# El problema de la existencia de retracciones en extensiones modulo finitas y la conjetura de Koh

por

Juan Felipe Pérez Vallejo

Trabajo presentado como requisito parcial
para optar al Título de

Magister en Matemáticas

Juan Diego Vélez

Universidad Nacional de Colombia
Sede Medellín

Facultad de Ciencias

Escuela de Matemáticas

Junio 2009

# Contenido

# Agradecimientos

Quisiera agradecer a a la Fundación Mazda para el Arte y la Ciencia por el apoyo económico que me brindó durante la Maestría, a la Universidad Nacional de Colombia Sede Medellín por todas las oportunidades que me ha dado. A mis profesores que durante todos estos años me han enseñado tanto, especialmente a Juan Diego Vélez, a quien le agradezco los consejos que me brindó en momentos indicados.

También quiero agradecer a mis padres, mi hermano, mis amigos y compañeros por su apoyo incondicional durante estos años y quiero agradecer especialmente a Diana, por todo.

# Introducción

Si $R \subset S$ es una extensión de anillos, una pregunta natural es cuándo existe una función $R$-lineal que envie el 1 en el 1; a ésto se le conoce como *retracción.* La pregunta acerca de retracciones en extensiones módulo finitas, es sin duda alguna una de las más importantes dentro del álgebra Commutativa, pues implica la solución de muchos otros problemas abiertos tales como la nueva conjetura de la intersección o la conjetura de la syzygia de Evans y Griffith. (ver [Ho83] y [EvG].)

En los dos casos que consideraremos en esta tesis nos preguntamos acerca de la existencia de retracciones cuando $R$ es un anillo regular, esta es la Conjetura del Sumando Directo, (C.S.D), o una hipótesis más débil, que $S$ tenga dimensión proyectiva finita sobre $R$, Conjetura de Koh. Veremos en el primer caso, que la respuesta a la pregunta de la existencia de retracciones es afirmativa cuando $R$ contiene un campo, utilizando la función traza si el campo tiene característica cero, o apoyándonos en el homomorfismo de Frobenius cuando la característica es prima. En el caso de la Conjetura de Koh veremos que el resultado es cierto siempre y cuando $R$ contenga un campo de característica cero. Para mostrarlo extenderemos la definición de polinomio característico a $R$-módulos proyectivos lo cual nos permite imitar la prueba de la C.S.D. en caracteríztica cero. Veremos luego que el resultado es falso si la característica del campo es prima. Para ello tendremos que utilizar la construcción de Yoneda para $Ext$, al igual que un computador para los cómputos necesarios.

Al lector interesado en abordar con mayor profundidad estos temas le recomiendo revisar [Ho83] allí encontrará una reducción de C.S.D. al caso en que $R$ es un anillo de series de potencias sobre un dominio de valuación discreta y, en el caso de la Conjetura de Koh, mirar [JD] donde encontrará una versión diferente del contraejemplo dado acá, al igual que otros contraejemplos, en particular un contraejemplo en característica mixta.

Para leer este trabajo se necesitan conocimientos en álgebra conmutativa, específicamente lo que se refiere a localizaciones, completaciones, módulos planos, etc. en álgebra Homológica todo aquello relacionado con las construcciones de funtores derivados y algunas de sus propiedades, y por último un conocimiento básico de la teoría de esquemas. Una buena referencia para esto es [DE] y [RH] de donde extraí la mayoría de los resultados.

Por último quiero hacer notar que este trabajo es parte de un seminario que se ha ido desarrollando desde el año pasado, 2008, dirigido por el profesor Juan Diego Vélez.

# Capítulo 1

# PRELIMINARES

En este capítulo daremos una serie de resultados necesarios para la comprensión de este trabajo. Algunos de ellos son bien conocidos y se encuentran en los textos básicos de álgebra conmutativa. Otros son un poco más elaborados y de más difícil acceso. Para estos daremos un tratamiento completo.

## 1.1 Extensiones enteras y módulo finitas

**Definición 1.1.1** *Una extensión de anillos $R \hookrightarrow S$ se dice* entera *si todo elemento de $S$ satisface un polinomio mónico en $R[x]$.*

**Definición 1.1.2** *Una extensión de anillos $R \hookrightarrow S$ se dice* módulo finita *si $S$ visto como $R-$módulo es finitamente generado.*

**Teorema 1.1.1** *Si $R$ es un anillo Noetheriano todo $R$-módulo $M$ finitamente generado es Noetheriano y por lo tanto admite una presentación finita.*

**Prueba.** [DE] Proposición 1.4, pág. 28. ■

**Teorema 1.1.2** *La extensión $R \hookrightarrow S$ es módulo finita sí, y sólo sí $S$ es una $R$ álgebra finitamente generada y entera sobre $R$.*

**Prueba.** [DE] Corolario 4.5, pág. 122. ■

**Lema 1.1.3** *Sea $R \hookrightarrow S$ una extensión entera de dominios, entonces $R$ es un campo sí, y sólo sí, $S$ lo es.*

**Prueba.** " $\Longrightarrow$ " Si $s \in S$ y $s \neq 0$, como $S$ es una extensión entera existe una relación

$$s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0,$$

con $a_i \in R$. Podemos suponer, sin pérdida de generalidad, que $n$ se escoge de manera minimal. De aquí se sigue que $a_0 \neq 0$, ya que de lo contrario podríamos cancelar $s$ y disminuir el grado de la ecuación. Ahora, como $R$ es un campo, y como

$$s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1) = -a_0$$

se sigue entonces que

$$s^{-1} = -a_0^{-1}(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1).$$

Por tanto $S$ también es un campo.

" $\Longleftarrow$ " Ahora, si $S$ es un campo y $r \in R$ es distinto de cero, tenemos que $r^{-1} \in S$. Luego se satisface una relación de la forma

$$(r^{-1})^n + a_{n-1}(r^{-1})^{n-1} + \cdots + a_0 = 0,$$

con $a_i \in R$. Si multiplicamos por $r^{n-1}$ obtenemos entonces que

$$r^{-1} = -(a_{n-1} + \cdots + a_0 r^{n-1}) \in R$$

y en consecuencia $R$ es un campo. ■

Una consecuencia inmediata de este lema es el hecho de que la contracción de un ideal maximal $p$ en $S$, $p^c = p \cap R$, es un ideal maximal de $R$. Para ver esto basta notar que $R/p^c \hookrightarrow S/p$ es una extensión entera de dominios y por consiguiente:

$$p \text{ es maximal} \Longleftrightarrow S/p \text{ es campo} \Longleftrightarrow R/p^c \text{ es campo} \Longleftrightarrow p^c \text{ es maximal.}$$

**Teorema 1.1.4** *(Lying Over y Going up) Supóngase que $R \subset S$ es una extensión entera de anillos. Dado un primo $p$ de $R$, existe un primo $q$ de $S$ tal que $s \cap q = p$. De hecho, $q$ se puede escoger de tal forma que contenga cualquier ideal $q_1$ que satisfaga la condición $R \cap q_1 \subset p$.*

**Prueba.** [DE] Proposición 4.15, pág. 129. ■

**Teorema 1.1.5** *(propiedad local global) Si $\gamma : M \to N$ es un morfismo de $R$-módulos entonces $\gamma$ es inyectivo (respectivamente, sobreyectivo, isomorfismo) si y sólo si para todo ideal maximal $m$ de $R$ el mapeo inducido*

$$\gamma_m : M_m \to N_m$$

*es inyectivo (respectivamente, sobreyectivo, isomorfismo).*

**Prueba.** [DE] Proposición 2.10, pág. 68. ■

**Teorema 1.1.6** *(Lema de Nakayama) Si $R$ es un anillo local con ideal maximal $m$, y $M$ es un $R$-módulo tal que $mM = M$, entonces $M = 0$.*

**Prueba.** [DE] Corolario 4.8, pág. 124. ■

**Teorema 1.1.7** *(Teorema chino del residuo) Sea $R$ un anillo y $q_1, \cdots, q_n$ ideales de $R$ tales que $q_i + q_j = R$, para todo $i \neq j$. Entonces existe un isomorfismo natural $R/(\cap_i q_i) \simeq \Pi_i(R/q_i)$.*

**Prueba.** [DE] Ejercicio 2.6, pág. 79. ■

**Teorema 1.1.8** *(De intersección de Krull) Sea $I$ un ideal en un anillo Noetheriano $R$. Si $M$ es un $R$-módulo finitamente generado, entonces existe un elemento $r \in I$ tal que $(1-r)(\overset{\infty}{\cap}_j I^j M) = 0$. De aquí que si $R$ es un dominio o un anillo local e $I$ es un ideal propio, entonces $\overset{\infty}{\cap}_j I^j = 0$.*

**Prueba.** [DE] Corolario 5.4, pág. 152. ■

## 1.2 Anillos completos y aplicaciones

Sea $R$ un anillo, $I \subset R$ un ideal y $M$ un $R$-módulo. Entonces la completación $I$-ádica de $M$ se denotará por $\widehat{M}^I$.

**Teorema 1.2.1** *Sea $\tau : R \to \widehat{R^I}$ el homomorfismo canónico de la completación. Entonces, vía $\tau$, el anillo $\widehat{R^I}$ es un $R$-módulo plano. Además, la completación $I$-ádica de $M$, $\widehat{M}^I$, puede obtenerse tensorizando con la completación $I$-ádica de $R$, es decir, $\widehat{M}^I = \widehat{R^I} \otimes_R M$.*

**Prueba.** [DE] Teorema 7.2, pág. 185. ■

**Lema 1.2.2** *(de Hensel) Sea $R$ un anillo local completo con ideal maximal $m$ y sea*

$$f(x) = x^d + r_1 x^{d-1} + \cdots + r_{d-1}x + r_d \in R[x]$$

*un polinomio mónico de grado $d$. Sea $\overline{f} = x^d + \overline{r_1}x^{d-1} + \cdots + \overline{r_{d-1}}x + \overline{r_d}$ en $(R/m)[x]$. Entonces, para cada factorización $\overline{f} = \overline{g}\overline{h}$ con grado de $\overline{g}$ igual a $a$ y grado de $\overline{h}$ igual a $b$ $(a+b = d)$ y tal que el M.C.D.$(\overline{g}, \overline{h}) = 1$, existen polinomios únicos $G$, $H \in R[x]$ de grados $a$ y $b$ respectivamente, tales que $\overline{G} = \overline{g}$, $\overline{H} = \overline{h}$ y $f = GH$.*

**Prueba.** [DE] Teorema 7.18, pág. 208. ■

**Proposición 1.2.3** *Sea $R$ un anillo y $S$ una $R$-algebra finitamente generada como $R$-módulo. Sí $I$ es un ideal de $R$ tal que $R$ es completo respecto a $I$, entonces $S$ es completo respecto a $IS$.*

**Prueba.** Esto es sigue del hecho de que $S \simeq R \otimes_R S \simeq \hat{R}^I \otimes_R S \simeq \hat{S}^{IS}$. ■

**Lema 1.2.4** *Sea $R \hookrightarrow S$ una extensión entera con $R$ un anillo local y $m$ su único ideal maximal. Entonces $S/mS$ es un anillo Artiniano.*

**Prueba.** Si $p$ es un ideal primo de $S$ que continene a $m$ entonces $p^c = m$. De 1.1.3 se sigue que $p$ es maximal. Luego, del teorema de correspondencia en $S/mS$ se sigue inmediatamente que en este anillo todos los primos son maximales. Es decir, $S/mS$ es un anillo Artiniano ( [DE],Teorema 2.14). ■

**Teorema 1.2.5** *(Teorema de estructura de Cohen, pág 191 [DE]). Sea $R$ un anillo local completo con ideal maximal $m$ y campo residual $K$. Si $R$ contiene un campo entonces*

$$R \simeq K[[x_1, \cdots, x_n]]/I$$

**Prueba.** [DE] Teorema 7.7, pág. 191. ■

### 1.2.1 Levantamiento de idempotentes

**Proposición 1.2.6** *Sea $S$ un anillo y $\{e_1, e_2, \cdots, e_n\}$ un conjunto completo de intempotentes ortogonales. Entonces si $S_i = Se_i$, existe un isomorfismo natural $S \simeq S_1 \times S_2 \times \cdots \times S_n$. (Notemos que cada $S_i$ tienen estructura natural de anillo conmutativo con unidad igual a $e_i$, ya que $e_i$ es idempotente).*

**Prueba.** Basta ver que como $S$-módulos los ideales $S_i$ son tales que $S = S_1 \oplus S_2 \oplus \cdots \oplus S_n$. La inclusión "$\supset$" es trivial. Para demostrar la otra inclusión, notemos que para cada $s \in S$

$$s = s \cdot 1 = s(e_1 + \cdots + e_n) = se_1 + \cdots + se_n \in S_1 \times S_2 \times \cdots \times S_n.$$

Luego $s \in S_1 + S_2 + \cdots + S_n$. Para ver que la suma es directa, notemos que si $s \in (S_1 + \cdots + S_{i-1} + S_{i+1} + \cdots + S_n) \cap S_i$ entonces

$$s = a_1e_1 + \cdots . + a_{i-1}e_{i-1} + a_{i+1}e_{i+1} + \cdots + a_ne_n = a_ie_i,$$

para ciertos $a_i \in S$. Multiplicando a ambos lados de la última igualdad por $e_j$ se obtiene que $a_j = 0$, para todo $j$, de donde se sigue que $s = 0$. Así, la suma es directa, de donde se sigue el resultado. ■

**Proposición 1.2.7** *Sean $(R, m)$ un anillo local completo y $S$ una $R-$álgebra finitamente generada como $R$-módulo. Si $\{\bar{f}_1, \cdots, \bar{f}_n\}$ es un conjunto de idempotentes ortogonales en $S/mS$, entonces existe un comjunto de idempotentes ortogonales en $S$, $\{e_1, \cdots, e_n\}$ tales que $\bar{e}_i = \bar{f}_i$.*

**Prueba.** Por una proposición anterior (la 1.2.3) sabemos que $S$ es completo respecto al ideal $mS$. Luego, si consideramos el polinomio $x^2 - x \in S[x]$ vemos que éste tiene, para cualquier $i$, a $\bar{f}_i$ por raíz en $S/mS$, ya que $x^2 - x = (x - \bar{f}_i)(x - (1 - \bar{f}_i))$. Luego, po el lema de Hensel (1.2.2) existen $e_i$ que pertenecen a $S$ tales que $e_i$ es raíz de $x^2 - x$ y $\bar{e}_i = \bar{f}_i$. Claramente los $e_i$ son idempotentes, así que lo único que falta por ver es que son ortogonales. Para ello notemos que $e_ie_j \in mS$ para todo $i \neq j$, y como $e_ie_j = (e_ie_j)^n \in m^nS$, para todo $n$, y como $S$ es un $R$-módulo finitamente generado, el teorema de intersección de Krull (1.1.8) nos dice que $e_ie_j \in \bigcap_{n=1}^{\infty} m^nS = (0)$, de donde se sigue el resultado. ■

## 1.3 Conexidad y Anillos Artinianos

**Definición 1.3.1** *Dado un anillo $R$, denotemos el espectro primo de $R$, $\{p \subset R : p$ un ideal primo$\}$, por $Spec(R)$. La topología de Zariski en $Spec(R)$, es aquella cuyos cerrados son de la forma $V(I) = \{p \in Spec(R) : p \supset I\}$, donde $I \subset R$ denota un ideal arbitrario.*

En [RH] se demuestra que en efecto ésta es una topología y se demuestran algunas de las propiedades más básicas.

**Definición 1.3.2** *Diremos que un anillo $R$ es conexo si $Spec(R)$ es conexo bajo la topología de Zariski.*

**Proposición 1.3.1** *$Spec(R)$ es la unión de dos cerrados no vacios y disjuntos $X_1$, $X_2$ (es decir $Spec(R)$ es disconexo) sí, y sólo sí, $R$ contiene elementos idempotentes no triviales.*

**Prueba.** Supongamos que $e$ es un elemento idempotente no trivial. Como

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e,$$

tenemos que $1 - e$ también es idempotente. Ahora, si $X_1 = V(e)$ y $X_2 = V(1-e)$, entonces:

$$V(e) \cup V(1-e) = V(e(1-e)) = V(e - e^2) = V(e - e) = V(0) = Spec(R)$$

y

$$V(e) \cap V(1-e) = V(e, 1-e) = V(1) = \phi$$

Luego $Spec(R)$ no es conexo.

Supongamos ahora que $Spec(R)$ es la unión de dos cerrados disjuntos $X_1 = V(I)$ y $X_2 = V(J)$. Como

$$V(e) \cup V(1-e) = V(IJ) = Spec(R)$$

y

$$V(e) \cap V(1-e) = V(I+J) = \phi$$

tenemos que $IJ \subset Rad(0)$ y que $I + J = R$, luego existen $a \in I$, $b \in J$ tales que $a + b = 1$ y un entero $n$ tal que $(ab)^n = 0$. Se sigue que

$$1 = (a+b)^{2n} = a^{2n} + \binom{2n}{1} a^{2n-1} b + \cdots + \binom{2n}{n} a^n b^n + \cdots + \binom{2n}{2n-1} a b^{2n-1} + b^{2n}.$$

Así que si hacemos

$$e_1 = a^{2n} + \binom{2n}{1} a^{2n-1} b + \cdots + \binom{2n}{n-1} a^{n+1} b^{n-1} = a^n k_1$$

y

$$e_2 = \binom{2n}{n+1} a^{n-1} b^{n+1} + \cdots + \binom{2n}{2n-1} a b^{2n-1} + b^{2n} = b^n k_2,$$

vemos que $e_1 + e_2 = 1$, y que $e_1 e_2 = 0$. Veamos finalmente que $e_1$ y $e_2$ son idempotentes. Esto se consigue fácilmente:

$$e_1 = e_1(e_1 + e_2) = e_1^2 + e_1 e_2 = e_1^2$$

y

$$e_2 = e_2(e_1 + e_2) = e_2^2 + e_1 e_2 = e_2^2$$

■

**Proposición 1.3.2** *$R$ es un producto directo de anillos $R_1 \times R_2$, si y sólo si existe $a \in R$ idempotente no trivial tal que $R_1 = Ra$. Más aún, $Ra = R[a^{-1}]$, donde $R[a^{-1}]$ denota la localización en el sistema multiplicativo de todas las potencias de $a$.*

**Prueba.** Si $R = R_1 \times R_2$ basta tomar $a = (1, 0)$. Recíprocamente, si $a \in R$ es idempotente no trivial, entonces $Ra$ es de forma natural un anillo con $a$ como unidad. Es más, como para cada $r \in R$, $r = ar + (1-a)r$, y esta escritura es única, ya que $a(1-a) = 0$, tenemos que $R = Ra \times R(1-a)$. Para demostrar la segunda afirmación, notemos que si $\phi : R \to Ra$ es tal que $\phi(r) = ar$, entonces todo elemento de $\{1, a, a^2, \cdots\} = \{1, a\}$, es enviado en un elemento invertible en $Ra$. Luego $\phi$ induce un homomorfismo de anillos $\Phi : R[a^{-1}] \to Ra$, tal que $\Phi(r/1) = ar$ y $\Phi(r/a) = ar$. Claramente $\Phi$ es sobre, y si $\Phi(r/s) = 0$, entonces $ar = 0$, lo cual implica $r/1 = 0$ en $R[a^{-1}]$. Así que $r/s = 0$, de donde se sigue que $\Phi$ también es inyectivo. ■

Un corolario inmediato es el siguiente.

**Corolario 1.3.3** *Si $R$ es un anillo tal que $Spec(R)$ tiene $n$ componentes conexas, entonces $R = R_1 \times \cdots \times R_n$ donde cada $R_i$ es un anillo con espectro conexo.*

**Prueba.** Se sigue de lo anterior y del hecho de que $Spec(R_1 \times R_2) \simeq Spec(R_1) \sqcup Spec(R_2)$. Para ver esto último notemos que

$$\begin{aligned}
Spec(R_1) \sqcup Spec(R_2) &\simeq Spec(R[(1,0)^{-1}]) \sqcup Spec(R[(0,1)^{-1}]) \\
&\simeq \{p \in Spec(R); (1,0) \notin p\} \sqcup \{p \in Spec(R); (0,1) \notin p\} \\
&\simeq V((1,0)) \sqcup V((0,1)) \\
&\simeq Spec(R_1 \times R_2)
\end{aligned}$$

■

**Teorema 1.3.4** *Supongamos que $R = R_1 \times \cdots \times R_k$, y sea $e_i$ el elemento cuya i-ésima componente es 1 y las demás son 0. Entonces todo R-módulo $M$ es expresable de forma única como $M = M_1 \oplus \cdots \oplus M_k$, donde cada $M_i$ es un $R_i$-módulo y la acción de $R$ sobre $M$ se define componente a componente. Más aún, $M_i = e_i M = M[e_i^{-1}]$ y cualquier homomorfismo de R-módulos $\gamma : M \to N$ es tal que $\gamma = \gamma_1 \oplus \cdots \oplus \gamma_k$, donde $\gamma_i : M_i \to N_i$, es el morfismo inducidos en las localizaciones.*

**Prueba.** Notemos que $\{e_i\}$ es un sistema ortonormal, y que dado $m \in M$,

$$m = (e_1 + \cdots + e_k)m = e_1 m + \cdots + e_k m.$$

Luego $M = M_1 + \cdots + M_k$, con $M_i = e_i M$. Ahora, si

$$e_1 m_1 + \cdots + e_k m_k = e_1 m_1' + \cdots + e_k m_k'$$

tenemos que al multiplicar por $e_i$ se obtiene $e_i m_i = e_i m_i'$, y por tanto la suma es directa. Ahora, como

$$M_i = e_i M = e_i R \otimes M = R[e_i^{-1}] \otimes M = M[e_i^{-1}],$$

para demostrar la unicidad basta ver que si

$$M_1 \oplus \cdots \oplus M_k = M_1' \oplus \cdots \oplus M_k'$$

donde $M_i$, $M_i'$ son $R_i$-módulos, entonces, como

$$R_i \otimes R_j = (e_i)(e_j R) = \begin{cases} o & \text{si } i \neq j \\ R_i & \text{si } i = j \end{cases}$$

tenemos que

$$\begin{aligned} R_i \otimes (M_1 \oplus \cdots \oplus M_k) &= R_i \otimes M_1 \oplus \cdots \oplus R_i \otimes M_k = (R_i \otimes R_1 \otimes M_1) \oplus \cdots \oplus (R_i \otimes R_k \otimes M_k) \\ &= R_i \otimes M_i = M_i \end{aligned}$$

y

$$\begin{aligned} R_i \otimes (M_1' \oplus \cdots \oplus M_k') &= R_i \otimes M_1' \oplus \cdots \oplus R_i \otimes M_k' = (R_i \otimes R_1 \otimes M_1') \oplus \cdots \oplus (R_i \otimes R_k \otimes M_k') \\ &= R_i \otimes M_i' = M_i'. \end{aligned}$$

Así que $M_i = M_i'$, lo cual completa la primera parte del teorema.

Supongamos ahora que $\gamma : M \to N$ es un $R$-homomorfismo. Sabemos que $\gamma$ induce homomorfismos $\gamma_i : M_i \to N_i$. Consideremos el diagrama

$$\begin{array}{ccc} M & \xrightarrow{\gamma} & N \\ \downarrow \phi & & \downarrow \phi' \\ M_1 \oplus \cdots \oplus M_k & \xrightarrow{\gamma_1 \oplus \cdots \oplus \gamma_k} & N_1 \oplus \cdots \oplus N_k \end{array}$$

donde $\phi$, $\phi'$, son los isomorfismos mostrados en la primera parte. Basta ver entonces que el diagrama anterior conmuta. Para ello sea $m \in M$; luego

$$\begin{aligned} \phi' \circ \gamma(m) &= e_1\gamma(m) + \cdots + e_k\gamma(m) \\ &= \gamma(e_1m) + \cdots + \gamma(e_km) \\ &= \gamma_1(e_1m) + \cdots + \gamma_k(e_km) \\ &= \gamma_1 \oplus \cdots \oplus \gamma_k(e_1m + \cdots + e_km) \\ &= (\gamma_1 \oplus \cdots \oplus \gamma_k) \circ \phi(m). \end{aligned}$$

■

En particular, los anillos Artinianos son anillos totalmente disconexos cuyos únicos ideales primos son los ideales maximales. Más aún, la siguiente proposición nos garantiza que este conjunto es finito.

**Proposición 1.3.5** *Sea $R$ un anillo. Entonces $R$ es Artiniano si y sólo si $R$ es Noetheriano y todos sus ideales primos son maximales. Más aún, en este caso $R$ sólo posee finitos ideales maximales.*

**Prueba.** [DE] Teorema 2.14, pág. 74. ■

De aquí se sigue el siguiente resultado:

**Teorema 1.3.6** *Si $R$ es un anillo Artiniano, entonces $R \simeq R_{m_1} \times \cdots \times R_{m_n}$ donde los $m_i$ son los ideales maximales de $R$.*

***Prueba.*** *[DE]Corolario 2.16, pág. 76.* ■

El objetivo ahora es probar el teorema siguiente:

**Teorema 1.3.7** *Sea $(R, m)$ un anillo local y completo. Si $S$ es una $R-$álgebra que es finitamente generada como $R$-módulo, entonces $S$ tiene finitos ideales maximales $m_i$. Es más, cada localización $S_{m_i}$ es un anillo local completo respecto a su ideal maximal, finitamente generado sobre $R$, y $S = \prod_i S_{m_i}$.*

**Prueba.** Probemos primero que $S$ tiene finitos ideales maximales y que además existe un conjunto completo de idempotentes ortogonales (tantos como ideales maximales) lo cual nos permite, por un teorema anterior, escribir a $S$ como un producto de anillos. Por 1.2.4 $S/mS$ es Artiniano, y por 1.3.5, este anillo tiene finitos ideales maximales. Del teorema de correspondencia se sigue que $S$ tiene finitos ideales maximales, digamos $m_1, \cdots, m_n$. Nuevamente, del hecho de que $S/mS$ es Artiniano, el teorema anterior implica que

$$S/mS \simeq \prod_i (S/mS)_{\overline{m_i}}.$$

Luego, si $\overline{f_1}, \cdots, \overline{f_n}$ son los elementos idempotentes ortogonales de $S/mS$ que realizan este producto, entonces existen elementos idempotentes ortogonales $\{e_1, \cdots, e_{n-1}\}$ en $S$ tales que $\overline{e_i} = \overline{f_i}$. Es más, si hacemos

$$e_n = 1 - \sum_{i=1}^{n-1} e_i,$$

entonces $\{e_1, \cdots, e_n\}$ es un conjunto completo de idempotentes ortogonales para $S$, y como $\overline{f_1}, \cdots, \overline{f_n}$ es un conjunto completo de idempotentes ortogonales, tenemos que

$$\overline{e_n} = 1 - \sum_{i=1}^{n-1} \overline{e_i} = 1 - \sum_{i=1}^{n-1} \overline{f_i} = \overline{f_n}.$$

Por tanto vemos que $S = Se_1 \times \cdots \times Se_n$. Hagamos $S_i = Se_i$; claramente cada $S_i$ un $R$-módulo finitamente generado, por ser sumandos directos de $S$. Ahora, si $n_i$ es un ideal maximal de $S_i$, tenemos que $n_i \cap e_i R = e_i m$, lo cual implica que todos los ideales maximales de $S_i$ contienen a $em_i$. Luego, como $S_i/mS_i$ es un anillo local, se sigue que $S_i$ también es local, y que $n_i$ es su único ideal maximal.

Ahora, si consideramos la proyección

$$S = Se_1 \times \cdots \times Se_n \to S_i$$

tenemos que la preimagen de $n_i$, llamémosla $m_i'$, debe ser un ideal maximal de $S$, y por consiguiente debe ser uno de los ideales del conjunto $\{m_j\}_{j=1,\cdots,n}$. Ahora, en la localización $A_{m_i'}$ el elemento $e_i$ se vuelve una unidad, y como $e_i e_j = 0$ para $i \neq j$, esto implica que $A_{m_i'} = (A_i)_{n_i} = A_i$, con lo cual se concluye el resultado. ■

## 1.4 La fórmula de Auslander-Buchsbaum, el criterio de Buchsbaum-Eisenbud y la construcción de Yoneda para $Ext^1$.

**Definición 1.4.1** *Sea $R$ un anillo, y $M$ un $R$-módulo. Una secuencia de elementos $x_1, \cdots, x_n \in R$ se llama* secuencia regular *en $M$ si se cumple que:*

*1) $(x_1, \ldots, x_n)M \neq M$*

*2) Para todo $i = 1, \cdots, n$ $x_i$ no es divisor de cero en $M/(x_1, \ldots, x_{i-1})M$*

Si $M = R$, a la secuancia $x_1, \ldots, x_n$ se le llama secuencia regular.

**Definición 1.4.2** *Sea $R$ un anillo Noetheriano, $I \subset R$ un ideal y $M$ un $R$-módulo arbitrario. Definimos la profundidad de $M$ en $I$, que denotaremos por $depth_I(M)$, como*

*1) $depth_I(M) = \infty$, si $IM = M$*

*2) $depth_I(M) = \sup\{r \geq 0 : x_1, \cdots, x_r \in I$ es regular en $M\}$, si $IM \neq M$.*

Un $R$-módulo $P$ se llama proyectivo si para cada función $R$-lineal $\phi : P \to M$ y para cada función $R$-lineal $\gamma : N \to M$ sobreyectiva, existe una función $R$-lineal $\widetilde{\phi} : P \to N$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd}
 & N \arrow[d, "\phi"] \\
P \arrow[ur, "\widetilde{\phi}"] \arrow[r, "\gamma"] & M \arrow[d] \\
 & 0
\end{tikzcd}$$

Más adelante veremos otras caracterizaciones de la noción de ser proyectivo y algunas de sus propiedades.

**Definición 1.4.3** *Sea $M$ un $R$-módulo. Una resolución proyectiva para $M$ es un complejo exacto*

$$\to P_n \xrightarrow{\phi_n} \cdots \to P_1 \xrightarrow{\phi_1} P_0$$

*de $R$-módulos proyectivos tal que $P_0/\operatorname{Im}(\phi_1) \simeq M$, como $R$-módulos. Diremos que la longitud de la resolución es igual a $n$ si $P_{n+1} = 0$ y $P_i \neq 0$, para $i \leq n$.*

**Definición 1.4.4** *Definimos la dimensión proyectiva de un módulo $M$, como $pd(M) =$ el mínimo de las longitudes de todas las resoluciones proyectivas para $M$. En el caso en que $M$ no tenga resoluciones proyectivas finitas se define $pd(M) = \infty$.*

**Teorema 1.4.1** *(Fórmula de Auslander-Buchsbaum) Sean $R$ un anillo local con ideal maximal $m$ y $M \neq 0$ un $R$-módulo finitamente generado de dimensión proyectiva finita. Entonces*

$$pd_R(M) = depth_m(R) - depth_m(M)$$

**Prueba.** [DE] Teorema 19.9, pág. 479. ■

Otra definición relevante para nuestro trabajo es la siguiente.

**Definición 1.4.5** *Sea $R$ un anillo y $\gamma : R^n \to R^m$ un $R$-homomorfismo. Definimos para cada entero $t \geq 0$ a $I_t(\gamma)$ como el ideal generado por todos los menores $t \times t$ de cualquier matriz que represente a $\gamma$, si $\min\{n, m\} > t > 0$, e $I_0(\gamma) = R$, e $I_t(\gamma) = (0)$, para todo $t > \min\{n, m\}$. Denotemos por $\Delta = I_t(\gamma)$, a aquel $I_t(\gamma)$ con $t$ igual al máximo valor posible tal que $I_t(\gamma) \neq 0$. Al entero $t$ lo llamaremos* el rango de $\gamma$ *y lo denotaremos por $rank(\gamma)$.*

La buena definición de $I_t(\gamma)$ al igual que la demostración del siguiente teorema se pueden encontrar en [DE] Teorema 20.9, pág. 500.

**Teorema 1.4.2** *(Criterio de Buchsbaum-Eisenbud) Sea $R$ un anillo. Un complejo*

$$0 \to F_n \overset{\gamma_n}{\to} F_{n-1} \to \cdots \to F_1 \to F_0$$

*de $R$-módulos libres es exacto sí, y sólo sí*

$$rank(F_k) = rank(\gamma_k) + rank(\gamma_{k+1})$$

*y*

$$depth_{I(\gamma_k)}(R) \geq k.$$

**Definición 1.4.6** *Un $R$-módulo $Q$ se dice que es inyectivo si, para cada $R$-homomorfismo inyectivo $\phi : N \to M$ y para cada $R$-homomorfismo $\gamma : N \to Q$, existe un $R$-homomorfismo $\widetilde{\gamma} : M \to Q$ tal que el siguiente diagrama conmuta*

$$\begin{array}{ccccc} 0 & \to & N & \overset{\phi}{\to} & M \\ & & \gamma \downarrow & \swarrow \widetilde{\gamma} & \\ & & Q & & \end{array}$$

En [DE] Corolario A.37, pág. 627, vemos que la categoría de $R$-módulos tiene suficientes inyectivos (este resultado es debido a Baer [1940]). Es decir, para cada módulo $M$ existe un módulo $Q$ inyectivo tal que $M$ se inyecta en $Q$. Esto nos permite construir resoluciones inyectivas para cualquier $M$.

**Definición 1.4.7** *Sea $M$ un $R$-módulo. Una* resolución inyectiva para $M$ *es un complejo exacto*

$$0 \to M \to Q_0 \to Q_1 \to Q_2 \to \cdots$$

*donde cada $Q_i$ es un módulo inyectivo.*

## 1.5 Los functores $Ext^i(M, N)$

El lector puede consultar en ([DE], Apéndice 3) una construcción detallada de los functores $Ext^i$ y la demostración de algunas de sus propiedades fundamentales. Recordemos que, en síntesis, si $A, B$ son dos $R$-módulos, $Ext^i(A, B)$ se puede definir de las siguientes dos maneras:

1. Se halla una resolución proyectiva para $A$, luego se "quita" $A$ y se aplica el funtor $Hom_R(-, B)$. La $i$-ésima homología del complejo que resulta es $Ext^i(A, B)$.

1. Se halla una resolución inyectiva para $B$; luego se "quita" $B$ y se aplica el funtor $Hom_R(A, -)$, y al complejo que resulta se le toma la homología $i$-ésima.

   Existe una construcción alternativa $Ext^i(A, B)$, conocida como construcción de Yoneda. Para nuestros propósitos será suficiente discutir el caso $i = 0, 1$. Comencemos con el siguiente lema general.

   **Lema 1.5.1** *(5-lema) Si el siguiente diagrama de grupos abelianos commuta*

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{a_1} & A_2 & \xrightarrow{a_2} & A_3 & \xrightarrow{a_3} & A_4 & \xrightarrow{a_4} & A_5 \\ \alpha_1 \downarrow & \#1 & \beta_1 \downarrow & \#2 & \gamma \downarrow & \#3 & \beta_2 \downarrow & \#4 & \alpha_2 \downarrow \\ B_1 & \xrightarrow{b_1} & B_2 & \xrightarrow{b_2} & B_3 & \xrightarrow{b_3} & B_4 & \xrightarrow{b_4} & B_5 \end{array}$$

   *y es tal que las filas son exactas, $\alpha_1$ es sobre, $\alpha_2$ es inyectivo y $\beta_1, \beta_2$ son isomorfismos, entonces $\gamma$ es un isomorfismo.*

   **Prueba.** Veamos primero que $\gamma$ es inyectivo. Sea $x \in A_3$ tal que $\gamma(x) = 0$. Por la conmutatividad del cuadrado #3 tenemos que $\beta_2 \circ a_3(x) = 0$; pero siendo $\beta_2$ un isomorfismo tenemos que $a_3(x) = 0$, así que $x \in \ker(a_3) = im(a_2)$. Por tanto existe $x'$ tal que $a_2(x') = x$, y por la conmutatividad de #2, $y' = \beta_1(x')$ es tal que $b_2(y') = 0$; y como $\ker(b_2) = im(b_1)$, existe $y''$ tal que $b_1(y'') = y'$. Además, como $\alpha_1$ es sobre, existe $x''$ tal que $\alpha_1(x'') = y''$. Luego, por la conmutatividad de #1 tenemos que $\beta_1 \circ a_1(x'') = \beta_1(x') = y'$. Pero como $\beta_1$ es isomorfismo se sigue que $a_1(x'') = x'$; luego $x = a_2(x') = a_2 \circ a_1(x'') = 0$, donde la última igualdad se sigue de la exactitud de la secuencia.

   Veamos ahora que $\gamma$ es sobreyectivo. Sea $y \in B_3$; por la exactitud de las filas tenemos que $y' = b_3(y)$ pertenece al $\ker(b_4)$, y si $x' = \beta_2^{-1}(y')$, la commutatividad de #4 implica que $\alpha_2 \circ a_4(x') = 0$. Por la inyectividad de $\alpha_2$ tenemos que $a_4(x') = 0$, así que $x' \in \ker(a_4) = im(a_3)$, y en consecuencia existe $x \in A_3$ tal que $a_3(x) = x'$. Luego

$$b_3(\gamma(x) - y) = b_3 \circ \gamma(x) - b_3(y) = \beta_2 \circ a_3(x) - y' = y' - y' = 0.$$

Por tanto $\gamma(x) - y \in \ker(b_3) = im(b_2)$ y así existe un elemento $y''$ en $B_2$ tal que $b_2(y'') = \gamma(x) - y$; ahora si $x'' = \beta_2^{-1}(y'')$, por la conmutatividad de #2, tenemos que $\gamma \circ a_2(x'') = \gamma(x) - y$. Pero esto es $\gamma(x - a_2(x'')) = y$, de donde se sigue el resultado. ■

**Definición 1.5.1** *Sea $R$ un anillo conmutativo, y $A$ y $C$ dos $R$-módulos.* Una extensión de $A$ por $C$ *es un secuencia exacta corta*

$$\alpha: \ 0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

Dos extensiones $\alpha$ y $\alpha'$ son equivalentes si existe un $R$-homomorfismo $f : B \to B'$ tal que el siguiente diagrama conmuta

$$\begin{array}{cccccccccc}
\alpha: & 0 & \to & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \to & 0 \\
 & & & \shortparallel & & \downarrow f & & \shortparallel & & \\
\alpha': & 0 & \to & A & \underset{i'}{\to} & B' & \underset{p'}{\to} & C & \to & 0
\end{array}$$

Esto fuerza, por el 5-lema, a que $f$ sea un isomorfismo y por tanto la relación es de equivalencia. Sea $E^1(C, A) = \{[\alpha] = \text{clase de equivalencia de la extención } A \text{ por } C\}$, entonces:

**a)** $E^1(C, A)$ es de forma natural un funtor contravariante de $C$.

Sea $v : C' \to C$ una función $R$-lineal y

$$[\alpha : 0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0] \in E^1(C, A),$$

Definamos $(p, -v) : B \oplus C' \to C$ tal que $(p, -v)(b, c) = p(b) - v(c)$ y $B' = \ker(p, -v)$. Construiremos funciones $R$-lineales $\phi : B' \to B$, $i' : A \to B$ y $p' : B' \to C'$ tales que el siguiente diagrama conmuta

$$\begin{array}{cccccccccc}
\alpha': & 0 & \to & A & \xrightarrow{i'} & B' & \xrightarrow{p'} & C' & \to & 0 \\
 & & & \shortparallel & & \downarrow \phi & & \downarrow v & & \\
\alpha: & 0 & \to & A & \underset{i}{\to} & B & \underset{p}{\to} & C & \to & 0
\end{array}$$

Si $i'(a) = (i(a), 0)$, tenemos que $i'$ queda bien definida, ya que $im(i) \times \{0\} = \ker p \times \{0\} \subset B'$. Y es claramente inyectiva. Como dado $c \in C'$ existe $b \in B'$ tal que $p(b) = v(c)$ (ya que $p$ es sobreyectiva) podemos definir $p'(b, c) = c$. Y es trivialmente sobreyectiva. Veamos que $\alpha'$ es exacta en $B'$. De las definiciones se sigue que $p' \circ i' = 0$; así, $im(i') \subset \ker\, p'$. Por otro lado, si $p'(b, c) = 0$, esto implica que $c = 0$, y como $p(b) = v(c) = 0$, tenemos que $b \in \ker p = im(i)$. Así vemos que existe $a \in A$ tal que $i(a) = b$. Pero esto claramente implica que $i'(a) = (i(a), 0) = (b, 0) = (b, c)$. Luego $im(i') \supset \ker\, p'$ y por tanto $\alpha'$ es exacta. Por último si definimos a $\phi(b,c) = b$ es inmediato que el diagrama conmuta. De esta forma definamos

$$E^1(v,A) : E^1(C,A) \to E^1(C',A)$$

que a la clase $[\alpha]$ la envía en la clase de $[\alpha']$.

Veamos que esta definición no depende de la clase escogida. Sea $\widetilde{\alpha} : 0 \to A \xrightarrow{\widetilde{i}} \widetilde{B} \xrightarrow{\widetilde{p}} C \to 0$ otro representante de la clase de $[a]$.Si $f$ es el isomorfismo que relaciona $\alpha$ y $\widetilde{\alpha}$, de la conmutatividad de

$$\begin{array}{ccccccccccc}
\alpha' : & 0 & \to & A & \xrightarrow{i'} & B' & \xrightarrow{p'} & C' & \to & 0 \\
& & & \parallel & & \downarrow \phi & & \downarrow v & & \\
\alpha : & 0 & \to & A & \xrightarrow[i]{} & B & \xrightarrow[p]{} & C & \to & 0 \\
& & & \parallel & & \downarrow f & & \parallel & & \\
\widetilde{\alpha} : & 0 & \to & A & \xrightarrow[\widetilde{i}]{} & \widetilde{B} & \xrightarrow[\widetilde{p}]{} & C & \to & 0
\end{array}$$

se sigue inmediatamente que $B'$ es isomorfo al kernel de $(\widetilde{p}, -v)$, de lo cual se sigue el resultado.

**b)** $E^1(C,A)$ es de forma natural un functor covariante de $A$

Sea $v : A \to A'$ una función $R$-lineal y $[\alpha : 0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0] \in E^1(C,A)$. Definamos $(v,-i) : A \to A' \oplus B$ tal que $(v,-i)(a) = (\ v(a), -i(a))$, y sea $B' = co\ker(v,-i)$. Igual que en el caso anterior, construiremos funciones $R$-lineales $\phi : B \to B'$, $i' : A' \to B'$ y $p' : B' \to C$ tales que el siguiente diagrama conmuta

$$\begin{array}{ccccccccccc}
\alpha' : & 0 & \to & A' & \xrightarrow{i'} & B' & \xrightarrow{p'} & C & \to & 0 \\
& & & \uparrow v & & \uparrow \phi & & \parallel & & \\
\alpha : & 0 & \to & A & \xrightarrow[i]{} & B & \xrightarrow[p]{} & C & \to & 0
\end{array}$$

Sean $i'(a) = \overline{(a,0)}$, $p'(\overline{(a,b)}) = p(b)$ y $\phi(b) = \overline{(0,b),\ \text{y}}$ veamos que $\alpha'$ es exacta. Para ello notemos que $i'(a') = 0$ implica que $(a',0) \in im(v,-i)$. De aquí se sigue que existe $a \in A$ tal que $v(a) = a', i(a) = 0$. Pero $i$ es inyectiva, luego $a = 0$, y por tanto $a' = v(a) = v(0) = 0$. Veamos que $p'$ esta bien definido. Si $\overline{(a,b)} = \overline{(c,d)}$ entonces $(a-c, b-d) \in im(v,-i)$. En particular existe $a \in A$ tal que $i(a) = b - d$. Como $\alpha$ es exacta tenemos que $p(b) = p(d)$, de donde se sigue la buena definición. Y como $p$ es sobre, también lo es $p'$. Nos queda por demostrar la exactitud en $B'$. Es claro de las definiciones que $im(i') \subset \ker p'$. Ahora, si $\overline{(a',b)} \in \ker p'$ tenemos que $p(b) = 0$, y por tanto existe $a \in A$ tal que $i(a) = b$. Luego, como $\overline{(v(a), -i(a))} = \overline{(v(a), -b))} = 0$, entonces

$$i'((a' + v(a), 0)) = \overline{(a' + v(a), 0)} = \overline{(a' - v(a) + v(a), b)} = \overline{(a', b)}$$

Así que $\alpha'$ es exacta. De las definiciones anteriores es inmediato que el diagrama conmuta y por consiguiente podemos definir $E^1(C,v) : E^1(C,A) \to E^1(C,A')$ que envíe a $[\alpha]$ en $[\alpha']$. Un razonamiento análogo al de la parte a) muestra que $E^1(C,v)$ está bien definida.

**c)** $E^1(C,A)$ tiene estructura natural de $R$-módulo.

Sabemos que si $r \in R$ existe una función $R$-lineal "multiplicación por $r$" que denotaremos por $r : A \to A$. Ahora, por la functorialidad de $A$, esta función induce otra función $E^1(C,r) = E^1(C,A) \to E^1(C,A)$, lo cual permite definir la acción de $r$ sobre $E^1(C,A)$. Usando la funtorialidad en $C$ obtenemos un resultado análogo. Consideremos el siguiente diagrama conmutativo

$$\begin{array}{ccccccccccc}
\alpha_1 : & 0 & \to & A & \overset{i_1}{\to} & B_1 & \overset{p_1}{\to} & C & \to & 0 \\
 & & & \shortparallel & & \downarrow \phi & & \downarrow r & & \\
\alpha : & 0 & \to & A & \underset{i}{\to} & B & \underset{p}{\to} & C & \to & 0 \\
 & & & \downarrow r & & \downarrow \gamma & & \shortparallel & & \\
\alpha_2 : & 0 & \to & A & \underset{i_2}{\to} & B_2 & \underset{p_2}{\to} & C & \to & 0
\end{array}$$

Por las construcciones hechas más arriba, si $\widetilde{\eta} : A \oplus B \to B \oplus C$ está definida como la función que toma el elemento $(a,b)$ y lo envía en $(rb + i(a), p(b))$, entonces $\eta$ es $R$-lineal. Más aún, como

$$(p,-r)((r \cdot b + i(a), p(b))) = r \cdot p(b) + p \circ i(a) - r \cdot p(b) = 0$$

tenemos que $im(\widetilde{\eta}) \subset B_1$. Por otro lado, como

$$\widetilde{\eta}(-ra, i(a)) = (p(i(a)), r \cdot i(a) - i(r \cdot a)) = (0,0)$$

vemos que $\widetilde{\eta}$ induce una función $R$-lineal $\eta$ en $co\ker(i,-r) = B_2$. Consideremos el siguiente diagrama:

$$\begin{array}{ccccccccccc}
\alpha_1 : & 0 & \to & A & \overset{i_1}{\to} & B_1 & \overset{p_1}{\to} & C & \to & 0 \\
 & & & \shortparallel & & \uparrow \eta & & \shortparallel & & \\
\alpha_2' : & 0 & \to & A & \underset{i_2}{\to} & B_2 & \underset{p_2}{\to} & C & \to & 0
\end{array}$$

Como $\eta(i_2(a)) = \eta(\overline{(a,0)}) = (i(a),0) = i_1(a)$ y

$$p_1(\eta\overline{(a,b)}) = p_1(rb + i(a), p(b)) = p(b) = p_2(\overline{(a,b)})$$

se sigue entonces que el diagrama conmuta y por tanto $[\alpha_1] = [\alpha_2]$. De esta manera queda definida la acción de $R$ sobre $E^1(C,A)$.

Definamos ahora la estructura de grupo abeliano. Dados $[\alpha : 0 \to A \to B_1 \to C \to 0]$ y

$$[\alpha' : 0 \to A \to B_2 \to C \to 0] \in E^1(C, A),$$

sea $\Delta : C \to C \oplus C$ el $R$-homomorfismo diagonal (esto es, $\Delta(c) = (c, c)$) y sea $\Sigma : A \oplus A \to A$ el homomorfismo suma (esto es, $\Sigma((a, a') = a + a')$. Sea

$$[\alpha] + [\alpha'] := E^1(\Delta, A) \circ E^1(C, \Sigma)(a \oplus \alpha') = E^1(C, \Sigma) \circ E^1(\Delta, A)(a \oplus \alpha').$$

Debemos ver que $E^1(\Delta, A) \circ E^1(C, \Sigma) = E^1(C, \Sigma) \circ E^1(\Delta, A)$. Para ello consideremos el siguiente diagrama

$$\begin{array}{ccccccccc}
 & 0 & \to & A & \underset{\tilde{\tilde{i}}}{\longrightarrow} & \tilde{\tilde{B}} & \underset{\tilde{\tilde{p}}}{\longrightarrow} & C & \to & 0 \\
 & & & \| & & \downarrow & & \downarrow \Delta & & \\
 & 0 & \to & A & \longrightarrow & \tilde{B} & \longrightarrow & C \oplus C & \to & 0 \\
 & & & \uparrow \Sigma & & \uparrow & & \| & & \\
\alpha \oplus \alpha' : & 0 & \to & A \oplus A & \underset{i_1 \oplus i_2}{\to} & B_1 \oplus B_2 & \underset{p_1 \oplus p_2}{\to} & C \oplus C & \to & 0 \\
 & & & \| & & \uparrow & & \uparrow \Delta & & \\
 & 0 & \to & A \oplus A & \longrightarrow & B' & \longrightarrow & C & \to & 0 \\
 & & & \downarrow \Sigma & & \downarrow & & \| & & \\
 & 0 & \to & A & \underset{i'}{\longrightarrow} & B'' & \underset{p''}{\longrightarrow} & C & \to & 0
\end{array}$$

Un cómputo algo laborioso y largo muestra que tanto $B''$ y $\tilde{\tilde{B}}$ son el mismo módulo (un cociente de un submódulo de $A \oplus A \oplus B_1 \oplus B_2 \oplus C$) y también que $i_1 = i_2$ y $p_1 = p_2$ (la idea para este cómputo es sencilla, basta recurrir a las definiciones dadas en a) y b)), de lo cual se sigue que existe una operación suma.

Ahora, si definimos $0 := [0 : 0 \xrightarrow{i_1} A \to A \oplus C \xrightarrow{p_1} C \to 0]$ entonces para cualquier

$$[\alpha : 0 \to A \xrightarrow{i_2} B \xrightarrow{p_2} C \to 0] \in E^1(C, A)$$

tenemos que $0 + [\alpha]$ está definida como la clase de la última fila del diagrama

$$
\begin{array}{ccccccccc}
0 \oplus \alpha : & 0 & \rightarrow & A \oplus A & \underset{i_1 \oplus i_2}{\rightarrow} & A \oplus C \oplus B & \underset{p_1 \oplus p_2}{\rightarrow} & C \oplus C & \rightarrow & 0 \\
& & & \shortparallel & & \uparrow & & \uparrow \Delta & & \\
& 0 & \rightarrow & A \oplus A & \underset{i'}{\longrightarrow} & B' & \underset{p'}{\longrightarrow} & C & \rightarrow & 0 \\
& & & \downarrow \Sigma & & \downarrow & & \shortparallel & & \\
& 0 & \rightarrow & A & \underset{\acute{i}}{\longrightarrow} & B'' & \underset{p''}{\longrightarrow} & C & \rightarrow & 0
\end{array}
$$

donde

$$
\begin{aligned}
B' &= \ker(p_1 \oplus p_2, -\Delta) = \{(a, c_1, b, c_2) \in A \oplus C \oplus B \oplus C : (p_1(a, c_1), p_2(b)) \\
&= (c_2, c_2)\} = \{(a, c, b, c) \in A \oplus C \oplus B \oplus C : p_2(b) = c\}.
\end{aligned}
$$

Ahora,

$$
\begin{aligned}
im(i_1, -\Sigma) &= \{(i'(a_1, a_2), -\Sigma(a_1, a_2)) \in A \oplus C \oplus B \oplus C \oplus A : a_1, a_2 \in A\} \\
&= \{(a_1, 0, i_2(a_2), 0, -(a_1 + a_2)) \in A \oplus C \oplus B \oplus C \oplus A : a_1, a_2 \in A\}
\end{aligned}
$$

Luego

$$
\begin{aligned}
B'' &= \frac{\{(a_1, c, b, c, a_2) \in A \oplus C \oplus B \oplus C \oplus A : p_2(b) = c\ \}}{\{(a_1, 0, i_2(a_2), 0, -(a_1 + a_2)) \in A \oplus C \oplus B \oplus C \oplus A : a_1, a_2 \in A\}} (*) \\
&\simeq \frac{\{(a_1, p_2(b), b, a_2) \in A \oplus C \oplus B \oplus A\}}{\{(a_1, 0, i_2(a_2), -(a_1 + a_2)) \in A \oplus C \oplus B \oplus A : a_1, a_2 \in A\}} \\
&\overset{*}{\simeq} B
\end{aligned}
$$

Para ver este último isomorfismo sean

$$M = \{(a_1, p_2(b), b, a_2) \in A \oplus C \oplus B \oplus A\}$$

$$N = \{(a_1, 0, i_2(a_2), -(a_1 + a_2)) \in A \oplus C \oplus B \oplus A : a_1, a_2 \in A\}$$

Si $\gamma : M \to B$ es la función que toma a $((a_1, p_2(b), b, a_2))$ y lo envía en $b + i_2(a_1 + a_2)$, entonces

$$\gamma(a_1, 0, i_2(a_2), -(a_1 + a_2)) = 0.$$

Luego $\gamma$ induce una función $\gamma' : M/N \to B$. Ahora, si $\gamma'(\overline{(a_1, p_2(b), b, a_2)}) = 0$, entonces $b + i_2(a_1 + a_2) = 0$, y como

$$0 = p(b + i_2(a_1 + a_2)) = p(b),$$

$b \in im(i_2)$ entonces $b = i_2(-(a_1 + a_2))$. Luego $(0,0,b,a_1+a_2) \in N$, y como $(a_1,0,0,-a_1) \in N$, entonces $(a_1, p_2(b), b, a_2) \in N$, de donde se sigue que $\gamma'$ es isomorfismo, ya que claramente $\gamma'$ es sobre. Notemos que $i''(a) = \overline{(0,0,0,0,a)}$ y que

$$p''(\overline{(a_1,c,b,c,a_2)}) = p'(a_1,c,b,c) = c.$$

Si $\phi : B'' \to B$ es el isomorfismo definido por $\phi\left(\overline{(a_1,c,b,c,a_2)}\right) = b + i_2(a_1+a_2)$, tenemos que el siguiente diagrama conmuta

$$\begin{array}{ccccccccccc}
\alpha: & 0 & \to & A & \underset{i_2}{\longrightarrow} & B & \underset{p_2}{\longrightarrow} & C & \to & 0 & \\
 & & & \| & & \uparrow \phi & & \| & & & , \\
 & 0 & \to & A & \underset{i''}{\longrightarrow} & B'' & \underset{p''}{\longrightarrow} & C & \to & 0 &
\end{array}$$

pues $\phi(i''(a)) = \phi(\overline{(0,0,0,0,a)}) = i_2(a)$ y

$$\begin{aligned}
p_2(\phi(\overline{(a_1,c,b,c,a_2)})) &= p_2(b + i_2(a_1+a_2)) \\
&= p_2(b) = c = p''(\overline{(a_1,c,b,c,a_2)}).
\end{aligned}$$

De (*), y de lo anterior, se sigue que $0 + [\alpha] = [\alpha]$.

**d)** Ahora, la suma así definida es trivialmente conmutativa, pues $\alpha \oplus \alpha' \simeq \alpha' \oplus \alpha$. El resto de propiedades que convierten a $E^1(C,A)$ en $R$-módulo se demuestran de forma similar a las anteriores.

Existe un isomorfismo entre $Ext^1(C,A)$ y $E^1(C,A)$.

**e)** Sea

$$0 \to A \xrightarrow{i} Q_0 \xrightarrow{\gamma_0} Q_1 \xrightarrow{\gamma_1} \cdots$$

una resolución inyectiva para $A$. $Ext^1(C,A)$ se define como la primera homología de la secuencia

$$0 \to Hom(C,Q_0) \xrightarrow{\gamma_0'} Hom(C,Q_1) \xrightarrow{\gamma_1'} \cdots$$

y como $Ext^1(C,A) = \frac{\ker(\gamma_1')}{im(\gamma_0')}$, y sabemos que todo elemento del $\ker(\gamma_0')$ es una función $R$-lineal $v : C \to Q_1$ tal que $\gamma_1 \circ v = 0$, para $v : C \to \ker \gamma_1$. Pero notemos que

$$\ker \gamma_1 = im(\gamma_0) = co\ker(i) = Q_0/A.$$

Así que $\ker(\gamma_0') = \hom(C, Q_0/A)$. Sea $\alpha$ la siguiente secuencia exacta:

$$\alpha : 0 \to A \to Q_0 \to Q_0/A \to 0,$$

y sea $[\varpi] \in E^1(C,A)$ tal que $\varpi = E^1(v,C)([\alpha])$. Es decir, la secuencia dada por la segunda fila del siguiente diagrama

$$\begin{array}{ccccccccc} \alpha: & 0 & \to & A & \underset{i}{\longrightarrow} & Q_0 & \underset{p}{\longrightarrow} & Q_0/A & \to & 0 \\ & & & \| & & \uparrow\eta & & \uparrow v & & \\ \varpi: & 0 & \to & A & \underset{i'}{\longrightarrow} & B & \underset{p'}{\longrightarrow} & C & \to & 0 \end{array},$$

donde $B = \ker(p,-v)$. Definamos $\varepsilon : \hom(C, Q_0/A) \to E^1(C,A)$ tal que $\varepsilon(v) = [\varpi]$, y veamos que esta función es sobreyectiva: sea

$$\varpi' : \quad 0 \to A \underset{i'}{\longrightarrow} B \underset{p'}{\longrightarrow} C \to 0$$

un representante de un elemento $[\varpi'] \in E^1(C,A)$. Ahora, como $i'$ es inyectiva y $i : A \to Q_0$, del hecho de que $Q_0$ sea inyectivo deducimos que existe una función $R$-lineal $\phi : B \to Q_0$ tal que $i = \phi \circ i'$. Esto implica que

$$\ker(p) = im(i) = im(\phi \circ i') = \phi(im(i')) = \phi(\ker(p')),$$

lo cual, a su vez, implica que $\phi$ induce una función $v : C \to Q_0/A$ dada por $v(c) = p \circ \phi(p'^{-1}(c))$. De esto se sigue inmediatamente que $\varepsilon(v) = [\varpi']$ (a pesar de que $B$ no es necesariamente el módulo por la parte a) se sigue de immediato que $[\varpi] = [\varpi']$).

Con métodos similares a los anteriores se puede ver que $\varepsilon$ es $R$-lineal. Ahora, si $\varepsilon(v) = 0$, entonces existe un $R$-homomorfismo $\sigma : C \to B$ tal que $\sigma \circ p' = Id_C$. Luego $\eta \circ \sigma : C \to Q_0$ es tal que

$$\gamma_0 \circ \eta \circ \sigma = p \circ \eta \circ \sigma = v$$

y por tanto $v \in im(\gamma_0')$. De aquí se sigue que $\varepsilon$ induce una función $R$-lineal

$$\widetilde{\varepsilon} : Ext^1(C,A) \to E^1(C,A),$$

y es inmediato que $\widetilde{\varepsilon}$ es inyectiva y por tanto que es un isomorfismo.

Dualmente, se puede mostrar que si

$$\to P_1 \to P_0 \to C \to 0$$

es una resolución proyectiva para $C$ entonces, si tomamos cualquier elemento de $Ext^1(C,A)$ que sea una clase de equivalencia de $v \in \hom(P_1, A), y$ tal que $v \circ \gamma_1 = 0$, esto es, tal que $\ker(v) \supset im(\gamma_1) = \ker(\gamma_0)$, entonces $v$ se puede representar como una función $R$-lineal

$v \in \hom(P_1/\ker(\gamma_0), A)$. Por tanto, si consideramos la secuencia exacta

$$0 \to P_1/\ker(\gamma_0) \to P_0 \to C \to 0$$

podemos definir $\varepsilon' : Ext^1(C, A) \to E^1(C, A)$, tal que $\varepsilon'(\overline{v}) = [\varpi]$, donde $\varpi$ está dado por el siguiente diagrama

$$\begin{array}{ccccccccccc}
\alpha: & 0 & \to & P_1/\ker(\gamma_0) & \underset{i}{\longrightarrow} & P_0 & \underset{p}{\longrightarrow} & C & \to & 0 \\
 & & & \downarrow v & & \downarrow \eta & & \parallel & & \\
\varpi: & 0 & \to & A & \underset{i'}{\longrightarrow} & B & \underset{p'}{\longrightarrow} & C & \to & 0
\end{array}$$

Finalmente, es fácil ver que $\varepsilon = \varepsilon'$.

# Capítulo 2

# El polinomio característico generalizado

En esta sección recordaremos algunos resultados básicos sobre el polinomio característico y la traza de un $R$-homomorfismo entre módulos libres y generalizaremos estos conceptos para $R$-homomorfismos entre $R$-módulos de dimensión proyectiva finita.

En el Álgebra Lineal la traza de una transformación lineal $\phi : V \to V$ entre espacios vectoriales de dimensión finita sobre un campo $K$, se define como la suma de las entradas de la diagonal de cualquier matriz que represente a dicha transformación. La buena definición de este concepto obviamente depende del hecho de que esta suma sea independiente de la base escogida. Para mostrar este hecho notemos primero lo siguiente:

**Proposición 2.0.2** *Sean A, y B dos matrices cuadradas. Entonces* $tr(AB) = tr(BA)$, *donde* $tr(\cdot)$ *denota la traza de la matriz correspondiente.*

**Prueba.** Si $A = (a_{ij})$ y $B = (b_{ij})$ entonces

$$tr(AB) = \sum_i (\sum_j a_{ij} b_{ji}) = \sum_j (\sum_i a_{ij} b_{ji}) = tr(BA).$$

■

Así, si la matriz $A$ representa a $\phi$ en la base $\beta$, $B$ representa a $\phi$ en la base $\beta'$, y si $C$ es la matriz de cambio de base de $\beta$ a $\beta'$, tenemos que

$$tr(A) = tr(C^{-1}BC) = tr(BC^{-1}C) = tr(B).$$

Luego la traza es una noción bien definida.

Por otro lado, si $K \subset E$ es una extensión finita de campos, entonces, dado $u \in E$, la multiplicación por $u$ define un morfismo $K$-lineal de $E$ en sí mismo. De aquí que podamos considerar a $tr_{E/K}(u)$ como la traza de la transformación lineal que acabamos de asociar a $u$. Algunas veces escribiremos $tr_{E/K}(u)$ como $tr(u)$, cuando el contexto sea claro. Los siguientes resultados se siguen fácilmente:

1. $tr : E \to K$ es $K$-lineal.

1. Si $\alpha \in K$ entonces $tr(\alpha) = n\alpha$, donde $n = [E : K]$.

1. Sean $K \subset E \subset F$ extensiones de campos. Entonces $tr_{F/K} = tr_{E/K} \circ tr_{F/E}$.

1. Si $E = K(u)$ y $f(x) = x^n + r_1 x^{n-1} + \cdots + r_n$ es el polinomio minimal para $u$, entonces $tr(u) = -r_1$. Como consecuencia de este resultado tenemos que si $K \subset K(u) = E \subset F$, entonces $tr(u) = -[F : E] \cdot r_1$.

**Prueba.** Las primeras dos afirmaciones se siguen de la definición de traza. Para demostrar la tercera notemos que fijadas bases $\beta = \{v_1, \ldots, v_n\}$ para $F$ como $K$-espacio vectorial, y $\beta' = \{w_1, \cdots, w_m\}$ para $F$ como $E$-espacio vectorial, el conjunto $\beta'' = \{v_1 w_1, \ldots, v_n w_m\}$ es una base para $F$ como $K$-espacio vectorial. Es más, se verifica fácilmente que dado $u \in F$, la matriz que representa al morfismo multiplicación por $u$ en la base $\beta''$ está dado por la matriz

$$\begin{pmatrix} [a_{11}]_{BB} & [a_{12}]_{BB} & \cdots & [a_{1m}]_{BB} \\ [a_{21}]_{BB} & [a_{22}]_{BB} & & [a_{2m}]_{BB} \\ \cdots & & \cdots & \cdots \\ [a_{m1}]_{BB} & [a_{m2}]_{BB} & \cdots & [a_{mm}]_{BB} \end{pmatrix},$$

donde $(a_{ij})$ es la matriz $m \times m$ que representa a multiplicación por $u$ en la base $\beta'$ y $[\cdot]$ representa multiplicación por $\cdot$ en la base $\beta$. Luego

$$tr_{F/K}(u) = \sum tr_{E/K}(a_{ii}) = tr_{E/K}(\sum a_{ii}) = tr_{E/K} \circ tr_{F/E}(u),$$

con lo cual queda demostrada la tercera afirmación. La última afirmación se ve fácilmente si tomamos por base para $K(u)$ a $\{1, u, u^2, \cdots, u^{n-1}\}$. En esta base una matriz para la multiplicación por $u$ está dada por

$$\begin{pmatrix} 0 & & \cdots & & -r_n \\ 1 & 0 & & & -r_{n-1} \\ & & \cdots & & \cdots \\ & & & 0 & -r_2 \\ & & \cdots & 1 & -r_1 \end{pmatrix}$$

luego es trivial que $tr(u) = -r_1$. La última parte de esta afirmación es una aplicación directa de la tercera. ■

Es fácil demostrar las propiedades básicas sobre polinomois característicos y la traza de funciones $R$-lineales entre módulos libres, ya que estos se comportan de manera muy similar a los espacios vectoriales. En [DE] Proposición 4.3, pág. 120 encontramos la demostración del siguiente resultado.

**Proposición 2.0.3** *Sea $f : F \to F$, un homomorfismo $R-$lineal, con $F$ un $R$-módulo libre de rango $n$. Definimos el polinomio característico de $f$ como $chr(f)(t) = \det(I_{n\times n}t - [f])$. Esta* *definición no depende de la base escogida, y además se cumple el teorema de Cayley-Hamilton, esto es,* $chr(f)(f) = 0$.

Nuestro objetivo en esta sección es extender esta noción a $R$-módulos de dimensión proyectiva finita, y ver cómo, con ayuda del polinomio característico, podemos construir funciones como la traza. Para ello necesitaremos los resultados que aparecen a continuación.

**Proposición 2.0.4** *Sea $R$ un anillo local. Si $M$ es un $R$-módulo proyectivo finitamente generado, entonces $M$ es libre.*

**Prueba.** Como $R$ es local y $M$ es finitamente generado, si $mM = M$, el lema de Nakayama implica que $M = 0$, que es libre. Supongamos entonces que $mM \neq M$. El módulo $M/mM$ es un $(R/m)$-espacio vectorial; escojamos $\overline{v_1}, \ldots, \overline{v_n}$ una base para este espacio. Se sigue que $mM + \langle v_1, \cdots, v_n \rangle = M$. Nuevamente, el lema de Nakayama nos dice que $\langle v_1, \cdots, v_n \rangle = M$. Ahora consideremos la siguiente secuencia exacta

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

donde $K$ es el kernel del homomorfismo $\rho : R^n \to M$ que envía a $(r_1, \cdots, r_n)$ en $r_1 v_1 + \cdots r_n v_n$. Como $M$ es proyectivo y $\rho$ es sobreyectiva, existe $\widetilde{\rho} : M \to R^n$ tal que $\rho \circ \widetilde{\rho} = Id$. De aquí se sigue que $R^n \simeq M \oplus K$. Además, si $r_1 v_1 + \cdots r_n v_n = 0$, entonces, pasando a $M/mM$ vemos que todos los $r_i \in m$. En particular tenemos que $K \subset mM \oplus mK$. Pero como $K \cap mM \subset K \cap M = \emptyset$ tenemos que $K \subset mK$. Luego como $K$ es un $R$-módulo finitamente generado, nuevamente, por Nakayama, se sigue que $K = 0$, con lo que se concluye el resultado. ■

Las siguientes son caracterizaciones de la noción de proyectivo.

**Proposición 2.0.5** *Las siguientes proposiciones son equivalentes:*

**a)** Un $R$-módulo $P$ es proyectivo.

**b)** Para cualquier epimorfismo de módulos $\alpha : M \to N$, el mapeo inducido $Hom_R(P, M) \to Hom_R(P, N)$ es sobreyectivo.

**c)** Para algún epimorfismo de módulos $\alpha : F \to P$, con $F$ un $R$-módulo libre, el mapeo inducido $Hom_R(P, F) \to Hom_R(P, P)$ es sobreyectivo.

**d)** $P$ es un sumando directo de un $R$-módulo libre.

**Prueba.** $a \iff b$ : $b$ es una reformulación de la definición.
$b \Rightarrow c$ : obvio

$c \Rightarrow d$ : Cualquier homomorfismo $\gamma \in Hom(P, F)$ en la preimagen de la función identidad $Id \in Hom_R(P, P)$, cumple que $Id = \alpha \circ \gamma$. Luego $\gamma$ es inyectivo y por tanto $P$ es un sumando directo de $F$.

$d \Rightarrow b$ : Sea $\alpha : M \to N$ un epimorfismo de módulos, y sea $F$ un $R$-módulo libre tal que $P$ es sumando directo de $F$, digamos, $F = P \oplus Q$. Luego, como $F$ es libre, es fácil ver que el homomorfismo inducido

$$\phi : Hom_R(F, M) \to Hom_R(F, N)$$

es sobreyectivo. Sean

$$\begin{aligned} \phi_1 &: Hom_R(P, M) \to Hom_R(P, N) \\ \phi_2 &: Hom_R(Q, M) \to Hom_R(Q, N) \end{aligned}$$

los homomorfismos inducidos. Como

$$\begin{aligned} Hom_R(F, M) &= Hom_R(P, M) \oplus Hom_R(Q, M) \\ Hom_R(F, M) &= Hom_R(P, N) \oplus Hom_R(Q, N) \end{aligned}$$

y $\phi = \phi_1 \oplus \phi_2$, tenemos que $\phi_1$ es sobreyectivo, de lo cual se sigue el resultado. ■

**Corolario 2.0.6** *Sea $R$ un anillo y $M$ un $R$-módulo. Entonces para todo primo $p \in Spec(R)$ el $R_p$-módulo $M_p$ es proyectivo (y por 2.0.4, es libre) sí, y sólo sí, $M$ es proyectivo.*

**Prueba.** Por la propoción anterior basta ver que $Hom_R(M, F) \to Hom_R(M, M)$ es sobreyectivo. Pero por la propiedad local global esto es cierto, si y sólo si $Hom_R(M, F)_p \to Hom_R(M, M)_p$ es sobreyectivo, para todo primo $p \in Spec(R)$. O equivalentemente, $Hom_{R_p}(M_p, F_p) \to Hom_{Rp}(M_p, M_p)$ es sobreyectiva, para todo primo $p \in Spec(R)$. Nuevamente, por la proposición anterior, esto es cierto si y sólo si para todo primo $p \in Spec(R)$ el $R_p$-módulo $M_p$ es proyectivo. ■

**Lema 2.0.7** *Sea $X = Spec(R)$, con $R$ un anillo con espectro conexo. Dados $q$, $q' \in X$ existen primos $q_0 = q$, $q_1, \cdots, q_n = q'$, $p_0, p_1, \cdots, p_{n-1}$ tales que $p_i \subset q_i$ y $p_i \subset q'_{i+1}$.*

**Prueba.** Sea $U_p = \{p' \in X :$ existen primos $q_0 = p, q_1, \cdots, q_n = p', p_0, p_1, \cdots, p_n$ tales que $p_i \subset q_i, p_i \subset q'_{i+1}\}$. Veamos que $U_p$ es un cerrado. Esto es cierto porque $U_p = \cup V(p')$, donde la unión se realiza sobre todos los primos minimales que pertenecen a $U_p$. Como sólo hay finitos primos minimales, esta unión debe ser finita. Ahora, es claro que si $p \in U_q$ entonces $U_p = U_q$. De aquí que $U_q = U_{q'}$, o $U_q \cap U_{q'} = \emptyset$. Pero este último caso no es posible pues $X$ es conexo. De aquí se sigue el resultado. ■

La siguiente proposición nos permitirá definir el rango de un $R$-módulo sobre un anillo conexo.

**Proposición 2.0.8** *Sea $R$ un anillo Noetheriano de espectro conexo, $M$ un $R$-módulo finitamente generado y proyectivo. Sea $X = Spec(R)$. Entonces la función $Rango(M_p)$ es constante en $X$ (nótese que la función rango queda bien definida pues $M_p$ es proyectivo como $R_p$-módulo, y por la proposición anterior es libre).*

**Prueba.** Sean $q$, $q' \in R$ y $q_0 = q$, $q_1$, $\cdots$, $q_n = q'$ , $p_0$, $p_1$, $\cdots$, $p_n$ como en el lema anterior. Si el rango de $M_q$ es $n$ tenemos que

$$M_{p_0} = (M_{q_0})_{p_0} = (R^n_{q_0})_{p_0} = R^n_{p_0}.$$

Usando este mismo argumento se muestra que

$$Rango(M_{p_i}) = Rango(M_{q_i}) = Rango(M_{q_{i+1}}),$$

de lo cual se sigue inmediatamente el resultado. ■

**Proposición 2.0.9** *Sea $R$ un anillo conexo y $U \subset R$ el conjunto de elementos en $R$ que no son divisores de 0. Entonces, si $M$ es un $R-$módulo de dimensión proyectiva finita tenemos que $U^{-1}M$ es un $U^{-1}R$-módulo proyectivo de rango constante. Esto es, el rango de $(U^{-1}M)_q$ es el mismo para todo primo $q \in spec(U^{-1}R)$.*

**Prueba.** Por la proposición 2.0.6 sólo debemos ver que para todo primo $q \in Spec(U^{-1}R)$, $(U^{-1}M)_q$ es libre. Equivalentemente, basta ver que para todo primo $q \in Ass(R)$, $M_q$ es libre. Pero esto se sigue de la fórmula de Auslander Buchsbaum, ya que $depth_{qR_q}(R_q) = 0$ (pues $qR_q$ sólo contiene divisores de cero para todo $q \in Ass(R)$). Tenemos que

$$pd(M_q) = depth_{qR_q}(R_q) - depth_{qR_q}(M_q) = 0$$

de lo cual se sigue que $U^{-1}M$ es localmente proyectivo y por ende localmente libre.

Demostremos ahora que el rango es constante. Para ello procedamos por inducción sobre la dimensión proyectiva de $M$.

Si $pd(M) = 0$, entonces $M$ es proyectivo y el resultado se sigue a partir de una proposición anterior. Supongamos entonces que el resultado es cierto para todo $R$-módulo con dimensión proyectiva menor que $d$.

Sea $0 \to M_1 \to P \to M \to 0$ una secuencia exacta con $P$ proyectivo y $dp(M_1) < d$ (tal secuencia se puede construir, tomando una resolución proyectiva para $M$, $dp(M) > 0$, y cortándola en el primer módulo de szygia). Localizando en $U$ se obtiene la siguiente secuencia exacta:

$$0 \to U^{-1}M_1 \to U^{-1}P \to U^{-1}M \to 0,$$

y por la primera parte, cada módulo es proyectivo. Luego

$$U^{-1}P = U^{-1}M_1 \oplus U^{-1}M,$$

y al localizar en cualquier primo $q \in U^{-1}R$, tenemos que

$$(U^{-1}P)_q = (U^{-1}M_1)q \oplus (U^{-1}M)_q$$

es la suma directa de dos módulos libres. De aquí

$$rango((U^{-1}M)_q) = rango((U^{-1}P)_q) - rango((U^{-1}M_1)_q).$$

Pero el término de la derecha es constante por la proposición anterior, y de la hipótesis inductiva se sigue el resultado. ■

**Proposición 2.0.10** *Sea $R$ un anillo con finitos ideales maximales $\{m_1, \cdots, m_k\}$. Si $M$ es $R$-proyectivo, finitamente generado y de rango constante, entonces $M$ es libre.*

**Prueba.** Sea $J = m_1 \cap \cdots \cap m_k$. Por el teorema chino del residuo tenemos que

$$R/J \simeq R/m_1 \times \cdots \times R/m_k.$$

Se sigue de 2.0.5 que existe un módulo $N$ tal que $M \oplus N \simeq R^s$. Tensorizando con $R/J$ se sigue que $M/JM \oplus N/JN \simeq (R/J)^s$. Nuevamente, de la proposición 2.0.5 se sigue que $M/JM$ es $(R/J)$-proyectivo. Ahora si $J \subset q$, un ideal primo de $R$, del hecho de que $M/JM$ sea proyectivo, y por 2.0.4 tenemos que

$$(M/JM)_q \simeq M \otimes R_q \otimes R/J \simeq R/J \otimes M_q \simeq R/J \otimes R^n \simeq (R/J)^n,$$

con $n = rango(M)$. Luego, por el teorema 1.3.4, todo módulo sobre $R/m_1 \times \cdots \times R/m_k$ tiene la forma $F_1 \times \cdots \times F_t$. Más aún, cada $F_i$ es de la forma $(M/JM)_{\overline{m_i}}$ para cierto $m_i$. Luego cada $F_i$ tiene rango $n$ sobre $R/m_i$. Así que

$$M/JM = (R/m_1)^n \times \cdots \times (R/m_k)^n = (R/m_1 \times \cdots \times R/m_k)^n = (R/J)^n.$$

Sea ahora $\phi : (R/J)^n \to M/JM$ un isomorfismo, y consideremos el siguiente diagrama:

$$\begin{array}{ccccc} & & & & M \\ & & & & \downarrow \pi \\ R^n & \xrightarrow{\pi} & (R/J)^n & \xrightarrow{\phi} & M/JM \\ & & & & \downarrow \\ & & & & 0 \end{array}$$

Sea $\widetilde{\phi} : R^n \to M$ un levantamiento para $\phi \circ \pi : R^n \to M/JM$ y $C = M/im(\widetilde{\phi})$. La secuencia

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

es exacta, y al tensorizar con $R/J$, obtenemos

$$(R/J)^n \xrightarrow{\phi} M/JM \to C/JC \to 0.$$

Como $\phi$ es un isomorfismo tenemos que $C = JC$, y como $J \subset \cap m_i$, se sigue que $C_m \subset JC_m$, para todo ideal maximal $m$ de $R$. Luego por el Lema de Nakayama 1.1.6, y por la propiedad local global 1.1.5 vemos que $C = 0$, y por tanto $\widetilde{\phi}$ es sobreyectiva. Ahora, si consideramos la secuencia exacta

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

con $K = \ker(\widetilde{\phi})$, y tensorizamos nuevamente con $R/J$, obtenemos la secuencia exacta

$$Tor^1(R/JR, M) \to K/JK \to (R/J)^n \xrightarrow{\phi} M/JM \to 0.$$

Y como $Tor^1(R/JR, M) = 0$, ya que $M$ es proyectivo, tenemos que

$$0 \to K/JK \to (R/J)^n \xrightarrow{\phi} M/JM \to 0$$

es exacta. Nuevamente, como $\phi$ es isomorfismo vemos que $K = JK$, y por un argumento análogo al anterior, tenemos que $K = 0$. Luego $\widetilde{\phi}$ es un isomorfismo, de lo cual se sigue el resultado. ■

**Corolario 2.0.11** *Sea $R$ un anillo conexo y $M$ un $R$-módulo finitamente generado de dimensión proyectiva finita. Entonces $U^{-1}M$ es libre.*

**Prueba.** Se sigue de la proposición anterior y del hecho de que $U^{-1}R$ tiene espectro finito. ■

**Definición 2.0.2** *Sea $R$ un anillo Noetheriano de espectro conexo y $M$ un $R-$módulo finita-*

*mente generado de dimensión proyectiva finita. Sea $U \subset R$ el conjunto de elementos que no son divisores de cero. Diremos que un polinomio característico $f_h(t)$ de un $R-$homomorfismo $h : M \to M$, es un polinomio que satisface:*

1. *$f_h(t)$ es un polinomio monico de grado igual al rango de $U^{-1}M$.*

2. *Si $U^{-1}f_h(t)$ denota el poliinomio que se obtiene al localizar los coeficientes de $f_h(t)$ entonces $U^{-1}f_h(t) = chr(U^{-1}h)$, es decir, el polinomio característico asociado al $U^{-1}R$-homomorfismo lineal inducido por $h$ entre los $U^{-1}R$-módulos libres $U^{-1}M$.*

Notemos que el corolario anterior nos garantiza la buena definición de la condición (*****).

A continuación demostraremos la existencia y la unicidad de dicho polinomio.

**Teorema 2.0.12** *(Unicidad) Si $f_h(t)$ existe, es único.*

**Prueba.** Sean $f_h(t)$, $f_h^*(t)$ dos polinomios mónicos para $h$. Entonces los coeficientes $c_k/1$ y $c_k^*/1$ en $U^{-1}R$ son iguales y por tanto existe $s \in U$ tal que $s(c_k - c_k^*) = 0$ en $R$. Pero como en $U$ no hay divisores de cero se tiene que $c_k = c_k^*$. ■

**Teorema 2.0.13** *(Existencia) Bajo las condiciones de la definición anterior el polinomio $f_h(t)$ existe.*

**Prueba.** Procederemos por inducción sobre $pd(M) < \infty$.

Si $pd(M) = 0$, entonces $M$ es proyectivo de rango constante $n$. Para cada $p \in Spec(R)$ sea $char(h_p)(t)$ el polinomio característico de $h_p : M_p \to M_p$

$$char(h_p)(t) = t^n + v_{p,1}t^{n-1} + \cdots + v_{p,n} \qquad \text{con } v_{p,j} \in R_p.$$

Definamos la función

$$\phi_k : X = Spec(R) \to \bigsqcup_{p \in X} R_p$$

como $\phi_k(p) = v_{p,k}$. Veamos que $\phi_k$ es regular en $X$: como $M_p$ es libre tomemos elementos $\{u_1, \cdots, u_n\}$ en $M$ tales que $\{u_1/1, \cdots, u_n/1\}$ es base para $M_p$, y sea $W = < u_1, \ldots, u_n >$. Consideremos las siguientes secuencias exactas:

$$1) \ \ 0 \to W \to M \xrightarrow{\pi} M/W \to 0$$

$$2) \qquad\qquad R^m \xrightarrow{[\phi]} R^n \to W \to 0$$

donde $[\phi]_{n\times m}$ es una matriz con entradas en $R$. Localizando en $p$ a cada una de las secuencias obtenemos que $(M/W)_p = 0$ y $[\phi]_p = 0$. Luego existen $s_1$, $s_2$ en $R - p$ tales que $s_1(M/W) = 0$

y $s_2[\phi] = 0$. Sea $s = s_1 s_2$; localizando en $s$ tenemos que $M_s \simeq W_s$ es $R_s$-libre. Sea $D(s) = \{p \in Spec(R) : s \notin p\}$. Como $M_s$ es $R_s$-libre, sea $\frac{a_k}{s^{r_k}}$ el coeficiente $k$-ésimo de $char(h_s)(t)$. Ahora, para todo $p \in D(s)$ la imagen de $\frac{a_k}{s^{r_k}}$ en $R_p$ es precisamente $v_{p,k}$, lo que demuestra que $\phi_k$ es regular.

Como $O_{Spec(R)}(Spec(R)) \simeq R$, existe $r_k \in R$ tal que $\phi_k(p) = r_k/1$, para todo $p \in Spec(R)$. Sea

$$L(t) = t^n + r_1 t^{n-1} + \cdots + r_n.$$

De la construcción anterior se sigue que $L_p(t) = char(h_p)(t)$, para todo $p \in Spec(R)$. Si $G(t) = char(U^{-1}h)(t)$ es el polinomio característico para $U^{-1}h : U^{-1}M \to U^{-1}M$, entonces, para todo primo $q^e = qU^{-1}R$ en $U^{-1}R$ se tiene que $G_{q^e}(t) = G_q(t)$. Pero como también ocurre que

$$G_q(t) = L_q(t) = (U^{-1}L_h(t))_{q^e}$$

se sigue entonces que $G_{q^e}(t) = (U^{-1}L_h(t))_{q^e}$, para todos los primos del anilllo $U^{-1}R$. Esto implica que $G(t) = U^{-1}L_h(t)$ y por consiguiente $G(t)$ es el polinomio característico para $h : M \to M$.

Sea $M$ un módulo de dimensión proyectiva finita, y supongamos ahora que el polinomio característico existe para todo $R$-módulo de dimensión proyectiva menor que $pd(M)$. Consideremos una secuencia exacta

$$0 \to M_1 \to F \to M \to 0$$

donde $M_1$ denota un primer módulo de szysigia, y $F$ es proyectivo con $pd(M_1) < pd(M)$. Como $F$ es proyectivo existe un diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \to & M_1 & \to & F & \to & M & \to & 0 \\ & & \downarrow g & & \downarrow f & & \downarrow h & & \\ 0 & \to & M_1 & \to & F & \to & M & \to & 0 \end{array}$$

Localizando en $U$ obtenemos

$$\begin{array}{ccccccccc} 0 & \to & U^{-1}M_1 & \to & U^{-1}F & \to & U^{-1}M & \to & 0 \\ & & \downarrow U^{-1}g & & \downarrow U^{-1}f & & \downarrow U^{-1}h & & \\ 0 & \to & U^{-1}M_1 & \to & U^{-1}F & \to & U^{-1}M & \to & 0 \end{array}$$

una secuencia de módulos libres. Tomando bases adecuadas vemos que

$$[U^{-1}f] = \begin{bmatrix} U^{-1}g & 0 \\ 0 & U^{-1}h \end{bmatrix}$$

Luego $chr(U^{-1}f) = chr(U^{-1}g)chr(U^{-1}h)$. Por la hipótesis inductiva existen $P_1(t)$, $P_2(t) \in R[t]$, polinomios característicos de $f : F \to F$ y $g : M_1 \to M_1$, es decir $U^{-1}P_1 = chr(U^{-1}f)$ y $U^{-1}P_2 = chr(U^{-1}g)$. Por el algoritmo de la división, en $R[t]$, existe un único par de polinomios mónicos, $A$ y $B$, tales que $P_1 = P_2A + B$. Al localizar en $U$ se obtiene

$$(U^{-1}P_1) = (U^{-1}P_2)(U^{-1}A) + (U^{-1}B).$$

Pero como

$$chr(U^{-1}f) = chr(U^{-1}g)chr(U^{-1}h) + 0$$

vemos que $U^{-1}B = 0$. Luego $B = 0$ y $U^{-1}A = chr(U^{-1}h)$. Esto implica que $A(t) \in R[t]$ es el polinomio característico de $h : M \to M$. ■

**Definición 2.0.3** *Un $R$-módulo se llama libre de torsión si $\forall m \neq 0$ en $M$, $u \cdot m \neq 0$, para todo $u \in U$.*

El polinomio característico general así construido cumple Caley-Hamilton, siempre y cuando, el módulo sea libre de torsión.

**Proposición 2.0.14** *Sea $R$ un anillo con espectro conexo y $M$ un $R$-módulo libre de torsión y de dimensión proyectiva finita. Entonces $f_h(h) = 0$.*

**Prueba.** Sea $f_h(t) = t^n + c_1t^{n-1} + \cdots + c_n$ el polinomio característico asociado a $h : M \to M$. Como $U^{-1}M$ es libre se cumple Caley-Hamilton para $(U^{-1}f_h)(t)$; esto es

$$(U^{-1}h)^n(m/1) + (c_1/1)(U^{-1}h)^{n-1}(m/1) + \cdots + (c_n/1)(m/1) = 0, \text{ para todo } m/1 \in U^{-1}M.$$

Luego existe $u \in U$ tal que

$$u \cdot (h^n(m) + c_1h^{n-1}(m) + \cdots + c_nm) = 0.$$

Pero como $M$ es libre de torsión tenemos que

$$h^n(m) + c_1h^{n-1}(m) + \cdots + c_nm = 0, \; \forall m \in M$$

de donde se sigue que $f_h(h) = 0$. ■

**Proposición 2.0.15** *Sea $R$ un anillo conexo y $R \subset S$ una extensión módulo finita. Si $s \in S$, denotemos por $s$ el $R$-homomorfismo "multiplicación por $s$". Si $pd(S) < \infty$, existe un $R$-homomorfismo $Tr : S \subset Hom_R(S,S) \to R$ tal que $Tr(1) = -n$, con $n = rango(U^{-1}S)$ y $Tr(s) =$ el coeficiente de $t^{n-1}$ del polinomio característico del homomorfismo $s$.*

**Prueba.** Sean $s$, $s' \in S$ y $r \in R$, sean

$$\begin{aligned} f_s(t) &= t^n + c_1 t^{n-1} + \cdots + c_n \\ f_{s'}(t) &= t^n + c'_1 t^{n-1} + \cdots + c'_n \\ f_{rs+s'}(t) &= t^n + d_1 t^{n-1} + \cdots + d_n \end{aligned}$$

los polinomios característicos de $s$, $s'$ y $rs + s'$, respectivamente. Como $U^{-1}S$ es libre, y la función traza es lineal, tenemos que $d_1/1 = r \cdot c_1/1 + c'_1/1$, y por tanto existe $u \in U$ tal que $u(d_1 - (rc_1 + c_2)) = 0$. Y como en $U$ no hay divisores de cero, vemos que $d_1 = rc_1 + c_2$. Asi que $Tr$ sea $R$-lineal.

Finalmente $g(t) = (t-1)^n$ cumple que

$$U^{-1}g = chr_{Id}(t) : U^{-1}S \to U^{-1}S.$$

Esto implica que $g(t)$ es el polinonio característico de multiplicación por 1. Luego $Tr(1) = -n$.
■

# Capítulo 3

# Conjeturas del sumando directo y de Koh

En este capítulo consideramos el caso donde $R \subset S$ es una extensión módulo finita de anillos Noetherianos. Estamos interesados en estudiar si existe una retracción, es decir, si existe un $R$-homomorfismo $\rho : S \to R$ que envie el 1 en el 1.

## 3.1 Conjetura del sumando directo

Sea $R$ un anillo conmutativo cualquiera y supongamos que deseamos probar que $R$ posee una cierta propiedad P. Existe una técnica bastante útil en álgebra conmutativa que permite probar que $R$ satisface P. Primero se sumerge a $R$ como subanillo de un anillo $S$, el cual se sabe que satisface P, y luego se intenta trasladar dicha propiedad de $S$ a $R$. Este último paso se puede llevar a cabo en muchos casos si se tiene alguna información adicional de la manera como $R$ está sumergido en $S$. Un caso muy importante es aquel en donde $R$ es un *sumando directo* de $S$, es decir, si consideramos a $S$ como un módulo sobre $R$ (la acción de $R$ sobre $S$ está definida de manera obvia como $r \cdot s = rs$, para $r$ perteneciente a $R$ y $s$ perteneciente a $S$) entonces $R$, visto como submódulo de $S$, tiene la propiedad de ser un sumando directo de $S$. Esto quiere decir que existe otro $R$-submódulo $C$ de $S$ tal que $S = R \oplus C$ (recordemos que esta notacíón significa que cada elemento $s$ perteneciente a $S$ se puede escribir de manera única como una suma $s = r + c$, $r$ perteneciente a $R$, $c$ perteneciente a $C$). Por ejemplo, es posible probar con esta técnica que los anillos de invariantes de grupos linealmente reductivos, actuando sobre anillos regulares, son Cohen-Macaulay ([HoEa]).

Uno de los problemas centrales en álgebra homológica que aún permanece sin resolverse es el problema o conjetura conocida con el nombre de *Conjetura del Sumando Directo (CSD).* Esta conjetura, *equivalente a la Conjetura Monomial*, juega un papel fundamental en el Álgebra Homológica local debido que ella implica la gran mayoría de las conjeturas más importantes en esta área [Ho75]. Desde su formulación en 1973 se ha realizado un esfuerzo considerable por parte de muchos algebristas encaminado a encontrar su demostración. A raíz de estos esfuerzos se han desarrollado nuevas teorías y ha aparecido así mismo un número considerable de nuevos resultados. Entre ellos se destacan la reciente solución en el caso de anillos de característica mixta de dimensión 3 [He], los trabajos de P. Roberts [Ro], en particular, su aplicación de la Teoría de la Intersección en Geometría álgebraica (desarrollada recientemente por Fulton-

McPhearson) a la solución de conjeturas relacionadas con la C.S.D., tales como la Conjetura de Serre, sobre la multiplicidad de la intersección de dos módulos [Se], [Ve3], así como la conjetura conocida como el Nuevo Teorema de la Intersección [Ro].

La Conjetura del Sumando Directo (C.S.D.) afirma que para cualquier extensión módulo finita $R \subset S$ de un anillo *regular* $R$, es decir, una extensión donde $S$ es finitamente generado como $R$-módulo, el anillo $R$ es un *sumando directo de* $S$. Este tipo de extensiones juegan un papel fundamental en álgebra conmutativa. Equivalentemente, $S$ es una *extensión módulo finita* de $R$, si cada elemento de $s$ perteneciente a $S$ satisface un polinomio mónico con coeficientes en $R$: $s^n + r_1 s^{n-1} + .... + r_n = 0$, y $S$ es un álgebra finitamente generada sobre $R$.

Esta conjetura ha sido probada para el caso de todos los anillos regulares que contienen un cuerpo [Ho73], y en general para todos los anillos con dimensión de Krull menor o igual a 3. Cuando el anillo $R$ no contiene un campo, la situación es muchísimo más complicada. Para dimensiones 1 y 2, la conjetura se deduce de la existencia de una normalización para $R$. Si la dimensión es 3, y $R$ es un anillo de característica mixta, la demostración es muy difícil y sólo se logró recientemente [He]. Sin embargo, cuando la dimensión de Krull de $R$ es mayor que 3, casi nada se conoce, ni siquiera en el caso en que $R$ sea un anillo de polinómios sobre los enteros, con más de dos variables; por ejemplo, cuando $R$ es el anillo $R = \mathbb{Z}[X_1, X_2, X_3]$.

En este capítulo daremos en detalle una prueba de la CSD cuando $R$ es un anillo normal que contiene un campo de característica cero, y en el caso en el que $R$ es regular y contiene un campo de característica prima.

## 3.2 La conjetura de Koh

Una línea de ataque para la CSD fue sugerida por J. Koh en 1983. La idea consistía en primero demostrar otra conjetura más fuerte, conocida como Conjetura de Koh, la cual implicaría la CSD, y que afirma lo siguiente: sea $R \subset S$ una extensión módulo-finita de $R$, un anillo Noetheriano cualquiera, tal que $S$ es un $R$-módulo con dimensión proyectiva finita $pd_R(S) < \infty$. Entonces la conjetura de Koh afirma que $R$ es un sumando directo de $S$. Esta conjetura permaneció abierta hasta 1993 cuando por primera vez se construyeron ejemplos que mostraban que esta conjetura, en su formulación más general, no era cierta ([Ve1], [Ve2] y [Ve-Ri]). En este capítulo daremos una demostración detallada de estos hechos.

Cuando $R$ es regular, la condición de tener dimensión proyectiva finita se da automáticamente (caracterización de Serre de los anillos regulares), de donde se deduce que *la conjetura de Koh implica la del sumando directo*. Se sabe que la conjetura de Koh es cierta cuando $R$ contiene un campo de característica 0. La prueba la haremos usando las ideas desarrolladas en el capítulo anterior. Un contraejemplo a la conjetura de Koh en el caso general en el que $R$ es un anillo que contiene un campo de característica prima será presentado en detalle al final de este capítulo.

Existe todavía la posibilidad de que esta conjetura sea cierta para anillos Cohen-McCauly o anillos de Gorenstein. Se puede probar, que si la conjetura de Koh es cierta para anillos de Gorenstein de dimensión 1, entonces la conjetura del sumando directo es cierta en dimensión 3. La existencia de un contraejemplo a la conjetura de Koh simplemente descarta la posibilidad de probar el caso general de la conjetura del sumando directo como su consecuencia.

Comencemos por mostrar que la existencia de retracciones equivale a la descomposición en suma directa.

**Proposición 3.2.1** *Sea $R \subset S$ una extensión módulo finita. La existencia de una retracción $\rho : S \to R$ es equivalente a la existencia de un $R$-módulo $M$ tal que $S = R \oplus M$.*

**Prueba.** Supongamos existe $\rho : S \to R$ tal que $\rho(1) = 1$, y sea $M = \{s - \rho(s) \in S : r \in R\}$. $M$ es claramente un $R$-módulo, y claramente $S = M + R$, ya que $S \subset M + \rho(S) = M + R \subset S$. Ahora, si $s - \rho(s) \in R \cap M$, entonces

$$\rho(s - \rho(s)) = \rho(s) - \rho \circ \rho(s) = \rho(s) - \rho(s) = 0.$$

Pero $s - \rho(s) \in R$, luego $\rho(s - \rho(s)) = s - \rho(s) = 0$. Esto muestra que la suma es directa.

Supongamos ahora que existe $M$ tal que $S = R \oplus M$, y definamos $\rho : S \to R$ como el morfismo que envia a $r + m$ en $r$. Se ve inmediatamente que $\rho$ es una retracción. ■

El problema de la existencia de retracciones se puede reducir rápidamente al caso donde $R$ es un anillo local.

**Proposición 3.2.2** *Existe una retracción $\rho : S \to R$ si, y sólo sí, el morfismo*

$$i^* : Hom_R(S, R) \to Hom_R(R, R)$$

*es sobreyectivo, donde $i^*$ es el morfismo inducido por la inclusión $i : R \to S$.*

**Prueba.** Supongamos que existe $\rho$, y sea $\gamma \in Hom(R, R)$. Si consideramos el morfismo $\gamma \circ \rho : S \to R$, vemos entonces que $i^*(\gamma \circ \rho) = \gamma \circ \rho \circ i = \gamma$, y por consiguiente $i^*$ es sobreyectiva.

Por otro lado, si $i^*$ es sobreyectiva existe $\rho \in Hom_R(S, R)$ tal que $i^*(p) = Id$. Esto es, $\rho \circ i = Id$; es decir $p$ es una retracción. ■

Las siguientes dos proposiciones funcionan independientemente de si nos encontramos en el caso de la conjetura del sumando directo o en la conjetura de Koh, pues las propiedades de ser regular o de dimensión proyectiva finita se preservan bajo localizaciones y completaciones.

**Proposición 3.2.3** *Si para toda extensión de anillos $R \subset S$ módulo finita con $R$ un anillo local existe una retracción, entonces para toda extension $R' \subset S'$ módulo finita también existe.*

**Prueba.** Sea $R' \subset S'$ una extensión módulo finita. Sabemos que

$$i^* : Hom_{R'}(S', R') \to Hom_{R'}(R', R')$$

es sobreyectiva, si y sólo si

$$i_m^* : Hom_{R'}(S', R')_m \to Hom_{R'}(R', R')_m$$

lo es, para todo ideal $m \subset R'$ maximal 1.1.5. Pero también sabemos que el morfismo anterior es canónicamente equivalente a

$$i_m^* : Hom_{R'_m}(S'[m]^{-1}, R'_m) \to Hom_{R'_m}(R'_m, R'_m)$$

(ya que $S$ tiene una presentación finita como $R$-módulo, pues es un $R$ módulo finitamente generado). Pero esta es sobreyectiva por hipótesis, ya que $R'_m \subset S'[m]^{-1}$ es una extensión módulo finita. ■

Supondremos de ahora en adelante $R$ un anillo local con ideal maximal $m$. Hagamos una segunda reducción del problema, esta vez a anillos completos.

**Proposición 3.2.4** *Si para toda extensión de anillos $R \subset S$ módulo finita, con $R$ un anillo completo, existe una retracción, entonces para toda extension $R' \subset S'$ módulo finita también existe una retracción.*

**Prueba.** Sea $R' \subset S'$ una extensión módulo finita. Veamos que

$$i^* : Hom_{R'}(S', R') \to Hom_{R'}(R', R').$$

es sobreyectiva.

Para esto notemos que

$$Hom_{R'}(S', R') \to Hom_{R'}(R', R') \to Co\ker(i^*) \to 0$$

es una secuencia exacta. Así dado cualquier ideal $j \subset R'$ tenemos que

$$Hom_{R'}(S', R') \otimes \widehat{R'}^J \to Hom_{R'}(R', R') \otimes \widehat{R'}^J \to Co\ker(i^*) \otimes \widehat{R'}^J \to 0$$

es exacta, (ya que $S$ tiene una presentación finita por ser un $R'$-módulo finitamente generado). Pero la secuencia anterior es canonicamente equivalente a

$$Hom_{\widehat{R'}^J}(\widehat{S'}^J, \widehat{R'}^J) \to Hom_{\widehat{R'}^J}(\widehat{R'}^J, \widehat{R'}^J) \to Co\ker(i^*) \otimes \widehat{R'}^J \to 0$$

Como $Hom_{\widehat{R'}^J}(\widehat{S'}^J, \widehat{R'}^J) \to Hom_{R'^{\widehat{J}}}(\widehat{R'}^J, \widehat{R'}^J)$ es sobreyectiva por hipótesis, se sigue que $Cok(i^*) \otimes \widehat{R'}^J = 0$. Ahora, como $\widehat{R'}^J$ es un módulo fiel, ya que $R^{'}$ es local, tenemos que $Co\ker(i^*) = 0$. Es decir, $i^*$ es sobreyectiva. ■

Supongamos que $R$ es un anillo regular. Como vimos antes, $R$ lo podemos suponer local y completo. Del Teorema 19.19, pág. 487 de [DE] se sigue que $R$ es un dominio de factorización única. Con estas observaciones pasemos a demostrar el siguiente resultado.

**Teorema 3.2.5** *Para demostrar la Conjetura del Sumando Directo se puede suponer, sin pérdida de generalidad, que $S$ es un dominio.*

**Prueba.** Como $R$ es un dominio, por el *Going Up* existe un ideal primo $P$ de $S$ tal que $P \cap R = 0$. Luego $R/(0) \to S/P$ es una extensión módulo finita. Si existiera una retracción $\phi : S/P \to R$ que envie el 1 en sí mismo entonces la compuesta $S \to S/P \to R$ es una retracción para el caso original. ■

**Teorema 3.2.6** *Si la Conjetura del Sumando Directo es cierta siempre que $S$ sea un anillo local completo, entonces la conjetura es cierta en general.*

**Prueba.** Si $R \hookrightarrow S$ es una extensión módulo finita de anillos con $R$ un anillo regular local completo, por un teorema anterior vemos que

$$S = S_1 \times \cdots \times S_n,$$

donde cada $S_i$ es un anillo local completo y un $R-$módulo finitamente generado. Ahora, como $i : R \hookrightarrow S_1 \times \cdots \times S_n$ es una inyección, y si $\pi_i : S \to S_i$ denota la proyección, entonces para algún $S_i$ el homomorfismo $\pi_i \circ i : R \to S_i$ es inyectivo: para ver esto último notemos que de no ser así, para cada $i$ existiría un $0 \neq r_i \in R$ tal que $\pi_i \circ i(r_i) = 0$. Entonces tendríamos que si $r = r_1 \cdot \cdots \cdot r_n$,

$$i(r) = \sum \pi_i \circ i(r) = 0.$$

Pero esto implicaría que $r = 0$, pues $i$ es inyectiva. Ahora, como $R$ es un anillo locar y regular, $R$ es un dominio, y por tanto algún $r_i$ debería ser cero, lo cual es un absurdo. Así tenemos que $\pi_i \circ i$ es inyectiva. Luego si la Conjetura del Sumando Directo es cierta para $R \hookrightarrow S'$, con $S'$ local completo entonces existe $\phi : S_i \to R$ un $R$-homomorfismo que envia el 1 en el 1. Por tanto $\phi \circ \pi_i : S \to R$ es un $R$-homomorfismo que envia el 1 en el 1, de alli que la conjetura sería cierta para el caso general. ■

Esta reducción nos permite suponer que tanto $R$ como $S$ son dominios locales completos en la Conjetura del Sumando Directo.

## 3.3 La Conjetura del Sumando Directo en el caso que $R$ contiene un campo de característica cero

En esta sección trataremos las soluciones conocidas tanto de la Conjetura del Sumando Directo como de la conjetura de Koh. Durante esta sección supondremos que $R \subset S$ es una extensión módulo finita, y que $R$ es un anillo local completo ($R$ es además un dominio regular y $S$ se puede suponer un dominio, en el caso de la Conjetura del Sumando Directo).

Este resultado se deduce rápidamente de dos hechos. Primero, como $R$ es un anillo regular completo entonces es un dominio de factorización única como ya vimos anteriormente, y por lo tanto es normal. Así sólo debemos probar el resultado para dominios normales, para lo cual utilizamos el segundo hecho:

**Proposición 3.3.1** *Sea $R \subset S$ una extensión módulo finita de dominios, con $R$ normal. Si $L_R$, $L_S$ denotan los campos de fracciones de $R$ y $S$ respectivamente, entonces $L_R \subset L_s$ es una extensión finita de campos. Sea $tr : L_S \to L_R$ la función traza definida en el primer capítulo. Entonces $tr|_S$ es un $R$-homomorfismo y es tal que $tr(s) \in R$, para todo $s \in S$.*

**Prueba.** Sea $s \in S$ y $g(t) = t^n + r_1 t^{n-1} + \cdots + r_n$ el polinomio minimal para $s$ sobre $L_R$. Veamos que todos los coeficientes de $g(t)$ están en $R$. En particular $r_1 \in R$ de lo cual se sigue que $tr(s) \in R$ (proposición sobre trazas).

Como $s \in S$ y $R \subset S$ es una extensión módulo finita, existe un polinomio $h(t)$ con coeficientes en $R$ que anula a $s$. Luego si $\overline{L_R}$ denota la clausura álgebraica de $L_R$ tenemos que allí las raices de $h(t)$ son enteras sobre $R$. Como en particular las raíces de $g(t)$ son también raíces de $h(t)$, ya que $g(t)$ es minimal, y por tanto $g(t)|h(t)$. Se sigue que los coeficientes de $g(t)$ son enteros, por ser funciones simétricas en las raíces de $h(t)$. Y como estos coeficientes pertenecen a $L_R$ y $R$ es normal, se deduce que los coeficientes de $g(t)$ pertenecen a $R$, de lo cual se sigue el resultado. ■

**Teorema 3.3.2** *(C.S.D. si $\mathbb{Q} \subset R$) Sea $R \subset S$ una extensión módulo finita de dominios con $R$ normal (en particular esto se tiene si $R$ es regular y local). Si $\mathbb{Q} \subset R$ entonces la extensión se parte, es decir existe una retracción.*

**Prueba.** Por la proposición anterior tenemos que $tr|_S : S \to R$ es un $R-$homomorfismo y además por 1 tenemos que $tr|_S(1) = n$, con $n = [L_s : L_R]$. Entonces, si definimos a $\phi : S \to R$, como $\phi = \frac{1}{n} tr|_S$ ($\frac{1}{n} \in R$ ya que $\mathbb{Q} \subset R$) tenemos el resultado deseado, ya que $\phi(1) = 1$. ■

## 3.4 La Conjetura del Sumando Directo en el caso que $R$ contiene un campo de característica prima

**Lema 3.4.1** *Sea $R \subset S$ una extensión módulo finita de dominios, entonces si $L_R \subset L_S$ son los campos de fracciones de $R$ y $S$ respectivamente, se tiene que $L_S$ es una extensión (de campos) finita de $L_R$.*

**Prueba.** Dado $s \in S$, como $S$ es dominio y módulo finito sobre $R$, existe un polinomio mónico

$$p(t) = t^n + a_1 t^{n-1} + .. + a_n \in R[t]$$

con $a_n \neq 0$, tal que $p(s) = 0$. En particular, existe $s' \in S$ tal que $s's \in R$ ya que

$$s(s^{n-1} + a_1 s^{n-2} + \cdots + a_{n-1}) = a_n \in R.$$

Además, como $S$ es módulo finita, existen $s_1, \cdots, s_k$ tales que

$$S = s_1 R + \cdots + s_k R.$$

Dado $t/s \in L_S$, tenemos entonces que

$$\begin{array}{ll} \frac{t}{s} = \frac{ts'}{ss'} = \frac{1}{ss'}(r_1 s_1 + \cdots + r_k s_k) & ; r_1 s_1 + \cdots + r_k s_k = ts' \\ \quad = (\frac{r_1}{ss'}) s_1 + \cdots + (\frac{r_k}{ss'}) s_k & ; \frac{r_i}{ss'} \in L_R \end{array}$$

Esto es lo mismo que decir que los elementos $s_1, \cdots, s_k$ generan a $L_S$ como $L_R$-espacio vectorial, con lo que se consigue el resultado. ■

**Lema 3.4.2** *Sea $F$ un $A$-módulo libre de rango $n$ con $A$ un anillo local de ideal maximal $m$, y sea $c \in F$ tal que $c \notin mF$. Entonces existen $c_2, .., c_n \in F$ tales que $\{c, c_2, \cdots, c_n\}$ es base para $F$.*

**Prueba.** Como $c \notin mF$ tenemos que la clase $\overline{c}$ de $c$ en $F/mF$ es distinta de cero, y como $F/mF$ es un $(A/m)$-espacio vectorial de dimensión $n$, existen $c_2, \cdots, c_n \in F$ tales que $\{\overline{c}, \overline{c_2}, \cdots, \overline{c_n}\}$ es base. Ahora es claro que $(cA + \cdots + c_n A) + mF = F$. Luego, del lema de Nakayama 1.1.6 se sigue que $F = cA + \cdots + c_n A$. Por otro lado, si consideramos la secuencia exacta

$$0 \to K \to A^n \xrightarrow{\gamma} F \to 0$$

donde

$$\gamma(a_1, .., a_n) = ca_1 + \cdots + c_n a_n$$

y $K = \ker \gamma$ tenemos que al tensorizar con $A/m$ el siguiente complejo queda exacto

$$Tor^1(A/m, F) \to K/mK \to (A/m)^n \xrightarrow{\widetilde{\gamma}} (F/mF) \to 0.$$

Como $Tor^1(A/m, F) = 0$, pues $F$ es libre, $\widetilde{\gamma}$ es un isomorfismo de espacios vectoriales. Así que $K/mK = 0$, y nuevamente, por el Lema de Nakayama, $K = 0$, de donde se sigue el resultado. ■

Dada una extensión módulo finita $R \subset S$ donde $R$ contiene un campo, el teorema de estructura de Cohen 1.2.5 nos dice que $R \simeq K[[x_1, \cdots, x_n]]/I$, donde $K$ es un campo de coeficientes para $R$. Ahora, si $\overline{K}$ es la clausura álgebraica para $K$ tenemos que $R' = \overline{K}[[x_1, \cdots, x_n]]/I$ es un $R$ módulo libre ya que si $\overline{K} = \bigoplus K u_\alpha$ entonces

$$R' = \bigoplus K u_\alpha [[x_1, \cdots, x_n]]/I.$$

Luego $R'$ es fielmente plano. Así, la extensión $R \subset S$, se parte si y sólo si la extensión $R' \subset S \otimes_R R'$ se parte. Por tanto, podemos considerar sin pérdida de generalidad que el campo $K$ que $R$ contiene es álgebraicamente cerrado.

**Teorema 3.4.3** *Sea $R \subset S$ una extensión módulo finita, donde $R$ es un anillo equicaracterístico de característica prima. Entonces existe una retracción de $S$ en $R$.*

**Prueba.** Por la discucción anterior podemos considerar que $R = K[[X_1, \cdots, X_n]]/I$, donde $K$ es un campo álgebraicamente cerrado. En particular, este campo es perfecto, esto es, $K^p = \{a^p : a \in K\}$ es igual a $K$ (equivalentemente todo elemento de $K$ tiene raíz $p$-ésima). Sean $L_R \subset L_S$ los campos de fracciones de $R$ y $S$ respectivamente. Sabemos por uno de los lemas anteriores que $L_S$ es una extensión finita de $L_R$, y por consiguiente que existen elementos $u_1, .., u_l \in S$ tales que $L_S = L_R u_1 \oplus \cdots \oplus L_R u_l$. Si $S = Rs_1 + \cdots + Rs_d$ con $\{s_1, \cdots, s_d\} \subset S$, entonces, si cada $s_j = (r_{1j}/a_{1j})u_1 + \cdots + (r_{lj}/a_{lj})u_l$ tenemos que $c = \prod a_{ij}$ es tal que $cS \subset Ru_1 \oplus \cdots \oplus Ru_l$. Sin pérdida de generalidad podemos suponer que $u_1 = 1$. Sea $\rho_1 : Ru_1 \oplus \cdots \oplus Ru_l \to R$ la proyección en la primera coordenada. Sea $\rho_2 = \rho_1 \circ \mu_c : S \to R$, donde $\mu_c : S \to S$ es la función $R$-lineal multiplicación por $c$. Es claro que $\rho_2(1) = \rho_1(c) = c$. Ahora, si $m = (x_1, .., x_n)$ denota el ideal maximal de $R$, como $\bigcap m^t = (0)$ por el teorema de intersección de Krull 1.1.8, se tiene que existe $q = p^e$, $e > 0$ tal que $c \notin m^q$. Notemos que

$$R^q = K^q[[x_1^q, \cdots, x_n^q]] = K[[x_1^q, \cdots, x_n^q]].$$

Además, como $R = \bigoplus_{0 \leq e_i < q} R^q x_1^{e_1} \cdots x_n^{e_n}$ tenemos, por el lema anterior, que $c$ fomar parte de una base para $R$ como $R^q$-módulo, y por ende existe un $R^q$-homomorfismo $\phi : R \to R^q$ que envia a $c$ en 1. Si componemos a $\rho_2$ con $\phi$, $\rho = \phi \circ \rho_2$, obtenemos una retracción $\rho : S \to R^q$, pero como el siguiente diagrama conmuta

$$\begin{array}{ccc} S & \rightarrow & S^q \\ \uparrow & & \uparrow \\ R & \rightarrow & R^q \end{array}$$

donde las flechas horizontales denotan el homomorfismo de Frobenius $F(r) = r^q$, entonces, para obtener una retracción de $S$ a $R$ basta restringir a $\rho$ a $S^q$ y componer con $F$ y $F^{-1}$. Es decir $F^{-1} \circ \rho|_{S^q} \circ F$ es una retracción de $S$ a $R$. $\blacksquare$

## 3.5 La Conjetura de Koh en característica cero

La construcción de un polinomio característico de mayor generalidad nos permite probar la Conjetura del Sumando Directo cuando $\mathbb{Q} \subset R$. Notemos para comenzar que si $R$ es local, entonces su espectro es conexo.

**Proposición 3.5.1** *Sea $R$ un anillo que contiene a $\mathbb{Q}$, y sea $R \subset S$ una extensión módulo finita tal que $pd(S) < \infty$. Entonces existe una retracción $\rho : S \to R$.*

**Prueba.** Por las reduciones hechas al problema anteriormente, podemos suponer que $R$ es local. Por el lema anterior tenemos que $Spec(R)$ es conexo. Ahora, el rango de $U^{-1}S$ es positivo, ya que si $U^{-1}S = 0$ tendríamos que $u1 = 0$ para algún $u \in U$, lo cual es un absurdo. Luego $rango(S) = n > 0$. Basta entonces definir el $R$-homomorfismo $\rho = -\frac{1}{n}Tr : S \to R$, donde $Tr$ se definió en la proposición 2.0.15. $\blacksquare$

## 3.6 Contraejemplo para la Conjetura de Koh

Sea $0 \to R^n \xrightarrow{X} R^m \xrightarrow{p} C \to 0$ una resolución libre, y por ende proyectiva, para el $R$-módulo $C$. La correspondencia en la construcción de Yoneda para $Ext$ (punto (e) 1.5) funciona de la siguiente manera:

**i)** Un elemento de $Ext^1(C, R)$ es una clase de equivalencia de $\overline{f} \in Hom(R^n, R)/X^*(Hom(R^m, R))$, donde $X^*$ denota la transpuesta.

**ii)** La siguiente relación es un isomorfismo de $R$-módulos

$$\begin{array}{ccc} Ext^1(C, R) & \rightarrow & E^1(C, R) \\ \overline{f} & \rightarrow & \alpha_{\overline{f}} \end{array}$$

donde $f : R^n \to R$ es un $R$-homomorfismo. Denotemos la bases canónicas para $R^n$ y $R^m$ por $\{e_1, \ldots, e_n\}$ y $\{\varepsilon_1, \ldots, \varepsilon_m\}$, respectivamente. Entonces

$$\begin{array}{cccccccccc}
\alpha_{\overline{f}}: & 0 & \to & R & \overset{i}{\hookrightarrow} & \frac{R\oplus R^m}{(f(e_i), -x(e_i))} & \overset{p'}{\to} & C & \to & 0 \\
 & & & \uparrow f & & \uparrow g & & \uparrow Id & & \\
 & 0 & \to & R^n & \underset{x}{\hookrightarrow} & R^m & \underset{p}{\to} & C & \to & 0
\end{array}$$

conmuta, donde $g(\varepsilon_j) = \overline{(0, \varepsilon_j)}, i(r) = \overline{(r, 0)}$ y $p'(\overline{(a, b)}) = p(b)$.

Sabemos que $[\alpha_{\overline{f}}] = [0]$, es decir, $\alpha_f$ se parte sí, y sólo sí $\overline{f} = 0$, sí, y sólo sí $f \in \mathrm{Im}(X^*)$, sí, y sólo sí existe $h : R^m \to R$ tal que $h \circ x = f$.

### 3.6.1 Construcción de un contraejemplo para la Conjetura de Koh en característica prima

Sean $K = \mathbb{Z}_2$, y

$$R_0 = K[x_{11}, x_{12}, x_{21}, x_{22}, x_{31}, x_{32}, t, z_1, z_2, y_{11}, y_{12}, y_{13}, y_{21}, y_{22}, y_{23}, w_{11}, w_{12}, w_{12}, w_{21}, w_{22}, w_{23}]$$

Sea $H$ el ideal generado por todas las entradas de las matrices siguientes: $A - NY$, $B - NW$, donde

$$\begin{aligned}
A &= \begin{bmatrix} 0 & 0 & 0 \\ z_1^2 - tx_{11} & 0 & 0 \\ 0 & z_1^2 - tx_{21} & 0 \\ 0 & 0 & z_1^2 - tx_{31} \end{bmatrix} \\
N &= \begin{bmatrix} z_1^2 & z_2^2 \\ -x_{11} & -x_{12} \\ -x_{21} & -x_{22} \\ -x_{31} & -x_{32} \end{bmatrix} \\
B &= \begin{bmatrix} 0 & 0 & 0 \\ z_2^2 - tx_{12} & 0 & 0 \\ 0 & z_2^2 - tx_{22} & 0 \\ 0 & 0 & z_2^2 - tx_{32} \end{bmatrix} \\
X &= [x_{ij}]_{3\times 2}, \; Y = [y_{ij}]_{2\times 3}, \; W = [w_{ij}]_{2\times 3}
\end{aligned}$$

Sea $R = R_0/H$ (denotaremos las clases de equivalencia por las mismas letras). Sea $f : R^2 \to R$ está definida por $f(e_1) = z_1^2$, $f(e_2) = z_2^2$, y sea $X : R^2 \to R^3$ dada por la matriz $X = [x_{ij}]_{3\times 2}$. Veamos que $X$ es inyectiva. Para ello utilizaremos el criterio de exactitud de Buchsbaum-Eisenbud 1.4.2. Consideremos la secuencia $0 \to R^2 \xrightarrow{X} R^3$. Sabemos que esta secuencia es exacta si $rank(x) = 2$ y si $depth_{\Delta} R \geqslant 1$ donde $\Delta$ es el ideal obtenido de los menores $2 \times 2$ de la matriz $X$. Podemos demostrar ambos resultados al mismo tiempo mostrando un elemento distinto de cero en $I_2(X)$ y que no sea divisor de cero en $R$. Sea

$$z = (x_{11}x_{22} - x_{21}x_{12}) + (x_{11}x_{32} - x_{31}x_{12}) + (x_{21}x_{32} - x_{31}x_{22}) \in I_2(X).$$

Para ver que $z$ no es divisor de cero en $R$ lo único que debemos ver es que no está contenido en los primos minimales de $H$. Pero esto se verifica rapidamente de la siguiente forma usando el programa *Maple*. Una descomposición primaria para $H$ se halla con el comando *PrimaryDecomposition(H)*. Para cada ideal $Q_i$ se verifica si $z \in Q_i$ usando el comando *IdealMembership(z, H)*. El cómputo muestra que la respuesta es negativa. Así, tenemos que la secuencia

$$0 \to R^2 \xrightarrow{X} R^3 \to R^3/im(X) \to 0$$

es exacta. Consideremos el siguiente diagrama

$$\begin{array}{ccccccccc} 0 & \to & R & \to & \frac{R \oplus R^3}{(f(e_i), -x(e_i))} & \to & C & \to & 0 \\ & & \uparrow f & & \uparrow g & & \shortparallel & & \\ 0 & \to & R^2 & \xrightarrow{x} & R^3 & \to & C & \to & 0 \end{array} \qquad (\#)$$

Si $T = R \oplus R^3$, este $R$-módulo libre puede dotarse de estructura de $R$-álgebra en forma natural, vía el siguiente isomorfismo:

$$T \cong R[x_1, x_2, x_3]/(x_1x_2, x_1x_3, x_2x_3, x_1^2 - tx_1, x_2^2 - tx_2, x_3^2 - tx_3)$$

Es claro que $R \to T$ es una extensión libre de rango 4 : $(R\overline{1} \oplus R\overline{x}_1 \oplus R\overline{x}_2 \oplus R\overline{x}_3)$.

Denotemos por $u_i$ la clase de $x_i$. Con el fin de dotar a $S = R \oplus R^3/(f(e_i), -x(e_i))_{i=1,2}$ de estructura de $R$-álgebra es necesario que el $R$-submódulo generado por

$$\begin{aligned} v_1 &= f(e_1) - x_{11}u_1 - x_{21}u_2 - x_{31}u_3 \\ v_2 &= f(e_2) - x_{12}u_1 - x_{22}u_2 - x_{32}u_3 \end{aligned}$$

sea un ideal de $T$. Pero para $i = 1, 2, 3$.

$$\begin{aligned}
u_i v_1 &= u_i(z_1^2 - x_{11}u_1 - x_{21}u_2 - x_{31}u_3) \\
&= u_i z_1^2 - x_{i1} t u_i = u_i(z_1^2 - x_{i1}t) \\
&= y_{i1}v_1 + y_{2i}v_2 \\
u_i v_2 &= u_i(z_2^2 - x_{12}u_1 - x_{22}u_2 - x_{32}u_3) \\
&= u_i z_2^2 - x_{i2} t u_i = u_i(z_2^2 - x_{i2}t) \\
&= w_{1i}v_1 + w_{2i}v_2
\end{aligned}$$

Es decir, en efecto, el $R$-submódulo generado por $v_1$, $v_2$ es un ideal de $T$ y por tanto $S$ es una $R$-álgebra módulo finita sobre $R$. Es más, si la siguiente secuencia fuese exacta entonces $pd(S) = 1 < \infty$:

$$0 \to R^2 \xrightarrow{X'} R \oplus R^3 \to \frac{R \oplus R^3}{(f(e_i), -x(e_i))} \to 0,$$

donde $X'$ esta dada por la matriz

$$\begin{bmatrix} f(e_1) & f(e_2) \\ -x_{11} & -x_{12} \\ -x_{21} & -x_{22} \\ -x_{31} & -x_{32} \end{bmatrix}$$

Pero del hecho de que $z$ (definido más arriba) esté en $I_2(x')$ y no sea divisor de cero, tenemos nuevamente, por el criterio de Buchsbaum-Eisenbud 1.4.2, que $X'$ es inyectiva y por tanto que la secuencia es exacta (la exactitud en el medio y a la derecha son triviales). Luego, para mostrar que no existe retracción, sólo debemos ver que no existe $h : R^3 \to R$ tal que $h \circ X = f$. Matricialmente que $[h]_{1\times 3}[x]_{3\times 2} = [f]_{1\times 2}$. Es decir, que no existen $h_1$, $h_2$ y $h_3$ tales que

$$\begin{bmatrix} h_1 & h_2 & h_3 \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \\ x_{31} & x_{32} \end{bmatrix} = \begin{bmatrix} z_1^2 & z_2^2 \end{bmatrix}$$

o, equivalentemente

$$\begin{bmatrix} z_1^2 \\ z_2^2 \end{bmatrix} \notin \left\langle \begin{bmatrix} x_{11} \\ x_{12} \end{bmatrix}, \begin{bmatrix} x_{21} \\ x_{22} \end{bmatrix}, \begin{bmatrix} x_{31} \\ x_{32} \end{bmatrix} \right\rangle$$

Pero esto es sencillo ya que ni siquiera $z_1^2 \in \overline{J} = (x_{ij})$ en $R$, puesto que de lo contrario

$z_1^2 \in (x_{ij}) + H$ en $R_0$, y en particular $z_1^2 \in \overline{H}$ en

$$R_0/(x_{ij}) = K[t, z_1, z_2, y_{11}, y_{12}, y_{13}, y_{21}, y_{22}, y_{23}, w_{11}, w_{12}, w_{12}, w_{21}, w_{22}, w_{23}]$$

y por tanto $\overline{H}$ sería el ideal generado por las matrices $A - NY$, $B - NW$, con

$$\begin{aligned} A &= \begin{bmatrix} 0 & 0 & 0 \\ z_1^2 & 0 & 0 \\ 0 & z_1^2 & 0 \\ 0 & 0 & z_1^2 \end{bmatrix} \\ N &= \begin{bmatrix} z_1^2 & z_2^2 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \\ B &= \begin{bmatrix} 0 & 0 & 0 \\ z_2^2 & 0 & 0 \\ 0 & z_2^2 & 0 \\ 0 & 0 & z_2^2 \end{bmatrix} \\ Y &= [y_{ij}]_{2\times 3},\ W = [w_{ij}]_{2\times 3} \end{aligned}$$

Pero nuevamente, usando *Maple* vemos que $z_1^2 \notin \overline{H}$. Por tanto existe una extensión módulo finita $R \subset S$ con $dp(S) < \infty$ tal que no tiene una retracción, es decir, un contraejemplo a la conjetura de Koh.

# Bibliografía


[DE] D. Eisenbud, Commutative álgebra with a view Toward álgebraic Geometry. Springer-Verlag. New York, 1994.

[JD] J.D. Vélez, Failure of Splitting from Module-Finite Extension Rings. Contributions to álgebra and Geometry, volume 41 (2000), No. 2, 345-357.

[EvG] E.G. Evans and P. Griffith, The sysygy problem. Ann. of Math, 114 (1981) 323-333

[Du] Dutta, S. P., On the canonical element conjecture, Trans. Amer. Math. Soc. 299 (1987) 803-811.

[He] Heitman, R., The Direct Summand Conjecture in dimension three, Annals of Mathematics, 156, no. 2 (2002), 695-712.

[HH] Hochster, M. and C. Huneke, Tight closure, invariant theory, and the Briancon-Skoda theorem, J. Amer. Math. Soc. 3 (1990) 31-116.

[Ho73] Hochster, M Contracted ideals from integral extensions of regular rings, Nagoya Math. J. Vol.51 (1973), 25-43.

[Ho75] Hochster, M., Topics in the homological theory of modules over commutative rings, C.B.M.S. Regional Conf. Ser. in Math. No. 24, A.M.S., Providence, R.I., 1975.

[Ho83] Hochster, M., Canonical elements in local cohomology modules and the direct summand conjecture, J. of álgebra 84 (1983) 503-553.

[Ho 2000] Hochster, M., Homological Conjectures Old and New, preprint, 2000.

[HoEa] Hochster, M., and Eagon, Cohen-Macaulay rings, invariant theory, and the generic perfection of determinental loci, Amer. J. Math. 93 (1971) 1020-1058.

[RH] R. Hartshorne, álgebraic Geometry. Springer-Verlag New York, 1977.

[Ve1] Vélez, J.D., Splitting Results in module-finite extensions rings and Koh's conjecture (Journal of álgebra, 172, 454-469, 1995.

[Ve2] Vélez, J.D., La conjetura del sumando directo y la conjetura de Koh, Revista de la Facultad de Ciencias de la Universidad Nacional de Colombia, Vo.3, No.2.

[Ve3] Vélez, J.D., La conjetura de Serre sobre la multiplicidad de la intersección de dos módulos, Revista de la Facultad de Ciencias de la Universidad Nacional, Abril de 1993, No.3.

[Ve-Ri] Vélez J.D. and Florez R., Failure of Splitting from Module-Finite Extension Rings, Beitrage zur álgebra und Geometrie, Vol. 41 (2000), N0.2, 345-357.