J \textit{ de } R : I \subseteq J\}$$

Definición 2.9. *(divisor de cero). Un divisor de cero del anillo R es un elemento x para el cual existe un elemento no-nulo tal que $xy = 0$. Un anillo R que no posee divisores de cero no-nulos es llamado Dominio Integral.*

Definición 2.10. *(unidad). Una unidad del anillo R es un elemento x para el cual existe un elemento y tal que $xy = 1$. El conjunto de unidades de R es denotado por R^*. Un anillo R es llamado Campo si $R^* = R \setminus \{0\}$.*

Definición 2.11. *(elemento nilpotente). Un elemento $r \in R$ de un anillo es llamado nilpotente si existe un natural $n > 0$ tal que $r^n = 0$. El conjunto de todos los elementos nilpotentes de un anillo R es llamado Nilradical y denotado por $\sqrt{R}$.*

Definición 2.12. *(Ideal primo). Un ideal $\mathfrak{p}$ del anillo R es primo si $\mathfrak{p} \neq (1)$ tal que si $xy \in \mathfrak{p}$ entonces $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$.*

Definición 2.13. *(Ideal primario). Un ideal $\mathfrak{q} \neq (1)$ de un anillo R es primario si para un $xy \in \mathfrak{q}$ entonces $x \in \mathfrak{q}$ o $y^n \in \mathfrak{q}$ para algún natural $n > 0$.*

Definición 2.14. *(Ideal maximal). Un ideal $\mathfrak{m}$ del anillo R es maximal si $\mathfrak{m} \neq (1)$ si no existe un ideal propio I y distinto de $\mathfrak{m}$ tal que $\mathfrak{m} \subset I \subset (1) = R$. Si el anillo R posee un único ideal maximal, entonces es llamado anillo local. La intersección de los ideales maximales es llamada de Radical de Jacobson.*

Proposición 2.15. *Sean $\mathfrak{p}$, $\mathfrak{m}$ ideales del anillo R, entonces:*

- *$\mathfrak{p}$ es primo, si y solo si, $R/\mathfrak{p}$ es un dominio integral.*
- *$\mathfrak{m}$ es maximal, si y solo si, $R/\mathfrak{m}$ es un campo.*

Demostración. Es fácil realizar la verificación usando solo la definición. □

Teorema 2.16. *Todo anillo $R \neq (0)$ contiene al menos un ideal maximal.*

Demostración. Ver **Teorema 1.3** en [AY]. $\square$

Corolario 2.16.1. *Si $I \neq (1)$ es un ideal del anillo R, entonces existe un ideal maximal de R que contiene a I .*

Demostración. Ver **Corolario 1.4** en [AY]. $\square$

Corolario 2.16.2. *Todo elemento no-unidad del anillo R pertenece a algún ideal maximal de R.*

Demostración. Ver **Corolario 1.5** en [AY]. $\square$

Definición 2.17. *(Anillo semi-local): Diremos que un anillo R es un anillo semi-local si R tiene un número finito de ideales maximales.*

Definición 2.18. *Sea R un anillo. $\sqrt{R}$ es la intersección de todos los ideales primos de R.*

Definición 2.19. *(radical de un ideal). El radical de un ideal I del anillo R se define como el conjunto de los $r \in R$ tal que existe un natural $n > 0$, con $r^n \in I$. Denotaremos a este conjunto por $\sqrt{I}$.*

Proposición 2.20. *Sea I un ideal de un anillo R. $\sqrt{I}$ es igual a la intersección de todos los ideales primos que contienen a I.*

Demostración. Ver **Proposición 1.14** en [AY]. $\square$

Proposición 2.21.

1. *Sea $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ ideales primos y I un ideal contenido en $\cup_{i=1}^{n} \mathfrak{p}_i$, entonces $I \subseteq \mathfrak{p}_j$, para algún j.*
2. *Sea $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ ideales primos y I un ideal conteniendo a $\cap_{i=1}^{n} \mathfrak{p}_i$, entonces $\mathfrak{p}_j \subseteq I$, para algún j.*

Demostración. Ver **Proposición 1.11** en [AY]. $\square$

Sea $f : R \to Q$ un homorfismo de anillos. si I es un ideal de R, el conjunto $f(I)$ no necesariamente es un ideal de Q. Definimos la extensión I^e de I al ideal generado por $f(I)$ en Q, esto es, el conjunto de todas las sumas finitas $\sum y_i f(x_i)$ donde $x_i \in I$ y $y_i \in Q$. Si J es un ideal de Q, entonces $f^{-1}(J)$ siempre es un ideal de R denotaremos a este ideal por J^c y es llamado contracción de J. Es fácil verificar que si J es primo, entonces J^c es primo.

2.2. Anillo de Fracciones

El anillo de fracciones es una construcción que generaliza la noción de «campo de fracciones» de un dominio integral a anillos conmutativos que pueden contener divisores cero. La construcción embebe un anillo en un anillo «más grande», dando a cada divisor distinto de cero un inverso en el anillo más grande.

Los términos «anillo de fracciones» o «campo de fracciones» se asocian a uno de los conceptos más importantes del álgebra conmutativa conocido como *localización*, debido a que el campo de fracciones coincide con la *localización* con respecto al conjunto de todos los divisores distintos de cero. El proceso de construcción (es análogo) se inspira en la técnica usada en teoría de conjuntos para la construcción del conjunto de números racionales $\mathbb{Q}$ sobre el conjunto de número enteros $\mathbb{Z}$. Más adelante veremos que dicho proceso se puede trasladar a la estructura de módulos.

Definición 2.22. *Sea R un anillo. Un subconjunto multiplicativamente cerrado de R es un conjunto S de R tal que $1 \in S$ y para todo $x, y \in S$, se tiene que $xy \in S$. Un subconjunto S del anillo R es llamado Saturado si para todo $x, y \in S$ se tiene que $x, y \in S$, si y solo si $xy \in S$.*

Definición 2.23. *(Anillo de Fracciones). Sea R un anillo y S un subconjunto multiplicativamente cerrado de R. Definimos la relación $\equiv$ sobre $R \times S$ como:*

$$(a, s) \equiv (b, t) \text{ si y solo si } (at - bs)u = 0 \text{ para algún } u \in S.$$

Dicha relación define una relación de equivalencia sobre el conjunto $R \times S$. Denotamos por a/s a la clase de equivalencia de (a, s) y por $S^{-1}R$ al conjunto de clases de equivalencia sobre $R \times S$.

El conjunto $S^{-1}R$ puede ser dotado de estructura de anillo definiendo la operación de adición y multiplicación sobre las «Fracciones» a/s como sigue:

$$(a/s) + (b/t) = (at + bs)/st.$$
$$(a/s)(b/t) = (ab/st).$$

Es posible verificar la definición de las operaciones anteriores son independientes de la escogencia de los representantes (a, s) y (b, t), que $S^{-1}R$ efectivamente puede ser dotado de estructuta de anillo conmutativo con unidad.

Ejemplo 2.24. *Sea R un anillo. Es trivial verificar que $S = \{1\}$ es un conjunto multiplicativamente cerrado, en este caso $S^{-1}R \cong R$.*

Ejemplo 2.25. *Sea R un anillo, S el conjunto de no divisores de cero de R. Se puede verificar que este conjunto es multiplicativamente cerrado. Un caso particular importante es cuando R es un dominio integral, por tanto $S = R \backslash \{0\}$. Tenemos que $S^{-1}R$ es un campo comúnmente llamado campo de fracciones.*

Ejemplo 2.26. *Para un elemento $r \in R$, el conjunto $S = \{r^n : n \in \mathbb{N}\}$ es multiplicativamente cerrado. $S^{-1}R$ es llamado localización en r denotada por R_r.*

Ejemplo 2.27. *Si $\mathfrak{p}$ es un ideal primo de un anillo R, entonces $S = R \setminus \mathfrak{p}$ es un conjunto multiplicativamente cerrado. el anillo de fracciones $S^{-1}R$, denotado por $R_{\mathfrak{p}}$ es llamado localización de R sobre el ideal $\mathfrak{p}$.*

Proposición 2.28. *Sea S un conjunto multiplicativamente cerrado de un anillo R. Entonces del homomorfismo $\phi : R \to S^{-1}R$ dado por $r \to r/1$ se tiene que:*

- *Para todo ideal I de R, $I^e = \{i/s \in S^{-1}R : i \in I, s \in S\}$.*

- *Para todo ideal J de $S^{-1}R$, $(J^c)^e = I$.*
- *Existe una correspondencia uno a uno entre los conjuntos:*

$$\{\textit{Ideales primos de } S^{-1}R\} \overset{1:1}{\longleftrightarrow} \{\textit{Ideales primos } \mathfrak{q} \textit{ de } R : \mathfrak{q} \cap S = \emptyset\}.$$

Demostración. Ver **Proposición 3.11** en [AY]. □

De la anterior propiedad podemos encontrar una relación entre los ideales de $R_{\mathfrak{p}}$ y R donde $\mathfrak{p}$ es un ideal primo de R. Existe una correspondencia uno a uno entre los siguientes conjuntos:

$$\{\textit{Ideales primos de } R_{\mathfrak{p}}\} \overset{1:1}{\longleftrightarrow} \{\textit{Ideales primos } \mathfrak{q} \textit{ de } R : \mathfrak{q} \subseteq \mathfrak{p}\}.$$

Proposición 2.29. *(Propiedad Universal). Sea ϕ un homomorfismo del anillo R al anillo Q. Sea S un subconjunto multiplicativamente cerrado de R tal que $\phi(s)$ es unidad en Q para todo $s \in S$. Entonces existe un único homomorfismo de anillos ψ de $S^{-1}R$ al anillo Q tal que $\phi = \psi \circ f$, donde f es el homomorfismo estandar del anillo R al anillo $S^{-1}R$ definido por $f(x) = x/1$.*

Demostración. Ver **Proposición 3.1** en [AY]. □

Corolario 2.29.1. *Sea ϕ un homomorfismo del anillo R al anillo Q tal que:*

- *Si $s \in S$, entonces $\phi(s)$ es unidad en Q.*
- *Si $\phi(a) = 0$, entonces $as = 0$ para algún $s \in S$.*
- *Todo $b \in B$ es de la forma $\phi(a)\phi(s)^{-1}$ para algún $a \in R$ y $s \in S$.*

Entonces existe un único isomorfismo ϕ de $S^{-1}R$ al anillo Q tal que $\phi = \psi \circ f$.

Demostración. Ver **Corolario 3.2** en [AY]. □

Proposición 2.30. *Sea I un ideal de un anillo R y $\mathfrak{p}$ un ideal primo. Entonces:*

$$(R/I)_{\mathfrak{p}} \cong R_{\mathfrak{p}}/I_{\mathfrak{p}}.$$

Demostración. Es fácil verificar que la aplicación $\psi : R_{\mathfrak{p}} \to (R/I)_{\mathfrak{p}} : r/s \to (r+I)/s$ es un homomorfismo de anillos bien definido tal que $nucleo(\psi) = I_{\mathfrak{p}}$. □

2.3. R-módulos noetherianos finitamente generados

La propiedad de «absorción» de un ideal es una buena aproximación para comenzar a estudiar la estructura de módulo. En un ideal I, intuitivamente podemos observar que existe una «acción» de cada elemento del anillo que contiene al ideal, sobre la estructura de grupo abeliano en I, definida por $R \times I \to I : (r, i) \to ri$. Dicha «acción» puede ser descrita por un homomorfismo entre anillos: $R \to E(I)$, donde $E(I)$ es el anillo de endomorfismos[1] de I. En un módulo, esta «acción» actua no sobre un ideal del anillo R, sino, sobre un grupo abeliano M. Lo anterior mencionado se describe más extensamente en la siguiente definición.

[1]El conjunto de homomorfismo de grupos puede ser dotado de estructura de módulo, conocido como anillo de endomorfismos.

Definición 2.31. *(módulo). Sea R un anillo. Un R-módulo es un par (M, ψ), donde M es un grupo abeliano respecto a la operación adición $(+)$ y ψ es una función de $R \times M$ sobre M tal que, para todo $a \in R$, $x, y \in M$ se tiene que:*

- $\psi(a, x + y) = \psi(a, x) + \psi(a, y)$.
- $\psi(a + b, x) = \psi(a, x) + \psi(b, x)$.
- $\psi(ab, x) = \psi(a, bx)$.
- $\psi(1, x) = x$.

De ahora en adelante abreviaremos la operación $\psi(a, x)$ como ax ó $a \cdot x$. En vez de hacer referencia al par (M, ψ), diremos que M es un R-módulo. A la funcíon ψ la llamaremos operación de multiplicación por elementos de R.

Ejemplo 2.32. *Todo grupo puede verse como un $\mathbb{Z}$-módulo mediante la operación: $(m, x) \to x + \cdots + x$.*

Ejemplo 2.33. *Si R es un anillo cualquiera y n un número natural, entonces el producto cartesiano R^n puede verse como un R-módulo.*

Definición 2.34. *Sea M, N R-módulos. Un homomorfismo de M a N es una función $f : M \to N$ lineal respecto a la operación de (+), esto es:*

$$f(\alpha x + y) = \alpha f(x) + (y), \text{ para todo } x, y \in M.$$

El conjunto de todos los homomorfismos de R-módulos de M a N puede ser dotado de estructura de R-módulo, el cual denotaremos por $Hom_R(M, N)$.

Definición 2.35. *Un submódulo N de M es un subgrupo de M el cual es cerrado bajo la operación de multiplicación por elemenos de R. Si N es un submódulo de M, entonces es posible dotar de estrucutra de R-módulo al grupo abeliano M/N, al cual llamaremos cociente de N por M.*

Definición 2.36. *Sea $f : M \to N$ un homomorfismo de M a N:*

- *Denotaremos al conjunto $\{m \in M : f(m) = 0\}$ por $nucleo(f)$. Es fácil verificar que este conjunto es submódulo de M.*
- *Denoratemos al conjunto $f(M)$ por $imagen(f)$. Es fácil verificar que este conjunto es submódulo de N.*

Definición 2.37. *Una secuencia de homomorfismos de módulos*

$$\cdots \xrightarrow{\phi_{n-1}} M_{n-1} \xrightarrow{\phi_n} M_n \xrightarrow{\phi_{n+1}} M_{n+1} \cdots.$$

es llamada secuencia exacta en M_n, si $nucleo(\phi_{n+1}) = imagen(\phi_n)$. La secuencia es exacta si dicha secuencia es exacta en todos los módulos M_i.

Definición 2.38. *Sea M un R-módulo y I un ideal de R. Definimos el producto entre I y M, denotado por IM, como el conjunto de todas las sumas finitas $\sum_i a_i m_i$, donde $a_i \in I$, $m_i \in M$. Es fácil verificar que este conjunto es submódulo de M.*

Definición 2.39. *Sea $(M_i)_{i\in J}$. Denotaremos por $\sum M_i$ al conjunto de todas las sumas (finitas) $\sum m_i$ donde $m_i \in M_i$ son cero, excepto en un número finitos de ellos. En caso de que el conjunto de indices J sea finito, denotaremos la suma por $M_1 + \cdots + M_n$.*

Definición 2.40. *Sean N_1 y N_2 submódulos del R-módulo M, definimos $N_1 : N_2 = \{r \in R \ / \ rN_2 \subseteq N_1\}$.*

De la definición anterior se puede verificar que $N_1 : N_2 = (0) : (N_1 + N_2)/N_1$. En particular, tenemos que el anulador de un R-módulo M, denotado por $ann(M)$, esta dado por $(0) : M$.

Una pregunta que puede surgir de la definición de módulo es si dado M un R-módulo y I un ideal de R, ¿será posible extender dicha estructura a R/I-módulo?. En general, esto no es posible, pero existe una relación entre el $ann(M)$ y esta estructura: M es extendible a R/I-módulo si y solo si $I \subseteq ann(M)$. Más adelante será usual pasar de la estructura de R-módulo a R/I-módulo.

Definición 2.41. *(Módulo finitamente generado) Si S es un subconjunto de M, denotaremos por (S), al conjunto de sumas finitas $\sum a_i m_i$, donde $a_i \in R$ y $m_i \in M$. Si S es finito, denotaremos a (S) por $(m_1, \cdots, m_n)$. Un R-módulo M es llamado finitamente generado si existe un conjunto finito $S \subseteq M$, tal que $M = (S) = (m_1, \cdots, m_n)$.*

Proposición 2.42. *(Lema de Nakayama): Sea M un R-módulo finitamente generado e I un ideal de R contenido en el Radical de Jacobson de R. Entonces si $IM = M$ implica que $IM = (0)$.*

Demostración. Ver **Proposición 2.6** en [AY]. □

Definición 2.43. *(Suma directa) Si $(M_i)_{i\in J}$ es una familia de R-módulos, denotaremos por $\oplus_{i\in j} M_i$, al conjunto de $(x_i)_{i\in J}$, donde $x_i \in M_i$ son cero, excepto para un número finito de ellos. En caso de que el conjunto de indices J sea finito, denotaremos la suma directa por $M_1 \oplus \cdots \oplus M_n$.*

Proposición 2.44. *Sea M un R-módulo. M es finitamente generado si y solo si M es isomorfo a un cociente de R^n para algún $n > 0$.*

Demostración. Ver **Proposición 2.3** en [AY]. □

Proposición 2.45. *Sea M un R-módulo finitamente generado, sea $I \subseteq R$ un ideal. Entonces:*

$$\sqrt{ann(M/IM)} = \sqrt{I + ann(M)}.$$

Demostración. Basta con demostrar solo la contención $ann(M/IM) \subseteq \sqrt{I + ann(M)}$. Sea $x \in ann(M/IM)$ y $m_1, \cdots, m_n$ un conjunto de generadores de M. Es fácil verificar que $xM \subseteq IM$. Considere el siguiente sistema de ecuaciones tomando como «incógnitas» los elementos generadores m_i de M:

$$xm_1 = b_{11}m_1 + \cdots + b_{1n}m_n$$
$$\cdots$$
$$xm_n = b_{n1}m_1 + \cdots + b_{nn}m_n$$

Donde $b_{ij} = a_{ij}r_{ij}$. Usando la regla de Cramer se puede verificar que existen elementos $c_i \in I$ tales que:

$$(x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0) \cdot m_1 = 0$$
$$\cdots$$
$$(x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0) \cdot m_n = 0$$

Por lo tanto, tomando $a = c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, obtenemos que $x^n + a \in ann(M)$. Lo anterior implica entonces que $x^n \in I + ann(M)$, es decir, $x \in \sqrt{I + ann(M)}$. □

Definición 2.46. *(Módulo noetheriano) Un R-módulo M es llamado noetheriano si satisface una (por lo tanto todas) de las siguientes condiciones equivalentes:*

1. *Toda cadena ascendente de submódulos de M es estacionaria.*
2. *Todo subconjunto no vacío de submódulos de M posee un elemento maximal.*

Un anillo R es llamado noetheriano si R es noetheriano como R-módulo.

Proposición 2.47. *Un R-módulo M es noetheriano, si y solo si, todo submódulo N de M es finitamente generado.*

Demostración. Ver **Proposición 6.2** en [AY]. □

Proposición 2.48. *(Lema de Artin–Rees) Sea R un anillo noetheriano e I un ideal de R. Si M es un R-módulo finitamente generado y N un submódulo de M, entonces para todo $n \geq 0$, existe un $m \geq 0$ tal que:*

$$I^m M \cap N \subseteq I^n N.$$

Demostración. Ver **Proposición 10.9** en [AY]. □

Proposición 2.49. *Sea R, un anillo noetheriano local con único ideal maximal $\mathfrak{m}$ y M un R-módulo finitamente generado. Sea $x \in \mathfrak{m}$, entonces:*

$$\bigcap_{n \geq 0} (x^n)M = (0).$$

Demostración. Sea $I = (x)$ y $N = \bigcap_{n \geq 0}(x^n)M$. Por la proposición 2.48, existe un $m \geq 0$ tal que $I^m M \cap N \subseteq IN$. Por otro lado, tenemos las inclusiones $N = \bigcap_{n \geq 0}(x^n)M \subseteq (x^m)M = I^n M$. Por lo tanto, $N \subseteq IN$. Dado que I esta contenido en el un único ideal maximal de R, por el Lema de Nakayama en 2.42 obtenemos el resultado buscado. □

Proposición 2.50. *Sea R un anillo noetheriano, M un R-módulo finitamente generado. Entonces M es un R-módulo noetheriano.*

Demostración. Ver **Proposición 6.5** en [AY]. □

2.4. Localización de Módulos

La localización se ha convertido en un herramienta comúnmente usada en álgebra conmutativa debido a que nos permite tratar problemas generales alrededor de la teoría de módulos, (en particular la teoría de anillos) , como unión de problemas «más pequeños» en un sentido local. Anteriormente, vimos la construcción del anillo de fracciones sobre un anillo R cualquiera, en el caso de módulos, la definición es análoga y se puede entender como una generalización. El final de esta sección veremos que la localización de un módulo es un caso especial de un producto tensorial.

Definición 2.51. *(R-módulo de Fracciones). Sea R un anillo y S un subconjunto multiplicativamente cerrado de R. Sea M un R-módulo. Definimos la relación $\equiv$ sobre $M \times S$ como:*

$$(m, s) \equiv (n, t) \text{ si y solo si } u \cdot (t \cdot m - s \cdot n) = 0 \text{ para algún } u \in S.$$

Dicha relación define una relación de equivalencia sobre el conjunto $M \times S$. Denotamos por m/s a la clase de equivalencia de (m, s) y por $S^{-1}M$ al conjunto de clases de equivalencia sobre $M \times S$.

El conjunto $S^{-1}M$ puede ser dotado de estructura de $S^{-1}R$-módulo definiendo las operaciones obvias de adición y multiplicación por escalar.

Ejemplo 2.52.
- *Sea R un anillo e $\mathfrak{p}$ un ideal primo de R. Al conjunto $S^{-1}M$, donde $S = R \setminus \mathfrak{p}$, denotado por $M_\mathfrak{p}$, es llamado localización sobre $\mathfrak{p}$.*

Proposición 2.53. *Si la secuencia $L \to M \to N$ es exacta en M entonces $S^{-1}L \to S^{-1}M \to S^{-1}N$ es una secuencia exacta en $S^{-1}M$.*

Demostración. Ver **Proposición 3.3** en [AY]. □

Proposición 2.54. *Sea M un R-módulo. Las siguientes afirmaciones son equivalentes:*

1. *$M = (0)$.*
2. *$M_\mathfrak{p} = (0)$ para todo ideal primo $\mathfrak{p}$ de R.*
3. *$M_\mathfrak{m} = (0)$ para todo ideal maximal $\mathfrak{m}$ de R.*

Demostración. Ver **Proposición 3.8** en [AY]. □

Definición 2.55. *(Soporte). Sea R un anillo y M un R-módulo. El soporte de M, denotado por $Sup(M)$, es el conjunto de ideales primos $\mathfrak{p}$ tales que $M_\mathfrak{p} \neq (0)$.*

Proposición 2.56. *Sea R un anillo y M un R-módulo. Entonces:*

1. *$M = (0)$, si y solo si, $Sup(M) = \emptyset$.*
2. *Si $(0) \to L \to M \to N \to (0)$ es una secuencia exacta, entonces $Sup(M) = Sup(L) \cup Sup(N)$.*

Demostración. 1. Consecuencia inmediada de la proposición 3.3.

2. Como consecuencia de la secuencia exacta, tenemos que $M \cong N/L$. Por lo tanto, $Sup(M) = Sup(N/L)$. Dado que $(N/L)_{\mathfrak{p}} \cong N_{\mathfrak{p}}/L_{\mathfrak{p}}$, es fácil verificar la igualdad $Sup(N/L) = Sup(N) \cup Sup(L)$.

$\square$

Proposición 2.57. *Sea S un conjunto multiplicativamente cerrado de un anillo R, y M un R-módulo. Entonces $S^{-1}M \cong M \otimes_R S^{-1}R$.*

Demostración. Ver **Proposición 3.5** en [AY]. $\square$

3. Teoría de Dimensión

Comenzaremos entonces estableciendo los objetos a los que hace referecia las *conjeturas homológicas* estudiadas en este documento. A partir de este momento supondremos que todos los anillos R serán *noetherianos* y todos los R-módulo *finitamente generados.*

3.1. Divisores de cero de un R-Módulo

Definición 3.1. *(divisores de cero). Sea R un anillo y M un R-módulo, definimos el conjunto de divisores de cero en M denotado como $Z(M) = \{r \in R : r \cdot m = 0,\ \text{para algún } m \in M \setminus \{0\}\}$.*

Proposición 3.2. *$S = R \setminus Z(M)$ es un subconjunto multiplicativamente cerrado de R.*

Demostración. Es fácil verificar que $1 \notin S(M)$. Por otro lado, sean $a, b \in S = R \setminus Z(M)$. Si $ab \notin S$ entonces existe un $m \neq 0$, tal que $(ab)m = a(bm) = 0$. Como $b \notin Z(M)$, tenemos, en particular, que $bm \neq 0$, y en consecuencia $a \in Z(M)$, lo cual contradice nuestra hipótesis. Por lo tanto $ab \in S$. □

Proposición 3.3. *Si $M \neq (0)$, $Z(M)$ puede ser escrito como unión de ideales primos de R.*

Demostración. Afirmamos que $Z(M)$ se puede expresar como unión de ideales primos de la forma $(0 : m) := ann(m) = \{r \in R : rm = 0\}$. En efecto, sea $\Sigma = \{(0 : m) := ann(m) \ :\ m \neq 0 \in M\}$. Dado que $M \neq (0)$, es facíl verificar que Σ es un conjunto no vacío de ideales de R. Como R es un anillo *noetheriano*, entonces existe al menos un elemento maximal $ann(m)$. Veamos que $ann(m)$ es un ideal primo de R. Sean $a, b \in R$ tales que $ab \in ann(m)$. Supongamos que $a \notin ann(m)$ y $b \notin ann(m)$. Se puede verificar de forma sencilla que $ann(m) \subseteq ann(bm)$. Por otro lado, dado que $b \notin ann(m)$, por definición, $bm \neq 0$, implicando así que $ann(bm) \in \Sigma$, y debido a la maximalidad de $ann(m)$, obtenemos la igualdad $ann(m) = ann(bm)$. Como $a \in ann(bm)$, entonces $a \in ass(m)$, hecho que contradice lo supuesto. En consecuencia, $ann(m)$ es un ideal primo. De momento, solo hemos probado que los elementos maximales de Σ son ideales primos de R, lo cual no garantiza que $Z(M)$ pueda expresarse como unión de estos ideales maximales. Veamos que todo $ann(m) \in \Sigma$ esta contenido en algún elemento maximal de Σ. Sea $ann(m) \in \Sigma$ y $N = R/ann(m)$. Es fácil que verificar $N \neq (0)$ y $ann(rm) = ann(r + ann(m))$, para todo $r \in R$. De nuevo, por ser R un anillo *noetheriano*, el conjunto $\overline{\Sigma} = \{ann(r + ann(m)) \ :\ r \notin ann(m)\}$, posee un elemento maximal $ann(r_{max} + ann(m)) = ann(r_{max}m)$. Veamos que $ann(r_{max}m)$ es un elemento maximal de Σ. Sea $ann(n) \in \Sigma$ tal que $ann(r_{max}m) \subseteq ann(n)$, es decir, $ann(r_{max} + ann(m)) \subseteq ann(1 + ann(n))$. Dado que $ann(1 + ann(n)) \in \overline{\Sigma}$, por la maximamidad de $ann(r_{max} + ann(m))$, obtenemos la igualdad $ann(r_{max} + ann(m)) = ann(1 + ann(n))$. Lo anterior, garantiza entonces que $ann(r_{max}m) = ann(n)$. Por último, $ann(m) \subseteq ann(r_{max}m)$ como se quería.

□

Lo anterior motiva entonces la siguiente definición.

Definición 3.4. *(Primo asociado). Un ideal primo $\mathfrak{p}$ de un anillo R es llamado primo asociado de M si existe un $m \neq 0 \in M$ tal que $\mathfrak{p} = ann(m) = \{r \in R \ : \ rm = 0\}$. Al conjunto $ann(m)$ lo llamaremos el anulador de m. Al conjunto de primos asociados de M lo denotaremos como Ass(M).*

Esta unión de ideales primos no necesariamente es finita, pero bajo las hipótesis de que R es un anillo *noetheriano* y M un R-módulo *finitamente generado* es posible extraer una colección finita de estos ideales que formen todo $Z(M)$.

Proposición 3.5. *Si R es un anillo noetheriano y M es un R-módulo finitamente generado, entonces Z(M) puede escribirse como una unión finita de ideales primos de M.*

Demostración. Ya vimos que $Z(M)$ se puede expresar como unión de ideales primos de la forma $ann(m_i)$. Por otro lado, como R es *noetheriano* y M es un R-módulo *finitamente generado*, entonces M es un R-módulo *noetheriano* por 2.50 por lo que el submódulo $N = \sum(m_i)$ es finitamente generado. Podemos encontrar finitos m_i tales que $N = (m_1, \dots, m_n)$. Afirmación que $Z(M) = \bigcup_{1 \leq i \leq n} ann(m_i)$. En efecto, Claramente, $\bigcup_{1 \leq i \leq n} ann(m_i) \subseteq Z(M)$. Ahora para cualquier $ann(m_{max})$ en $Z(M)$, es fácil ver que $ann(m_1) \cap \cdots \cap ann(m_n) \subseteq ann(m_{max})$, a partir del hecho $m_{max} = r_1 m_1 + \cdots + r_n m_n$, para ciertos $r_i \in R$. En consecuencia, dado que $ann(m_{max})$ es primo, concluimos por la proposición 2.21, que $ann(m_i) \subseteq ann(m_{max})$, para algún i y por la maximalidad de $ann(m_i)$, se sigue $ann(m_i) = ann(m_{max})$. De esta forma, $Z(M) \subseteq \bigcup_{1 \leq i \leq n} ann(m_i)$. $\square$

Proposición 3.6. *Sea R un anillo y M un R-módulo, entonces:*

1. *Si $\mathfrak{p}$ es un ideal primo de R, entonces $Ass(R/\mathfrak{p}) = \{\mathfrak{p}\}$ ($R/\mathfrak{p}$ como R-módulo).*

2. *$Ass(M) = \emptyset$ si y solo si $M = (0)$.*

3. *Sea $N \subseteq M$ un R-módulo. Entonces, $Ass(N) \subseteq Ass(M) \subseteq Ass(N) \cup Ass(M/N)$.*

Demostración.

1. Sea $\mathfrak{p}$ un ideal primo de R. Basta con demostrar que para todo $ann(r + \mathfrak{p}) \in Ass(R/\mathfrak{p})$ se tiene que $ann(r + \mathfrak{p}) = \mathfrak{p}$. Sea $ann(r + \mathfrak{p}) \in Ass(R/\mathfrak{p})$, donde $r \notin \mathfrak{p}$, y $t \in ann(r + \mathfrak{p})$. Como $(t + \mathfrak{p})(r + \mathfrak{p}) = tr + \mathfrak{p} = 0 + \mathfrak{p}$ y $R/\mathfrak{p}$ es un dominio integral por ser $\mathfrak{p}$ primo, entonces $t + \mathfrak{p} = 0 + \mathfrak{p}$ (puesto que $r + \mathfrak{p} \neq 0 + \mathfrak{p}$), es decir, $t \in \mathfrak{p}$. Por otro lado, sea $t \in \mathfrak{p}$, es claro que $tr + \mathfrak{p} = 0 + \mathfrak{p}$ por ser $\mathfrak{p}$ ideal, por lo tanto $t \in ann(r + \mathfrak{p})$.

2. Consecuencia de la proposición 3.3.

3. Por definión se puede ver que $Ass(N) \subseteq Ass(M)$. Veamos la otra contención. Sea un ideal primo $\mathfrak{p} = ann(m) \in Ass(M)$ para algún $m \neq 0 \in M$. Supongamos que $\mathfrak{p} \notin Ass(N)$, por lo tanto, $m \notin N$. Es fácil verificar que $ann(m) \subseteq ann(m + N)$. Afirmamos que $(m) \cap N = (0)$. En efecto, si $(m) \cap N \neq (0)$, entonces por el item anterior, $Ass((m) \cap N)) \neq \emptyset$, Sea $I \in Ass((m) \cap N)$ un primo asociado de $(m) \cap N)$. Del homomorfismo natural $\phi : R \to (m)$, se tiene que $(m) \cong R/nucleo(\phi) = R/ann(m) = R/\mathfrak{p}$, implicando que $I = \mathfrak{p}$. Por otro lado, dado que $(m) \cap N \subseteq N$, tenemos que $\mathfrak{p} = I \in Ass(N)$, lo cual contadice nuestra suposición,

en consecuencia, $(m)\cap N=(0)$. Lo anterior implica que $ann(m+N)\subseteq ann(m)$, por lo tanto, $ann(m+N)=ann(m)=\mathfrak{p}$.

$\square$

Ejemplo 3.7.

- *Sea M un R-módulo, entonces $Ass(M\oplus\cdots\oplus M)=Ass(M)$. Se puede verificar por inducción y aplicando el item 3 de la proposición 3.6.*
- *Si M un R-módulo libre, entonces $Ass(M)=Ass(R)$. Consecuencia del anterior ejemplo.*
- *Sea M un submódulo de un R-módulo libre, entonces $Ass(M)\subseteq Ass(R)$. Consecuencia de la proposición 3.6.*
- *Sea I un ideal de R. Si I admite una descomposición primaria irreducible, entonces $Ass(R/I)=\{\sqrt{Q_i}\ /\ Q_i$ es un ideal primario en la descomposición primaria irreducible de $I\}$. Esto es un poco más desafiante de demostrar, pero podemos observar que los primos $\sqrt{Q_i}$ que aparecen en una descomposición primaria de I son únicamente determinados, es decir, solo dependen de I, no de la descomposición en sí.*

Se sabe que existe una caracterización del ideal conocido como *radical* de un ideal I como la intersección de todos los ideales primos que contienen a I. Esta caracterización se puede trasladar a la estructura de módulos, en donde se estudia el objeto conocido como *radical* de un submódulo. Veremos que existe una relación cercana entre este *radical* y el concepto de primos asociados.

Definición 3.8. *(Radical de un módulo). Sea M un R-módulo y N un submódulo de M. Definimos el radical de N sobre M como:*

$$\textbf{\textit{radical de }} N := \sqrt{N:M}.$$

Es importante notar que el *radical* de un submódulo N es un ideal del anillo R, no un submódulo de M. Lo primero que podemos observar de este ideal es que $\sqrt{N:M}\subseteq Z(M/N)$. En efecto, sea $r\in\sqrt{N:M}$. Dado que $\sqrt{N:M}=\sqrt{ann(M/N)}$, entonces sea n el menor natural $n>0$ tal que $r^n\in ann(M/N)$, por lo tanto, $r^n(M/N)=(0)$. Es claro que $r^{n-1}(M/N)\neq(0)$, implicando que existe un $x\neq 0\in r^{n-1}(M/N)$, tal que $rx=0$, es decir, $r\in Z(M/N)$.

De la observación anterior y aplicando el resultado en 2.21, vemos que $\sqrt{N:M}$ esta contenido en algún ideal $\mathfrak{p}\in Ass(M/N)$. Mas adelante veremos que $\sqrt{N:M}=\bigcap_{\mathfrak{p}\in Ass(M/N)}\mathfrak{p}$.

Teorema 3.9. *Sea M un R-módulo, entonces:*

1. *$Sup(M)=Sup(R/ann(M))$.*
2. *$Ass(M)\subseteq Sup(M)$. Mas general, todo ideal $\mathfrak{q}$ primo conteniendo un primo asociado $\mathfrak{p}$ de M pertenece a $Sup(M)$.*
3. *Si $\mathfrak{p}\in Sup(M)$, entonces $\mathfrak{p}$ contiene algún $\mathfrak{q}\in Ass(M)$.*

Demostración. 1. Como M es finitamente generado, consideremos un conjunto de generadores $m_1, \cdots, m_n$ para M. Es fácil verificar que $ann(M) = \bigcap_i ann(m_i)$. Veamos sucede con los soportes de estos conjuntos. Sea $\mathfrak{p}$ un ideal primo de R, y $S = R \setminus \mathfrak{p}$, entonces:

$$\begin{gathered}\mathfrak{p} \notin Sup(R/ann(M)) \text{ sii} \\ R_\mathfrak{p}/ann(M)_\mathfrak{p} = (0) \text{ sii (proposición 2.30)} \\ R_\mathfrak{p} = ann(M)_\mathfrak{p} = \bigcap_i ann(m_i)_\mathfrak{p} \neq (0) \text{ sii} \\ \mathfrak{p} \notin \bigcup Sup(ann(m_i)).\end{gathered}$$

De la misma manera se puede obtener que $Sup(M) = \bigcup_i Sup(ann(m_i))$, lo que demuestra la afirmación.

2. Sea $\mathfrak{q}$ un ideal primo tal que $\mathfrak{p} \subseteq \mathfrak{q}$, para un primo $\mathfrak{p} = ann(m) \in Ass(M)$. Dado que $R \setminus \mathfrak{q} \subseteq R \setminus \mathfrak{p}$, es claro que, $M_\mathfrak{p} \neq (0)$ implica que $M_\mathfrak{q} \neq (0)$, es decir, $M_\mathfrak{q} = (0) \Rightarrow M_\mathfrak{p} = (0)$. Dado que $M_\mathfrak{p} = 0$ implica que $Ass(M_\mathfrak{p}) = \emptyset$ se sigue que para probar $\mathfrak{q} \in Sup(M)$ solo resta verificar que $Ass(M_\mathfrak{p}) \neq \phi$, por la afirmación previa. Afirmamos que $\mathfrak{p}_\mathfrak{p} = ann(m/1) = \{r/s \in R_\mathfrak{p} : (r/s) \cdot (m/1) = 0/1\}$ (Recordemos que $S^{-1}M$ tiene estructura de $S^{-1}R$-módulo). En efecto, lo primero que tenemos que garantizar es que $m/1 \neq 0/1$. Suponiendo que $m/1 = 0/1$, por definición debe existir un $u \in S$ tal que $um = 0$, es decir, $u \in ann(m) = \mathfrak{p}$, pero esto contradice el hecho de que $u \in S = R \setminus \mathfrak{p}$. Ahora veamos efectivamente $\mathfrak{p}_\mathfrak{p} = ann(m/1)$. Sea $r/s \in \mathfrak{p}_\mathfrak{p} = \{r/s \in R_\mathfrak{p} : r \in \mathfrak{p}, s \in S\}$, entonces tenemos $(r/s) \cdot (m/1) = rm/s = 0/s = 0/1$, por lo tanto $r/s \in ann(m/1)$. Por otro lado, sea $r/s \in ann(m/1)$, es decir, $(r/s) \cdot (m/1) = rm/s = 0/1$, luego por definición tenemos que debe existir un $u \in S$ tal que $urm = 0$, es decir, $ur \in \mathfrak{p}$, pero por ser $\mathfrak{p}$ primo tenemos que $r \in \mathfrak{p}$ ($u \in S$, por lo que $u \notin \mathfrak{p}$) implicando que $r/s \in \mathfrak{p}_\mathfrak{p}$. Así fue demostrado que $\mathfrak{p}_\mathfrak{p} \in Ass(M_\mathfrak{p})$, lo que prueba la afirmación.

3. Sea $\mathfrak{p} \in Sup(M)$, esto es, $M_\mathfrak{p} \neq (0)$, implicando que $Ass(M_\mathfrak{p}) \neq \emptyset$. Es fácil verificar que estos primos asociados necesariamente tienen la forma de $\mathfrak{q}_\mathfrak{p}$, con $\mathfrak{q} \subseteq \mathfrak{p}$ y $\mathfrak{q} \in Ass(M)$.

□

Corolario 3.9.1. *Para todo R-módulo M, se tiene que los siguientes conjuntos son iguales:*

1. *El conjunto de los elementos minimales de $Ass(M)$.*

2. *El conjunto de los elementos minimales de $Sup(M)$.*

3. *El conjunto de los elementos minimales de $Sup(R/ann(M))$.*

Denotatemos al conjunto arriba descrito como $Min(M)$.

Demostración. Por ser R un *anillo conmutativo noetheriano* entonces toda cadena descendente de ideales primos se estabiliza, implicando la existencia de un elemento minimal en cualquier conjunto no vacío de ideales primos (ver **Corolario 11.12 en [AY]**). Veamos que $Min(Ass(M)) = Min(Sup(M))$.

- $Min(Ass(M)) \subseteq Min(Sup(M))$: Sea $\mathfrak{p} \in Min(Ass(M))$. Por la proposición 3.9, $\mathfrak{p} \in Sup(M)$. Veamos que $\mathfrak{p}$ es minimal en $Ass(M)$. Sea $\mathfrak{q} \in Sup(M)$ tal que $\mathfrak{q} \subseteq \mathfrak{p}$. Por la proposición 3.9, $\mathfrak{q}$ contiene un ideal primo $\mathfrak{o} \in Ass(M)$, por lo tanto, $\mathfrak{o} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$. Ahora, por la minimalidad de $\mathfrak{p}$ en el $Ass(M)$, $\mathfrak{o} = \mathfrak{p}$, implicando que $\mathfrak{q} = \mathfrak{p}$.

- $Min(Sup(M)) \subseteq Min(Ass(M))$: Sea $\mathfrak{p} \in Min(Sup(M))$. Por la proposición 3.9, $\mathfrak{p}$ contiene un ideal primo $\mathfrak{q} \in Ass(M)$. Dado que $Ass(M) \subseteq Sup(M)$ y por la minimalidad de $\mathfrak{p}$ en el $Sup(M)$, tenemos que $\mathfrak{p} = \mathfrak{q} \in Ass(M)$. Nuevamente, la proprosición 3.9 implica la minimalidad de $\mathfrak{p}$ en $Ass(M)$.

□

Corolario 3.9.2. *Sea M un R-módulo y N un submódulo de M. Entonces:*

$$\sqrt{N : M} = \bigcap_{\mathfrak{p} \in Min(M/N)} \mathfrak{p}.$$

Demostración. Es claro que si un ideal primo $\mathfrak{p} \in Ass(R/(N : M))$, entonces $N : M \subseteq \mathfrak{p}$. Afirmamos que $\sqrt{N : M} = \bigcap_{\mathfrak{p} \in Ass(R/(N:M))} \mathfrak{p}$. En efecto, $\bigcap_{\mathfrak{p} \in Ass(R/(N:M))} \mathfrak{p} \subseteq \sqrt{N : M}$ se garantiza debido a que $\sqrt{N : M}$ es la intersección de todos los ideales primos que contiene a $N : M$, en particular todos los $\mathfrak{p} \in Ass(R/(N : M))$ son ideales primos que contienen a $N : M$. Por otro lado, sea $r \in \sqrt{N : M}$, por lo tanto existe un natural $n > 0$ tal que $r^n \in N : M$. Como $N : M \subseteq \mathfrak{p}$ para todo ideal primo $\mathfrak{p} \in Ass(R/(N : M))$, entonces $r^n \in \mathfrak{p}$, y por ser $\mathfrak{p}$ primo se concluye que $r \in \mathfrak{p}$ para todo ideal primo $\mathfrak{p} \in Ass(R/(N : M))$. Finalmente, dado que $N : M = ann(M/N)$, tenemos:

$$\sqrt{N : M} = \bigcap_{\mathfrak{p} \in Ass(R/(N:M))} \mathfrak{p} = \bigcap_{\mathfrak{p} \in Ass(R/ann(M/N))} \mathfrak{p}.$$

Por lo que esta última intesección se puede restringir a los elementos mínimos de $Ass(R/ann(M/N))$. Así, aplicando el corolario 3.9.1 tenemos el resultado. □

Proposición 3.10. *Sea M un R-módulo. Las siguientes afirmaciones son equivalentes:*

1. *$Ass(M)$ posee un solo elemento.*
2. *$Z(M) \subseteq \sqrt{ann(M)}$.*

Demostración. *1 ⇒ 2*: Si $Ass(M)$ solo tiene un solo elemento, entonces $Min(M) = \{\mathfrak{p}\}$. Por el corolario 3.9.2, $\sqrt{ann(M)} = \mathfrak{p}$, pero $Z(M) = \mathfrak{p}$, implicando así el resultado.

2 ⇒ 1: Anteriormente vimos que $\sqrt{ann(M)} \subseteq Z(M) = \bigcup_{\mathfrak{p} \in Ass(M)} \mathfrak{p}$ (recordemos que esta unión es finita), por la proposición 2.21, debe existir un $\mathfrak{p} \in Ass(M)$ tal que $\sqrt{ann(M)} \subseteq \mathfrak{p}$. Por otro lado, por hipótesis tenemos que $Z(M) \subseteq \sqrt{ann(M)}$, implicando entonces que $\mathfrak{p} \subseteq \sqrt{ann(M)}$, es decir, $\mathfrak{p} = \sqrt{ann(M)}$. Por lo anterior, tenemos $\mathfrak{p} = \sqrt{ann(M)} = Z(M)$ concluyendo así que $Ass(M) = \{\mathfrak{p}\}$. □

Aplicando el resultado anterior al módulo M/N, obenemos la equivalencia: $Ass(M/N)$ tiene un solo elemento $\iff$ $Z(M/N) \subseteq \sqrt{N : M}$, motivando entonces la siguiente definición.

Definición 3.11. *(Submódulo primario). Sea M un R-módulo y N un submódulo de M. N es llamado **submódulo primario** si satisface alguna de las condiciones de la proposición anterior.*

Un hecho destacables es que si N un submódulo propio de un R-módulo M es primario, entonces $N : M$ es un ideal primario de R. En efecto, para ver que $N : M \neq (1)$ basta observar que si $1 \in N : m$, implicaria que $M = N$. Por otro lado, sean $r, s \in R$ tal que $rs \in N : M$ y $r \notin \sqrt{N : M}$. Como N es primario, entonces $r \notin Z(M/N)$. Por hipótesis $rs \in N : M$, es decir, $r(s(M/N)) = rs(M/N) = (0)$, por lo que necesariamente $s(M/N) = (0)$, implicando que $s \in N : M$.

Como consecuencia de la proposición 3.10, si N un submódulo de un R-módulo M es primario, entonces $\sqrt{N : M}$ es el único ideal primo tal que $Ass(M/N) = \{\sqrt{N : M}\}$.

Recordemos que $Z(M)$ puede escribirse como una unión finita de ideales primos pertenecientes al $Ass(M)$, pero este hecho no implica necesariamente que este último conjunto sea finito. Debido a las hipótesis de R unillo *noetheriano* y M R-módulo *finitamente generado* es posible garantizar que efectivamente dicho conjunto es finito.

Proposición 3.12. *Sea M un R-módulo. $Ass(M)$ es un conjunto finito.*

Demostración. Supongamos que $M \neq (0)$ (en caso contrario no hay nada que probar). Como $Ass(M) \neq \emptyset$, sea $\mathfrak{p}_1 \in Ass(M)$. Dado que $\mathfrak{p}_1 = ann(m_1)$ con $m_1 \neq 0 \in M$, es claro que $R/\mathfrak{p}_1 \cong (m_1)$. Por la proposición 3.6, $Ass(M) \subseteq Ass((m_1)) \cup Ass(M/(m_1)) = \{\mathfrak{p}_1\} \cup Ass(M/(m_1))$. Si $Ass(M) \nsubseteq \{\mathfrak{p}_1\}$, podemos escoger un $\mathfrak{p}_2 \in Ass(M)$ tal que $\mathfrak{p}_2 \in Ass(M/(m_1))$. En este caso, $\mathfrak{p}_2 = ann(m_2 + (m_1))$, donde $m_2 \notin (m_1)$. Es claro que $R/\mathfrak{p}_2 \cong (m_2 + (m_1)) \cong ((m_2) + (m_1))/(m_1)$. Lo anterior implica entonces que $Ass(M) \subseteq \{\mathfrak{p}_1\} \cup Ass$. De nuevo, por la proposición 3.6, $Ass(M/(m_1)) \subseteq Ass((m_2 + (m_1))) \cup Ass((M/(m_1))/(((m_2) + (m_1))/(m_1))) = \{\mathfrak{p}_2\} \cup Ass(M/((m_2) + (m_1)))$, por lo tanto, $Ass(M) \subseteq \{\mathfrak{p}_1, \mathfrak{p}_2\} \cup Ass(M/((m_2) + (m_1)))$. Si $Ass(M) \nsubseteq \{\mathfrak{p}_1, \mathfrak{p}_2\}$, de manera análoga a lo anterior, podemos encontrar un $m_3 \in M$ y $\mathfrak{p}_3 \in Ass(M/((m_2) + (m_1)))$ tal que $Ass(M) \subseteq \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\} \cup Ass(M/((m_3) + (m_2) + (m_1)))$. Si continuáramos de esta forma, podríamos obtener una cadena de submódulos de M, $(m_1) \subseteq (m_1) + (m_2) \subseteq (m_1) + (m_2) + (m_3) \subseteq \cdots$ tales que $R/\mathfrak{p}_1 \cong (m_1), R/\mathfrak{p}_2 \cong ((m_2) + (m_1))/((m_1), R/\mathfrak{p}_3 \cong ((m_3) + (m_2) + (m_1))/((m_2) + (m_1)), \cdots$. Ahora, dado que M es *noetheriano*, debe existir algún natural t, tal que $(m_1) + (m_2) + \cdots + (m_t) = (m_1) + (m_2) + (m_3) + \cdots + (m_t) + (m_{t+1})$, implicando entonces que $((m_{t+1}) + \cdots + (m_2) + (m_1))/((m_t) + \cdots + (m_2) + (m_1)) = (0)$, es decir, $R/\mathfrak{p}_{t+1} \cong (0)$, lo cual contradice el hecho de $\mathfrak{p}_{t+1}$ ser un ideal primo. Concluimos entonces que debe existir un natural n tal que $Ass(M) \subseteq \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n\}$. $\square$

Otro importante hecho en relación al $Ass(M)$ lo destacamos en la siguiente proposición:

Proposición 3.13. *Sea M un R-módulo. Para todo subconjunto $H \subseteq Asss(M)$, existe un submódulo N de M tal que $Ass(M/N) = H$ y $Ass(N) = Ass(M) \setminus H$.*

Demostración. Sea $H \subseteq Ass(M)$. Sea Σ el conjunto de submódulos Q de M tales que $Ass(Q) \subseteq Ass(M) \setminus P$. Dado que M es *noetheriano* y $\Sigma \neq \emptyset$ ($(0) \in \Sigma$), Σ admite un submódulo máximal N. Veamos que $Ass(M/N) = H$. Sea $\mathfrak{p} \in Ass(M/N)$, tenemos entonces que existe submódulo L de M tal que $R/\mathfrak{p} \cong L/N$. Por la proposición 3.6, $Ass(L) \subseteq Ass(N) \cup Ass(L/N) = Ass(N) \cup \{\mathfrak{p}\} \subseteq Ass(M) \setminus H \cup \{\mathfrak{p}\}$. Dado que $N \subseteq L$, entonces por la maximalidad de N, que $Ass(L) \nsubseteq Ass(M) \setminus H$, es decir, debe existir un $\mathfrak{s} \in Ass(L)$ tal que $\mathfrak{s} \notin Ass(M) \setminus H$. Es claro que $\mathfrak{s} = \mathfrak{p}$, implicando entonces que $\mathfrak{p} \in H$ ($\mathfrak{p} \in Ass(M)$). Para la otra contención, sea $\mathfrak{p} \in H$. De nuevo por la proposición 3.6, $\mathfrak{p} \in H \subseteq Ass(M) \subseteq Ass(N) \cup Ass(M/N)$. Es claro que $\mathfrak{p} \notin Ass(N)$, por lo tanto, $\mathfrak{p} \in Ass(M/N)$. Por otro lado, sabemos que $Ass(N) \subseteq Ass(M) \setminus H$, veamos la igualdad. Sea $\mathfrak{p} \in Ass(M) \setminus H$, por lo anterior tenemos que $Ass(M) \subseteq Ass(M) \cup Ass(M/N) = Ass(M) \cup H$, es claro entonces que $\mathfrak{p} \in Ass(N)$. □

Teorema 3.14. *(Descomposición primaria de un submódulo). Sea M un R-módulo. Todo submódulo N de M puede ser escrito de la forma:*

$$N = \bigcap_{i=1}^{n} Q_i.$$

Donde Q_i es un submódulo primario de M, para todo $i = 1, \cdots, n$.

Demostración. Sin perdidad de generalidad, podemos suponer que $N = (0)$. Por la proposicíon anterior, para cada $\mathfrak{p} \in Ass(M)$ existe un submódulo $N_\mathfrak{p}$ tal que $Ass(M/N_\mathfrak{p}) = \{\mathfrak{p}\}$ y $Ass(N_\mathfrak{p}) = Ass(M) \setminus \{\mathfrak{p}\}$. Por definición, los submódulos $N_\mathfrak{p}$ son prímarios. Veamos que $(0) = \cap_{\mathfrak{p} \in Ass(M)} N_P$, mostrando que $Ass(\cap_{\mathfrak{p} \in Ass(M)} N_\mathfrak{p}) = \emptyset$. Sea $\mathfrak{q} \in Ass(\cap_{\mathfrak{p} \in Ass(M)} N_\mathfrak{p})$, es claro que $\mathfrak{q} \in Ass(N_\mathfrak{p})$ para todo $\mathfrak{p} \in Ass(M)$, pero por la construcción de los $Ass(N_\mathfrak{p})$, se tiene que $\cap_{\mathfrak{p} \in Ass(M)} Ass(N_\mathfrak{p}) = \emptyset$, lo cual es absurdo. Por lo tanto, $Ass(\cap_{\mathfrak{p} \in Ass(M)} N_\mathfrak{p}) = \emptyset$. La finitud de la intercción de los submódulos primarios se garantiza por el hecho de que $Ass(M)$ es un conjunto finito. Ahora veamos el caso general. Sea N un submódulo de M. Sea $\psi : M \to M/N : m \to m + N$ el homomorfiso natural al cociente de M/N. Por el caso base, $(0 + N) = \cap_{i=1}^{n} \overline{N}_i$ donde $\overline{N}_i$ son submódulos primarios de M/N. Es fácil ver que $N = \cap_{i=1}^{n} \psi^{-1}(\overline{N}_i)$. Ahora veamos entonces que los submódulos $\psi^{-1}(\overline{N}_i)$ son primarios. En efecto, es fácil ver que la aplicación $\phi : M/N \to M/\psi^{-1}(\overline{N}_i) : m + N \to m + \psi^{-1}(\overline{N}_i)$ es un homomorfismo de módulos. Veamos $nucleo(\phi) = \overline{N}_i$. Sea $x + N \in nucleo(\phi)$, entonces $x \in \overline{N}_i$, es decir, $\psi(x) \in \overline{N}_i$, y por definición de ψ, $x + N \in \overline{N}_i$. Ahora sea $x + N \in \overline{N}_i$, es claro que $\phi(x + N) = 0 + \psi^{-1}(\overline{N}_i)$. Lo anterior implica entonces que $(M/N)/\overline{N}_i \cong M/\psi^{-1}(\overline{N}_i)$, por lo tanto, $Ass(M/\psi^{-1}(\overline{N}_i)) = Ass((M/N)/\overline{N}_i) = \{\mathfrak{p}_i\}$, es decir, los submódulos $\psi^{-1}(\overline{N}_i)$ son primarios. □

Corolario 3.14.1. *Para todo R-módulo M, $Ass(M) = Ass(R/ann(M))$.*

Demostración. Sea $(0) = \cap_{\mathfrak{p} \in Ass(M)} N_\mathfrak{p}$ una descomposición primaria del submódulo (0). Tomando anuladores a ambos lados tenemos que $ann(M) = \cap_{\mathfrak{p} \in Ass(M)} (N_\mathfrak{p} : M)$. Se puede verificar, por la construcción de los $N_\mathfrak{p} : M$ que dicha descomposición es irreducible. Lo anterior implica que los $N_\mathfrak{p} : M$ son ideales primarios tales que $\sqrt{N_\mathfrak{p} : M} = \text{radical de } N_\mathfrak{p} = \mathfrak{p}$. Se sigue entonces por el ejemplo 3.7 que $Ass(M) = Ass(R/ann(M))$. □

3.2. Dimensión de Krull

A la suposición de que todo anillo será *noetherianos* y todo R-módulo *finitamente generados* añadieros que todo anillo R será *local* con único ideal máximal $\mathfrak{m}$.

Definición 3.15. *(Dimensión de Krull de un anillo). Sea R un anillo. La dimensión de Krull de R, denotado $dim(R)$, se define como el supremo sobre las longitudes de las cadenas $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$, donde $\mathfrak{p}_i$ son ideales primos de R. La altura de un ideal primo $\mathfrak{p}$, denotado por $alt(\mathfrak{p})$, será el supremo de las longitudes de las cadenas truncadas a derecha en el ideal $\mathfrak{p}$.*

Dado un ideal primo I del anillo R, al hallar la $dim(R/I)$, por definición tendríamos que cálcular las longitudes de las cadenas de ideales primo:

$$\overline{\mathfrak{p}}_0 \subsetneq \overline{\mathfrak{p}}_1 \subsetneq \cdots \subsetneq \overline{\mathfrak{p}}_n \cdots, \text{ con } \overline{\mathfrak{p}}_i \text{ ideal primo de } R/I.$$

Pero por la corrrespondecia uno a uno que existe entre los ideales primos de R/I y los ideales primos $\mathfrak{q}$ en R que contiene a I, sería equivalente considerar las cadenas de ideales primos en R:

$$I \subsetneq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \cdots$$

Esto nos lleva a la siguiente igualdad:

$$dim(R/I) = \sup_{I \subseteq \mathfrak{p}} \{ dim(R/\mathfrak{p})\}.$$

Por otro lado, dado un ideal primo $\mathfrak{p}$, veamos que $\mathfrak{p} \in Sup(R/I)$ si y solo si $I \subseteq \mathfrak{p}$. Supontamos que por $\mathfrak{p} \in Sup(R/I)$, esto es, existe un $r \notin I$ y $s \in R \setminus \mathfrak{p}$, tal que $(r+I)/s \neq (0+I)/1$; por definición tenemos entonces que para todo $t \in R \setminus \mathfrak{p}$, $rt \notin I$. Si existíese un $i \in I$, tal que $i \notin \mathfrak{p}$, por lo anterior $ri \notin I$, pero esto contradice el hecho de ser I un ideal, así tenemos que $I \subseteq \mathfrak{p}$. Ahora supongamos que $I \subseteq \mathfrak{p}$ y ademas que $\mathfrak{p} \notin Sup(R/I)$, esto es, $(R \setminus \mathfrak{p})^{-1}(R/I) = (0)$. Por lo tanto, $(1+I)/1 = (0+I)/1$, es decir, debe existir un $s \in S$ tal que $s \in I$ (por definición), lo cual es absurdo dado que $I \subseteq \mathfrak{p}$. Lo anterior implica que:

$$\sup_{I \subseteq \mathfrak{p}}\{dim(R/\mathfrak{p})\} = \sup_{\mathfrak{p} \in Sup(R/I)} \{ dim(R/\mathfrak{p})\} = \sup_{\mathfrak{p} \in Min(R/I)} \{ dim(R/\mathfrak{p})\}$$

La anterior observación implica que dado N un submódulo de un R-módulo M, si I es un ideal primo de R, entonces $Sup(N/IN) = Sup(N) \cap Sup(R/I)$.

Es natural entonces trasladar el concepto de *dimensión de Krull* a la estructura de módulo:

Definición 3.16. *(Dimensión de Krull de un módulo). De lo anterior, es natural definir la dimensión de un R-módulo $M \neq (0)$ como:*

$$dim(M) = \sup_{\mathfrak{p} \in Sup(M)} \{ dim(R/\mathfrak{p})\} = \sup_{\mathfrak{p} \in Min(M)} \{ dim(R/\mathfrak{p})\}.$$

Proposición 3.17. *Sea M un R-módulo. Entonces, $dim(M) = dim(R/ann(M))$*

Demostración. Resulta inmediado del hecho $Sup(M) = Sup(R/ann(M))$. □

Definición 3.18. *(Sistema de parámetros). Sea M un R-módulo. Una secuencia $x_1, \cdots, x_n$ de elementos de R son llamados un sistema de parámetros de M, si n es el menor entero que satisface la condición $Sup(M/(x_1, \cdots, x_n)M) = \{\mathfrak{m}\}$. Al entero n lo denotaremos por $s(M)$.*

Es posible demostrar que existe al menos una secuencia $x_1, \cdots, x_n$ de elementos de R tales que $Sup(M/(x_1, \cdots, x_n)M) = \{\mathfrak{m}\}$. En efecto, primero veamos que si R es un anillo local con único ideal máximal $\mathfrak{m}$, entonces $Ass(M/\mathfrak{m}M) = \{\mathfrak{m}\}$. Sea $\mathfrak{p} \in Ass(M/\mathfrak{m}M)$. Por definición de primos asociados, existe un $n \in M$, con $n \notin \mathfrak{m}M$ tal que $\mathfrak{p} = ann(n+\mathfrak{m}M)$. Es claro que para todo $r \in \mathfrak{m}$, $r \in ann(n+\mathfrak{m}M) = \mathfrak{p}$, es decir, $\mathfrak{m} \subseteq \mathfrak{p}$; por la maximalidad de $\mathfrak{m}$ tenemos que $\mathfrak{p} = \mathfrak{m}$. Lo anterior implica entonces que $Ass(M/\mathfrak{m}M) = \{\mathfrak{m}\}$. Ahora veamos que $Sup(M/\mathfrak{m}M) = \{\mathfrak{m}\}$. Sea $\mathfrak{p} \in Sup(M/\mathfrak{m}M)$. Por la proposición 3.9, tenemos que $\mathfrak{m} \subseteq \mathfrak{p}$, y de nuevo por la maximalidad de $\mathfrak{m}$, concluimos entonces que $\mathfrak{p} = \mathfrak{m}$, implicando entonces que $Sup(M/\mathfrak{m}M) = \{\mathfrak{m}\}$. Finalmente, como R es un anillo *noetheriano*, existe un conjunto finito de generados $m_1, \cdots, m_n$ de m, los cuales satisfacen que $Sup(M/(m_1, \cdots, m_n)M) = Sup(M/\mathfrak{m}M) = \{\mathfrak{m}\}$.

Proposición 3.19. *Para todo R-módulo M, $s(M) \leq dim(M)$.*

Demostración.

- Por la observación anterior, en caso de que $dim(M) = \infty$ no hay nada que probar.
- Supogamos que $dim(M) = n$ y procedamos por inducción sobre dicha dimensión. Si $dim(M) = 0$ entonces para todo $\mathfrak{p} \in Sup(M)$, $\mathfrak{p} = m$ (recordemos que todo ideal de R está contenido en m, por lo que $\mathfrak{p} \subseteq \mathfrak{m}$, no puede ser una contección estricta), implicando que $Sup(M) = \{\mathfrak{m}\}$, por lo tanto $s(M) = 0$. Para el caso inductivo, supongamos que $dim(M) = r \geq 1$. Sea $U = \bigcup_{\mathfrak{p} \in Sup(M)} \mathfrak{p}$, tales que $dim(M) = dim(R/\mathfrak{p})$. Si $m \subseteq U$, entonces por la proposición 2.21 existiría un $\mathfrak{p} \in Sup(M)$ tal que $\mathfrak{m} \subseteq \mathfrak{p}$ y $dim(R/\mathfrak{p}) = dim(M)$, pero por la maximalidad de $\mathfrak{m}$ tendríamos que $\mathfrak{m} = \mathfrak{p}$ implicando que $dim(M) = dim(R/\mathfrak{p}) = dim(R/\mathfrak{m}) = 0$, lo cual contradice nuestra hipótesis, por tanto $\mathfrak{m} \nsubseteq U$. Por otro lado, sea un $x \in \mathfrak{m} \backslash U$. Es fácil verificar que si $\mathfrak{p} \in Sup(M/(x)M)$, entonces $\mathfrak{p} \in Sup(M)$, implicando que $dim(M/(x)M) \leq dim(M)$. Veamos que $dim(M/(x)M) \neq dim(M)$. Supongamos lo contrario, que $dim(M/(x)M) = dim(M)$. Como $dim(M/(x)M) < \infty$, entonces debe existir un $\mathfrak{p} \in Sup(M/(x)M)$ tal que $dim(M/(x)M) = dim(R/\mathfrak{p})$. Por otro lado, dado que $Sup(M/(x)M) = Sup(M) \cap Sup(R/(x))$, entonces $(x) \subseteq \mathfrak{p}$ y $\mathfrak{p} \subseteq U$ ($\mathfrak{p} \in Sup(M)$ y $dim(M) = dim(R/\mathfrak{p})$), conllevando a que $(x) \subseteq U$, lo cual contradice lo supuesto con x. Lo anterior implican entonces que $dim(M/(x)M) \leq dim(M) - 1$, así, aplicando hipótesis inductiva, $s(M/(x)M) \leq dim(m/(x)M)$. Finalmente, sea $(x_1, \cdots x_t)$ un sistema de parámetros de $M/(x)M$; es fácil ver que $(M/(x)M)/((x_1, \cdots, x_t)(M/(x)M)) \cong M/(x, x_1, \cdots, x_t)M$ (considerando el homomorfismo $M/(x)M \to M/(x_1, \cdots, x_t)M : m+(x)M \to m+(x, x_1, \cdots, x_t)M$ se concluye claramente el isomorfismo), por lo tanto, $s(M) \leq s(M/(x)M) + 1$. Se sigue entonces que $s(M) \leq dim(M)$.

□

Teorema 3.20. *(Teorema de Krull). Para todo R-módulo M, $dim(M) \leq s(M)$.*

Demostración. Consecuencia directa de las desigualdades $s(M) \geq d(M)$ y $d(M) \leq dim(M)$, donde $d(M)$ demota el grado del polinomio de Samuel de un R-módulo finitamente generado. Para la demostración de estas desigualdades ver **Teorema 7.4.31** en [AS]. □

Corolario 3.20.1. *Para todo R-módulo M, $dim(M) = s(M) < \infty$.*

Demostración. Inmediato de las proposiciones 3.20 y 3.19. □

Proposición 3.21. *Si M es un R-módulo, entonces para todo $x \in \mathfrak{m} \setminus \cup\mathfrak{p}$, donde $\mathfrak{p}$ son primos tales que $dim(M) = dim(R/\mathfrak{p})$, existe un sistema de parámetros de M que inicia con x.*

Demostración. Sea $x_1, \cdots, x_n$ un sistema de parametros de $M/(x)M$. Por lo tanto, n es el mínimo entero tal que:

$$Sup((M/(x))/((x_1, \cdots, x_n)(M/(x)))) = Sup(M/(x, x_1, \cdots, x_n)M) = \{\mathfrak{m}\}.$$

Basta demostrar entonces que $s(M) = n + 1$. En efecto, dado que $x \in \mathfrak{m} \setminus \cup\mathfrak{p}$ donde $\mathfrak{p}$ son primos tales que $dim(M) = dim(R/\mathfrak{p})$, entonces $dim(M/(x)M) \leq dim(M) - 1$. Por otro lado, dado que $s(M) \leq n + 1$, y $s(M) = dim(M)$, tenemos que:

$$s(M) \leq n + 1 = s(M/(x)M) + 1 \leq dim(M/(x)M) + 1 \leq dim(M) - 1 + 1 = s(M).$$

□

Proposición 3.22. *Sea M un R-módulo y sea $x_1, \cdots, x_k$ una secuencia de elementos de $\mathfrak{m}$. Entonces:*

$$dim(M) \leq dim(M/(x_1, \cdots, x_k)M) + k.$$

Además las siguientes condiciones son equivalentes:

1. *$dim(M) = dim(M/(x_1, \cdots, x_k)M) + k$.*

2. *$x_1, \cdots, x_k$ hace parte de un sistema de parámetros de M.*

Demostración. Ya hemos visto que $s(M) \leq s(M/(x)M) + 1$, para todo $x \in R$. Procedamos por inducción sobre la longitud de la secuencia de elementos de $\mathfrak{m}$ en la desigualdad $s(M) \leq s(M/(x_1, \cdots, x_k)M) + k$. El caso base se tiene al particularizar en elementos de $\mathfrak{m}$ en la desigualdad $s(M) \leq s(M/(x)M) + 1$. Para el vaso inductivo, consideremos una secuencia de elementos $x_1, \cdots, x_k$ de $\mathfrak{m}$. Sea $N = M/(x_2, \cdots, x_k)M$. Aplicando caso inductivo a la secuencia $x_2, \cdots, x_k$, obtenemos que $s(M) \leq s(N) + (k-1) \leq s(N/(x_1)N) + 1 + (k-1) = s(M/(x_1, \cdots, x_k)) + k$. Por el corolario 3.20.1 obtenemos el resultado.

Ahora veamos la equivalencia. *1* $\implies$ *2*: Sea $x_1, \cdots, x_k$ una secuencia de elementos de $\mathfrak{m}$ tal que $dim(M) = dim(M/(x_1, \cdots, x_k)M) + k$ y $N = M/(x_1, \cdots, x_{k-1})M$. Sea $\mathfrak{p} \in Sup(N)$ un ideal primo tal que $dim(N) = dim(R/\mathfrak{p})$. Afirmamos que $x_k \notin \mathfrak{p}$. En efecto, supongamos que $x_k \in \mathfrak{p}$. Dado que $\mathfrak{p} \in Sup(N) = Sup(M) \cap Sup(R/(x_1, \cdots, x_{k-1}))$, obtenemos la contención $(x_1, \cdots, x_{k-1}) \subseteq \mathfrak{p}$. Ahora, como $(x_1, \cdots, x_{k-1}, x_k) \subseteq \mathfrak{p}$, entonces $\mathfrak{p} \in Sup(M/(x_1, \cdots, x_k)M)$, implicando que $dim(R/\mathfrak{p}) \leq dim(M/(x_1, \cdots, x_k)M)$. Usando la proposición 3.22 obtenemos las siguientes desiguadades:

$$dim(M) - (k-1) \leq dim(N) = dim(R/\mathfrak{p}) \leq dim(M/(x_1, \cdots, x_k)M) = dim(M) - k.$$

Implicando que $1 \leq 0$, lo cual es absurdo. Por lo tanto, $x_k \notin \mathfrak{p}$. Puesto que, $x_k \in \mathfrak{m} \setminus \mathfrak{p}$, por la proposición 3.21, existe un sistema de parámetros de $N = M/(x_1, \cdots, x_{k-1})M$ que inicia con x_k. El resuldo buscado se obtiene como consecuencia del isomorfismo $(M/(x_1, \cdots, x_{k-1})M)/((x_k, \cdots, x_d)M/(x_1, \cdots, x_{k-1})M) \cong M/(x_1, \cdots, x_k, \cdots x_d)M$.

2 $\implies$ *1*: Sea $x_1, \cdots x_k, x_{k+1}, \cdots x_n$ un sistema de parámetros de M. De nuevo, como consecencia del isomorfismo $(M/(x_1, \cdots, x_k)M)/((x_{k+1}, \cdots, x_n)M/(x_1, \cdots, x_{k-1})M) \cong M/(x_1, \cdots, x_k, \cdots x_n)M$, obtenemos la igualdad:

$$Sup((M/(x_1, \cdots, x_k)M)/((x_{k+1}, \cdots, x_n)M/(x_1, \cdots, x_{k-1})M)) = \\ Sup(M/(x_1, \cdots, x_k, \cdots x_n)M) = \{\mathfrak{m}\}.$$

Implicando que:

$$dim(M/(x_1, \cdots, x_k)M) = s(M/(x_1, \cdots, x_k)M) \leq n - k.$$

Por otro lado, usando la desigualdad de la proposición 3.22 tenemos que:

$$n - k = dim(M) - k \leq dim(M/(x_1, \cdots, x_k)M).$$

Por consiguiente, $dim(M) = dim(M/(x_1, \cdots, x_k)M) + k$. $\square$

4. Módulos de Cohen-Macaulay

4.1. M-secuencias y profundidades

Definición 4.1. *(Secuencia regular). Sea M un R-módulo. Una secuencia $x_1, \cdots, x_n$ de elementos de R es llamados M*-secuencia o secuencia regular *si cumple las siguientes condiciones:*

1. $(x_1, \cdots, x_n)M \neq M$.
2. $x_i \notin Z(M/(x_1, \cdots, x_{i-1})M)$, *para todo* $i = 1, \cdots, n$.

Definición 4.2. *(I-profundidad): Sea I un ideal del anillo R y M un R-módulo. La I-profundidad de M, denotado por $prof_I(M)$, se define como el supremo de la longitud de las M-secuencias de elementos en I. Tendremos en cuenta la siguiente notación: $prof_I(R)$ sera sustituido por $prof(I)$. Si R es un anilo local con único ideal maximal $\mathfrak{m}$, $prof_{\mathfrak{m}}(R)$ sera sustituido por $prof(R)$.*

Dado un ideal I del anillo R, para un R-módulo M, la existencia de estas M-secuencias en I se puede garantizar tomando $r_1, \cdots, r_n$ el mínimo de generadores del ideal I (recordemos que R es un anillo *noetheriano*), para los cuales es fácil ver que cumplen las dos condiciones en 4.1. Más aún, se puede demostrar que dichas M-secuencias no pueden crecer indefinidamente, basta observar que si un $x_i \notin Z(M/(x_1, \cdots, x_{i-1})M)$, entonces la contención de ideales $(x_1, \cdots, x_{i-1}) \subseteq (x_1, \cdots, x_i)$ es propia. Lo anterior sumado al hecho de que R es *noetheriano* implica la existencia de M-secuencias de longitud máxima. No obstante, de aquí no se infiere directamente que $prof_I(M) < \infty$ para todo ideal I de R, pero veremos mas adelante que esto si se cumple.

Proposición 4.3. *Sea I un ideal del anillo R tal que $IM \neq M$. Sea $\underline{x} = x_1, \cdots, x_n$ una M-secuencia de elementos de I. Entonces, las siguientes afirmaciones son equivalentes:*

1. $x_1, \cdots, x_n$ *es máxima, es decir, no se puede extender a otra M-secuencia.*
2. $I \subseteq Z(M/(\underline{x})M)$.
3. $I \subseteq ann(\overline{a})$, *para algún* $\overline{a} \neq 0 \in M/(\underline{x})M$.
4. $Hom_R(R/I, M/(\underline{x})M) \neq (0)$.

Demostración. *1* $\Rightarrow$ *2*: Supongamos que $x_1, \cdots, x_n$ es una M-secuencia máxima en I y que I no esta contenido en $Z(M/(\underline{x})M)$, es decir, que existe un $x \in I$ tal que $x \notin Z(M/(\underline{x})M)$. Dado que $IM \neq M$, es claro que $(x_1, \cdots, x_n, x)M \neq M$, por lo tanto, $x_1, \cdots, x_n, x$ sería una M-secuencia en I, lo cual contradice nuestra hipótesis.

2 $\Rightarrow$ *3*: Inmediato.

3 $\Rightarrow$ *4*: Supongamos que $I \subseteq ann(a + (\underline{x})M)$, con $a \notin (\underline{x})M$. Definamos el siguiente homomorfismo $\psi : R/I \to M/(\underline{x})M : r + I \to r \cdot a + (\underline{x})M$. Claramente ψ es bien definida dado que $I \subseteq ann(a + (\underline{x})M)$ y efectivamente es un homomorfismo de R-módulos. Por otro lado, $\psi(1 + I) = 1 \cdot a + (\underline{x})M = a + (\underline{x})M \neq 0 + (\underline{x})M$, por lo tanto, $\psi \neq 0$, implicando el resultado.

4 $\Rightarrow$ *1*: Supongamos que $Hom_R(R/I, M/(\underline{x})M) \neq (0)$ y que $x_1, \cdots, x_n$ no es una M-secuencia máxima de elementos de I, es decir, existe un $x \in I$ tal que $x \notin Z(M/(\underline{x})M)$. Ahora considere un homomorfismo no nulo $\psi : R/I \to M/(\underline{x})M$, es decir, existe un $r + I$, tal que $\psi(r + I) \neq 0 + (\underline{x})M$. Por hipótesis tenemos que $x \cdot \psi(r + I) \neq 0 + (\underline{x})M$ ($x \notin Z(M/(\underline{x})M)$), pero $x \cdot \psi(r + I) = \psi(x \cdot r + I) = \psi(0 + I) = 0 + (\underline{x})M$, lo que contradice nuestra hipótesis. Así se sigue la afirmación. $\square$

Proposición 4.4. *Dado M un R-módulo y I un ideal de R tal que $IM \neq M$. Si $\{x_1, \cdots, \cdots x_m\}$ y $\{y_1, \cdots, \cdots y_m\}$ son M-secuencias máximas de elementos pertenecientes al ideal I (con $m \geq n$). Entonces:*

$$Hom_R(R/I, M/(x_1, \cdots, x_n)M) \cong Hom_R(R/I, M/(y_1, \cdots, y_n)M).$$

Corolario 4.4.1. *Sea M un R-módulo y I un ideal de R. Si $IM \neq M$, todas las M-secuencias máximas de elementos en I tienen la misma longitud. En particular si $IM \neq M$, entonces $prof_I(M) < \infty$.*

Demostración. Implicación inmediata de las proposiciones 4.4.1 y 4.3. $\square$

Ejemplo 4.5. *Veamos algunas propiedades destacables:*

- *Sea M un R-módulo y $x_1, \cdots, x_n$ una M-secuencia. Si $I = (x_1, \cdots, x_n)$, entonces $prof_I(M) = n$. Es claro que $x_1, \cdots, x_n$ es una M-secuencia máxima de elementos en I.*

- *Para todo $\mathfrak{p} \in Ass(M/(x_1, \cdots, x_n)M) \cap Sup(M)$, $prof_{\mathfrak{p}}(M) = n$. Como $\mathfrak{p} \in Sup(M)$, se garantiza que $\mathfrak{p}M \neq M$. Por otro lado, si $\mathfrak{p} \in Ass(M/(x_1, \cdots, x_n)M) \subseteq Sup(M/(x_1, \cdots, x_n)M)$ entonces $(x_1, \cdots, x_n) \subseteq \mathfrak{p} \subseteq Z(M/(x_1, \cdots, x_n)M))$, y como consecuencia de la proposición 4.3, $x_1, \cdots, x_n$ es una M-secuencia máxima en $\mathfrak{p}$.*

Proposición 4.6. *Sea M un R-módulo e I un ideal de R tal que $IM \neq M$. Entonces:*

$$prof_I(M) = \inf_{\mathfrak{p} \in Ass(M/IM)} \{prof_{\mathfrak{p}}(M)\}$$

Demostración. Si $\mathfrak{p} \in Ass(M/IM) \subseteq Sup(M/IM)$, entonces $I \subseteq \mathfrak{p}$, por lo tanto, $prof_I(M) \leq prof_R(M)$, para todo $\mathfrak{p} \in Ass(M/IM)$. Basta entonces mostrar que $prof_I(M) = prof_{\mathfrak{p}}(M)$, para algún $\mathfrak{p} \in Ass(M/IM)$. Sea $n = prof_I(M)$ ($prof_I(M)$ es finita) y $x_1, \cdots, x_n$ una M-secuencia máxima en I. Entonces $I \subseteq Z(I/MI)$, por lo tanto, $I \subseteq \mathfrak{p}$ para algún $\mathfrak{p} \in Ass(M/(x_1, \cdots, x_n)M)$. Por lo mencionado en el ejemplo 4.5, es suficiente mostrar que $\mathfrak{p} \in Sup(M/IM) \subseteq Sup(M)$ (La contención anterior se tiene debido a que M es finitamente generado, entonces $Sup(M/IM) = V(I + Ann(M)) = V(I) \cap Sup(M) \subseteq Sup(M)$). Como $(x_1, \cdots, x_n) \subseteq I \subseteq \mathfrak{p}$, entonces $ann(M) \subseteq ann(M/IM) = ann(M/IM) \subseteq \mathfrak{p}$, por lo tanto, $I + ann(M) \subseteq \mathfrak{p}$. Por la proposición 2.45, $\sqrt{ann(M/IM)} = \sqrt{I + ann(M)}$, resulta entonces $ann(M/IM) \subseteq \mathfrak{p}$ ($\sqrt{ann(M/IM)} = \sqrt{I + ann(M)} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$. Dado que $\mathfrak{p}$ es un ideal primo, entonces $\mathfrak{p} \in Sup(R/ann(M/IM))$, por lo tanto, $\mathfrak{p}$ debe contener un $\mathfrak{q} \in Ass(R/ann(M/IM)) = Ass(M/IM)$. Por la proposición 3.9, $\mathfrak{p} \in Sup(M/IM)$. Finalmente, puesto que $\mathfrak{p} \in Ass(M/(x_1, \cdots, x_n)M) \cap Sup(M)$, obtenemos la igualdad $prof_{\mathfrak{p}}(M) = n = prof_I(M)$. $\square$

Observemos que, para el $\mathfrak{q}$ mensionado en la prueba satisface que $prof_{\mathfrak{q}}(M) = n = prof_I(M)$. En efecto, por un lado, como $\mathfrak{q} \in Ass(M/IM) \subseteq Sup(M/IM)$, entonces $I \subseteq \mathfrak{q}$, lo cual implica entonces $n = prof_I(M) \leq prof_{\mathfrak{q}}(M)$. Ahora, como $\mathfrak{q} \subseteq \mathfrak{p}$, entonces $prof_{\mathfrak{q}}(M) \leq prof_{\mathfrak{p}}(M) = n$, donde $\mathfrak{p}$ es el primo mensionado en la prueba anterior.

Es de destacar las siguientes relaciones:

- $prof_I(M) \leq prof_{I_{\mathfrak{p}}}(M_{\mathfrak{p}})$, para todo ideal primo $I \subseteq \mathfrak{p}$ y todo R-módulo M.
- $prof_{\mathfrak{m}}(M) \leq dim(M)$, para todo módulo M sobre un anillo local R, con único máximal $\mathfrak{m}$.

Usando estas desigualdades, para todo ideal primo P de un anillo R (no nesesariamente local) podemos observar que:

$$prof_{\mathfrak{p}} = prof_{\mathfrak{p}}(R) \leq prof_{\mathfrak{p}_{\mathfrak{p}}}(R_{\mathfrak{p}}) \leq dim(R_{\mathfrak{p}}) = alt(\mathfrak{p}).$$

Por lo tanto, usando la proposición 4.6, para todo ideal I de R:

$$prof_I = prof_I(R) = \inf_{\mathfrak{p} \in Ass(R/I)} \{prof_{\mathfrak{p}}(R)\} \leq \inf_{\mathfrak{p} \in Sup(R/I)} \{prof_{\mathfrak{p}}(R)\} \leq \inf_{I \subseteq \mathfrak{p}, \mathfrak{p} \text{ primo}} \{prof_{\mathfrak{p}}(R)\} \leq \inf_{I \subseteq \mathfrak{p}, \mathfrak{p} \text{ primo}} \{alt(\mathfrak{p})\} \leq alt(I).$$

Es decir, para todo ideal I, $prof_I = prof_I(R) \leq alt(I)$. En los módulos de *Cohen-Machauley* veremos las propiedades de anillos R para los cuales, todos sus ideales satisfacen la igualdad $prof_I = alt(I)$.

Proposición 4.7. *Sea $\phi : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ un homomorfismo de anillos locales tal que S sea, por este homomorfismo un R-módulo finitamente generado. Si N es un S-módulo finitamente generado, entonces $prof_{\mathfrak{m}}(N) = prof_{\mathfrak{n}}(N)$.*

Demostración. La hipótesis de que S sea finitamente generado como R-módulo implica que $\phi(\mathfrak{m}) \subseteq \mathfrak{n}$. Sea $\underline{x} = x_1, \cdots, x_n \in \mathfrak{m}$ una N-secuencia máxima, considerando a N como un R-módulo via ϕ. Es fácil verificar que $\phi(x_1), \cdots, \phi(x_n) \in \mathfrak{n}$ es una N-secuencia, ahora considerando N como un S-módulo. Por ser $x_1, \cdots, x_n \in \mathfrak{m}$ una secuencia máxima, implica que $\mathfrak{m} \subseteq Z(N/(\underline{x})N)$, por lo tanto, $\mathfrak{m} \in Ass_R(N/(\underline{x})N)$. Para el $n \in N$ tal que $\mathfrak{m} = ann_R(n + (\underline{x})N)$, definamos el siguiente S-homomorfismo: $\psi : S \to N/(\phi(\underline{x}))N : r \to r \cdot (n + (\phi(\underline{x})N))$. Veamos que $S \cdot \phi(\mathfrak{m}) \subseteq nucleo(\psi)$. Efectivamente, sea $r \in S$ y $x \in \phi(\mathfrak{m})$, entonces:

$$\psi(r \cdot x) = (r \cdot x) \cdot (n + (\phi(\underline{x})N)) = r \cdot (x \cdot (n + (\phi(\underline{x})N)) = r \cdot (\phi(l) \cdot n + (\phi(\underline{x})N) = r \cdot (0 + (\phi(\underline{x})N) = (0 + (\phi(\underline{x})N).$$

Donde $x = \phi(l)$. Por otro lado, dado que $\phi(\mathfrak{m}) \subseteq \mathfrak{n}$, entonces $\mathfrak{n} = \sqrt{\phi(m) \cdot S}$, por lo tanto, $\sqrt{nucleo(\psi)} = \mathfrak{n}$. Lo anterior implica que $\mathfrak{n} \in Ass_S(N/(\phi(\underline{x}))N)$, por lo tanto, aplicando la proposición 4.3, concluimos que $\phi(\underline{x})$ es una N-secuencia máxima en $\mathfrak{n}$. $\square$

Proposición 4.8. *Sea R un anillo noetheriano. Sea $(0) \to N \to M \to K \to (0)$ es una secuencia exacta de R-módulos. Si I es un ideal de R tal que $IN \neq N$, $IM \neq M$, $IK \neq K$, entonces:*

- *Si* $prof_I(M) < prof_I(K)$, *entonces* $prof_I(N) = prof_I(K) + 1$.
- *Si* $prof_I(M) > prof_I(K)$, *entonces* $prof_I(N) = prof_I(M)$.
- *Si* $prof_I(M) = prof_I(K)$, *entonces* $prof_I(N) \geq prof_I(M)$.

Demostración. Ver **Corolario 18.6** en [EI]. □

Corolario 4.8.1. *Sea* R *un anillo local con único maximal* $\mathfrak{m}$*, y* M *un* R*-módulo tal que* $\mathfrak{m}M \neq M$*. Si* $x \notin Z(M)$*, entonces* $prof_{\mathfrak{m}}(M) = prof_{\mathfrak{m}}((x)M) = prof_{\mathfrak{m}}(M/(x)M) + 1$.

Demostración. Sea $x_1, \cdots, x_n$ una $M/(x)M$-secuencia en $\mathfrak{m}$. Dado que $x \notin Z(M)$, es fácil verificar que $x, x_1, \cdots, x_n$ es una M-secuencia en $\mathfrak{m}$, implicando que $prof_{\mathfrak{m}}(M) > prof_{\mathfrak{m}}(M/(x)M)$, por lo tanto, aplicando la proposicíon 4.8 a la secuencia exacta $(0) \to (x)M \to M \to M/(x)M$, obtenemos, $prof_{\mathfrak{m}}((x)M) = prof_{\mathfrak{m}}(M/(x)M) + 1$. Por otro lado, dado que $\mathfrak{m}$ es el único ideal maximal de R, entonces $(x) \subseteq \mathfrak{m}$. Ahora, por la proposición 4.6 es fácil ver que $prof_{\mathfrak{m}}((x)M) = prof_{\mathfrak{m}}(M)$. □

4.2. Módulos de Cohen-Macaulay

En la sección anterior vimos que, dado un R-módulo M e I un ideal de R tal que $IM \neq M$, existe un ideal primo $\mathfrak{p} \in Ass(M/IM)$ tal que $prof_I(M) = prof_{\mathfrak{p}}(M)$. De hecho, es posible demostrar que para el mismo ideal primo de $\mathfrak{p}$, $prof_I(M) = prof_{I_{\mathfrak{p}}}(M_{\mathfrak{p}})$. Destacaremos este hecho en el siguiente lema cuya demostración se desarrolla en base a la prueba de la proposición 4.6.

Lema 4.9. *Para todo* R*-módulo* M *y todo ideal* I *tal que* $IM \neq M$*, existe un ideal primo* $\mathfrak{p} \in Ass(M/IM)$ *tal que* $prof_I(M) = prof_{\mathfrak{p}}(M)$.

Para estudiar las propiedades de los anilos para los cuales sus ideales I satisfacen $prof(I) = alt(I)$, plantearemos el caso general en la estructura de módulos.

Definición 4.10. *(Módulo de Cohen-Macaulay): Un módulo* M *es llamado de Cohen-Macaulay (C-M) si satisface una de las siguientes condiciones equivalentes:*

1. $prof_{\mathfrak{p}_{\mathfrak{p}}}(M_{\mathfrak{p}}) = dim(M_{\mathfrak{p}})$*, para todo* $\mathfrak{p} \in Sup(M)$.
2. $prof_{\mathfrak{m}_{\mathfrak{m}}}(M_{\mathfrak{m}}) = dim(M_{\mathfrak{m}})$*, para todo* $m \in Sup(M)$*, con* m *ideal maximal.*
3. $prof_{\mathfrak{m}}(M) = alt(\mathfrak{m}/ann(M))$*, para todo* $\mathfrak{m} \in Sup(M)$*, con* $\mathfrak{m}$ *ideal maximal.*
4. $prof_{\mathfrak{p}}(M) = alt(\mathfrak{p}/ann(M))$*, para todo* $\mathfrak{p} \in Sup(M)$.
5. $prof_I(M) = alt(I/ann(M))$*, para todo ideal* I *tal que* $ann(M) \subseteq I$.

La condicion *2* de la definición 4.10 implica que toda localización de un módulo *C-M* es *C-M*. Un anillo R es llamado anillo de *Cohen-Macaulay* si lo es como R-módulo. Para el caso de un anillo local R con único ideal maximal $\mathfrak{m}$, un R-módulo M es *C-M*, si $prof_{\mathfrak{m}}(M) = dim(M)$.

Proposición 4.11. *Sea* R *un anillo local con único ideal maximal* $\mathfrak{m}$*, y* $M \neq (0)$ *un* R*-módulo. Entonces para todo ideal primo* $\mathfrak{p} \in Ass(M)$*, se tiene que:*

$$prof_{\mathfrak{m}}(M) \leq dim(R/\mathfrak{p}).$$

Demostración. Sea $\mathfrak{p} \in Ass(M)$. procedamos por inducción sobre $dim(R/\mathfrak{p})$ (sabemos que $dim(R/\mathfrak{p}) < \infty$). Si $dim(R/\mathfrak{p}) = 0$, entonces $\mathfrak{p} = \mathfrak{m}$. Por otro lado, dado que $\mathfrak{m} \in Ass(M)$, entonces $prof_{\mathfrak{m}}(M) = 0$ (no puede existir un $x \in \mathfrak{m}$ tal que $x \notin Z(M)$). Para el caso inductivo, supongamos que $dim(R/\mathfrak{p}) \geq 1$. Podemos suponer que $prof_{\mathfrak{m}}(M) \geq 1$, en caso contrario no hay nada que probar. Sea $x \in \mathfrak{m}$ tal que $x \notin Z(M)$ ($prof_{\mathfrak{m}}(M) \geq 1$). En particular $x \notin \mathfrak{p}$. Afirmamos que existe un ideal primo $\mathfrak{q} \in Ass(M/(x)M)$ tal que $\mathfrak{p} + (x) \subseteq \mathfrak{q}$. En efecto, sabemos que $\mathfrak{p} = ann(a)$, para algún $a \in M \setminus \{0\}$. Por la proposición 2.49, $\bigcap_{n\geq 0} x^n M = (0)$, entonces existe un $r \geq 0$ tal que $a \in x^r M \setminus x^{r+1}M$. Sea $b \in M \setminus (x)M$ tal que $a = x^r b$. Como $x \notin Z(M)$, entonces $\mathfrak{p}(b) = (0)$, por lo tanto, $(\mathfrak{p} + (x))(b) \subseteq \mathfrak{p}(b) + (x)(b) \subseteq (0) + (x)M = (x)M$. Lo anterior, implica que $\mathfrak{p} + (x) \subseteq Z(M/(x)M)$, por lo tanto, como consecuencia de la proposición 2.21, $\mathfrak{p} + (x) \subseteq \mathfrak{q}$, para algún $\mathfrak{q} \in Ass(M/(x)M)$. Volviendo a la demostración, tenemos que $dim(R/\mathfrak{q}) < dim(R/\mathfrak{p})$, por lo tanto, aplicando hipótesis inductiva obtenemos:

$$prof_{\mathfrak{m}}(M) = prof_{\mathfrak{m}}(M/(x)M) + 1 \leq dim(R/\mathfrak{q}) + 1 \leq dim(R/\mathfrak{p}) - 1 + 1 = dim(R/\mathfrak{p}).$$

□

Corolario 4.11.1. *Sea R un anillo local con único ideal máximal $\mathfrak{m}$ y M un R-módulo C-M. Entonces, $dim(R/\mathfrak{p}) = dim(M)$, para todo $\mathfrak{p} \in Ass(M)$. Consecuentemente, para este tipo de módulos, $Ass(M) = Min(M)$.*

Demostración. Dado que M un R-módulo *C-M*, entonces $prof_{\mathfrak{m}}(M) = dim(M)$. Aplicando la proposicíon anterior tenemos:

$$dim(M) = prof_{\mathfrak{m}}(M) \leq dim(R/\mathfrak{p}) \leq dim(M).$$

La última desigualdad se tiene por definición.

□

Corolario 4.11.2. *Sea R un anillo local con único ideal máximal $\mathfrak{m}$, M un R-módulo C-M, entonces:*

1. *Todo sistema de parámetros de M es una M-secuencia.*
2. *Si $x_1, \cdots, x_k$ es parte de un sistema de parámetros de M, entonces $M/(x_1, \cdots, x_k)M$ es C-M y $dim(M/(x_1, \cdots, x_k)M) = dim(M) - k$.*

Demostración. 1. Procedamos por inducción sobre la longitud de un sistema de parámetros de un módulo *Cohen-Macaulay* M. Supongamos que x es un sistema de parámetros de M, es decir, $\{x\}$ es el mínimo número de elementos que safisface $Sup(M/(x)M) = Sup(M) \cap Sup(R/(x)) = \{\mathfrak{m}\}$, por lo tanto, $Sup(M) \neq \{\mathfrak{m}\}$. Para verificar que x es una M-secuencia, por definición, debemos garantizar que $x \notin Z(M)$. Sea $\mathfrak{p} \in Sup(M)$ tal que $\mathfrak{p} \neq \mathfrak{m}$. Es claro que $\mathfrak{p} \notin Sup(R/(x))$ (de lo contrario $\mathfrak{p} \in Sup(M/(x)M)$), por lo tanto $(x) \not\subseteq \mathfrak{p}$, implicando entonces que $x \notin \mathfrak{p}$. Dado que M es *C-M*, $Ass(M) = Min(M) = Min(Sup(M))$. Supongamos que $x \in Z(M)$, es decir, debe existir un $\mathfrak{q} \in Ass(M) = Min(Sup(M))$ tal que $x \in \mathfrak{q}$, implicando entonces que $x \in \mathfrak{q} \subseteq \mathfrak{p}$, lo cual contradice nuestra hipótesis. Concluyendo así $x \notin Z(M)$. Veamos el caso inductivo: Sea $x_1, \cdots, x_n$ un sistema de parámetros de

M. Sea $N = M/(x_n)M$. Dado que $M/(x_1, \cdots, x_n)M \cong N/(x_1, \cdots, x_{n-1})N$, es fácil verificar que $x_1, \cdots, x_{n-1}$ es un sistema de parámetros para N. Para poder aplicar la hipótesis inductiva necesitamos garantizar que N es *C-M*. En efecto, por lo anterior mencionado $dim(N) = dim(M/(x_n)M) = dim(M) - 1$. Por otro lado, usando el mismo argumento empleado en el caso base, se puede verificar que $x_n \notin Z(M)$ y $x_n \notin Z(M/(x_1, \cdots, x_{n-1})M)$, por lo tanto, $prof_{\mathfrak{m}}(N) = prof_{\mathfrak{m}}(M/(x_n)M) = prof_{\mathfrak{m}}(M) - 1$ (la última igualdad estada dada por la proposición 4.8.1). Por ser M un R-módulo *C-M*, $prof_{\mathfrak{m}}(M) = dim(M)$, implicando así, $dim(N) = prof_{\mathfrak{m}}(N)$ (es decir, N es *C-M*). Aplicando hipótesis inductiva, $x_1, \cdots, x_{n-1}$ es entonces una M-secuencia, y dado que $x_n \notin Z(M/(x_1, \cdots, x_{n-1})M)$, se concluye que $x_1, \cdots, x_n$ es una M-secuencia.

2. Procedamos por inducción. El caso base ya se mencionó en el item anterior. Veamos el caso inductivo. Sea $x_1, \cdots, x_k \in R$ parte de un sistema de parámetros de M. Sea $N = M/(x_k)M$. En el item anterior vimos que N es un R-módulo *C-M*, por lo tanto, aplicando la hipótesis inductiva en N, tenemos que $M/(x_1, \cdots, x_k)M \cong N/(x_1, \cdots, x_{k-1})N$ es *C-M* y $dim(M/(x_1, \cdots, x_k)M)) = dim(N/(x_1, \cdots, x_{k-1})N) = dim(N) - (k-1) = dim(M/(x_k)M) - (k-1) = dim(M) - 1 - (k-1) = dim(M) - k$. □

Ejemplo 4.12. *Veamos algunos ejemplos:*

- *Todo anillo R de dimensión 0 es C-M; todo domínio de dimensión 1 es un anillo C-M.*
- *Todo domínio local normal de dimensión 2 es un anillo C-M.*
- *Dados enteros $0 \leq r \leq d$, existe al menos un anillo local de dimensión d y profundidad r. $R = (k[X_0, \cdots, X_r, \cdots, X_d]/(X_r^2, X_r X_{r+1}, \cdots, X_r X_d))_{(X_0, \cdots, X_d)}$, k un campo.*
- *Si R es un aillo C-M, entonces $R[X]$ es un anillo C-M.*
- *Si k es un cuerpo, entonces $k[X_1, \cdots, X_n]$ es un anillo C-M.*

5. Teoría Homológica

Anteriormente, estudiamos varias propiedades interesantes derivadas del concepto de *profundidad* de un módulo, y como este, es de gran importancia en cierta familia conocida como *módulos de Cohen-Macaulay.* En este capítulo, introduciremos un nuevo concepto llamado *dimensión homológica*, el cual es primordial para relacionar *profundidad* de un módulo con la *profundidad* de su anillo.

5.1. Resoluciones libres

Definición 5.1. *Sea M un R-módulo. Decimos que M admite una resolucion libre finita de longitud n, si existe a una secuencia de homomorfismos:*

$$(0) \to F_n \xrightarrow{\phi_n} F_{n-1} \xrightarrow{\phi_{n-1}} \ldots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to (0),$$

tales que nucleo(ϕ_i) = imagen(ϕ_{i+1}) y los $F_n, F_{n-1}, \ldots, F_1, F_0$ son módulos libres.

Definición 5.2. *Sea M un R-módulo. La dimensión homológica de M, denotado por $d.h(M)$ o $d.h_R(M)$, se define como la menor longitud que puede admitir una resolución libre finita de M.*

Proposición 5.3. *(Lema de Schannuel): Dadas dos resoluciones de un mismo módulo M (no necesariamente Z_n y $Z_n^{'}$ libres):*

$$(0) \to Z_n \to \ldots \to F_1 \to F_0 \xrightarrow{\phi_0} M \to (0)$$
$$(0) \to Z_n^{'} \to \ldots \to F_1^{'} \to F_0^{'} \xrightarrow{\phi_1} M \to (0)$$

Se tiene que:

$$Z_n \oplus F_{n-1}^{'} \oplus F_{n-2} \ldots \cong Z_n^{'} \oplus F_{n-1} \oplus F_{n-2}^{'} \ldots .$$

Demostración. Veamos primero un caso más simple de lema de Schannuel: Sea $(0) \to K \to F_0 \xrightarrow{\psi} M_1 \to (0)$ y Sea $(0) \to L \to F_1 \xrightarrow{\phi} M_2 \to (0)$ dos secuencias exactas tales que $M_1 \cong M_2$ mediante el isomorfismo γ, entonces $K \oplus F_1 \cong L \oplus F_0$, es decir, el siguiente diagrama conmuta:

$$\begin{tikzcd}
(0) \arrow[r] & K \oplus F_1 \arrow[r] \arrow[d, equal] & F_0 \oplus F_1 \arrow[r] \arrow[d, equal] & M_1 \arrow[r] \arrow[d, equal] & (0) \\
(0) \arrow[r] & L \oplus F_0 \arrow[r] & F_0 \oplus F_1 \arrow[r] & M_2 \arrow[r] & (0)
\end{tikzcd}$$

Sea $N = \{(a, b) \in F_1 \oplus F_2 / \gamma(\psi(a)) = \phi(b)\}$, y definiendo $\tau : F_0 \oplus F_1 \to M : (a, b) \to \gamma(\psi(a)) + \phi(b)$ es fácil verificar que la siguiente secuencia:

$$(0) \to N \xrightarrow{i} F_0 \oplus F_1 \xrightarrow{\tau} M_2 \to (0)$$

es una secuencia corta exacta. Como F_1 y F_2 son proyectivos (son libres) entonces tenemos las siguientes relaciones:

$$F_0 \cong K \oplus M_1 \cong K \oplus M_2$$
$$F_1 \cong L \oplus M_2$$
$$F_0 \oplus F_1 \cong N \oplus M_2$$

Es fácil verificar que $L \oplus F_0 \cong K \oplus F_1$.

Para el caso general, considere las secuencias exactas truncadas:

$$(0) \to Z_n \to \ldots \to F_1 \to Z_1 \to (0)$$
$$(0) \to Z_n' \to \ldots \to F_1' \to Z_1' \to (0)$$

Donde $Z_1 = nucleo(\phi_0)$ y $Z_1' = nucleo(\phi_1)$. Es fácil ver que las siguientes secuencias son exactas:

$$(0) \to Z_n \to \ldots \to F_2 \to F_1 \oplus F_0' \to Z_1 \oplus F_0' \to (0)$$
$$(0) \to Z_n' \to \ldots \to F_2' \to F_1' \oplus F_0 \to Z_1' \oplus F_0 \to (0)$$

Por el caso más simple aplicado a las secuencias exactas cortas $(0) \to Z_1 \to F_0 \to M \to (0)$ y $(0) \to Z_1' \to F_0' \to M \to (0)$ se sigue que $Z_1 \oplus F_0' \cong Z_1' \oplus F_0$. Así, procediendo por induccion sobre n y usando el caso base se tiene el caso general. □

Definición 5.4. *(Módulo establemente libre): Decimos que N es un módulo* establemente libre *si existen módulos libres F y F' tal que $N \oplus F' \cong F$.*

Corolario 5.4.1. *Sea R un anillo tal que todo módulo establemente libre es libre. Sea M un R-módulo tal que $d.h_R(M) < \infty$. Entonces de toda resolución libre (posiblemente infinita) de M es posible la extracción de una resolución libre de longitud $d.h_R(M)$.*

Demostración. Sea $\ldots \to F_1 \to F_0 \xrightarrow{\phi_0} M \to (0)$ una resolución libre posiblemente infinita de M. Como $d.h_R(M) < \infty$ podemos encontrar una resolución libre de longitud n. Ahora aplicando la proposición 5.3 (Lema de Schanuel) al truncar la resolución libre inicial en la etapa n y usando la definición de módulos establemente libres se tiene el resultado. □

Proposición 5.5. *Sea R anillo local y $(0) \to Z \xrightarrow{\phi} F \xrightarrow{\psi} M \to (0)$ una resolución proyectiva de M un R-módulo. Entonces una de las siguientes condiciones se tiene:*

1. *$d.h_R(M) = d.h._R(Z) = \infty$.*
2. *M es libre (luego Z es libre).*
3. *$d.h_R(M) = d.h._R(Z) + 1 < \infty$.*

Demostración. Z es libre si y solo si M es libre, es decir que $d.h_R(M) = 0$ si y solo si, $d.h_R(Z) = 0$. Supongamos M no libre y sea $\ldots \to F_2 \to F_1 \to F_0 \to Z \to (0)$ una resolución de libre de Z (posiblemente infinita). Entonces la siguiente es una resolución libre de N:

$$
\begin{tikzcd}
\dots F_1 \arrow[r] & F_0 \arrow[rr] \arrow[dr] & & F \arrow[r] & N \arrow[r] & (0) \\
& & Z \arrow[ur] \arrow[dr] & & & \\
& (0) \arrow[ur] & & (0) & &
\end{tikzcd}
$$

Por el corolario 5.4.1, $d.h_R(M) = \infty$ si y solo si, $d.h_R(Z) = \infty$. Supongamos $d.h_R(Z) = n < \infty$, y sea $(0) \to F_n \to \dots \to F_1 \to F_0 \to Z \to (0)$ una resolución libre de Z. Nuevamente $(0) \to F_n \to \dots \to F_0 \to F \to M \to (0)$ es una resolución libre de M de la cual podemos extraer una resolución de longitud $d.h_R(M)$, por lo tanto, $d.h_R(M) = d.h._R(Z) + 1 < \infty$ ($(0) \to F_n \to \dots \to F_1 \to F_0 \to Z \to (0)$ es de longitud mínima para Z).

$\square$

Proposición 5.6. *Sea $R, \mathfrak{m}$ un anillo local, N un R-módulo y $x \in \mathfrak{m}$ tal que $x \notin Z(N)$. Si $N/(x)N$ es $R/(x)$-módulo libre, entonces N es $R/(x)$-módulo libre.*

Demostración. Para la construcción del funtor derivado **Tor** ver **Capítulo 6.2** en [EI]. Sea $(0) \to Z \xrightarrow{\phi} F \xrightarrow{\psi} N \to (0)$ resolución de N tal que $Z \subseteq \mathfrak{m}F$ (todo homomorfismo con dominio R, su núcleo debe estar contenido en $\mathfrak{m}$. Ahora, dado que todo módulo proyectivo sobre un anillo local es libre y todo homomorfismo sobre un módulo libre se reduce a sus valores sobre los elementos de la base, se sigue (por la propiedad universal del coproducto y) por la afirmación anterior que su núcleo está contenido en $\mathfrak{m}F$). Mediante la multiplicación tensorial por $R/(x)$, tenemos que:

$$
\begin{tikzcd}
(0) \arrow[r] & Tor_1^R(R/(x), N) \arrow[r] \arrow[d, equal] & R/(x) \otimes Z \arrow[r] \arrow[d, equal] & R/(x) \otimes F \arrow[r] \arrow[d, equal] & R/(x) \otimes N \arrow[r] \arrow[d, equal] & (0) \\
(0) \arrow[r] & (Z \cap (x)F)/(x)Z \arrow[r] & Z/(x)Z \arrow[r] & F/(x)F \arrow[r] & N/(x)N \arrow[r] & (0)
\end{tikzcd}
$$

Veamos que existe un homomorfismo sobrejector $ann_N(x) = \{n \in N \ / \ x \cdot n = 0\} \to (Z \cap (x)F)/(x)Z$. Sea $\gamma : ann_N(x) \to (Z \cap (x)F)/(x)Z$ definida como sigue: para un $a \in ann_N(x)$, tomamos un $b \in F$, tal que $\psi(b) = a$ y asígnamos $\gamma(a) = xb + (x)Z$. γ esta bien definida. En efecto, veamos primero que $\gamma(a) = xb + (x)Z \in (Z \cap (x)F)/(x)Z$. Como $\psi(xb) = x\psi(b) = xa = 0$, entonces $xb \in nucleo(\psi) = imagen(\phi) = Z$. Es fácil verificar que si $a - b \in ann_N(x)$, entonces $\gamma(a) = \gamma(b)$ y que dicha aplicación efectivamente es un homomorfismo. Veamos que es un homorfismo sobreyector. Sea $y \in Z \cap (x)F$, por lo tanto $y = xf$, con $f \in F$. Por otro lado, $\psi(y) = \psi(xf) = x\psi(f) = 0$ ($y \in Z$), es fácil ver que $\gamma(\psi(f)) = y + (x)Z$.

Como $ann_N(x) = (0)$, entonces $(Z \cap (x)F)/(x)Z = (0)$ (γ es sobreyector), entonces tenemos la secuencia exacta:

$$(0) \to Z/(x)Z \to F/(x)F \to N/(x)N \to (0).$$

Al tensorizar la contención $Z \subseteq \mathfrak{m}F$ por $R/(x)$ se sigue que $Z/(x)Z \subsetneq mF/xF$. Ahora por ser $N/(x)N$ un $R/(x)$-módulo libre, tenemos $F/(x)F \cong (Z/(x)Z) \oplus (N/(x)N)$, nesariamente $Z/(x)Z = 0$, luego por el Lema de Nakayama en 2.42 obtenemos la igualdad $Z = (0)$, lo que implica que N es libre. $\square$

Proposición 5.7. *Sea R un anillo local con único ideal maximal $\mathfrak{m}$ y $x \in \mathfrak{m}$ tal que $x \notin Z(R)$. Si M es un R-módulo tal que $x \notin Z(M)$, entonces:*

$$d.h_{R/(x)}(M/(x)M) = d.h_R(M).$$

Demostración. Veamos primero que si $d.h_{R/(x)}(M/(x)M < \infty$, entonces $d.h_R(M) < \infty$. Sea $\ldots \to F_n \to F_{n-1} \to \ldots \to F_1 \to M \to (0)$ una resolución libre de M posiblemente infinita. Aplicando producto tensorial por $R/(x)$, obtenemos la secuencia exacta $\ldots \to F_n/(x)F_n \to F_{n-1}/(x)F_{n-1} \to \ldots \to F_1/(x)F_1 \to M/(x)M \to (0)$. Por el colorario 5.4.1 $Z_n/(x)Z_n$ es $R/(x)$-libre para algún n. Por la proposición 5.6, Z_n es libre, por lo tanto $d.h_R(M) < \infty$. Ahora es fácil ver que si $d.h_R(M) = n$, entonces $d.h_{R/(x)}(M/(x)M) = n$. $\square$

5.2. Teorema de Auslander-Buchsbaum

Proposición 5.8. *(Teorema de Auslander-Buchsbaum): Sea R un anillo local con único ideal maximal $\mathfrak{m}$. Si $M \neq (0)$ es un R-módulo tal que su dimensión homológica es finita ($d.h(M) < \infty$), entonces:*

$$d.h_R(M) + prof_{\mathfrak{m}}(M) = prof_{\mathfrak{m}}(R).$$

Demostración. Distingamos el problema en 3 casos:

- $prof_{\mathfrak{m}}(R) = 0$: Veamos que en este caso $d.h._R(M) = 0$. Supongamos $d.h._R(M) = 1$, (ya que en caso de que $d.h._R(M) > 1$ por el argumento que se dará en la prueba dicha hipótesis es irrelevante para conseguir la contradicción). Sea $(0) \to F_1 \to F_0 \to M \to (0)$ una resolución libre de M tal que $F_1 \subseteq \mathfrak{m}F_0$. Veamos que $prof_{\mathfrak{m}}(R) = 0$, implica $\mathfrak{m} \in Ass(R)$. En efecto, como $prof_{\mathfrak{m}}(R) = 0$ entonces para todo $x \in \mathfrak{m}$, $(x) = R$ ó $x \in Z(R)$. Como $\mathfrak{m}$ es maximal solo es posible que $x \in Z(R)$, es decir, $\mathfrak{m} \subseteq Z(R)$. Ahora de la proposición 2.21 y por ser $\mathfrak{m}$ maximal se tiene que $\mathfrak{m} \in Ass(R)$. Luego, $\mathfrak{m} = ann(r)$ para algún $r \neq 0 \in R$, por lo tanto $rF_1 \subseteq r\mathfrak{m}F_0 = 0$. Como F_1 es libre entonces $r = 0$, lo cual contradice lo antes mencionado. Como consecuencia $d.h_R(M) = 0$, es decir, M es libre, consecuentemente, $prof_{\mathfrak{m}}(M) = 0 = prof_{\mathfrak{m}}(R)$.
- $prof_{\mathfrak{m}}(R) \geq 0$ y $prof_{\mathfrak{m}}(M) = 0$: Procedamos por inducción sobre $prof(R)$. El caso base esta probado en el caso anterior. Para el caso inductivo escojamos un $x \notin Z(R)$. Por la proposición 4.8.1, $prof_{\mathfrak{m}}(R/(x)) = prof_{\mathfrak{m}}(R) - 1$. Necesitamos de un $R/(x)$-módulo para aplicar la hipótesis inductiva. El candidato es $Y/(x)Y$, donde $(0) \to Y \xrightarrow{\phi} F \xrightarrow{\psi} M \to (0)$ es una resolución de M. Antes de aplicar induccion debemos garantizar que $d.h_{R/(x)}(Y/(x)Y) < \infty$ y $prof_{\mathfrak{m}/(x)}(Y/(x)Y) = 0$. Ya que $x \notin Z(Y)$ (esto por ser F libre y Y estas embebido en F) por la proposición 5.7 se tiene la primera condución. Veamos como garantizar la segunda condición: Como $prof_{\mathfrak{m}}(M) = 0$, entonces $\mathfrak{m} \in Ass(M)$. Sea $a \neq 0 \in M$ tal que $a\mathfrak{m} = 0$. Escojamos

una pre-imagen e de a en F. Como $a \neq 0$, $e \notin \phi(Y) \cong Y$ ($imagen(\phi) = nucleo(\psi)$), luego $xe \notin (x)\phi(Y) \cong (x)Y$ (sí $xe \in (x)\phi(Y)$, por ser F libre, entonces $e \in \phi(Y)$). Por otro lado $e\mathfrak{m} \subseteq \phi(Y) \cong Y$, luego $xe\mathfrak{m} \subseteq (x)\phi(Y) \cong (x)Y$. Así, $\mathfrak{m}$ esta contenido en un primo asociado de $Y/(x)Y$, y por ser maximal debe ser ese primo asociado. Consecuentemente, $prof_{\mathfrak{m}/(x)}(Y/(x)Y) = 0$. Ahora podemos aplicar la hipótesis inductiva, obteniendo las siguientes relaciones:

$$d.h_{R/(x)}(Y/(x)Y) = prof_{\mathfrak{m}/(x)}(R/(x)).$$
$$d.h_{R/(x)}(Y/(x)Y) = d.h_R(Y) \text{ (proposición 5.7).}$$
$$d.h_R(Z) = d.h_R(M) - 1 \text{ (proposición 5.5).}$$
$$prof_{\mathfrak{m}/(x)}(R/(x)) = prof_{\mathfrak{m}/(x)}(R) - 1 = prof_{\mathfrak{m}}(R) - 1 \text{ (proposición 4.8.1).}$$

Por consiguiente $d.h_R(M) = prof_{\mathfrak{m}}(R)$.

- $prof_{\mathfrak{m}}(R) > 0$ y $prof_{\mathfrak{m}}(M) > 0$: En este caso podemos escoger $x \in \mathfrak{m}$ tal que $x \notin Z(R)$ y $x \notin Z(M)$ (existe al menos una M-secuencia y R-secuencia en $\mathfrak{m}$). Por lo tanto:

$$d.h_{R/(x)}(M/(x)M) = d.h_R(M) \text{ (proposición 5.7). } prof_{\mathfrak{m}/(x)}(R/(x)) = prof_{\mathfrak{m}}(R) - 1$$
$$\text{(igual que en el caso anterior).}$$
$$prof_{\mathfrak{m}/(x)}(M/(x)M) = prof_{\mathfrak{m}}(M/(x)M) \text{ (proposicón 4.7).}$$
$$prof_{\mathfrak{m}/(x)}(M/(x)M) = prof_{\mathfrak{m}/(x)}(M) - 1 = prof_{\mathfrak{m}}(M) - 1. \text{ (proposición 4.8.1)}$$

Entonces, de la hipótesis inductiva del caso anterior y usando las igualdades anteriores se optiene el resultado.

□

Corolario 5.8.1. *Sea R un anillo noetheriano y $M \neq (0)$ un R-módulo. Entonces, para todo ideal $\mathfrak{p} \in Ass(M)$ se tiene que:*

$$prof(\mathfrak{p}) \leq d.h_R(M).$$

Demostración. Solo interesa el caso donde $d.h_R(M) < \infty$, sea $\mathfrak{p} \in Ass(M)$. Entonces:

$$prof_{\mathfrak{p}}(R) \leq prof_{\mathfrak{p}_{\mathfrak{p}}}(R_{\mathfrak{p}}).$$
$$prof_{\mathfrak{p}_{\mathfrak{p}}}(R_{\mathfrak{p}}) = d.h_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) + prof_{\mathfrak{p}_{\mathfrak{p}}}(M_{\mathfrak{p}}) \text{ (proposicipon 5.8).}$$
$$prof_{\mathfrak{p}_{\mathfrak{p}}}(M_{\mathfrak{p}}) = 0 \ (\mathfrak{p}_{\mathfrak{p}} \in Ass(M_{\mathfrak{p}})).$$
$$d.h_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) \leq d.h_R(M).$$

De las relaciones anteriores se obtiene el resultado. □

6. Conjeturas Homológicas

En los capítulos anteriores observamos que existe una relación bastante fuerte entre la profundidad de un módulo y la profundidad de su anillo dado por el *teorema de Auslander-Bushsbaum* en 5.8:

$$d.h_R(M) + prof_{\mathfrak{m}}(M) = prof_{\mathfrak{m}}(R).$$

Por este hecho, se podría plantear la siguiente pregunta: ¿es posible prolongar un sistema de parámetros de M a un sistema de parámetros de R?. Una primera aproximación para responder esta inquietud se observa en el siguiente proposición:

Proposición 6.1. *Si R es un anillo local con único ideal maximal $\mathfrak{m}$. Las siguientes afirmaciones son equivalentes:*

1. *Dados M, N R-módulos tales que si $Sup(M) \cap Sup(N) = \{\mathfrak{m}\}$, entonces $dim(M) + dim(N) \leq dim(R)$.*
2. *Dado un R-módulo M, todo sistema de parámetros de M se puede prolongar a un sistema de parámetros de R.*

Demostración. *1* $\Rightarrow$ *2*: Sea $x_1, \cdots, x_n$ un sistema de parámetros de M. Dado que $Sup(M) \cap Sup(R/(x_1, \cdots, x_n)) = Sup(M/(x_1, \cdots, x_n)M) = \{\mathfrak{m}\}$, entonces por hipótesis, $n = dim(M) + dim(R/(x_1, \cdots, x_n)) \leq dim(R)$. Por otro lado, aplicando la proposición 3.22, $dim(R) \leq dim(R/(x_1, \cdots, x_n)) + n$ (ya que $(x_1, \cdots, x_n) \subseteq \mathfrak{m}$). Por lo tanto, $dim(R/(x_1, \cdots, x_n)) = dim(R) - n$. De nuevo, aplicando la proposición 3.22, $x_1, \cdots, x_n$ se puede prolongar a un sistema de parámetros de R.

2 $\Rightarrow$ *1*: Sean M y N R-módulos tales que $Sup(M) \cap Sup(N) = \{\mathfrak{m}\}$. Sea $I = ann(N)$. Por la proposición 3.9, $Sup(N) = Sup(R/ann(N))$, implicando la igualdad $Sup(M/IM) = Sup(M) \cap Sup(R/I) = \{\mathfrak{m}\} \neq \emptyset$. Luego, I contiene un sistema de parámetros $x_1, \cdots, x_n$ de M. Por hipótesis, tal sistema de parámetros de M se puede prolongar a un sistema de parámetros de R. Por lo tanto, $dim(R/(x_1, \cdots, x_n)) = dim(R) - n$ de a cuerdo a la proposición 3.22. Dado que, $(x_1, \cdots, x_n) \subseteq I$, entonces $dim(N) = dim(R/I) \leq dim(R/(x_1, \cdots, x_n))$, implicando así que $dim(N) \leq dim(R) - n = dim(R) - dim(M)$. □

Corolario 6.1.1. *Sea R un anillo local con único anillo maximal $\mathfrak{m}$. Considere las siguientes afirmaciones:*

1. *Dados M, N R-módulos tales que si $Sup(M) \cap Sup(N) = \{\mathfrak{m}\}$, entonces $dim(M) + dim(N) \leq dim(R)$.*
2. *Dado un R-módulo M, toda M-secuencia es una R-secuencia.*

Si R es Cohen-Macaulay, 1 $\Rightarrow$ 2. Si alguno de los módulos M o N es Cohen-Macaulay, 2 $\Rightarrow$ 1.

En general, no es fácil responder a la pregunta de si toda M-secuencia es una R-secuencia. En 1961 el matemático *Maurice Auslander* en su trabajo *Modules over unramified regular local rings* (ver [AU]) propuso un primer acercamiento a la validez de dicha inquitud con el siguiente teorema:

(Teorema de Auslander): Sea R un anillo local, M un R-módulo finitamente generado tal que si $Tor_1^R(M,N)=0$, entonces $Tor_i^R(M,N)=0$, para todo $i\geq 1$, para algún R-módulo N. Entonces toda M-secuencia es una R-secuencia.

Desafortunadamente, a principios de los años 90, el matemático *Ray Heitmann* en [HE] construyó un contraejemplo de un módulo con dimensión homológica finita sobre un anillo local el cual no cumple la propiedad de rigidez mencionada en el *teorema de Auslander*. Dicha inquietud es conocida hoy en día como la *conjetura del divisor de cero*. Este problema llamó la atención de diferentes matemáticos en los siguientes años desde que fue dada a conocer por *Auslander*, *C. Peskine y L. Szpiro* a finales de los 60 probaron su validez para anillos locales equicaracterísticos de característica p, hipótesis empleada en las demostraciones de otras conjeturas relacionadas. En este capítulo, nos ocuparemos de profundizar en algunas de las relaciones que dicha conjetura tiene con otros resultados equivalentes tales como la *conjetura de codimensión* o la *conjetura de intersección de Pesquine-Szpiro*, las cuales nos permitirán proponer una posible prueba a la *conjetura del divisor de cero*.

6.1. Conjetura del divisor de cero; Conjetura de Pesquine-Szpiro

Conjetura 6.2. *(Conjetura del divisor de cero): Sea R un anillo local, y M un R-módulo tal que su dimensión homológica es finita ($d.h(M)<\infty$). Entonces, toda M-secuencia es una R-secuencia.*

Conjetura 6.3. *(Conjetura de codimensión): Sea R un anillo local y $M\neq 0$ un R-módulo tal que su dimensión homológica es finita ($d.h(M)<\infty$). Entonces:*

$$dim(M)+prof(ann(M))=dim(R)$$

Conjetura 6.4. *(Conjetura de Serre, Pesquine-Szpiro) Sea R un anillo local con único ideal maximal $\mathfrak{m}$, M, N R-módulos tales que:*

1. *La dimensión homológica de M es finita ($d.h(M)<\infty$).*
2. *$Sup(M)\cap Sup(N)=\{\mathfrak{m}\}$.*

Entonces:

$$dim(M)+dim(N)\leq dim(R).$$

Conjetura 6.5. *(Conjetura de intersección de Peskine-Szpiro): Sea R un anillo local con único ideal maximal $\mathfrak{m}$, M, N R-módulos tales que:*

1. *La dimensión homológica de M es finita ($d.h(M)<\infty$).*
2. *$Sup(M)\cap Sup(N)=\{\mathfrak{m}\}$.*

Entonces:

$$dim(N)\leq d.h_R(M).$$

Es importante notar que, si un anillo local R pertenece a una clase de anillos locales cerrada al pasar al cociente por un no divisor de cero, las siguientes propiedades continuan válidas para dichos anillos:

1. Todo elemento no divisor de cero de un anillo no puede ser una unidad en dicho anillo, por lo tanto, pertenece a su único ideal maximal.

2. El ideal generado por una R-secuencia no puede contener todo el anillo R.

Proposición 6.6. *Sea R un anillo local. Suponga este pertenece a una clase de anillos locales que es cerrada al pasar al cociente por un no-divisor de cero. Así mismo, suponga que todo R-módulo M satisface $d.h_R(M) < \infty$. Si $x \notin Z(M)$ implica $x \notin Z(R)$ entonces, para toda $\underline{x} = x_1, \ldots, x_n$ M-secuencia se tiene que $d.h_{R/\underline{x}}(M/\underline{x}M) < \infty$.*

Demostración. Sea M un R-módulo tal que $d.h_R(M) < \infty$. Procedamos por inducción sobre la longitud de la M-secuencia. Para el caso base es fácil ver que por la proposición 5.7, basta notar que x_1 no es una unidad en R, es decir, $x_1 \in \mathfrak{m}$. Veamos el caso inductivo: Sea $x_1, \ldots, x_{n+1}$ una M-secuencia. Por definicion, $\underline{x} = x_1, \ldots, x_n$ es una M-secuencia de longitud n, y, por la hipótesis de inducción, podemos afirmar que:

$$d.h_{R/(x_1,\ldots,x_n)}(M/(x_1, \ldots, x_n)M) < \infty.$$

Por otro lado, es fácil verificar que si $x_{n+1} \notin Z_R(M/(\underline{x})M)$ entonces $x_{n+1} + (\underline{x}) \notin Z_{R/(\underline{x})}(M/(\underline{x})M)$, en concecuencia $x_{n+1} + (\underline{x}) \notin Z(R/(\underline{x}))$. Podemos garantizar que $x_{n+1}+(\underline{x})$ pertenece al único ideal maximal de $R/(\underline{x})$. Aplicando entonces la proposición 5.7, tenemos que:

$$d.h._{\overline{R}/(x_{n+1}+(\underline{x}))}(\overline{M}/(x_{n+1} + (\underline{x}))\overline{M}) = d.h_{\overline{R}}(\overline{M}) < \infty.$$

Donde $\overline{R} = R/(x_1, \ldots, x_n)$ y $\overline{M} = M/(x_1, \ldots, x_n)M$. El resultado final se obtiene de las relaciones:

- $\overline{R}/(x_{n+1} + (x_1, \ldots, x_n)) \cong R/(x_1, \ldots, x_{n+1})$.
- $\overline{M}/(x_{n+1} + (x_1, \ldots, x_n)\overline{M}) \cong M/(x_1, \ldots, x_{n+1})M$.

□

Proposición 6.7. *(Principio de inducción): Si para todo anillo R pertenciente a una clase de anillos locales cerrada al pasar al cociente por un no divisor de cero de R y para todo R-módulo M tal que $d.h_R(M) < \infty$ se tiene que: si $x \notin Z(M)$ implica que $x \notin Z(R)$ entonces, toda M-secuencia es una R-secuencia.*

Demostración. Procedamos por inducción sobre la longitud de una M-secuencia. El caso base se tiene dado que R pertenece a una clase de anillos locales cerrada al pasar al cociente por un no divisor de cero.

Veamos el caso inductivo: Sea $x_1, \ldots, x_{n+1}$ una M-secuencia. Por la proposicion 6.6 tenemos:

$$d.h_{R/(x_1,\ldots,x_n)}(M/(x_1, \ldots, x_n)M) < \infty.$$

Como $x_{n+1} \notin Z_R(M/(x_1,\ldots,x_n)M)$, entonces $x_{n+1}+\underline{x} \notin Z_{R/(x_1,\ldots,x_n)}(M/(x_1,\ldots,x_n)M)$ y $x_{n+1}+\underline{x} \notin Z(R/(x_1,\ldots,x_n))$, donde $\underline{x}=(x_1,\ldots,x_n)$. Es fácil ver que si $x_{n+1}+\underline{x} \notin Z_{R/(x_1,\ldots,x_n)}(R/(x_1,\ldots,x_n))$ entonces $x_{n+1} \notin Z_R(R/(x_1,\ldots,x_n))$. Por último, podemos garantizar que $(x_1,\ldots,x_{n+1}) \neq R$, por lo tanto, $x_1,\ldots,x_{x+1}$ es una R-secuencia. □

Proposición 6.8. *Sea R un anillo Cohen-Macaulay y M un R-módulo tal que $d.h_R(M) < \infty$. Entonces, toda M-secuencia es una R-secuencia, si y solo si, todo divisor de cero de M es un divisor de cero de R.*

Demostración. Consecuencia inmediata de la proposición 6.7. □

Proposición 6.9. *Asumiendo como cierta la conjetura 6.3 y la conjetura 6.4, entonces la conjetura 6.5 es válida.*

Demostración. Sea R, m un anillo local y M y N R-módulos tales que $d.h_R(M) < \infty$ y $Sup(M) \cap Sup(N) = \{\mathfrak{m}\}$. Por lo tanto:

$$\begin{aligned} dim(N) &\leq dim(R) - dim(M) = \text{(proposición 6.4)} \\ &= dim(R) - (dim(R) - prof(ann(M))) = \text{(proposición 6.3)} \\ &= prof(ann(M)) \leq d.h_R(M) \text{ (corolario 5.8.1)}. \end{aligned}$$

□

Para poder aplicar el principio inductivo, debemos garantizar que la condición de la conjetura 6.5 sigue siendo aplicable al pasar al cociente por un no divisor de cero del anillo, es decir, que la clase de anillos que satisface la condición de la conjetura sea cerrada pasar al cociente por un no divisor de cero del anillo.

Proposición 6.10. *(Propiedad inductiva de la conjetura de intersección de Peskine-Szpiro): Asumiendo como cierta la conjetura 6.5, entonces para todo anillo local R, $\mathfrak{m}$, M un R-módulo no nulo tal que $d.h_R(M) < \infty$ y N un $R/(x)$-módulo tal que $Sup(M/(x)M) \cap Sup(N) = \{\mathfrak{m}/(x)\}$, donde $x \notin Z(M)$ y $x \notin Z(R)$, se tiene que:*

$$dim(N) \leq d.h_{R/(x)}(M/(x)M).$$

Demostración. Sea M un R-módulo tal que $d.h_R(M) < \infty$ y N un $R/(x)$-módulo tal que $Sup(M/(x)M) \cap Sup(N) = \{\mathfrak{m}/(x)\}$, donde $x \notin Z(M)$ y $x \notin Z(R)$. Considerando N como R módulo via el homomorfismo $R \to R/(x)$, es posible demostrar que $Sup(M) \cap Sup(N) = \{\mathfrak{m}\}$, así por la proposición 6.5, $dim(N) < d.h_R(M)$. Por otro lado, como $x \notin Z(M)$ y $x \notin Z(R)$, usando la proposición 5.7, $d.h_{R/(x)}(M/(x)M) = d.h_R(M)$, por consiguiente $dim(N) \leq d.h_{R/(x)}(M/(x)M)$. □

Proposición 6.11. *Asumiendo como cierta la conjetura 6.5, entonces para todo anillo local R y todo R-módulo M tal que $d.h_R(M) < \infty$, se tiene que: Si $\mathfrak{p} \in Ass(R)$, entonces para algún $\mathfrak{q} \in Ass(M)$, $\mathfrak{p} \subseteq \mathfrak{q}$.*

Demostración. Procedamos por inducción sobre $dim(M)$ (sabemos que $dim(M) < \infty$). Si $dim(M) = 0$, implica que $Sup(M) = \{\mathfrak{m}\}$. En este caso, es claro que todo ideal $\mathfrak{p} \in Ass(R)$ esta contenido en el maximal $\mathfrak{m}$. Ahora sea M un R-módulo tal que $dim(M) > 0$ y $\mathfrak{p} \in Ass(R)$. Existen dos posibilidades:

- El único ideal primo en el $Sup(M)$ conteniendo $\mathfrak{p}$ es $\mathfrak{m}$. En este caso $Sup(M) \cap Sup(R/\mathfrak{p}) = \{\mathfrak{m}\}$. Aplicando la conjetura 6.5, $dim(R/\mathfrak{p}) \leq d.h_R(M)$. Por otro lado, por la proposición 4.11, viendo a R como R-módulo, $prof(R) \leq dim(R/\mathfrak{p})$, por lo tanto:

$$-d.h_R(M) \leq -dim(R/\mathfrak{p})$$
$$prof(R) \leq dim(R/\mathfrak{p})$$
$$d.h_R(M) + prof(M) = prof(R) \text{ (proposición 5.8)}$$

  De lo anterior, $prof_{\mathfrak{m}}(M) = prof(M) = 0$. Por la proposición 4.3 se tiene que $\mathfrak{m} \subseteq Z(M)$, es decir, $\mathfrak{m} \in Ass(M)$.

- Existe un ideal $\mathfrak{q} \in Sup(M)$ tal que $\mathfrak{p} \subseteq \mathfrak{q}$ y $\mathfrak{q} \neq \mathfrak{m}$. En este caso, podemos aplicar la hipótesis inductiva a $M_{\mathfrak{q}}$ dado que $dim(M_{\mathfrak{q}}) \subsetneqq dim(M)$ y $d.h_{R_{\mathfrak{q}}}(M_{\mathfrak{q}}) \leq d.h_R(M) < \infty$ (aplicando la la conjetura 6.5 a $M_{\mathfrak{q}}$), por consiguiente, existe un $\mathfrak{q}^{'} R_{\mathfrak{q}} \in Ass(M_{\mathfrak{q}})$ tal que $\mathfrak{p}R_{\mathfrak{q}} \subseteq \mathfrak{q}^{'} R_{\mathfrak{q}}$. De lo anterior, es posible concluir que $\mathfrak{p} \subseteq \mathfrak{q}^{'}$, $\mathfrak{q}^{'} \in Ass(M)$.

□

Corolario 6.11.1. *(Problema tesis): Asumiendo como cierta la conjetura 6.3 y la conjetura 6.4 es posible demostrar la validez de la conjetura 6.2.*

Demostración. Es fácil verificar que, por la proposición 6.11, todo R-módulo M tal que $d.h_R(M) < \infty$, cumple la afirmación: si $x \notin Z(M)$ implica que $x \notin Z(R)$. Por otro lado, la conjetura de intersección en 6.5 garantiza que R pertenece a una clase de anillos locales cerrada al pasar al cociente por un no divisor de cero de R, por lo tanto, es posible aplicar el principio de inducción de la proposición 6.7. □

6.2. Panorama actual de las conjeturas

Desde el momento en que empezó a surgir todo tipo de problemas e inquietudes abiertas en relación a propiedades homológicas de un anillo conmutativo al estudiar su *dimensión de Krull*, *dimensión global* y *profundidad*, matemáticos como M. Auslander, C. Peskine, L. Szpiro, M. Hochster, E. Graham Evans, P. Griffith, entre otros, encontráron una serie de conexiones entre diversas conjeturas/teoremas que han permitido dar respuestas parciales o totales a muchas de estas inquietudes (Ver [HO]). Entre las conjeturas/teoremas más destacadas y de mayor importancia en el área se encuentran las siguientes:

- *Conjetura de intersección fuerte (SIC): Sea $R, \mathfrak{m}$ un anillo local y M, N un R-módulo tal que $Sup(M) \cap Sup(N) = \{\mathfrak{m}\}$ y $d.h_R(M) < \infty$.* Entonces $dim(N) \leq Grade(M)$, donde $Grade(M) := inf\{i \geq 0 : Ext^i_R(M, R) \neq 0\}$.

- *Conjetura de Bass (BC): Sea $R, \mathfrak{m}$ un anillo local y suponga que existe un R-módulo finitamente generado de dimensión inyectiva finita, entonces R es un anillo de Cohen-Macaulay.*

- *Conjetura de Superaltura (SC): Sea $R, \mathfrak{m}$ un anillo local y M un R-módulo tal que $d.h_R(M) < \infty$, entonces $superalt(ann(M)) \leq d.h_R(M)$, donde $superalt(I) := sup\{alt(IS) : R \to S$ es un homomorfismo, S es Noetheriano, $IS \neq S\}$.*

- *Nueva conjetura de intersección (NIC): Sea $R, \mathfrak{m}$ un anillo local y $F : (0) \to F_s \to F_{s-1} \to \cdots \to F_0 \to (0)$ un complejo de un R-módulo libre finitametne generado. Suponga que F se convierte en un complejo exacto al localizar por un ideal primo distinto de $\mathfrak{m}$, entonces $s \geq dim(R)$.*

- *Conjetura del sumando directo (DSC): Sea $R, \mathfrak{m}$ un anillo local regular. Si $R \subseteq S$ es una extensión módulo-finita, entonces R es sumando directo de S como R-módulo, es decir, existe un R-homomorfismo $\psi : S \to R$ tal que $\psi(r) = r$ para todo $r \in R$.*

- *Conjetura del monomio (MC): Sea $R, \mathfrak{m}$ un anillo local y $x_1, \cdots, x_n$ un sistema de parámetros de R, entonces para todo $t \geq 1$, $x_1^t \cdots x_n^t \notin (x_1^{t+1} \cdots x_n^{t+1})$.*

- *Conjetura de Syzygy: Sea $R, \mathfrak{m}$ un anillo local y L un R-módulo finitamente generado no-libre i^{th} syzygy* [2] *tal que $d.h_R(L) < \infty$, entonces $rango(L) \geq i$.*

- *Conjetura Big Cohen-Macaulay: Todo sistema de parámetros de un anillo local tiene un Big Cohen-Macaulay* [3] *módulo.*

- *Conjetura Small Cohen-Macaulay: Sea $R, \mathfrak{m}$ un anillo local completo, entonces R tiene un módulo Cohen-Macaulay finitamente generado maximal.*

Hasta la fecha, solo se han podido encontrar las siguientes relaciones respecto a estos problemas:

$$
\begin{tikzcd}
 & \textit{Conjetura Small Cohen-Macaulay} \arrow[d, Rightarrow] & \\
 & \textit{Conjetura Big Cohen-Macaulay} \arrow[dd, Rightarrow] & \\
\textit{Conjetura DSC} \arrow[rr, Leftrightarrow] \arrow[d, Rightarrow] & & \textit{Conjetura MC} \\
\textit{Conjetura de Syzygy} & \textit{Conjetura NIC} \arrow[d, Rightarrow] & \\
\textit{Conjetura divisor de cero} & \textit{Conjetura IC} \arrow[l, Rightarrow] \arrow[d, Rightarrow] & \textit{Conjetura SIC} \arrow[l, Rightarrow] \\
 & \textit{Conjetura BC} &
\end{tikzcd}
$$

El *problema del divisor de cero de Auslander* tuvo el estatus de conjetura hasta mediados de los años 80. En [P-S], C. Peskine y L. Szpiro mostraron como el *problema de Auslander* es consecuencia de su teorema de intersección y, por lo tanto, demostraron su validez para una amplia clase de anillos locales. P. Roberts en [RO] demostró la

[2] Sea $R, \mathfrak{m}$ un anillo y M un R-módulo finitamente generado. El i^{th} syzygy de M se define como el $nucleo(\phi_{i-1}) = imagen(\phi_i)$ en una resolución proyectiva mínima de M. Si un R-módulo L es isomorfo a un i^{th} syzygy de M, diremos que L es i^{th} syzygy.

[3] Sea $\underline{x} = x_1, \cdots, x_n$ un sistema de parámetros de un anillo local R. Un R-módulo M es llamado *Big Cohen-Macaulay* para $\underline{x}$ si $x_1, \cdots, x_n$ es una M-secuencia.

validez del teorema de la intersección de C. Peskine y L. Szpiro a finales de los años 80, concluyendo así con una de las inquietudes más importantes en el área del *algebra conmutativa* hasta entonces. Sin embargo, el caso general del problema, es decir, en donde el anillo R no necesariamente sea local y el R-módulo M no necesariamente sea finitamente generado, permanece como un problema abierto en la actualidad. Inspirados por el *problema del divisor de cero*, hoy en día se estudia las estructuras conocidas como *módulos de Auslander*, donde por definición, son módulos sobre un anillo conmutativo tales que $Z(R) \subseteq Z(M)$. Por útimo, veamos algunas propiedades generales sobre los *módulos de Auslander*:

Proposición 6.12. *Sea M un R-módulo. Entonces:*

- *Si R es un dominio integral, entonces M es un R-módulo de Auslander.*
- *Sea M es un R-módulo tal que $ann(M) = (0)$, entonces $Hom_R(M, M)$ un R-módulo de Auslander.*
- *Sea M es un R-módulo, si N es un R-submódulo de Auslander de M, entonces M es un R-módulo de Auslander.*
- *Si, M es un R-módulo de Auslander, entonces $M \oplus N$ es un R-módulo de Auslander para cualquier R-módulo N. En particular, sea $\{M_i\}_{i\in\Lambda}$ es una familia de R-módulos tal que existe al menos un R-módulo de Auslander M_j, entonces $\bigoplus_{i\in\lambda} M_i$ y $\prod_{i\in\lambda} M_i$ son R-módulos de Auslander.*

Demostración. Ver **Proposición 1.2** en [PN]. □

Referencias

[AS] Simis, A. (2020). *Commutative Algebra*. De Gruyter Textbook, De Gruyter graduate, 2020.

[AU] Auslander, M. (1961). *Modules over unramified local rings*. I11. J. of Math. 5 (1961) 631-645.

[AY] Atiyah, M. F., amp; MacDonald, I. G. (1969). *Introduction To Commutative Algebra Addison-Wesley series in mathematics*. Avalon Publishing, 1994.

[BH] Bhatt, B. (2016), *On the direct summand conjecture and its derived variant*. arXiv preprint arXiv:1608.08882.

[DU] Dutta, S. P. (1989). *Syzygies and homological conjectures*. In Commutative algebra (pp. 139-156). Springer New York.

[EI] Eisenbud, D. (1995). *Commutative Algebra: With a View Toward Algebraic Geometry Graduate Texts in Mathematics*. Springer Science Business Media, 1995.

[HC] Hochster, M. (1974). *The equicharacteristic case of some homological conjectures on local rings*. Bulletin of the American Mathematical Society, 80(4), 683-686.

[HE] Heitmann, R. (1993). *A contraexample to the rigidity conjeture for rings*. Bulletin (New Series) Of The American Mathematical Society, Volume 29, Number 1, July 1993.

[HO] Hochster, M. (1975), *Topics in the homological theory of modules over commutative rings*, Expository lecture s from the CBMS regional conference held at the University of Nebraska , June 24-28 , 1974.

[MH] Hochster, M. (2007), *Homological conjectures, old and new* Illinois Journal of Mathematics, 51(1), 151-169.

[PN] Nasehpour, P. (2018), *Auslander Modules* arXiv:1705.03980.

[PE] Peskine, C., Szpiro, L. (1973), *dimensión projective finie et cohomologie locale*, Publications mathématiques de lÍHÉS, 42(1), 47-119.

[P-S] Peskine, P. and Szpir, L. (1973). *dimensión projective finie et cohomologie locale*. ubl. Math. IHES 42, (1973), 47-119.

[RO] Roberts, P. (1989). *Intersection theorems, in: Commutative Algebra, in: Math. Sci. Res. Inst. Publ.*. Vol. 15, Springer-Verlag, Berlin, 1989, 417–436.

[VE] Velez, Juan Diego (1993). *La conjetura del sumando directo y la conjetura de Koh*. Revista de la Facultad de Ciencias, Universidad Nacional de Colombia. Vol 3, No 2, Oct 1993.