Una Introducción a la Teoría de las Sicigias

Umberto Martínez Peñas

Trabajo de Fin de Grado
Grado en Matemáticas
Universidad de Valladolid, 3 de julio de 2013

Índice

Introducción

La presente memoria se debe a la realización de un trabajo de fin de Grado en Matemáticas y consiste, como indica su título, en una introducción a la Teoría de las Sicigias, centrada en ideales y módulos graduados finitamente generados sobre el anillo de polinomios con coeficientes en un cuerpo.

El resultado central será el famoso Teorema de las Sicigias, de David Hilbert, el cual forma parte de los tres grandes teoremas del Álgebra Conmutativa demostrados por Hilbert a finales del siglo XIX: el de las Sicigias, el de la Base y el de los Ceros. Todos ellos son teoremas fundamentales que tienen múltiples aplicaciones en Geometría Algebraica, Teoría de Números o Combinatoria, entre otras ramas de las matemáticas.

En el **primer capítulo** de la memoria introduciremos las nociones básicas que necesitaremos más adelante, como anillos, módulos y complejos graduados, e introduciremos los conceptos centrales del proyecto, que son las resoluciones libres graduadas, las sicigias y los invariantes de las resoluciones libres minimales graduadas, además de enunciar al final el Teorema de las Sicigias. En el **segundo capítulo** daremos una demostración de dicho teorema utilizando herramientas del Álgebra Homológica, básicamente algunas propiedades del funtor Tor y el complejo de Koszul. En el **tercer capítulo** daremos una demostración constructiva basada en las bases de Groebner. Finalmente, en el **cuarto capítulo** estudiaremos algunas consecuencias del Teorema de las Sicigias, sobre todo en lo que refiere a la función de Hilbert, que fue lo que motivó en su primer momento el estudio de las sicigias.

Capítulo 1

Resoluciones Libres y Sicigias

El problema que se nos plantea cuando tenemos un ideal I del anillo de polinomios $k[x_1, ..., x_n]$ es conocer su estructura. Ya sabemos que I estará finitamente generado, pues $k[x_1, ..., x_n]$ es un anillo noetheriano por el Teorema de la Base de Hilbert (ver [**AM**, 7.5] o [**CLO1**, Chapter 2]). Si dichos generadores fueran libres, ya conoceríamos cómo es I, pues sería isomorfo (como módulo) a una potencia finita del anillo de polinomios, y habríamos acabado. Sin embargo, si consideramos al menos dos generadores, esto no ocurrirá y dichos generadores tendrán unas relaciones lineales (con coeficientes polinómicos, claro) que complicarán este estudio (por ejemplo, $fg - gf = 0$ si f y g están entre los generadores).

Es entonces donde entran en juego las sicigias, que serán las relaciones (lineales) entre dichos generadores (primeras sicigias), las relaciones entre los generadores de estas primeras sicigias (segundas sicigias), etcétera. Lo que viene a decir el Teorema de las Sicigias es que este proceso terminará en algún momento, es decir, que llegaremos a un módulo de sicigias que será un módulo libre y las sicigias de una base suya constituirán el módulo 0.

Por otro lado, nos interesarán aquellos ideales que heredan la estructura graduada de $k[x_1, ..., x_n]$, pues en ellos el proceso descrito arriba se traslada a cada componente homogénea del ideal, que será un k-espacio vectorial, y nos permitirá hallar la dimensión sobre k de cada una de ellas, lo que determinará la función de Hilbert, que definiremos más adelante. En el último capítulo veremos que esto ya supone una gran cantidad de información.

Los conceptos y resultados que se utilizarán en este capítulo (y básica-

mente en toda la memoria) son los básicos de Álgebra Conmutativa, y se pueden encontrar en las referencias de la bibliografía. Prácticamente todos ellos se pueden encontrar en [**AM**], que quizá sea el libro más elemental de entre los citados, aunque una referencia más completa es [**Eis1**]. Por tanto, no entraremos en dichos detalles para no extender innecesariamente la memoria.

Notación. La notación que usaremos a lo largo de toda la memoria será la siguiente:

$\mathbb{N} = \{0, 1, 2, 3, ...\}$,

k será un cuerpo,

S el anillo de polinomios $k[x_1, ..., x_n]$ (el contexto nos dirá cual es n, el número de indeterminadas),

$\alpha = (\alpha_1, ..., \alpha_n)$ los elementos de $\mathbb{N}^n$,

$|\alpha| = \alpha_1 + ... + \alpha_n$,

$\underline{\mathrm{x}}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ los monomios de S,

$f = \sum \lambda_\alpha \underline{\mathrm{x}}^\alpha$ será un polinomio genérico de S,

$\mathrm{Rad}(I)$ y $\mathrm{ann}(I)$ denotarán el radical y el anulador del ideal I, respectivamente,

R será un anillo graduado, aunque normalmente será un cociente de S por un ideal homogéneo,

$\mathfrak{m}$ será el ideal maximal homogéneo de S, es decir, $\mathfrak{m} = \langle x_1, ..., x_n \rangle$, y

$\mathrm{rank}(M)$ será el rango de un R-módulo libre M.

Además, normalmente los elementos de R^m se escribirán en negrita.

1.1. Anillos graduados

La principal propiedad del anillo de polinomios que nos va a interesar es que es graduado, es decir, que será suma directa de grupos, cumpliendo cierta propiedad con el producto. Concretamente,

Definición 1.1. Sea R un anillo. Diremos que es **graduado** si existen subgrupos $\{R_i\}_{i\in\mathbb{N}}$ de R tales que

1. $R = \bigoplus_{i\in\mathbb{N}} R_i$ (como grupos), y
2. $R_iR_j \subset R_{i+j}$, $\forall i, j \in \mathbb{N}$.

R_i se denomina **componente homogénea i-ésima** de R y a sus elementos, f, **elementos homogéneos** o **formas** de grado i de R, y escribiremos $\deg(f) = i$.

Si $f \in R$, se escribe de forma única como $f = \sum_i f_i$ con $f_i \in R_i$ y $f_i = 0$ salvo para una cantidad finita. Decimos entonces que f_i es la **componente homogénea** i-ésima de f y definimos su **grado** como $\deg(f) = \text{máx}\{i/f_i \neq 0\}$.

Observemos que de $R_0R_0 \subset R_0$ se deduce que R_0 en realidad es un subanillo de R, y de $R_0R_i \subset R_i$ se deduce que cada R_i es un R_0-módulo, y la suma directa es suma directa de R_0-módulos.

Por otro lado, podríamos haber definido un anillo graduado de la misma forma, pero utilizando un monoide (conmutativo) cualquiera que no tenga por qué ser $\mathbb{N}$ (ver [**Eis1**, Section 1.5]), y se seguiría cumpliendo que R_0 es un subanillo de R, los R_i son R_0-módulos y la suma directa es suma directa de R_0-módulos (donde 0 es el neutro del monoide). En nuestro caso, utilizaremos $\mathbb{N}$, pero no habría ningún problema en considerar $\mathbb{Z}$, sólo que raramente necesitaremos considerar grados negativos.

En cuanto al anillo $S = k[x_1, ..., x_n]$, tenemos una graduación natural, aunque hay otras formas de graduarlo (ver [**DFX**, Sección 3.12]):

Definición 1.2. Dado un monomio $\underline{x}^\alpha \in S$, decimos que tiene **grado** $\deg(\underline{x}^\alpha) = |\alpha|$. Si $f = \sum \lambda_\alpha \underline{x}^\alpha \in S$, decimos que tiene **grado** $\deg(f) = \text{máx}\{|\alpha|/\lambda_\alpha \neq 0\}$, y decimos que es **homogéneo** si todos sus monomios tienen el mismo grado.

Definimos en S la **graduación estándar** por:

$$S_i = \{f \in S/f \text{ es homogéneo con } \deg(f) = i\}.$$

Es claro entonces que la graduación estándar es realmente una graduación en S, pues la propiedad $S_iS_j \subset S_{i+j}$ equivale a $|\alpha + \beta| = |\alpha| + |\beta|$.

Observación 1.3. No hay que confundir el **grado** de un polinomio $f = \sum \lambda_\alpha \underline{x}^\alpha \in S$, $\deg(f) = \max\{|\alpha| / \lambda_\alpha \neq 0\}$, con su **multigrado** respecto a un orden monomial, que definiremos más adelante como $\mathrm{mdeg}(f) = \max\{\alpha / \lambda_\alpha \neq 0\}$.

Ahora lo que nos interesará será ver cuándo un ideal de un anillo graduado hereda esta propiedad:

Proposición 1.4. *Sea I un ideal de un anillo graduado $R = \bigoplus_{i\in\mathbb{N}} R_i$. Son equivalentes:*

1. *Si $f \in I$, entonces toda componente homogénea de f está en I.*
2. *$I = \bigoplus_{i\in\mathbb{N}} I_i$ (como grupos), donde $I_i = I \cap R_i$.*
3. *I está generado por sus elementos homogéneos.*
4. *I tiene un sistema de generadores homogéneos.*

*A todo ideal que cumpla estas propiedades se le denomina **ideal homogéneo** o **graduado** de R, y a I_i se le denomina **componente homogénea** i-ésima de I.*

Demostración. Primero, las implicaciones $1 \Longrightarrow 2$, $2 \Longrightarrow 3$ y $3 \Longrightarrow 4$ son triviales. Veamos la implicación $4 \Longrightarrow 1$: Dado $f \in I$, por hipótesis, se puede escribir como $f = \sum_j a_j g_j$, donde los g_j son generadores homogéneos de I y los a_j elementos homogéneos de R. Basta agrupar los $a_j g_j$ del mismo grado para ver que cada componente de f está en I. □

Además, cumplen las siguientes propiedades:

Proposición 1.5. *Sean R un anillo graduado e I un ideal homogéneo de R. Entonces:*

1. $\mathrm{Rad}(I)$ *es homogéneo.*
2. $\mathrm{ann}(I)$ *es homogéneo.*
3. *Si I es finitamente generado, podemos tomar un sistema de generadores homogéneos finito.*

4. *I es primo si, y sólo si, para todos $f, g \in R$ homogéneos con $fg \in I$ se cumple que $f \in I$ ó $g \in I$.*

Demostración. 1. Sea $f = f_1 + ... + f_r \in \mathrm{Rad}(I)$ con f_i homogéneo y $\deg(f_i) < \deg(f_{i+1})$. Entonces existe un $n \in \mathbb{N}$ con $f^n \in I$. Por ser I homogéneo, cada componente de f^n está en I, y por ser f_1^n la de menor grado, se tiene que $f_1^n \in I$, es decir, $f_1 \in \mathrm{Rad}(I)$. Por inducción, como $f - f_1 = f_2 + ... + f_r \in \mathrm{Rad}(I)$, llegamos a que cada f_i está en $\mathrm{Rad}(I)$, por lo que este es homogéneo.

2. Sea $f = f_1 + ... + f_r \in \mathrm{ann}(I)$ con f_i homogéneo y $\deg(f_i) < \deg(f_{i+1})$, y sea $g \in I$ homogéneo. Entonces, $0 = fg = f_1g + ... + f_rg$, y $\deg(f_ig) < \deg(f_{i+1}g)$. Por tanto, $f_ig = 0$ para cada i, es decir, $f_i \in \mathrm{ann}(I)$ para cada i, por lo que $\mathrm{ann}(I)$ es homogéneo.

3. Basta tomar las componentes homogéneas de los elementos de un sistema de generadores finito.

4. La implicación hacia la derecha es trivial, veamos la otra. Sean $f, g \in R$ con $fg \in I$, $f = f_1 + ... + f_r$, $g = g_1 + ... + g_s$, con f_i homogéneo y $\deg(f_i) < \deg(f_{i+1})$, e igual para las g_i. Supongamos que $f_1, ..., f_{j-1}$, $g_1, ..., g_{k-1} \in I$, pero $f_j, g_k \notin I$, para ciertos j, k. Entonces $(f - f_1 - ... - f_{j-1})(g - g_1 - ... - g_{k-1}) = f_jg_k + ... \in I$, y como I es homogéneo y f_jg_k es la componente de menor grado, deducimos que $f_jg_k \in I$. Pero $f_i, g_k \notin I$, por lo que llegamos a una contradicción. Por tanto, $f_1, ..., f_r \in I$ y entonces $f \in I$, ó $g_1, ..., g_s \in I$ y entonces $g \in I$.

□

Observación 1.6. Con la graduación estándar, es claro que todo ideal monomial de S es homogéneo, pero no al revés. Por tanto, los resultados que obtendremos se aplican como caso particular a los ideales monomiales, que son muy importantes en Álgebra Conmutativa.

Por otra parte, también los cocientes heredarán la graduación:

Proposición 1.7. *Sea I un ideal homogéneo del anillo graduado R. Entonces:*

1. *$R_iI_j \subset I_{i+j}$.*

2. *$R/I = \bigoplus_{i\in\mathbb{N}}(R/I)_i \cong \bigoplus_{i\in\mathbb{N}}(R_i/I_i)$ (como grupos), donde $(R/I)_i \cong R_i/I_i$ y $(R/I)_i(R/I)_j \subset (R/I)_{i+j}$. Es decir, R/I adquiere de forma natural una graduación a partir de la de R.*

3. *La biyección entre los ideales de R que contienen a I y los ideales de R/I se restringe a los ideales homogéneos.*

Demostración. 1. Inmediato de $I_j \subset R_j$.

2. Como $I_i \subset R_i$ y son grupos conmutativos, podemos considerar el grupo R_i/I_i. Ahora, es bien conocido que $\bigoplus_{i\in\mathbb{N}} R_i/\bigoplus_{i\in\mathbb{N}} I_i \cong \bigoplus_{i\in\mathbb{N}}(R_i/I_i)$. Para obtener el resultado, basta tomar como $(R/I)_i$ la contraimagen por dicho isomorfismo de R_i/I_i.

3. Resulta sencillo usando sistemas de generadores homogéneos.

□

En el resto de la memoria tomaremos como R un anillo graduado de la forma S/I, con I un ideal propio homogéneo de S, considerando en S la graduación estándar y en R la obtenida en la proposición 1.7. Observemos que $S = S/0$ y 0 es un ideal homogéneo de S, por lo que S entra dentro de los anillos graduados de la forma $R = S/I$.

Por comodidad de notación, denotaremos también por $\mathfrak{m}$ al ideal $\mathfrak{m}/I$ de $R = S/I$ (nótese que si I es un ideal propio homogéneo de S, entonces $I \subset \mathfrak{m}$).

En realidad, las propiedades que iremos usando de estos anillos serán las siguientes, por lo que muchos de los resultados que veremos se podrán generalizar a anillos graduados que cumplan alguna de estas propiedades:

Proposición 1.8. *Sea $R = S/I$ con la graduación estándar. Entonces:*

1. *R es un anillo noetheriano y por tanto, cada ideal homogéneo tiene un sistema de generadores homogéneos finito.*

2. *$R_0 \cong k$ y, por tanto, todo R_i es un k-espacio vectorial (además, de dimensión finita).*

3. *$\bigoplus_{i\geq 1} R_i = \mathfrak{m}$, que es un ideal homogéneo maximal de R. De hecho, es máximo entre los ideales homogéneos propios.*

4. $R = R_0 \oplus \mathfrak{m}$.

Demostración. 1. Por el teorema de la base de Hilbert, S es noetheriano, y como los ideales de R son los cocientes de los ideales de S que contienen a I, se deduce que también están finitamente generados.

2. Sale de que $R_0 \cong S_0/I_0 = k/I_0 \cong k$, donde el primer isomorfismo en realidad es un isomorfismo de anillos, y el segundo isomorfismo sale de que $I_0 = I \cap S_0 = I \cap k = 0$, por ser I un ideal propio.

3. Se deduce de que $S = S_0 \oplus (\bigoplus_{i\geq 1} S_i) = k \oplus \mathfrak{m}$. Que sea máximo entre los ideales homogéneos se deduce de que todo ideal homogéneo propio de S está contenido en $\mathfrak{m}$ y de que la biyección entre ideales de S que contienen a I e ideales de R se restringe a ideales homogéneos.

4. Inmediato de 3.

□

1.2. Módulos graduados

Como vimos en la sección anterior, no sólo los anillos se pueden graduar, sino que sus ideales también. Como la noción de ideal de un anillo R se generaliza a la noción de R-módulo, cabe esperar que los módulos también se puedan graduar, y que dicha graduación guarde relación con la del anillo. Recordemos que estamos tomando $R = S/I$ con I homogéneo y S con su graduación estándar.

Definición 1.9. Sea M un R-módulo. Diremos que está **graduado** si existen subgrupos $\{M_i\}_{i\in\mathbb{N}}$ de M tales que

1. $M = \bigoplus_{i\in\mathbb{N}} M_i$ (como grupos), y
2. $R_i M_j \subset M_{i+j}$, $\forall i, j \in \mathbb{N}$.

M_i se denomina **componente homogénea i-ésima** de M y a sus elementos, m, **elementos homogéneos** o **formas** de grado i de M, y escribiremos $\deg(m) = i$.

Si $m \in M$, se escribe de forma única como $m = \sum_i m_i$ con $m_i \in M_i$ y $m_i = 0$ salvo para una cantidad finita. Decimos entonces que m_i es la **componente homogénea** i-ésima de m y definimos su **grado** como $\deg(m) = \text{máx}\{i/m_i \neq 0\}$.

De nuevo, de $R_0 M_i \subset M_i$ se deduce que M_i es un R_0-módulo, y como $R_0 = k$, en realidad, cada M_i es un k-espacio vectorial y la suma directa es suma directa de k-espacios vectoriales.

Y como ocurría con ideales, se tiene que:

Proposición 1.10. *Si M es un R-módulo graduado, entonces admite un sistema de generadores homogéneos, que será finito si M es finitamente generado.*

Por otro lado, podemos cambiar la graduación de un módulo graduado M, simplemente desplazando sus grados, lo cual resultará de gran utilidad en lo que veremos posteriormente.

Definición 1.11. Dada la graduación $M = \bigoplus_{i \in \mathbb{N}} M_i$, definimos la graduación de M **desplazada** o **trasladada** (**shifted** en inglés) como $M(p)$, donde $M(p)_i = M_{i+p}$. A $p \in \mathbb{Z}$ se le denomina **desfase** (**shift** en inglés).

Normalmente nos interesaremos por desplazamientos de la forma $M(-p)$, con $p > 0$. Observemos que $M(-p)_p = M_0$, es decir, si $p > 0$, los elementos homogéneos de $M(-p)$ tienen grados que van desde p "hasta ∞". Y como estamos considerando las graduaciones en $\mathbb{N}$ (grados no negativos), no surgen incoherencias si $p > 0$.

Ejemplo 1.12. El ejemplo de módulo graduado que más usaremos, y que se obtiene a partir de R mediante desplazamientos, será el módulo libre $M = R(-p_1) \oplus ... \oplus R(-p_r)$ (suma directa de R-módulos). Su graduación se define sobre la **base canónica** de R^r, $\{\mathbf{e}_1, ..., \mathbf{e}_r\}$, con $\mathbf{e}_i = (0, ..., 0, 1, 0, ..., 0)$, donde el 1 está en la posición i-ésima:

Definimos $\deg(\mathbf{e}_i) = p_i$ o, de forma equivalente,

$$M_i = \{m = \sum_{j=1}^{r} q_j \mathbf{e}_j / q_j \text{ es homogéneo y } \deg(q_j) = i - p_j\} =$$

$$= R_{i-p_1}\langle \mathbf{e}_1 \rangle \oplus ... \oplus R_{i-p_r}\langle \mathbf{e}_r \rangle,$$

donde la suma directa es suma directa de k-espacios vectoriales, y donde $R_{i-p_j}\langle \mathbf{e}_j \rangle$ denota al k-espacio vectorial formado por productos de un elemento de R_{i-p_j} por $\mathbf{e}_j$.

Por otro lado, también nos interesará considerar submódulos graduados, cocientes graduados, homomorfismos graduados, sus núcleos, etc. Todas estas cuestiones las abordamos ahora de forma concisa. Omitimos las demostraciones de las dos siguientes proposiciones, por ser similares a las de las proposiciones 1.4 y 1.7, respectivamente.

Proposición 1.13. *Sea N un submódulo de un R-módulo graduado $M = \bigoplus_{i\in\mathbb{N}} M_i$. Son equivalentes:*

1. *Si $n \in N$, entonces toda componente homogénea de n está en N.*
2. *$N = \bigoplus_{i\in\mathbb{N}} N_i$ (como grupos), donde $N_i = N \cap M_i$.*
3. *N está generado por sus elementos homogéneos.*
4. *N tiene un sistema de generadores homogéneos.*

*A todo submódulo que cumpla estas propiedades se le denomina **submódulo homogéneo** o **graduado** de M, y es un módulo graduado con la graduación heredada de M, $N = \bigoplus_{i\in\mathbb{N}} N_i$.*

Proposición 1.14. *Sea N un submódulo homogéneo del R-módulo graduado M. Entonces:*

1. *$M/N = \bigoplus_{i\in\mathbb{N}}(M/N)_i \cong \bigoplus_{i\in\mathbb{N}}(M_i/N_i)$ (como grupos), donde $(M/N)_i \cong M_i/N_i$ y $R_i(M/N)_j \subset (M/N)_{i+j}$. Es decir, M/N adquiere de forma natural una graduación a partir de la de M.*
2. *La biyección entre los submódulos de M que contienen a N y los submódulos de M/N se restringe a los submódulos homogéneos.*

Definición 1.15. Decimos que un homomorfismo $\phi : M \longrightarrow N$ entre R-módulos graduados es **graduado** de **grado** i, ó simplemente **de grado** i, si lleva elementos homogéneos en homogéneos y $\deg(\phi(m)) = i + \deg(m)$, para todo elemento homogéneo fuera de $\ker(\phi)$. Si ϕ tiene grado 0, diremos simplemente que ϕ es **graduado**. El conjunto de homomorfismos de grado i de M en N lo denotaremos por $\mathrm{Hom}_i(M, N)$.

En [**Pee**, 2.7] se ve que, aunque en general es $\bigoplus_{i\in\mathbb{N}} \mathrm{Hom}_i(M,N) \subset \mathrm{Hom}(M,N)$, si M es finitamente generado entonces se da la igualdad, es decir, $\mathrm{Hom}(M,N)$ también es un R-módulo graduado.

Ahora, una propiedad inmediata de los homomorfismos graduados es que sus núcleos, imágenes y conúcleos son homogéneos:

Proposición 1.16. *Si $\phi : M \longrightarrow N$ es un homomorfismo graduado, entonces* $\ker(\phi)$ *y* $\mathrm{Im}(\phi)$ *son submódulos homogéneos de M y N, respectivamente, y* $\mathrm{Coker}(\phi)$ *es un R-módulo graduado.*

Y para finalizar la sección, daremos unos resultados que serán fundamentales en el resto de los capítulos, y que en particular, nos dan una prueba de que si M es graduado y libre, entonces tiene una base formada por elementos homogéneos, lo que quiere decir que las graduaciones de R^n son todas de la forma $R(-p_1) \oplus \cdots \oplus R(-p_n)$.

Para ello, usaremos una versión graduada del lema de Nakayama, que no es un caso particular de [**AM**, 2.6, 2.7] (nótese que $\mathfrak{m}$ no está contenido en el radical de Jacobson de S). Sin embargo, esta versión tiene una demostración más sencilla.

Lema 1.17 (de Nakayama). *Sean J un ideal propio homogéneo de R y M un R-módulo graduado finitamente generado. Se cumple que:*

1. *Si $M = JM$, entonces $M = 0$.*
2. *Si $M = JM + N$, donde N es un submódulo homogéneo de M, entonces $M = N$.*

Demostración. Basta ver 1, pues para 2 tomamos M/N. Si $M \neq 0$, tomamos m un generador homogéneo de grado mínimo sobre M, entonces $m \in JM$, y como los elementos homogéneos de J tienen grado positivo, llegamos a la contradicción $\deg(m) > \deg(m)$. □

Teorema 1.18. *Sean M un R-módulo graduado finitamente generado y $\overline{M} = M/\mathfrak{m}M$, que es un k-espacio vectorial de dimensión p, finita. Se cumple que:*

1. *Si $\{\overline{m}_1, ..., \overline{m}_p\}$ es una base de $\overline{M}$, con m_i un elemento homogéneo de M, entonces $\{m_1, ..., m_p\}$ es un sistema minimal de generadores homogéneos de M.*

2. *Todo sistema minimal de generadores homogéneos de M se obtiene como en 1.*

3. *Todo sistema minimal de generadores homogéneos de M tiene p elementos, y de los cuales,* $\dim_k(\overline{M}_i)$ *tienen grado i.*

Demostración. 1. Se tiene que $M = \mathfrak{m}M + \langle m_1, ..., m_p\rangle$, por lo que, por el lema de Nakayama, $M = \langle m_1, ..., m_p\rangle$. Si $\{m_1, ..., m_p\}$ no fuera minimal, tendríamos $m_j = \sum_{i\neq j} a_i m_i$, y pasando al cociente, $\overline{m}_j = \sum_{i\neq j} \overline{a}_i\overline{m}_i$, lo que es absurdo.

2. Si $\{m_1, ..., m_p\}$ es un sistema minimal de generadores homogéneos de M, entonces claramente $\{\overline{m}_1, ..., \overline{m}_p\}$ genera $\overline{M}$. Si no fueran una base, habría un sistema de generadores estrictamente contenido, que al pasar a M como en 1, formarían un sistema de generadores de M estrictamente contenido en $\{m_1, ..., m_p\}$, lo que es una contradicción.

3. Inmediato de 1 y 2.

□

Finalmente, obtenemos el resultado que habíamos anticipado:

Teorema 1.19. *Sean M un R-módulo graduado libre finitamente generado y $\{m_1, ..., m_s\}$ un sistema minimal de generadores homogéneos. Entonces forma una base de M y, en particular, la aplicación $\varphi : R(-p_1) \oplus \cdots \oplus R(-p_s) \longrightarrow M$, tal que $\varphi(\mathbf{e}_i) = m_i$, es un isomorfismo de grado* 0.

Demostración. Sea $\varphi : R^s \longrightarrow M$ tal que $\varphi(\mathbf{e}_i) = m_i$, y sea $N = \ker(\varphi)$. Por el teorema anterior, se deduce que $N \subset \mathfrak{m}R^s$, pues $\{\overline{m}_1, ..., \overline{m}_s\}$ es una base del k-espacio vectorial $M/\mathfrak{m}M$, donde $s = \dim_k(M/\mathfrak{m}M) = \operatorname{rank}(M)$.

Ahora, $M \cong R^s/N$, por lo que existen $\mathbf{g}_1, ..., \mathbf{g}_s \in R^s$ tales que $\{\overline{\mathbf{g}}_1, ..., \overline{\mathbf{g}}_s\}$ forma una base del R-módulo R^s/N. Por tanto, $R^s = \langle \mathbf{g}_1, ..., \mathbf{g}_s\rangle + N = \langle \mathbf{g}_1, ..., \mathbf{g}_s\rangle + \mathfrak{m}R^s$, por lo que, por el lema de Nakayama, se deduce que $R^s = \langle \mathbf{g}_1, ..., \mathbf{g}_s\rangle$.

Por otro lado, $\langle \mathbf{g}_1, ..., \mathbf{g}_s\rangle \cap N = 0$, pues si tomamos $a_1, ..., a_s \in R$ tales que $a_1\mathbf{g}_1 + ... + a_s\mathbf{g}_s \in N$, entonces $a_1\overline{\mathbf{g}_1} + ... + a_s\overline{\mathbf{g}_s} = 0$ en el R-módulo R^s/N, de donde se deduce que $a_1 = ... = a_s = 0$. Por tanto, $R^s = \langle \mathbf{g}_1, ..., \mathbf{g}_s\rangle \oplus N$, lo que implica que $N = 0$, es decir, $\ker(\varphi) = 0$, $\{m_1, ..., m_s\}$ es una base de M y φ, el isomorfismo buscado. □

1.3. Complejos graduados

El proceso que decribimos al principio del capítulo sobre las sicigias se traducirá en una resolución libre sobre el ideal en el que estamos interesados. Por ello necesitamos introducir las resoluciones libres, que son en particular complejos de módulos. Y como queremos realizar el proceso de forma graduada, tenemos que introducir los complejos graduados de módulos. Pero para ver la motivación de todo esto, comenzaremos con la noción de sicigias y presentación de un módulo asociados a un sistema de generadores.

Definición 1.20. Sea M un R-módulo con generadores $f_1, ..., f_s \in M$. Definimos las **sicigias** del sistema de generadores $F = \{f_1, ..., f_s\}$ como todo elemento $(a_1, ..., a_s) \in R^s$ tal que $a_1 f_1 + ... + a_s f_s = 0$. Denominamos **módulo de sicigias** de F al R-módulo

$$\mathrm{Sic}(f_1, ..., f_s) = \{(a_1, ..., a_s) \in R^s / a_1 f_1 + ... + a_s f_s = 0\}.$$

Observemos que realmente $\mathrm{Sic}(f_1, ..., f_s)$ es un R-módulo, de hecho, es un submódulo de R^s. Para verlo, definimos la aplicación $\epsilon : R^s \longrightarrow M$ tal que $\epsilon(\mathbf{e}_i) = f_i$, para $i = 1, ..., s$. Entonces, se cumple que $\mathrm{Sic}(f_1, ..., f_s) = \ker(\epsilon)$.

Por otra parte, si M es graduado y $f_1, ..., f_s$ son homogéneos con $\deg(f_i) = a_i$, entonces $\epsilon : R(-a_1) \oplus ... \oplus R(-a_s) \longrightarrow M$ tiene grado 0 y $\mathrm{Sic}(f_1, ..., f_s)$ es un módulo graduado. En ese caso tenemos, por tanto, **sicigias graduadas**.

Las sicigias son entonces las relaciones lineales con coeficientes en R de los generadores de un R-módulo. Se puede sospechar, por tanto, que juegan un papel importante en la estructura de un módulo, como habíamos comentado al comienzo del capítulo. Esto viene dado por la noción de presentación:

Definición 1.21. Sea M un R-módulo con generadores $f_1, ..., f_s \in M$. Se denomina **presentación** de M respecto al sistema $F = \{f_1, ..., f_s\}$ a todo homomorfismo $\varphi : R^t \longrightarrow R^s$ tal que, si $\epsilon : R^s \longrightarrow M$ es la aplicación anterior, es decir, $\epsilon(\mathbf{e}_i) = f_i$, entonces la siguiente sucesión

$$R^t \xrightarrow{\varphi} R^s \xrightarrow{\epsilon} M \longrightarrow 0$$

es exacta, es decir, $\mathrm{Im}(\varphi) = \ker(\epsilon) = \mathrm{Sic}(f_1, ..., f_s)$. A la matriz A de φ en las bases canónicas se le denomina **matriz de la presentación**.

Si M es graduado y los $f_1, ..., f_s$ son homogéneos, llamamos **presentación graduada** de M respecto a F a toda presentación de grado 0 de la forma $\varphi : R(-b_1) \oplus ... \oplus R(-b_t) \longrightarrow R(-a_1) \oplus ... \oplus R(-a_s)$.

Observemos ahora que dar una presentación de M respecto a F consiste en dar unos generadores $G = \{\mathbf{g}_1, ..., \mathbf{g}_t\}$ del módulo $\mathrm{Sic}(f_1, ..., f_s)$, ya que entonces obtenemos una presentación $\varphi : R^t \longrightarrow R^s$ dada por $\varphi(\mathbf{e}_i) = \mathbf{g}_i$. Recíprocamente, dada una presentación $\varphi : R^t \longrightarrow R^s$, de la condición $\mathrm{Im}(\varphi) = \ker(\epsilon) = \mathrm{Sic}(f_1, ..., f_s)$ se deduce que $\{\varphi(\mathbf{e}_1), ..., \varphi(\mathbf{e}_t)\}$ es un sistema de generadores de $\mathrm{Sic}(f_1, ..., f_s)$. De hecho, las columnas de la matriz de la presentación, A, generan el módulo de sicigias.

Ahora ya podemos afirmar que los generadores de un módulo junto con sus sicigias (en resumen, una presentación de dicho módulo) determinan completamente su estructura:

Proposición 1.22. *Sean M y N dos R-módulos generados por $F = \{f_1, ..., f_s\}$ y $G = \{g_1, ..., g_s\}$, respectivamente, tales que $\varphi : R^t \longrightarrow R^s$ es una presentación de ambos respecto a F y a G. Entonces $M \cong N$. En el caso graduado el isomorfismo es de grado* 0.

Demostración. Basta observar que $M \cong R^s/\mathrm{Sic}(f_1, ..., f_s) = R^s/\mathrm{Im}(\varphi) = R^s/\mathrm{Sic}(g_1, ..., g_s) \cong N$. □

Antes de continuar, podemos preguntarnos qué relación hay entre los módulos $\mathrm{Sic}(f_1, ..., f_t)$ y $\mathrm{Sic}(g_1, ..., g_s)$, donde $\{f_1, ..., f_t\}$ y $\{g_1, ..., g_s\}$ son generadores de un mismo módulo M:

Definición 1.23. Decimos que dos R-módulos M y N son **equivalentes** si existen R-módulos libres L y L' tales que $M \oplus L \cong N \oplus L'$.

Proposición 1.24. *Sean M y N dos R-módulos generados por $F = \{f_1, ..., f_t\}$ y $G = \{g_1, ..., g_s\}$, respectivamente. Si M y N son equivalentes, entonces $\mathrm{Sic}(f_1, ..., f_t)$ y $\mathrm{Sic}(g_1, ..., g_s)$ son equivalentes. Esto ocurre en particular si $M = N$.*

Demostración. Observemos que basta considerar el caso en el que $M = N$. Es decir, basta ver que si $F = \{f_1, ..., f_t\}$ y $G = \{g_1, ..., g_s\}$ son generadores de M, entonces $\mathrm{Sic}(f_1, ..., f_t)$ y $\mathrm{Sic}(g_1, ..., g_s)$ son equivalentes.

Definimos el homomorfismo $\epsilon : R^{t+s} \longrightarrow M$ tal que $\epsilon(\mathbf{e}_i) = f_i$, si $1 \leq i \leq t$, y $\epsilon(\mathbf{e}_{j+t}) = g_j$, si $1 \leq j \leq s$. Definimos también $\eta : R^{t+s} \longrightarrow M$ tal que $\eta(\mathbf{e}_i) = f_i$, si $1 \leq i \leq t$, y $\eta(\mathbf{e}_{j+t}) = 0$, si $1 \leq j \leq s$.

Por otra parte, si $\mathbf{g}_j = \sum_{i=1}^{t} a_{ij}\mathbf{f}_i$, con $a_{ij} \in R$, entonces definimos $\varphi : R^{t+s} \longrightarrow R^{t+s}$ tal que $\varphi(\mathbf{e}_i) = \mathbf{e}_i$, si $1 \leq i \leq t$, y $\varphi(\mathbf{e}_{j+t}) = \sum_{i=1}^{t} a_{ij}\mathbf{e}_i + \mathbf{e}_{j+t}$, si $1 \leq j \leq s$. Tenemos entonces el diagrama conmutativo siguiente, donde es sencillo comprobar que φ es un isomorfismo, ya que lleva la base canónica en otra base:

$$\begin{array}{ccc} R^{t+s} & \xrightarrow{\varphi} & R^{t+s} \\ \epsilon \downarrow & & \downarrow \eta \\ M & \xrightarrow{\mathrm{Id}} & M. \end{array}$$

Por lo tanto, tomando los núcleos de ϵ y η, obtenemos que

$$\mathrm{Sic}(f_1, ..., f_t, g_1, ..., g_s) \cong \mathrm{Sic}(f_1, ..., f_t) \oplus R^s.$$

De la misma forma, obtenemos que $\mathrm{Sic}(f_1, ..., f_t, g_1, ..., g_s) \cong \mathrm{Sic}(g_1, ..., g_s) \oplus R^t$, y se concluye el resultado. □

Ahora, dados unos generadores $F = \{f_1, ..., f_s\}$ de M y una presentación $\varphi : R^t \longrightarrow R^s$, ya vimos que $G = \{g_1, ..., g_t\} = \{\varphi(\mathbf{e}_1), ..., \varphi(\mathbf{e}_t)\}$ son unos generadores de $\mathrm{Sic}(f_1, ..., f_s)$. Podemos ahora considerar una presentación $\psi : R^u \longrightarrow R^t$ de $\mathrm{Sic}(f_1, ..., f_s)$ respecto al sistema G. Esto nos da una sucesión de homomorfismos:

$$R^u \xrightarrow{\psi} R^t \xrightarrow{\varphi} R^s \xrightarrow{\epsilon} M \longrightarrow 0,$$

que verifica que $\mathrm{Im}(\psi) = \ker(\varphi)$, $\mathrm{Im}(\varphi) = \ker(\epsilon)$ y ϵ es sobreyectiva, es decir, $\mathrm{Im}(\epsilon) = \ker(0)$ en el diagrama.

Vemos que podemos iterar este proceso indefinidamente o hasta llegar al módulo cero. Este era el proceso descrito al comienzo del capítulo, y que motiva el estudio de complejos de módulos, que empezamos a continuación. Como el anillo que consideraremos en toda la sección siempre será el mismo, R, escribiremos "módulo" en vez de "R-módulo".

Definición 1.25. Un **complejo de módulos F** ó $(\mathbf{F}, d)$ es una sucesión de módulos $\{F_i\}_{i\in\mathbb{Z}}$ junto con homomorfismos $d_i : F_i \longrightarrow F_{i-1}$, llamados **diferenciales** de $\mathbf{F}$, tales que $d_{i-1}d_i = 0$:

$$\mathbf{F} \equiv ... \longrightarrow F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \longrightarrow ... \quad .$$

Diremos que es un **complejo por la izquierda** si $F_i = 0$, $\forall i < 0$. Lo llamaremos **complejo sobre** un módulo M si es un complejo por la izquierda

y existe un homomorfismo $\epsilon : F_0 \longrightarrow M$ tal que $\epsilon d_1 = 0$ (a ϵ se le llama **aumento**).

Finalmente, diremos que es un **complejo graduado** si cada F_i es graduado y cada d_i tiene grado 0 (igualmente, un complejo sobre M es gruaduado si además de ser un complejo graduado, el aumento tiene grado 0).

En general se dice que F_i es la componente de **grado homológico** i de $\mathbf{F}$, y en el caso graduado, como $F_i = \bigoplus_{j\in\mathbb{N}} F_{i,j}$, se dice que $F_{i,j}$ tiene **grado homológico** i y **grado interno** j. Como en el caso de módulos graduados, definimos el complejo **desplazado** o **trasladado** (en grado homológico) $\mathbf{F}(p)$, como aquel obtenido a partir de $\mathbf{F}$ mediante $F(p)_i = F_{p+i}$.

Como la condición $d_i d_{i+1} = 0$ es equivalente a $\mathrm{Im}(d_{i+1}) \subset \ker(d_i)$, tenemos las siguientes definiciones naturales:

Definición 1.26. Llamamos i-ésimo **módulo de homología** del complejo $\mathbf{F}$ a $H_i = H_i(\mathbf{F}) = \ker(d_i)/\mathrm{Im}(d_{i+1})$. También se definen $Z_i = Z_i(\mathbf{F}) = \ker(d_i)$, $B_i = B_i(\mathbf{F}) = \mathrm{Im}(d_{i+1})$, como los módulos de **ciclos** y **bordes**, respectivamente. Diremos que $\mathbf{F}$ es **exacto** o **acíclico** (resp. en F_i) si $H_i = 0$, para cada i (resp. para dicho i).

Por lo visto en la sección 1.2, si la diferencial d es graduada, los módulos de homología están graduados mediante la fórmula $H_i = \bigoplus_{j\in\mathbb{Z}} H_{i,j}$, con $H_{i,j} \cong Z_{i,j}/B_{i,j}$.

Por otro lado, como hemos construido nuevos objetos, que son los complejos y los complejos graduados, necesitaremos definir los morfismos entre estos objetos y sus subobjetos:

Definición 1.27. Dados dos complejos $(\mathbf{F}, d)$ y $(\mathbf{G}, \partial)$, un **homomorfismo de complejos**, $\varphi : \mathbf{F} \longrightarrow \mathbf{G}$, es una sucesión de homomorfismos $\varphi_i : F_i \longrightarrow G_i$ tales que

$$\varphi_{i-1} d_i = \partial_i \varphi_i$$

para cada $i \in \mathbb{Z}$. Si $\mathbf{F}$ y $\mathbf{G}$ son graduados, diremos que φ es **graduado** de grado $q \in \mathbb{Z}$ si cada φ_i tiene grado q (el mismo para todo i).

Teniendo en cuenta el siguiente diagrama (el cual siempre hay que tener

presente cuando tratamos con homomorfismos de complejos),

$$\begin{array}{rccccc} \mathbf{F}: & \ldots \longrightarrow & F_i & \xrightarrow{d_i} & F_{i-1} & \longrightarrow \ldots \\ & & \varphi_i \downarrow & & \downarrow \varphi_{i-1} & \\ \mathbf{G}: & \ldots \longrightarrow & G_i & \xrightarrow{\partial_i} & G_{i-1} & \longrightarrow \ldots \end{array}$$

se observa que φ_i lleva ciclos en ciclos y bordes en bordes, por lo que se puede comprobar fácilmente que está bien definida y es homomorfismo, la aplicación

$$H_i(\varphi) : H_i(\mathbf{F}) \longrightarrow H_i(\mathbf{G}) : \overline{f} \longmapsto \overline{\varphi_i(f)},$$

donde si φ tenía grado q, entonces $H_i(\varphi)$ tiene grado q.

En cuanto a los subcomplejos:

Definición 1.28. Decimos que $(\mathbf{G}, \partial)$ es un **subcomplejo** de $(\mathbf{F}, d)$ si $G_i \subset F_i$, y las inclusiones $\imath_i$ forman un homomorfismo de complejos (en otras palabras, si ∂ es la restricción de d a $\mathbf{G}$).

Ahora bien, si $\mathbf{F}$ es graduado, observemos que podemos construir los subcomplejos (como k-espacios vectoriales, no R-módulos) $\mathbf{F}_j$, cuyo k-espacio vectorial en grado homológico i es $F_{i,j}$, y cuya diferencial $d_{i,j}$ es la restricción de d_i al grado interno j. Además, como $F_i = \bigoplus_{j\in\mathbb{N}} F_{i,j}$ y $d_i = \bigoplus_{j\in\mathbb{N}} d_{i,j}$, tenemos que $\mathbf{F}$ está graduado en el sentido de que $\mathbf{F} = \bigoplus_{j\in\mathbb{N}} \mathbf{F}_j$.

A $\mathbf{F}_j$ lo llamaremos **componente homogénea** o **graduada** de grado j de $\mathbf{F}$. Claramente, por ser $H_i = \bigoplus_{j\in\mathbb{N}} H_{i,j} = \bigoplus_{j\in\mathbb{N}} H_i(\mathbf{F}_j)$, $\mathbf{F}$ será exacto si, y sólo si, cada $\mathbf{F}_j$ es exacto.

Finalmente, la última noción que nos interesará sobre complejos será la de homotopía:

Definición 1.29. Decimos que dos homomorfismos de complejos $\varphi, \psi : (\mathbf{F}, d) \longrightarrow (\mathbf{G}, \partial)$ son **homótopos**, y se escribe $\varphi \simeq \psi$, si existen homomorfismos $h_i : F_i \longrightarrow G_{i+1}$ tales que $\varphi_i - \psi_i = \partial_{i+1}h_i + h_{i-1}d_i$, $i \in \mathbb{Z}$. A la familia de homomorfismos h_i se le denomina **homotopía**.

Hay que tener siempre en cuenta el siguiente diagrama:

$$\begin{array}{ccccccccc} \ldots \longrightarrow & F_{i+1} & \longrightarrow & F_i & \xrightarrow{d_i} & F_{i-1} & \longrightarrow \ldots & \\ & & \swarrow h_i & \downarrow \varphi_i - \psi_i & \swarrow h_{i-1} & & & \\ \ldots \longrightarrow & G_{i+1} & \xrightarrow{\partial_{i+1}} & G_i & \longrightarrow & G_{i-1} & \longrightarrow \ldots & . \end{array}$$

Cuando $\mathbf{F}$, $\mathbf{G}$, φ y ψ son graduados (φ y ψ del mismo grado c), si $\varphi \simeq \psi$ mediante una homotopía h, dicha h no tiene por qué ser graduada, pero sí podemos extraer de ella otra homotopía h' entre φ y ψ que sí estará graduada, de la siguiente forma:

Definimos $h'_i : \bigoplus_{j\in\mathbb{N}} F_{i,j} \longrightarrow \bigoplus_{j\in\mathbb{N}} G_{i,j}$ como $h'_i = \sum_{j\in\mathbb{N}}(p_{i,j+c}h_i q_{i,j})$, donde $q_{i,j} : F_{i,j} \longrightarrow \bigoplus_{j\in\mathbb{N}} F_{i,j}$ es la inmersión j-ésima, y $p_{i,j} : \bigoplus_{j\in\mathbb{N}} G_{i,j} \longrightarrow G_{i,j}$ es la proyección j-ésima. Entonces claramente h'_i es un homomorfismo de grado c, y se puede comprobar fácilmente que $\varphi_i - \psi_i = \partial_{i+1}h'_i + h'_{i-1}d_i$.

Dos propiedades importantes de las homotopías son las siguientes:

Proposición 1.30. *Si $\varphi \simeq \psi$, entonces $H_i(\varphi) = H_i(\psi)$, para cada $i \in \mathbb{Z}$.*

Demostración. $H_i(\varphi) - H_i(\psi) = H_i(\varphi - \psi) = H_i(\partial_{i+1}h_i + h_{i-1}d_i) = 0$. La última igualdad se debe a que, si $x \in \ker(d_i)$, entonces $\overline{h_{i-1}d_i(x)} = \overline{0}$ y $\partial_{i+1}h_i(x) \in \mathrm{Im}(\partial_{i+1})$, es decir, $\overline{\partial_{i+1}h_i(x)} = \overline{0}$. □

Corolario 1.31. *Si* $\mathrm{Id} : \mathbf{F} \longrightarrow \mathbf{F}$ *es homótopa al homomorfismo* 0*, entonces* $\mathbf{F}$ *es exacto.*

1.4. Resoluciones libres graduadas

De entre todos los complejos, nos interesarán los que son complejos sobre un módulo M, que además estén formados por módulos libres y sean exactos. Con más precisión:

Definición 1.32. Llamamos **resolución libre** sobre un módulo (finitamente generado) M a un complejo por la izquierda $(\mathbf{F}, d)$ ($F_i = 0$ si $i < 0$), tal que cada F_i es un módulo libre finitamente generado y el complejo

$$\ldots \longrightarrow F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{\epsilon} M \longrightarrow 0$$

es exacto (en particular, ϵ es sobreyectivo y $M \cong F_0/\mathrm{Im}(d_1)$).

Si además F_i, M, d_i y ϵ son graduados (con d_i y ϵ de grado 0), entonces se llama **resolución libre graduada** de M.

Cuando tengamos un módulo finitamente generado, siempre podremos construir una resolución libre, y si es graduado, podemos construir la resolución de forma graduada. Recogemos este hecho en la siguiente proposición,

cuya demostración hay que tener en cuenta como un "algoritmo" para hallar resoluciones libres (no da un procedimiento del todo explícito, pero casi):

Teorema 1.33. *Si M es un módulo finitamente generado, entonces admite una resolución libre. Si además M es graduado, se puede construir dicha resolución de forma graduada.*

Demostración. Basta ver el caso graduado, pues el caso general es igual pero sin tener en cuenta la graduación. Lo realizaremos por inducción en $i \in \mathbb{N}$:

Para $i = 0$: Escogemos generadores homogéneos de M, $M = \langle m_1, ..., m_r \rangle$, con $\deg(m_j) = a_j$. Definimos $F_0 = R(-a_1) \oplus ... \oplus R(-a_r)$ y $\epsilon : F_0 \longrightarrow M$ utilizando la base canónica graduada de F_0: $\epsilon(\mathbf{e}_j) = m_j$. Claramente ϵ es un homomorfismo graduado de grado 0 y sobreyectivo (es decir, $F_0 \longrightarrow M \longrightarrow 0$ es una sucesión exacta).

Para $i \geq 1$: Tenemos definidos $F_0, ..., F_{i-1}$ y $\epsilon, d_0, ..., d_{i-1}$. Como F_{i-1} es un módulo noetheriano (R^n es noetheriano, ver [**AM**, 6.4]), tenemos que $\ker(d_{i-1})$ es un módulo graduado finitamente generado. Escogemos generadores homogéneos suyos, $\ker(d_{i-1}) = \langle \mathbf{f}_1, ..., \mathbf{f}_s \rangle$, donde $\deg(\mathbf{f}_j) = b_j$. Definimos $F_i = R(-b_1) \oplus ... \oplus R(-b_s)$ y $d_i : F_i \longrightarrow \ker(d_{i-1})$ utilizando igualmente la base: $d_i(\mathbf{e}_j) = \mathbf{f}_j$. De nuevo, d_i es un homomorfismo graduado sobreyectivo, y extendiéndolo a $d_i : F_i \longrightarrow F_{i-1}$, tenemos que $F_i \longrightarrow F_{i-1} \longrightarrow F_{i-2}$ es exacta (pues por construcción, $\mathrm{Im}(d_i) = \ker(d_{i-1})$). □

Podemos recordar el paso i-ésimo mediante el siguiente diagrama:

$$F_i \xrightarrow{d_i} F_{i-1} \xrightarrow{d_{i-1}} F_{i-2}.$$
$$\searrow \nearrow$$
$$\ker(d_{i-1})$$

En dicho proceso, si los generadores de M nos vienen dados, lo que debemos hacer para hallar generadores (homogéneos en el caso graduado) de cada módulo $\ker(d_i)$, es resolver los sistemas de ecuaciones lineales (en R) $d_i(\mathbf{f}) = 0$, donde d_i estará dada por una matriz (ya que es una aplicación lineal entre módulos libres).

Observemos que lo que estamos haciendo al construir una resolución libre de M es justo lo que habíamos descrito al principio: dados unos generadores (homogéneos en el caso graduado) de M, hallamos $\ker(\epsilon)$, que es el módulo

de sus "relaciones", es decir, de sus sicigias, y vamos hallando las relaciones entre los generadores de cada $\ker(d_i)$, sucesivamente.

En general, no podremos garantizar que siempre terminemos el proceso. Como ya hemos comentado, lo que garantizará el Teorema de las Sicigias de Hilbert será que hay una resolución libre que sí que termina, y que, de hecho, es más "pequeña" que el resto de resoluciones libres. Es lo que se denomina resolución libre minimal graduada, que definimos ahora (en la definición y los dos lemas siguientes, hacemos la consideración $\epsilon = d_0$, $d_{-1} = 0$ y $M = F_{-1}$):

Definición 1.34. Sean M un R-módulo graduado finitamente generado y $\mathbf{F}$ una resolución libre graduada sobre M. Decimos que $\mathbf{F}$ es **minimal** si, dada una base $\{f_1, ..., f_s\}$ de F_{i+1} formada por elementos homogéneos, las imágenes $d_{i+1}(f_1), ..., d_{i+1}(f_s) \in F_i$, forman un sistema de generadores minimal de $\ker(d_i) \subset F_i$, para cada $i \geq -1$.

Lo primero que debemos hacer es comprobar que esta definición es correcta, es decir, que no depende de la base de F_{i+1} escogida. Esto nos lo garantiza el siguiente lema:

Lema 1.35. *Sean M y N dos R-módulos graduados y $\varphi : M \longrightarrow N$ un homomorfismo graduado, donde M es libre y finitamente generado. Sean $\{f_1, ..., f_r\}$ y $\{g_1, ..., g_r\}$ dos bases de M formadas por elementos homogéneos. Si $\{\varphi(f_1), ..., \varphi(f_r)\}$ es un sistema de generadores minimal de $\mathrm{Im}(\varphi)$, entonces $\{\varphi(g_1), ..., \varphi(g_r)\}$ también lo es.*

Demostración. Supongamos que $\{\varphi(g_1), ..., \varphi(g_r)\}$ no es minimal. Podemos suponer entonces que existen $b_1, ..., b_{r-1} \in R$ tales que $\varphi(g_r) = \sum_{i=1}^{r-1} b_i \varphi(g_i)$, y sean $a_{i,j} \in R$, con $1 \leq i, j \leq r$, tales que $f_i = \sum_{j=1}^{r} a_{i,j} g_j$.

En notación matricial (usando la notación obvia, $\mathbf{m} = (m_1, ..., m_r)$ y $\varphi(\mathbf{m}) = (\varphi(m_1), ..., \varphi(m_r))$, donde $m_1, ..., m_r \in M$), si escribimos

$$\mathbf{b} = (b_1, ..., b_{r-1}, -1), \quad A = (a_{i,j}) \quad \text{y} \quad \mathbf{c} = \mathbf{b}A^{-1}$$

(A es invertible), entonces $\mathbf{b} = \mathbf{c}A$ y $c_1 a_{1,r} + ... + c_r a_{r,r} = -1$. Por tanto, existe un c_j cuya componente homogénea de grado 0 es no nula.

Como los $\varphi(f_1), ..., \varphi(f_r)$ son homogéneos, tomando las componentes homogéneas de menor grado en la expresión

$$0 = \mathbf{b} \cdot \varphi(\mathbf{g}) = \mathbf{c}A \cdot \varphi(\mathbf{g}) = \mathbf{c} \cdot \varphi(\mathbf{f}),$$

obtenemos una combinación lineal de $\varphi(f_1), ..., \varphi(f_r)$ con un coeficiente no nulo que está en $k = R_0$ (la componente de grado 0 de c_j) y podemos poner $\varphi(f_j)$ como combinación lineal del resto, por lo que $\{\varphi(f_1), ..., \varphi(f_r)\}$ no es minimal, en contradicción con el enunciado. □

Y ahora, tenemos la siguiente caracterización, que será la que nos interesará en muchos casos:

Lema 1.36. *Una resolución libre graduada* $\mathbf{F}$ *de* M *(finitamente generado) es minimal si, y sólo si,* $\ker(d_i) = d_{i+1}(F_{i+1}) \subset \mathfrak{m}F_i$*, para cada* $i \in \mathbb{N}$ *(recordemos que* $\mathfrak{m} = \langle x_1, ..., x_n \rangle$*).*

Demostración. Supongamos que para un cierto $i \geq -1$, existe un elemento homogéneo $g \in \ker(d_{i+1})$ que no está en $\mathfrak{m}F_{i+1}$, por lo que es de la forma $g = f_r - \sum_{j \neq r} q_j f_j$, donde los q_j son homogéneos y $\{f_1, ..., f_r\}$ una base de F_{i+1} formada por elementos homogéneos. Entonces, $d_{i+1}(f_r) = \sum_{j \neq r} q_j d_{i+1}(f_j)$, es decir, los elementos $d_{i+1}(f_j)$ no forman un sistema minimal de generadores homogéneos de $\ker(d_i)$.

Recíprocamente, supongamos que para cierto $i \geq -1$, los $d_{i+1}(f_j)$ forman un sistema de generadores homogéneos de $\ker(d_i)$, pero no minimal, donde $\{f_1, ..., f_r\}$ es como antes. Entonces, podemos suponer que $d_{i+1}(f_r) = \sum_{j \neq r} q_j d_{i+1}(f_j)$. Por tanto, $f = f_r - \sum_{j \neq r} q_j f_j$ está en $\ker(d_{i+1})$, pero no en $\mathfrak{m}F_{i+1}$. □

Como comentamos antes, las resoluciones libres minimales graduadas serán las más "pequeñas" entre todas las resoluciones libres graduadas de un módulo graduado M. En particular, esto supondrá que, salvo isomorfismo de complejos, sólo habrá una resolución libre minimal graduada. Esto es lo que detallamos con más precisión en la siguiente definición y el siguiente teorema:

Definición 1.37. Llamamos **complejo trivial corto** (graduado) a todo aquel de la forma $0 \longrightarrow R(-p) \xrightarrow{\mathrm{Id}} R(-p) \longrightarrow 0$, $p \geq 0$. Y llamamos **complejo trivial** a todo aquel que sea suma directa de complejos triviales cortos, donde la suma directa de complejos $\{(\mathbf{F}_\alpha, d_\alpha)\}_{\alpha \in A}$ se define como el complejo $\mathbf{F}$ tal que $F_i = \bigoplus_{\alpha \in A} F_{\alpha,i}$, y $d_i = \bigoplus_{\alpha \in A} d_{\alpha,i}$.

Teorema 1.38 (**de unicidad de la resolución minimal**)**.** *Sea* M *un* R*-módulo graduado finitamente generado:*

1. *Si* $\mathbf{F}$ *es una resolución libre minimal graduada de* M*, y* $\mathbf{G}$ *es otra resolución libre graduada de* M *(minimal o no), entonces existe un complejo trivial* $\mathbf{T}$ *tal que* $\mathbf{G} \cong \mathbf{F} \oplus \mathbf{T}$ *(donde el isomorfismo es de grado* 0*).*

2. *Dos resoluciones libres minimales graduadas de* M *son isomorfas y además mediante un isomorfismo de grado* 0*.*

Demostración. El apartado 2 se deduce inmediatamente del 1, el cual no demostraremos aquí por ser la demostración larga y técnica. Ver [**Pee**, Section 9], que a su vez requiere [**Pee**, Section 6]. □

Por tanto, para cada R-módulo graduado M finitamente generado, por 1.33 existe una resolución libre minimal graduada de M, y por 1.38, ésta es única. Además, por cómo se ha definido, nos da una descripción de "cómo es la estructura" del módulo M sin ninguna información "extra", ya que lo que hacemos en cada paso i de la resolución es tomar un sistema minimal de generadores homogéneos del módulo de relaciones o sicigias i-ésimas.

Antes de pasar a la siguiente sección, hacemos una observación sencilla pero que tendrá importancia en capítulos posteriores:

Proposición 1.39. *Sea* I *un ideal de* R*. Entonces,*

$$... \longrightarrow F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \longrightarrow ... \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{\epsilon} I \longrightarrow 0$$

es una resolución libre sobre I *si, y sólo si,*

$$... \longrightarrow F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \longrightarrow ... \longrightarrow F_0 \xrightarrow{\epsilon} R \longrightarrow R/I \longrightarrow 0$$

es una resolucion libre sobre R/I*, donde el último homomorfismo es el paso al cociente.*

En el caso graduado, con las graduaciones estándar en R*,* I *y* R/I*, una resolución es minimal graduada si, y sólo si, lo es la otra.*

Demostración. Es consecuencia directa de que $\mathrm{Im}(\epsilon) = I$ y el núcleo del paso al cociente también es I. □

1.5. Sicigias e invariantes

Aunque ya hayamos definido las sicigias de un sistema de generadores de un R-módulo, un caso especial serán las de un sistema minimal de generadores homogéneos. La ventaja de este caso particular será que dichos módulos de sicigias vienen dados por la resolución libre minimal graduada del módulo, por definición. Definiremos también algunos invariantes y, al final de la sección, para concluir el capítulo, enunciamos el Teorema de las Sicigias de Hilbert.

A lo largo de esta sección, M será un R-módulo graduado finitamente generado y $\mathbf{F}$ su resolución libre minimal graduada.

Definición 1.40. Llamamos i-ésimo **módulo de sicigias** de M al submódulo $\mathrm{Sic}_i(M) = \ker(d_{i-1}) = \mathrm{Im}(d_i) \subset F_{i-1}$, para $i > 0$. Se define también $\mathrm{Sic}_0(M) = M$. Se llaman simplemente **sicigias** i-ésimas a los elementos de $\mathrm{Sic}_i(M) \subset F_{i-1}$.

Lo primero que hay que tener en cuenta es que, según el convenio de índices que hemos adoptado, $\mathrm{Sic}_i(M)$ es un submódulo de F_{i-1}, y no de F_i.

Por otro lado, tenemos el siguiente par de propiedades inmediatas de las sicigias:

Lema 1.41. *1.* $\ldots \longrightarrow F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} \mathrm{Sic}_i(M) \longrightarrow 0$ *es la resolución libre minimal graduada de* $\mathrm{Sic}_i(M)$.

2. $\mathrm{Sic}_i(\mathrm{Sic}_j(M)) = \mathrm{Sic}_{i+j}(M)$.

Ahora pasamos a definir los invariantes de las resoluciones libres graduadas de M:

Definición 1.42. Se definen:

1. **Números de Betti**: De M sobre R son los números $b_i^R(M) = \mathrm{rank}(F_i)$.
2. **Números de Betti graduados**: De M sobre R son los números $b_{i,p}^R(M) = c_{i,p}$, donde $F_i = \bigoplus_{p\in\mathbb{N}} R(-p)^{c_{i,p}}$ ($b_{i,p}^R(M) < \infty$ pues F_i es finitamente generado).
3. **Dimensión proyectiva**: De M sobre R es $\mathrm{dp}_R(M) = \max\{i \in \mathbb{N} / b_i^R(M) \neq 0\}$.

Si el contexto nos dice cuál es el anillo R, pondremos simplemente $b_i(M)$, $\mathrm{dp}(M)$ y $b_{i,p}(M)$.

Observación 1.43. Para resoluciones libres cualesquiera de M, $\mathbf{G}$, se suele definir su longitud como $\mathrm{long}(\mathbf{G}) = \mathrm{máx}\{i \in \mathbb{N}/G_i \neq 0\}$. Por tanto, en particular, $\mathrm{dp}_R(M) = \mathrm{long}(\mathbf{F})$. Igualmente, podríamos haber definido sus números de Betti como $\mathrm{rank}(G_i)$, y análogamente la versión graduada.

Observación 1.44. También hay que tener en cuenta que, si $i \geq 0$,

$$b_i^R(M) = \sum_{p=0}^{\infty} b_{i,p}^R(M).$$

Una propiedad interesante de los números de Betti graduados es la siguiente:

Proposición 1.45. *Sea $c = \mathrm{mín}_j \deg(m_j)$, donde $m_1, ..., m_r$ es un sistema minimal de generadores homogéneos de M (por 1.18, dicho c no depende del sistema minimal elegido). Entonces, $b_{i,p}^R(M) = 0$, siempre que $p < i + c$.*

Demostración. Lo haremos por inducción en i (grado homológico).

Para $i = 0$: Como $\epsilon(\mathbf{e}_j) = m_j$, está claro que $\deg(\mathbf{e}_j) = \deg(m_j)$, por lo que F_0 no tiene elementos de grado menor que c, es decir, $b_{0,p}^R(M) = 0$, si $p < c$.

Suponiendo que se cumple para $i \geq 0$, veámoslo para $i + 1$: Por ser la resolución minimal, tenemos que los $d_{i+1}(\mathbf{e}_j)$ forman un sistema minimal de generadores homogéneos de $\ker(d_i) \subset \mathfrak{m}F_i$. Por tanto, como los elementos homogéneos de F_i tienen grado $p \geq i + c$, entonces los $\mathbf{e}_j$ tienen grados $p \geq i + 1 + c$. Es decir, F_{i+1} no tiene elementos de grado $p < i + 1 + c$. □

Observación 1.46. Se suele denotar por $\mathrm{mín}(M)$ al número c de la proposición anterior, es decir, $\mathrm{mín}(M) = \mathrm{mín}_j \deg(m_j)$, y también se define $\mathrm{máx}(M) = \mathrm{máx}_j \deg(m_j)$. Como antes, ni $\mathrm{máx}(M)$ ni $\mathrm{mín}(M)$ dependen del sistema minimal de generadores homogéneos, por 1.18. Por tanto, la proposición anterior se puede escribir como $b_{i,p}^R(M) = 0$, $\forall p < i + \mathrm{mín}(M)$.

Finalmente, enunciamos el Teorema de las Sicigias de Hilbert. Damos primero la versión no graduada y después la graduada:

Teorema 1.47 (**De las Sicigias de Hilbert**). *Tomando $S = k[x_1, ..., x_n]$, todo S-módulo finitamente generado M admite una resolución libre finita de longitud a lo sumo n.*

Teorema 1.48 (**De las Sicigias de Hilbert, versión graduada**). *Tomando $S = k[x_1, ..., x_n]$, y M un S-módulo graduado finitamente generado, se verifica que*

$$\mathrm{dp}_S(M) \leq n.$$

Capítulo 2

Una demostración homológica del Teorema de las Sicigias

En este segundo capítulo daremos una demostración del Teorema de las Sicigias utilizando herramientas de Álgebra Homológica.

Una de ellas será el **funtor Tor** (en lenguaje homológico, será el funtor derivado del funtor "tensorizar", aunque no entraremos en detalles sobre esto), que nos permitirá considerar una resolución libre minimal graduada del módulo $k = S/\mathfrak{m}$ sobre S (o del ideal $\mathfrak{m}$, por 1.39), en lugar de una resolución libre minimal graduada del módulo en cuestión que estamos considerando.

Seguidamente, construiremos dicha resolución libre minimal graduada de k sobre S, que será el **complejo de Koszul** sobre $x_1, ..., x_n$. Utilizaremos que los números de Betti se pueden escribir en términos de Tor, y como podremos considerar el complejo de Koszul, obtendremos como cota superior de dp_S la dimensión proyectiva de k sobre S, que será n. Esto concluirá la demostración del teorema.

Para el desarrollo de este capítulo, necesitaremos unos preliminares de Álgebra Homológica, que iremos desarrollando en cada sección. Algunos no los demostraremos, por brevedad, pero se pueden encontrar en cualquier libro sobre el tema, por ejemplo, en [**Wei**].

2.1. El homomorfismo conector

Un hecho crucial en Álgebra Homológica es que una sucesión exacta corta de complejos da lugar a una sucesión exacta larga de módulos, mediante los módulos de homología y un homomorfismo especial, llamado **homomorfismo conector**. Todo ello vendrá dado por el famoso **lema de la serpiente**. Para nuestros propósitos, no necesitaremos considerar el caso graduado en esta sección.

Definición 2.1. Una **sucesión exacta corta** (de módulos o de complejos) será un complejo exacto de la forma

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0.$$

Aunque no lo hayamos hecho, claramente podemos considerar complejos de complejos y decir cuándo estos son exactos, de la misma forma que con módulos. Basta definir el núcleo e imagen de un homomorfismo de complejos como el complejo formado por los núcleos e imágenes de cada homomorfismo de módulos (con diferenciales las restricciones de las diferenciales correspondientes).

Según esto, observemos que una sucesión de complejos $0 \longrightarrow \mathbf{F} \xrightarrow{f} \mathbf{F}' \xrightarrow{g} \mathbf{F}'' \longrightarrow 0$ es exacta corta si, y sólo si, cada sucesión $0 \longrightarrow F_i \xrightarrow{f_i} F_i' \xrightarrow{g_i} F_i'' \longrightarrow 0$ es exacta corta.

Lema 2.2 (**de la serpiente**). *Dado un diagrama conmutativo de R-módulos de la forma siguiente, con las filas exactas,*

$$\begin{array}{ccccccccc} & & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C', & & \end{array}$$

existe un homomorfismo $\tau : \ker(h) \longrightarrow \mathrm{Coker}(f)$ tal que la siguiente sucesión es exacta:

$$\ker(f) \longrightarrow \ker(g) \longrightarrow \ker(h) \xrightarrow{\tau} \mathrm{Coker}(f) \longrightarrow \mathrm{Coker}(g) \longrightarrow \mathrm{Coker}(h)$$

(los otros homomorfismos de este diagrama son las restricciones y pasos al cociente de los homomorfismos de las filas en el primer diagrama).

Demostración. Daremos la definición de τ. Escogemos $x \in \ker(h)$, por la exactitud de la primera fila, existe $y \in B$ contraimagen de x. Se tiene que la imagen de $g(y)$ en C' es 0, y por exactitud de la segunda fila, existe $z \in A'$ contraimagen de $g(y)$. Definimos $\tau(x) = \overline{z}$.

La comprobación de que τ está bien definida, es homomorfismo, y la sucesión citada es exacta es lo que se suele denominar una "cacería de diagramas", sólo requiere seguir el diagrama. Omitimos los detalles por brevedad. Conviene tener en mente el diagrama siguiente:

$$\begin{array}{ccccccccc} & & \ker(f) & \longrightarrow & \ker(g) & \longrightarrow & \ker(h) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \mathrm{Coker}(f) & \longrightarrow & \mathrm{Coker}(g) & \longrightarrow & \mathrm{Coker}(h). & & \end{array}$$

□

Teorema 2.3 (**Sucesión exacta larga de homología**). *Dada una sucesión exacta corta de complejos*

$$0 \longrightarrow \mathbf{F} \xrightarrow{f} \mathbf{F}' \xrightarrow{g} \mathbf{F}'' \longrightarrow 0,$$

existen homomorfismos $\tau_i : H_i(\mathbf{F}'') \longrightarrow H_{i-1}(\mathbf{F})$ tales que la siguiente sucesión de módulos es exacta:

$$\ldots \longrightarrow H_{i+1}(\mathbf{F}'') \xrightarrow{\tau_{i+1}} H_i(\mathbf{F}) \xrightarrow{H_i(f)} H_i(\mathbf{F}') \xrightarrow{H_i(g)} H_i(\mathbf{F}'') \xrightarrow{\tau_i} H_{i-1}(\mathbf{F}) \longrightarrow \ldots \quad .$$

A τ se le denomina ***homomorfismo conector****.*

Demostración. Vamos a utilizar la notación de la definición 1.26 y aplicaremos el lema de la serpiente dos veces. Consideramos primero, para cada i, el diagrama siguiente

$$\begin{array}{ccccccccc} & & F_i & \xrightarrow{f} & F'_i & \xrightarrow{g} & F''_i & \longrightarrow & 0 \\ & & \downarrow d & & \downarrow d' & & \downarrow d'' & & \\ 0 & \longrightarrow & F_{i-1} & \xrightarrow{f} & F'_{i-1} & \xrightarrow{g} & F''_{i-1}. & & \end{array}$$

De donde deducimos, por el lema, que las filas del siguiente diagrama son exactas para cada i:

$$\begin{array}{ccccccccc} & & F_i/B_i & \xrightarrow{f} & F'_i/B'_i & \xrightarrow{g} & F''_i/B''_i & \longrightarrow & 0 \\ & & \downarrow d & & \downarrow d' & & \downarrow d'' & & \\ 0 & \longrightarrow & Z_{i-1} & \xrightarrow{f} & Z'_{i-1} & \xrightarrow{g} & Z''_{i-1}. & & \end{array}$$

pues la segunda fila es la sucesión de núcleos de d_{i-1}, d'_{i-1} y d''_{i-1} (donde además f_i es inyectiva, $\forall i$), y la primera fila es la sucesión de conúcleos de d_i, d'_i y d''_i (donde además g_i es sobreyectiva, $\forall i$). De nuevo, aplicando el lema, obtenemos la sucesión exacta

$$H_i(\mathbf{F}) \xrightarrow{H_i(f)} H_i(\mathbf{F}') \xrightarrow{H_i(g)} H_i(\mathbf{F}'') \xrightarrow{\tau_i} H_{i-1}(\mathbf{F}) \xrightarrow{H_{i-1}(f)} H_{i-1}(\mathbf{F}') \xrightarrow{H_{i-1}(g)} H_{i-1}(\mathbf{F}'').$$

Y basta unir cada una de estas sucesiones.

Por otro lado, ahora τ_i viene dado de la siguiente forma:

Cogemos la clase $\overline{x} \in H_i(\mathbf{F}'')$, existe un $y \in F'_i$ con $g(y) = x$. Se tiene que $g(d'(y)) = 0$ y, por tanto, existe un $z \in F_{i-1}$ tal que $f(z) = d'(y)$. Finalmente, se tiene que $d(z) = 0$ y se define $\tau_i(\overline{x}) = \overline{z}$. El siguiente diagrama puede ayudar a visualizarlo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_i & \xrightarrow{f} & F'_i & \xrightarrow{g} & F''_i & \longrightarrow & 0 \\ & & \downarrow d & & \downarrow d' & & \downarrow d'' & & \\ 0 & \longrightarrow & F_{i-1} & \xrightarrow{f} & F'_{i-1} & \xrightarrow{g} & F''_{i-1} & \longrightarrow & 0 \\ & & \downarrow d & & \downarrow d' & & \downarrow d'' & & \\ 0 & \longrightarrow & F_{i-2} & \xrightarrow{f} & F'_{i-2} & \xrightarrow{g} & F''_{i-2} & \longrightarrow & 0. \end{array}$$

También podríamos haber definido así los homomorfismos conectores τ_i y haber demostrado directamente el teorema, sin pasar por el lema de la serpiente. En realidad, estaríamos haciendo lo mismo. □

Un corolario inmediato, que es una de las primeras consecuencias fundamentales del teorema, es el siguiente:

Corolario 2.4. *Dada una sucesión exacta corta de complejos como en el teorema anterior, si dos son exactos, el otro también lo es.*

Observemos que si lo que nos interesa es mirar la exactitud de una resolución, no nos importa tanto considerar homomorfismos graduados, pues lo que nos interesa es saber cuándo los módulos de homología se anulan.

2.2. El funtor Tor

En esta sección introduciremos de la forma más elemental posible el funtor Tor. Para ello, haremos uso de algunas propiedades del producto tensorial, las cuales no demostraremos (se pueden consultar en [**AM**, Capítulo 2] o cualquier libro de Álgebra Conmutativa).

Empezamos con un lema que nos será de utilidad:

Lema 2.5 (**de elevación**). *Sean M y N dos R-módulos, $f : M \longrightarrow N$ un homomorfismo, y sean $(\mathbf{F}, d)$ y $(\mathbf{G}, \partial)$ resoluciones libres sobre M y N con aumentos ϵ y η, respectivamente (ver la definición 1.25). Entonces:*

1. *Existe un homomorfismo de complejos $\varphi : \mathbf{F} \longrightarrow \mathbf{G}$ que extiende a f, es decir, tal que $f\epsilon = \eta\varphi_0$.*

2. *Si $\psi : \mathbf{F} \longrightarrow \mathbf{G}$ es otro que cumple lo mismo, entonces $\varphi \simeq \psi$.*

Además, si M, N, $\mathbf{F}$, $\mathbf{G}$ son graduados y f, ψ son graduados de grado q, φ y la homotopía se pueden elegir de grado q.

Demostración. Como se verá a lo largo de la demostración, no es necesario que M y N sean finitamente generados, ni que el complejo $\mathbf{F}$ sea exacto, ni que los G_i sean libres. Lo haremos por inducción en el grado homológico.

1. Para $i = 0$: Tengamos presente el diagrama:

$$\begin{array}{ccccccccc} \ldots & \longrightarrow & F_1 & \xrightarrow{d_1} & F_0 & \xrightarrow{\epsilon} & M & \longrightarrow & 0 \\ & & & & \downarrow \varphi_0 & & \downarrow f & & \\ \ldots & \longrightarrow & G_1 & \xrightarrow{\partial_1} & G_0 & \xrightarrow{\eta} & N & \longrightarrow & 0. \end{array}$$

   Tomamos una base de F_0, $\{m_1, ..., m_r\}$ (graduada en el caso graduado), y contraimágenes $n_j \in G_0$ de $f(\epsilon(m_j))$ a través de η (η es sobreyectiva). Definimos entonces $\varphi_0(m_j) = n_j$ y extendemos φ_0 por linealidad. Claramente, $\eta\varphi_0 = f\epsilon$, y en el caso graduado, φ_0 tiene grado q si f tiene grado q.

Para $i \geq 1$: Supongamos que tenemos definidos $\varphi_0, ..., \varphi_{i-1}$ como en el enunciado. Tengamos de nuevo presente el diagrama:

$$\begin{array}{ccccccccc} ... & \longrightarrow & F_i & \xrightarrow{d_i} & F_{i-1} & \xrightarrow{d_{i-1}} & F_{i-2} & \longrightarrow & ... \\ & & \downarrow \varphi_i & & \downarrow \varphi_{i-1} & & \downarrow \varphi_{i-2} & & \\ ... & \longrightarrow & G_i & \xrightarrow{\partial_i} & G_{i-1} & \xrightarrow{\partial_{i-1}} & G_{i-2} & \longrightarrow & ... \quad . \end{array}$$

Tomamos de nuevo una base de F_i, $\{m_1, ..., m_s\}$ (graduada en el caso graduado). Se cumple que

$$\partial_{i-1}\varphi_{i-1}d_i(m_j) = \varphi_{i-2}d_{i-1}d_i(m_j) = 0,$$

por lo que $\varphi_{i-1}d_i(m_j) \in \ker(\partial_{i-1})$. Por exactitud, existe $n_j \in G_i$ tal que $\partial_i(n_j) = \varphi_{i-1}d_i(m_j)$. Definimos entonces $\varphi_i(m_j) = n_j$ y extendemos φ_i por linealidad. Como antes, se verifica que $\varphi_{i-1}d_i = \partial_i\varphi_i$, y en el caso graduado, φ_i tiene grado q si $f, \varphi_0, ..., \varphi_{i-1}$ tienen grado q.

2. Observemos que basta considerar el caso $f = 0$ y $\varphi = 0$, ya que en el caso general, $\varphi - \psi$ y 0 elevan al homomorfismo 0 y encontrar una homotopía entre φ y ψ es lo mismo que entre $\varphi - \psi$ y 0.

   Para $i = 0$: Ahora el diagrama que consideramos es:

$$\begin{array}{ccccccccc} ... & \longrightarrow & F_1 & \xrightarrow{d_1} & F_0 & \xrightarrow{\epsilon} & M & \longrightarrow & 0 \\ & & & \swarrow h_0 & \downarrow \psi_0 & \swarrow 0 & \downarrow 0 & & \\ ... & \longrightarrow & G_1 & \xrightarrow{\partial_1} & G_0 & \xrightarrow{\eta} & N & \longrightarrow & 0. \end{array}$$

   Volvemos a tomar la base $\{m_1, ..., m_r\}$ de F_0. Como $\eta\psi_0(m_j) = 0$, por exactitud, existe $x_j \in G_1$ tal que $\partial_1(x_j) = \psi_0(m_j)$. Definimos entonces $h_0(m_j) = x_j$ y extendemos h_0 por linealidad. Se verifica que $\psi_0 = \partial_1 h_0$ y que h_0 tiene grado q en el caso graduado.

   Para $i \geq 1$: Supongamos que tenemos definidos $h_0, ..., h_{i-1}$. Consideramos el diagrama:

$$\begin{array}{ccccccccc} ... & \longrightarrow & F_{i+1} & \xrightarrow{d_{i+1}} & F_i & \xrightarrow{d_i} & F_{i-1} & \longrightarrow & ... \\ & & \downarrow \psi_{i+1} & \swarrow h_i & \downarrow \psi_i & \swarrow h_{i-1} & \downarrow \psi_{i-1} & & \\ ... & \longrightarrow & G_{i+1} & \xrightarrow{\partial_{i+1}} & G_i & \xrightarrow{\partial_i} & G_{i-1} & \longrightarrow & ... \quad . \end{array}$$

   Tomamos de nuevo la base $\{m_1, ..., m_s\}$ de F_i. Como

$$\partial_i(\psi_i - h_{i-1}d_i)(m_j) = (\psi_{i-1} - \partial_i h_{i-1} - h_{i-2}d_{i-1})d_i(m_j) = 0,$$

entonces por exactitud, existe $x_j \in G_{i+1}$ tal que $\partial_{i+1}(x_j) = (\psi_i - h_{i-1}d_i)(m_j)$. Definimos entonces $h_i(m_j) = x_j$ y extendemos h_j por linealidad. Se verifica que $\psi_i = \partial_{i+1}h_i + h_{i-1}d_i$ y que h_i tiene grado q en el caso graduado.

□

El siguiente corolario inmediato es lo que nos interesará más adelante para definir Tor. Veamos la similitud con el teorema 1.38. En aquel caso obteníamos que todas las resoluciones libres minimales graduadas de un módulo graduado (finitamente generado) son isomorfas. Ahora vemos que lo mismo ocurre para todas las resoluciones libre de un módulo (finitamente generado) M, pero sólo en los módulos de homología.

Corolario 2.6. *Sean* $\mathbf{F}$ *y* $\mathbf{G}$ *dos resoluciones libres de un R-módulo* M*. Entonces existen homomorfismos de complejos* $\varphi : \mathbf{F} \longrightarrow \mathbf{G}$ *y* $\psi : \mathbf{G} \longrightarrow \mathbf{F}$ *que extienden a la identidad en* M *y tales que* $\psi\varphi \simeq \mathrm{Id}_{\mathbf{F}}$ *y* $\varphi\psi \simeq \mathrm{Id}_{\mathbf{G}}$*. En el caso graduado,* φ*,* ψ *y las homotopías se pueden definir graduadas de grado* 0*.*

Ahora, utilizando la propiedad universal del producto tensorial, definiremos productos tensoriales de homomorfismos y veremos que de esta forma podremos formar un complejo mediante productos tensoriales, que será lo que utilizaremos para definir Tor. Incluimos antes, por completitud, la propiedad universal del producto tensorial, que se puede consultar en [**AM**, 2.12]:

Teorema 2.7. *Dados R-módulos* $M_1, ..., M_r$*, existe un R-módulo* $M_1 \otimes ... \otimes M_r$ *y una aplicación multilineal* $\bigotimes : M_1 \times ... \times M_r \longrightarrow M_1 \otimes ... \otimes M_r$ *tales que:*

1. *Para todo R-módulo* N *y toda aplicación multilineal* $f : M_1 \times ... \times M_r \longrightarrow N$*, existe un único homomorfismo* $\overline{f} : M_1 \otimes ... \otimes M_r \longrightarrow N$ *tal que* $f = \overline{f} \bigotimes$*.*
2. *Si* T *es otro R-módulo junto con una aplicación multilineal* $t : M_1 \times ... \times M_r \longrightarrow T$ *que cumplen la propiedad 1, entonces existe un único isomorfismo* $\Phi : M_1 \otimes ... \otimes M_r \longrightarrow T$ *tal que* $\Phi \bigotimes = t$*.*

Lema 2.8. *Dados homomorfismos de R-módulos* $f : M \longrightarrow P$ *y* $g : N \longrightarrow Q$*, existe un único homomorfismo, que denotaremos por* $f \otimes g : M \otimes N \longrightarrow P \otimes Q$*, tal que* $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ *para todos* $m \in M$*,* $n \in N$*.*

Demostración. Definimos la aplicación bilineal $f \times g : M \times N \longrightarrow P \otimes Q$ dada por $(f \times g)(m, n) = f(m) \otimes g(n)$. Por la propiedad universal del producto tensorial, existe un único homomorfismo $f \otimes g : M \otimes N \longrightarrow P \otimes Q$ tal que $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ para todos $m \in M$, $n \in N$. □

Observación 2.9. Si M y N son R-módulos graduados, entonces $M \otimes N$ es graduado por la graduación

$$(M \otimes N)_k = \bigoplus_{i+j=k} (M_i \otimes N_j),$$

pues $M \otimes N \cong \bigoplus_{i,j}(M_i \otimes N_j)$ (ver [**AM**, 2.14]). Si además estamos en la situación del lema anterior y P, Q, f y g también son graduados con f y g de grados q_1 y q_2, respectivamente, entonces $f \otimes g$ también es un homomorfismo de grado $q_1 + q_2$.

Lema 2.10. *Sean M y N dos R-módulos, y sea $(\mathbf{F}, d)$ un complejo sobre M con aumento ϵ. Entonces las aplicaciones $d_i \otimes \mathrm{Id} : F_i \otimes N \longrightarrow F_{i-1} \otimes N$ $(i > 0)$ forman el siguiente complejo:*

$$\mathbf{F}\otimes N \equiv ... \longrightarrow F_{i+1}\otimes N \xrightarrow{d_{i+1}\otimes \mathrm{Id}} F_i \otimes N \xrightarrow{d_i \otimes \mathrm{Id}} F_{i-1}\otimes N \longrightarrow ... \longrightarrow F_0 \otimes N \longrightarrow 0$$

sobre $M \otimes N$ con aumento $\epsilon \otimes \mathrm{Id}$.

Si además M, N y $(\mathbf{F}, d)$ son graduados (con aumento ϵ graduado), entonces $\mathbf{F} \otimes N$ también es graduado con aumento $\epsilon \otimes \mathrm{Id}$ de grado 0.

Demostración. Es inmediato, pues los $f \otimes n$, donde $f \in F_i$, $n \in N$, generan $F_i \otimes N$, y se verifica que

$$(d_{i-1} \otimes \mathrm{Id})(d_i \otimes \mathrm{Id})(f \otimes n) = (d_{i-1}d_i(f)) \otimes n = 0 \otimes n = 0.$$

El caso graduado es consecuencia de la observación anterior. □

Lema 2.11. *Sean M y N dos R-módulos. Si $(\mathbf{F}, d)$ y $(\mathbf{G}, \partial)$ son dos resoluciones libres de M, entonces existen homomorfismos de complejos $\varphi : \mathbf{F} \longrightarrow \mathbf{G}$ y $\psi : \mathbf{G} \longrightarrow \mathbf{F}$ que extienden a la identidad en M y tales que*

$$(\psi \otimes \mathrm{Id})(\varphi \otimes \mathrm{Id}) \simeq \mathrm{Id}_{\mathbf{F}\otimes N} \quad y \quad (\varphi \otimes \mathrm{Id})(\psi \otimes \mathrm{Id}) \simeq \mathrm{Id}_{\mathbf{G}\otimes N}.$$

Si además M, N, $(\mathbf{F}, d)$ y $(\mathbf{G}, \partial)$ son graduados, las homotopías se pueden elegir graduadas.

Demostración. Por 2.6, obtenemos dichos $\varphi : \mathbf{F} \longrightarrow \mathbf{G}$ y $\psi : \mathbf{G} \longrightarrow \mathbf{F}$ tales que $\psi\varphi \simeq \mathrm{Id}_{\mathbf{F}}$ y $\varphi\psi \simeq \mathrm{Id}_{\mathbf{G}}$. Ahora basta considerar sus productos tensoriales, y los de las homotopías respectivas, con $\mathrm{Id} : N \longrightarrow N$. El caso graduado vuelve a ser consecuencia de la observación anterior. □

Estos dos últimos lemas nos garantizan que la siguiente definición es consistente, salvo isomorfismo:

Definición 2.12. Dados M y N dos R-módulos y $(\mathbf{F}, d)$ una resolución libre de M, definimos $\mathrm{Tor}_i^R(M,N) = H_i(\mathbf{F} \otimes N)$ para $i \geq 0$. Cuando el contexto nos indique cuál es el anillo R que estamos considerando, escribiremos simplemente $\mathrm{Tor}_i(M,N)$.

Si M y N son graduados, entonces $\mathrm{Tor}_i^R(M,N)$ también es graduado, y pondremos $\mathrm{Tor}_i^R(M,N) = \bigoplus_{p\in\mathbb{N}} \mathrm{Tor}_i^R(M,N)_p$.

Las propiedades básicas de Tor que serán de interés para nuestros propósitos son las siguientes:

Proposición 2.13. *Sean M y N dos R-módulos. Entonces:*

1. $\mathrm{Tor}_0^R(M,N) \cong M \otimes N$.
2. $\mathrm{Tor}_i^R(M,N) \cong \mathrm{Tor}_i^R(N,M)$, *para todo* $i \geq 0$.

Demostración. 1. Del hecho de que $- \otimes_R N$ es un funtor exacto por la derecha (ver [**AM**, 2.18]), obtenemos que la sucesión

$$F_1 \otimes N \xrightarrow{d_1\otimes \mathrm{Id}} F_0 \otimes N \xrightarrow{\epsilon\otimes \mathrm{Id}} M \otimes N \longrightarrow 0$$

es exacta, de donde se deduce que $\mathrm{Tor}_0^R(M,N) = H_0(\mathbf{F}\otimes N) \cong M \otimes N$.

2. Omitimos la demostración de esta propiedad. Una demostración, que hace uso de resultados que no hemos expuesto aquí, puede encontrarse en [**Wei**, 2.7].

□

Por otra parte, el principal motivo para introducir el funtor Tor es su estrecha relación con los números de Betti, lo que será fundamental en la demostración del Teorema de las Sicigias:

Proposición 2.14. *Sea M un R-módulo graduado finitamente generado. Entonces:*

1. $b_i^R(M) = \dim_k(\mathrm{Tor}_i^R(M,k))$, *donde consideramos a k como R-módulo dado por $k = R/\mathfrak{m}$, y a $\mathrm{Tor}_i^R(M,k)$ como k-espacio vectorial por restricción de escalares.*

2. $b_{i,p}^R(M) = \dim_k(\mathrm{Tor}_i^R(M,k)_p)$, *donde hacemos la misma consideración que en 1.*

Demostración. 1. Sea $(\mathbf{F}, d)$ la resolución libre minimal graduada de M. Suponiendo que $F_i = R^{b_i(M)}$, tenemos que $F_i \otimes_R k = R^{b_i(M)} \otimes_R k \cong k^{b_i(M)}$. Por ser $\mathbf{F}$ minimal, se tiene que $\mathrm{Im}(d_i) \subset \mathfrak{m}F_{i-1}$, por lo que, para todos $f \in F_i$ y $a \in k$, existen $q \in \mathfrak{m}$ y $g \in F_{i-1}$ tales que $d_i(f) \otimes a = qg \otimes a = g \otimes qa = g \otimes 0 = 0$ (recordemos que $k = R/\mathfrak{m}$).

   Por tanto, $d_i \otimes \mathrm{Id} = 0$ y $\mathrm{Tor}_i^R(M,k) = H_i(\mathbf{F} \otimes_R k) \cong k^{b_i(M)}$, de donde se deduce el resultado.

2. Se razona igual que antes, utilizando las componentes graduadas de la resolución libre minimal graduada $\mathbf{F}$ de M.

□

2.3. Preliminares de Álgebra Multilineal

Para definir el complejo de Koszul, que será la última herramienta que utilizaremos para esta demostración del Teorema de las Sicigias, necesitamos unas nociones sobre Álgebra Multilineal. Se derivan de forma sistemática de las propiedades básicas del producto tensorial. En [**AM**] se encuentran las propiedades del producto tensorial, pero no del producto exterior ni del simétrico, y en [**Eis1**] se dedica un apéndice a esta materia, pero en el que rápidamente se pasa a cuestiones más avanzadas. Por eso damos una breve introducción en esta sección.

Nuestro objetivo será construir tres R-álgebras a partir de un R-módulo M, una de ellas no conmutativa, otra anticonmutativa, y otra conmutativa. De ellas la que nos interesará será la anticonmutativa (damos las tres por analogía y completitud). Recordemos que una R-álgebra es un anillo B que

es un R-módulo de forma que el producto en B y el producto por escalares en R conmutan ($a(bc) = (ab)c = b(ac)$ si $b, c \in B$ y $a \in R$). Recordemos también que dar en un anillo B una estructura de R-módulo es lo mismo que definir un homomorfismo de anillos $f : R \longrightarrow B$.

Empezamos con las definiciones básicas:

Definición 2.15. Sea M un R-módulo y $r \in \mathbb{N}$. Se define su **potencia tensorial** r-ésima como el R-módulo $\bigotimes^r(M) = M \otimes ... \otimes M$, r veces, si $r \geq 2$. Definimos también $\bigotimes^1(M) = M$ y $\bigotimes^0(M) = R$.

Definición 2.16. Sea M un R-módulo y $r \geq 2$. Definimos los submódulos de $\bigotimes^r(M)$ siguientes:

$$A_r = \langle\{m_1 \otimes ... \otimes m_i \otimes ... \otimes m_j \otimes ... \otimes m_r + m_1 \otimes ... \otimes m_j \otimes ... \otimes m_i \otimes ... \otimes m_r / m_k \in M\}\rangle,$$

$$B_r = \langle\{m_1 \otimes ... \otimes m_i \otimes ... \otimes m_j \otimes ... \otimes m_r - m_1 \otimes ... \otimes m_j \otimes ... \otimes m_i \otimes ... \otimes m_r / m_k \in M\}\rangle.$$

Definimos ahora la **potencia exterior** y la **potencia simétrica** r-ésima de M, respectivamente, como los cocientes

$$\bigwedge^r(M) = \bigotimes^r(M)/A_r \quad \text{y} \quad \mathbf{S}^r(M) = \bigotimes^r(M)/B_r,$$

para $r \geq 1$, donde $A_1 = B_1 = 0$. Como antes, $\bigwedge^0(M) = \mathbf{S}^0(M) = R$.

Además, si $m_1, ..., m_r \in M$, escribiremos:

$$m_1 \wedge ... \wedge m_r = m_1 \otimes ... \otimes m_r + A_r,$$

$$m_1 \odot ... \odot m_r = m_1 \otimes ... \otimes m_r + B_r.$$

Ahora, a la propiedad universal del producto tensorial (2.7), que ya conocíamos, tenemos que añadir las propiedades universales de las potencias exterior y simétrica. Ambas se deducen de la del producto tensorial. Incluimos las tres en la siguiente proposición (denotamos siempre por S_r al grupo de permutaciones de r elementos):

Proposición 2.17. *Dado un R-módulo M y $r \in \mathbb{N}$, $r \geq 1$, se verifica:*

1. *La aplicación $\bigwedge : M^r \longrightarrow \bigwedge^r(M) : (m_1, ..., m_r) \longmapsto m_1 \wedge ... \wedge m_r$ es multilineal alternada, y para todo R-módulo N y toda aplicación multilineal alternada $f : M \times ... \times M \longrightarrow N$, existe un único homomorfismo $\overline{f} : \bigwedge^r(M) \longrightarrow N$ tal que $f = \overline{f} \bigwedge$.*

2. *La aplicación* $\bigodot : M^r \longrightarrow \mathbf{S}^r(M) : (m_1, ..., m_r) \longmapsto m_1 \odot ... \odot m_r$ *es multilineal simétrica, y para todo* R*-módulo* N *y toda aplicación multilineal simétrica* $f : M \times ... \times M \longrightarrow N$*, existe un único homomorfismo* $\overline{f} : \mathbf{S}^r(M) \longrightarrow N$ *tal que* $f = \overline{f} \bigodot$.

Además, cualquier otro R*-módulo* P *con una aplicación* $t : M \times ... \times M \longrightarrow P$ r*-multilineal alternada (respectivamente simétrica) que cumpla la misma propiedad, es isomorfo a* $\bigwedge^r(M)$ *(respectivamente a* $\mathbf{S}^r(M)$*) mediante un isomorfismo que hace factorizar a* $\bigwedge$ *a través de* t *(respectivamente* $\bigodot$*).*

Demostración. 1. Claramente $\bigwedge$ es multilineal, y si $\tau \in S_r$ es la transposición $\tau = (i, j)$,

$$\bigwedge(m_{\tau(1)}, ..., m_{\tau(r)}) = m_1 \otimes ... \otimes m_j \otimes ... \otimes m_i \otimes ... \otimes m_r + A_r =$$

$$= -m_1 \otimes ... \otimes m_i \otimes ... \otimes m_j \otimes ... \otimes m_r + A_r = -\bigwedge(m_1, ..., m_r),$$

por lo que es alternada para las transposiciones. Como éstas generan a todo el grupo S_r y el índice de una permutación es la paridad del número de transposiciones que lo generan, entonces $\bigwedge$ es alternada.

Ahora, por ser f multilineal, existe $F : \bigotimes^r(M) \longrightarrow N$ tal que $f = F \bigotimes$. Y por ser f alternada, se tiene que $A_r \subset \ker(F)$, ya que F se anula en los generadores de A_r que hemos dado en la definición. Por tanto, por la propiedad universal del módulo cociente, existe un homomorfismo $\overline{f} : \bigwedge^r(M) \longrightarrow N$ tal que $F = \overline{f}\rho$, donde $\rho : \bigotimes^r(M) \longrightarrow \bigwedge^r(M)$ es el paso al cociente. Como $\bigwedge = \rho \bigotimes$, tenemos que $f = F \bigotimes = \overline{f} \bigwedge$.

Por último, la unicidad es obvia de la condición $f = \overline{f} \bigwedge$.

2. La demostración es análoga al caso de la potencia exterior.

La unicidad salvo isomorfismo de estos R-módulos se demuestra de la forma usual cuando estamos ante propiedades universales. □

Y ahora pasamos a definir los R-módulos que acabarán siendo las R-álgebras citadas al comienzo de la sección. Aunque aún no hemos definido en ellos su operación interna, las denominamos "álgebras" de antemano.

Definición 2.18. Dado un R-módulo M, definimos su:

1. **Álgebra Tensorial**: Es el R-módulo $\bigotimes(M) = \bigoplus_{r\in\mathbb{N}}(\bigotimes^r(M))$.
2. **Álgebra Exterior**: Es el R-módulo $\bigwedge(M) = \bigoplus_{r\in\mathbb{N}}(\bigwedge^r(M))$.
3. **Álgebra Simétrica**: Es el R-módulo $\mathbf{S}(M) = \bigoplus_{r\in\mathbb{N}}(\mathbf{S}^r(M))$.

Y ahora definimos sus operaciones internas, lo cual haremos en dos pasos:

Lema 2.19. *Sea M un R-módulo. Entonces, para todos $r, s \in \mathbb{N}$, $r, s \geq 1$, existen unas únicas aplicaciones bilineales:*

1. $\bigotimes : \bigotimes^r(M) \times \bigotimes^s(M) \longrightarrow \bigotimes^{r+s}(M)$ *tal que* $\bigotimes(m_1 \otimes ... \otimes m_r, n_1 \otimes ... \otimes n_s) = m_1 \otimes ... \otimes m_r \otimes n_1 \otimes ... \otimes n_s$, *para todos* $m_1, ..., m_r, n_1, ..., n_s \in M$.
2. $\bigwedge : \bigwedge^r(M) \times \bigwedge^s(M) \longrightarrow \bigwedge^{r+s}(M)$ *tal que* $\bigwedge(m_1 \wedge ... \wedge m_r, n_1 \wedge ... \wedge n_s) = m_1 \wedge ... \wedge m_r \wedge n_1 \wedge ... \wedge n_s$, *para todos* $m_1, ..., m_r, n_1, ..., n_s \in M$.
3. $\bigodot : \mathbf{S}^r(M) \times \mathbf{S}^s(M) \longrightarrow \mathbf{S}^{r+s}(M)$ *tal que* $\bigodot(m_1 \odot ... \odot m_r, n_1 \odot ... \odot n_s) = m_1 \odot ... \odot m_r \odot n_1 \odot ... \odot n_s$, *para todos* $m_1, ..., m_r, n_1, ..., n_s \in M$.

Para $r = 0$, $s \in \mathbb{N}$, dichas aplicaciones bilineales las definimos como el producto por escalares en R.

Demostración. En los tres casos se procede de la misma manera, utilizando la propiedad universal correspondiente. Por eso, haremos sólo el caso del producto tensorial:

Fijamos un $n = n_1 \otimes ... \otimes n_s \in \bigotimes^s(M)$. Definimos la aplicación $\varphi_n : M^r \longrightarrow \bigotimes^{r+s}(M)$ por $\varphi_n(m_1, ..., m_r) = m_1 \otimes ... \otimes m_r \otimes n_1 \otimes ... \otimes n_s$. Claramente es multilineal, por lo que existe una única $\phi_n : \bigotimes^r(M) \longrightarrow \bigotimes^{r+s}(M)$ tal que $\phi_n \bigotimes = \varphi_n$.

Fijamos ahora $m = \sum_i m_1^i \otimes ... \otimes m_r^i \in \bigotimes^r(M)$. Definimos la aplicación $\psi_m : M^s \longrightarrow \bigotimes^{r+s}(M)$ por $\psi_m(n_1, ..., n_s) = \phi_{n_1 \otimes ... \otimes n_s}(m) = \sum_i (m_1^i \otimes ... \otimes m_r^i \otimes n_1 \otimes ... \otimes n_s)$. Es sencillo comprobar que es multilineal, por lo que existe una única $\Psi_m : \bigotimes^s(M) \longrightarrow \bigotimes^{r+s}(M)$ tal que $\Psi_m \bigotimes = \psi_m$.

Finalmente, la aplicación $\bigotimes : \bigotimes^r(M) \times \bigotimes^s(M) \longrightarrow \bigotimes^{r+s}(M)$ definida por $\bigotimes(m, n) = \Psi_m(n)$ es la aplicación bilineal buscada, ya que su expresión viene dada de la siguiente manera:

$$\bigotimes\left(\sum_i m_1^i \otimes ... \otimes m_r^i, \sum_j n_1^j \otimes ... \otimes n_s^j\right) = \sum_{i,j}(m_1^i \otimes ... \otimes m_r^i \otimes n_1^j \otimes ... \otimes n_s^j).$$

Por último, por ser ésta su expresión sobre unos generadores de $\bigotimes^r(M) \times \bigotimes^s(M)$, entonces debe ser la única que lo cumple. □

De ahora en adelante, escribiremos $m \otimes n$ para $\bigotimes(m,n)$, si $m \in \bigotimes^r(M)$, $n \in \bigotimes^s(M)$. Igualmente para $\wedge$ y $\odot$.

Si nos fijamos, lo que acabamos de hacer es definir una operación interna en $\bigotimes(M)$, en $\bigwedge(M)$ y en $\mathbf{S}(M)$ definida sólo para los elementos de las potencias, tal que conmuta con el producto por escalares en R y es distributiva con respecto a la suma (que es lo que quiere decir el hecho de ser bilineal). Ahora lo único que nos queda es extenderla por linealidad a todo el álgebra:

Lema 2.20. *Sea M un R-módulo. Entonces:*

1. *La operación $\bigotimes : \bigotimes(M)^2 \longrightarrow \bigotimes(M)$ definida por $\bigotimes(\sum_i m_i, \sum_j n_j) = \sum_{i,j} m_i \otimes n_j$, junto con la suma y producto por escalares, hacen que $\bigotimes(M)$ sea una álgebra unitaria (no conmutativa) sobre R.*

2. *La operación $\bigwedge : \bigwedge(M)^2 \longrightarrow \bigwedge(M)$ definida por $\bigwedge(\sum_i m_i, \sum_j n_j) = \sum_{i,j} m_i \wedge n_j$, junto con la suma y producto por escalares, hacen que $\bigwedge(M)$ sea una álgebra anticonmutativa ($m \wedge n = -n \wedge m$, si $m, n \in M = \bigwedge(M)_1$) y unitaria sobre R.*

3. *La operación $\bigodot : \mathbf{S}(M)^2 \longrightarrow \mathbf{S}(M)$ definida por $\bigodot(\sum_i m_i, \sum_j n_j) = \sum_{i,j} m_i \odot n_j$, junto con la suma y producto por escalares, hacen que $\mathbf{S}(M)$ sea una álgebra conmutativa y unitaria sobre R.*

Además, estas álgebras están graduadas (como anillos, según la definición 1.1) por la suma directa que las definen.

Demostración. La existencia de dichas operaciones, que vuelven a ser aplicaciones bilineales, se debe a la propiedad universal de la suma directa de módulos (se realiza en dos pasos, como en el lema anterior). De la propia expresión se deduce la asociatividad de dicha operación, y de la bilinealidad se deducen la propiedad distributiva respecto de la suma y la conmutatividad con respecto al producto por escalares.

Por otro lado, $1 \in R \subset \bigotimes(M)$ es la unidad, ya que habíamos definido $a \otimes m = am$, para todos $a \in R$, $m \in \bigotimes^r(M)$ (e igualmente para $\wedge$ y $\odot$).

La no conmutatividad, anticonmutatividad y conmutatividad, respectivamente, de estas operaciones es un ejercicio rutinario que se deduce de la expresión que tienen.

Finalmente, el hecho de que estén graduadas es obvio de que, por definición, $\bigotimes^r(M)\bigotimes^s(M) \subset \bigotimes^{r+s}(M)$, e igualmente para $\wedge$ y $\odot$. □

Por fin tenemos las álgebras que habíamos anunciado. Ahora, veremos qué ocurre cuando M es un R-módulo libre. El siguiente resultado, en el caso del producto tensorial se puede encontrar en [**AM**, 2.14], y en el caso general, en [**Eis1**, A2.3.1].

Proposición 2.21. *Sea M un R-módulo libre finitamente generado, de base $\{e_1, ..., e_q\}$, y sea $r \in \mathbb{N}$, $r \geq 1$. Entonces:*

1. *$\bigotimes^r(M)$ es libre de base $\{e_{i_1} \otimes ... \otimes e_{i_r} / 1 \leq i_j \leq q\}$. Por tanto,* $\operatorname{rank}(\bigotimes^r(M)) = q^r$.

2. *$\bigwedge^r(M)$ es libre de base $\{e_{i_1} \wedge ... \wedge e_{i_r} / 1 \leq i_1 < i_2 < ... < i_r \leq q\}$. Por tanto,* $\operatorname{rank}(\bigwedge^r(M)) = \binom{q}{r}$. *Observemos que en este caso, $\bigwedge^r(M) = 0$ si $r > q$.*

3. *$\mathbf{S}^r(M)$ es libre de base $\{e_{i_1} \odot ... \odot e_{i_r} / 1 \leq i_1 \leq i_2 \leq ... \leq i_r \leq q\}$. Por tanto,* $\operatorname{rank}(\mathbf{S}^r(M)) = \binom{q-1+r}{r}$.

Demostración. La primera propiedad se deduce de que $(\bigoplus_{i\in I} M_i) \otimes N \cong \bigoplus_{i\in I}(M_i \otimes N)$. Como consecuencia se deducen las respectivas propiedades para el álgebra exterior y el álgebra simétrica.

Por ejemplo, para el álgebra exterior, claramente $\{e_{i_1} \wedge ... \wedge e_{i_r} / 1 \leq i_1 < i_2 < ... < i_r \leq q\}$ generan $\bigwedge^r(M)$. Para la independencia lineal, introducimos el homomorfismo $A : \bigotimes^r(M) \longrightarrow \bigotimes^r(M)$ tal que

$$A(m_1 \otimes ... \otimes m_r) = \sum_{\sigma \in S_r} \operatorname{ind}(\sigma)(m_{\sigma(1)} \otimes ... \otimes m_{\sigma(r)}),$$

que está bien definido gracias a la propiedad universal del producto tensorial, pues $A\bigotimes$ es multilineal. Además, es sencillo comprobar que es alternada, por lo que $A_r \subset \ker(A)$. Ahora, si existen $a_{i_1,...,i_r} \in R$, $1 \leq i_1 < i_2 < ... < i_r \leq q$,

tales que $\sum_{i_k<i_{k+1}} a_{i_1,...,i_r}(e_{i_1} \wedge ... \wedge e_{i_r}) = 0$, es decir, $\sum_{i_k<i_{k+1}} a_{i_1,...,i_r}(e_{i_1} \otimes ... \otimes e_{i_r}) \in A_r$, entonces

$$0 = A\left(\sum_{i_k<i_{k+1}} a_{i_1,...,i_r}(e_{i_1} \otimes ... \otimes e_{i_r})\right) = \sum_{j_l} b_{j_1,...,j_r}(e_{j_1} \otimes ... \otimes e_{j_r}),$$

donde $b_{j_1,...,j_r} = \pm a_{i_1,...,i_r}$, si $(j_1, ..., j_r) = (i_{\sigma(1)}, ..., i_{\sigma(r)})$ para algún $\sigma \in S_r$. Por independencia lineal de los $e_{j_1} \otimes ... \otimes e_{j_r}$, tenemos que los $b_{j_1,...,j_r}$ son nulos, y por tanto, también los $a_{i_1,...,i_r}$. □

Podríamos ir más lejos y ver que, tomando $M = R^n$, lo que estamos haciendo es volver a construir el anillo de polinomios sobre R en n indeterminadas, que sería $\mathbf{S}(R^n)$, al que podríamos denominar álgebra libre conmutativa sobre R. También estaríamos obteniendo una álgebra libre no conmutativa sobre R, que sería $\bigotimes(R^n)$. Tanto $\bigotimes(R^n)$ como $\bigwedge(R^n)$ tienen ciertas propiedades en común con $R[x_1, ..., x_n] = \mathbf{S}(R^n)$, pero no entraremos en los detalles.

2.4. El complejo de Koszul

En esta sección culminaremos la prueba del Teorema de las Sicigias de Hilbert utilizando propiedades de Álgebra Homológica. Utilizaremos el complejo de Koszul, que se define utilizando el álgebra exterior $\bigwedge(R^q)$ definida en la sección anterior. Otra noción clave será la de sucesión regular de elementos de un anillo.

Definición 2.22. Sea M un R-módulo. Se dice que $f \in R$ es un **divisor de cero** en M si existe $m \in M$ no nulo tal que $fm = 0$.

Definición 2.23. Sea M un R-módulo y $f_1, ..., f_q \in R$. Se dice que la sucesión $(f_1, ..., f_q)$ es M**-regular** si:

1. $\langle f_1, ..., f_q\rangle M \neq M$ ó, equivalentemente, $M/\langle f_1, ..., f_q\rangle M \neq 0$.
2. f_i no es un divisor de cero en $M/\langle f_1, ..., f_{i-1}\rangle M$, si $1 \leq i \leq q$.

(El caso $i = 1$ quiere decir que f_1 no es un divisor de cero en M.)

En lo que sigue, pondremos $\mathbf{f} = (f_1, ..., f_q)$ para denotar una sucesión (en otras palabras, una q-upla) en R, que en principio no tiene por qué ser regular para algún R-módulo M.

Definición 2.24. Se llama **complejo de Koszul** sobre $\mathbf{f}$ al complejo $(\mathbf{K}(\mathbf{f}), d)$, donde $\mathbf{K}(\mathbf{f})_i = K_i = \bigwedge^i(R^q)$, $i \in \mathbb{N}$, y cuya diferencial d está definida en la base canónica $\{\mathbf{e}_1, ..., \mathbf{e}_q\}$ de R^q de la siguiente forma:

$$d_i(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i}) = \sum_{p=1}^{i} (-1)^{p+1} f_{j_p}(\mathbf{e}_{j_1} \wedge ... \wedge \widehat{\mathbf{e}_{j_p}} \wedge ... \wedge \mathbf{e}_{j_i}),$$

si $1 \leq j_1 < j_2 < ... < j_i \leq q$, y donde $\widehat{\mathbf{e}_{j_p}}$ quiere decir que omitimos $\mathbf{e}_{j_p}$.

Proposición 2.25. *El complejo de Koszul realmente es un complejo, es decir,* $d_{i-1}d_i = 0$, $\forall i \in \mathbb{N}$.

Demostración. Primero, se tiene que

$$d_{i-1}d_i(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i}) = \sum_{1 \leq p < s \leq i} g_{p,s}(\mathbf{e}_{j_1} \wedge ... \wedge \widehat{\mathbf{e}_{j_p}} \wedge ... \wedge \widehat{\mathbf{e}_{j_s}} \wedge ... \wedge \mathbf{e}_{j_i}).$$

Si nos fijamos, al quitar primero $\mathbf{e}_{j_p}$ y después $\mathbf{e}_{j_s}$, obtenemos el coeficiente $(-1)^{p+s+1} f_{j_p} f_{j_s}$, y si quitamos primero $\mathbf{e}_{j_s}$ y después $\mathbf{e}_{j_p}$, obtenemos el coeficiente $(-1)^{p+s+2} f_{j_p} f_{j_s}$. Por tanto, $g_{p,s} = (-1)^{p+s+1} f_{j_p} f_{j_s} + (-1)^{p+s+2} f_{j_p} f_{j_s} = 0$. □

Ya que $\bigwedge^i(R^q) = 0$ si $i > q$, observamos que el complejo de Koszul adquiere la siguiente forma:

$$\mathbf{K}(\mathbf{f}) \quad \equiv \quad 0 \longrightarrow K_q \xrightarrow{d_q} K_{q-1} \longrightarrow ... \longrightarrow K_1 \xrightarrow{d_1} K_0 \longrightarrow 0.$$

Definición 2.26. Dado un R-módulo M, definimos el **complejo de Koszul** sobre $\mathbf{f}$ asociado a M como el complejo $\mathbf{K}(\mathbf{f}; M) = \mathbf{K}(\mathbf{f}) \otimes M$, con diferenciales $d_i \otimes \mathrm{Id}$, como hicimos en la sección 2.2.

Hasta aquí tenemos, por un lado, una sucesión de elementos de R que acabaremos considerando regular sobre cierto módulo, y un complejo construido a partir de dicha sucesión, utilizando las nociones de Álgebra Multilineal que vimos en la sección anterior. Lo que haremos ahora será ver cómo todo esto se combina para proporcionarnos una resolución de k sobre S.

Pero antes, necesitamos algunos lemas técnicos:

Lema 2.27. *Si* $1 \leq j_1 < j_2 < ... < j_i < p \leq q$, *entonces*

$$d(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i} \wedge \mathbf{e}_p) = d(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i}) \wedge \mathbf{e}_p + (-1)^i f_p(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i}).$$

Demostración. Por la definición de la diferencial,

$$d(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i} \wedge \mathbf{e}_p) =$$

$$\left(\sum_{s=1}^{i}(-1)^{s+1} f_{j_s}\mathbf{e}_{j_1} \wedge ... \wedge \widehat{\mathbf{e}_{j_s}} \wedge ... \wedge \mathbf{e}_{j_i}\right) \wedge \mathbf{e}_p + (-1)^{i+2} f_p(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i}) =$$

$$d(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i}) \wedge \mathbf{e}_p + (-1)^i f_p(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i}).$$

□

Lema 2.28. *Sean* $\overline{\mathbf{f}} = (f_1, ..., f_{q-1})$ *y* $\mathbf{f} = (f_1, ..., f_{q-1}, f_q)$ *sucesiones en* R. *Entonces la sucesión de complejos siguiente es exacta:*

$$0 \longrightarrow \mathbf{K}(\overline{\mathbf{f}}) \xrightarrow{\alpha} \mathbf{K}(\mathbf{f}) \xrightarrow{\beta} \mathbf{K}(\overline{\mathbf{f}})(-1) \longrightarrow 0,$$

donde, si $1 \leq i \leq q$, $\mathbf{K}(\mathbf{f})_i = \mathbf{K}(\overline{\mathbf{f}})_i \oplus (\mathbf{K}(\overline{\mathbf{f}})_{i-1} \wedge \mathbf{e}_q)$, α *es la inmersión canónica y* β *es la "proyección"* $\beta(m + (n \wedge \mathbf{e}_q)) = n$.

Demostración. Es inmediato comprobar que $\mathbf{K}(\mathbf{f})_i = \mathbf{K}(\overline{\mathbf{f}})_i \oplus (\mathbf{K}(\overline{\mathbf{f}})_{i-1} \wedge \mathbf{e}_q)$, basta tomar la expresión de un elemento de $\mathbf{K}(\mathbf{f})_i$ en la base $\{\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i} / 1 \leq j_1 < j_2 < ... < j_i \leq q\}$. Ahora bien, cuando tengamos un complejo de la forma $\mathbf{F} = \mathbf{G} \oplus \mathbf{H}$, la sucesión $0 \longrightarrow \mathbf{G} \longrightarrow \mathbf{F} \longrightarrow \mathbf{H} \longrightarrow 0$, donde estamos considerando la inmersión de $\mathbf{G}$ en $\mathbf{F}$ y la proyección de $\mathbf{F}$ en $\mathbf{H}$, siempre es exacta corta. Aunque la aplicación β no sea exactamente una proyección canónica, casi lo es (de hecho es la proyección canónica compuesta con el isomorfismo $n \wedge \mathbf{e}_q \longmapsto n$). □

Corolario 2.29. *En la situación del lema anterior, tenemos la sucesión exacta larga:*

$$... \longrightarrow H_i(\mathbf{K}(\overline{\mathbf{f}})) \xrightarrow{H_i(\alpha)} H_i(\mathbf{K}(\mathbf{f})) \xrightarrow{H_i(\beta)} H_{i-1}(\mathbf{K}(\overline{\mathbf{f}})) \xrightarrow{\tau_i} H_{i-1}(\mathbf{K}(\overline{\mathbf{f}})) \longrightarrow ...,$$

donde τ_i *es el homomorfismo conector, que en este caso está dado por la expresión* $\tau_i(\overline{m}) = (-1)^{i+1} f_q \overline{m}$.

Demostración. La existencia de la sucesión exacta larga en los módulos de homología es el teorema 2.3. Veamos la expresión de τ_i siguiendo la demostración de 2.3:

Sea $\overline{m} \in H_{i-1}(\mathbf{K}(\bar{\mathbf{f}}))$, cojamos $n = m \wedge \mathbf{e}_q \in \mathbf{K}(\mathbf{f})_i$. Por tanto, por el lema 2.27, $d(n) = d(m \wedge \mathbf{e}_q) = d(m) \wedge \mathbf{e}_q + (-1)^{i+1} f_q m = (-1)^{i+1} f_q m = \alpha_{i-1}((-1)^{i+1} f_q m)$. Teniendo en cuenta la demostración de 2.3, tenemos que $\tau_i(\overline{m}) = (-1)^{i+1} f_q \overline{m}$. □

Y ahora veamos el resultado clave que relaciona el complejo de Koszul con las sucesiones regulares, donde también escribiremos $\mathbf{f} = \langle f_1, ..., f_q \rangle$:

Teorema 2.30. *Sea M un R-módulo graduado finitamente generado y no nulo. Sea $\mathbf{f} = (f_1, ..., f_q)$ una sucesión de elementos homogéneos de R de grados positivos. Entonces, se verifica que $H_0(\mathbf{K}(\mathbf{f}; M)) = M/\mathbf{f}M$ y que las siguientes propiedades son equivalentes:*

1. $H_i(\mathbf{K}(\mathbf{f}; M)) = 0$ *para* $i > 0$.
2. $H_1(\mathbf{K}(\mathbf{f}; M)) = 0$.
3. $\mathbf{f}$ *es M-regular.*

Demostración. Lo primero, $K_1 \otimes M \longrightarrow K_0 \otimes M \longrightarrow 0$ es en realidad $R^q \otimes M \longrightarrow R \otimes M \longrightarrow 0$, donde la aplicación de la izquierda está dada en los productos tensoriales por $(a_1, ..., a_q) \otimes m \longmapsto (\sum_{p=1}^{q} a_p f_p) \otimes m$. Es decir, siempre se verifica que $H_0(\mathbf{K}(\mathbf{f}; M)) = M/\mathbf{f}M$. Obsevamos que estamos utilizando el isomorfismo de $R \otimes M$ en M dado por $a \otimes m = 1 \otimes (am) \longmapsto am$.

Veamos que 3 implica 1: Lo probamos por inducción en $q \geq 1$.

Para $q = 1$, es fácil convencerse, a partir de $R \otimes M \cong M$, de que lo que tenemos es el complejo $0 \longrightarrow M \longrightarrow M \longrightarrow 0$, cuya aplicación es multiplicar por f_1. Por la regularidad de la sucesión (f_1), f_1 no es divisor de cero en M, por lo que $H_1(\mathbf{K}(\mathbf{f}); M) = \{m \in M / f_1 m = 0\} = 0$.

Supongamos que 1 se verifica para $q-1$, y veamoslo para $q \geq 2$. Ponemos $\bar{\mathbf{f}} = (f_1, ..., f_{q-1})$ y $\overline{\mathbf{K}} = \mathbf{K}(\bar{\mathbf{f}}; M)$. Por 2.29, tenemos la sucesión exacta siguiente:

$$\begin{array}{ccccccc} H_1(\overline{\mathbf{K}}) & \longrightarrow & H_1(\mathbf{K}(\mathbf{f}; M)) & \longrightarrow & H_0(\overline{\mathbf{K}}) & \xrightarrow{\times f_q} & H_0(\overline{\mathbf{K}}) \\ \| & & & & \| & & \| \\ 0 & & & & M/\bar{\mathbf{f}}M & & M/\bar{\mathbf{f}}M. \end{array}$$

Por tanto, como f_q no es divisor de cero en $M/\bar{\mathbf{f}}M$, debe ser $H_1(\mathbf{K}(\mathbf{f};M)) = 0$.

Para $i > 1$, usamos también 2.29, y obtenemos la sucesión exacta siguiente:

$$\begin{array}{ccccc} H_i(\overline{\mathbf{K}}) & \longrightarrow & H_i(\mathbf{K}(\mathbf{f};M)) & \longrightarrow & H_{i-1}(\overline{\mathbf{K}}) \\ \| & & & & \| \\ 0 & & & & 0. \end{array}$$

De donde claramente se deduce que $H_i(\mathbf{K}(\mathbf{f};M)) = 0$.

Es trivial ver que 1 implica 2. Veamos ahora que 2 implica 3:

Primero veremos que $M/\mathbf{f}M \neq 0$. Si no fuera así, sería $M = \mathbf{f}M = \mathfrak{m}M$, ya que los f_j tienen grados positivos. Aplicando el lema de Nakayama, tenemos que entonces $M = 0$, en contra de nuestra hipótesis de que M es no nulo.

Ahora veamos la otra condición de sucesión M-regular, la cual haremos por inducción en q.

Para $q = 1$, como vimos antes, el complejo tiene la forma $0 \longrightarrow M \longrightarrow M \longrightarrow 0$, cuya aplicación es multiplicar por f_1. La hipótesis (la propiedad 2) nos dice que dicha aplicación tiene núcleo nulo, es decir, f_1 no es divisor de cero en M, es decir, (f_1) es M-regular.

Supongamos que 3 se verifica para $q-1$, y veamoslo para $q \geq 2$. Tenemos la sucesión exacta:

$$H_1(\overline{\mathbf{K}}) \xrightarrow{\times f_q} H_1(\overline{\mathbf{K}}) \longrightarrow H_1(\mathbf{K}(\mathbf{f};M)) = 0.$$

De donde $H_1(\overline{\mathbf{K}}) = (f_q)H_1(\overline{\mathbf{K}}) = \mathfrak{m}H_1(\overline{\mathbf{K}})$, de nuevo por tener f_q grado positivo, y de nuevo por el lema de Nakayama, $H_1(\overline{\mathbf{K}}) = 0$. Por tanto, por hipótesis de inducción, $\bar{\mathbf{f}} = (f_1, ..., f_{q-1})$ es M-regular. Gracias a esto, lo único que nos falta ver para que $\mathbf{f}$ sea M-regular es que f_q no sea divisor de cero en $M/\bar{\mathbf{f}}M$. Pero esto se deduce de que, de nuevo por 2.29, tenemos la sucesión exacta:

$$\begin{array}{ccccc} H_1(\mathbf{K}(\mathbf{f};M)) & \longrightarrow & H_0(\overline{\mathbf{K}}) & \xrightarrow{\times f_q} & H_0(\overline{\mathbf{K}}) \\ \| & & \| & & \| \\ 0 & & M/\bar{\mathbf{f}}M & & M/\bar{\mathbf{f}}M. \end{array}$$

□

Antes de dar la resolución libre minimal graduada de k sobre S, damos como corolario del teorema un par de propiedades interesantes:

Corolario 2.31. *Sea M un R-módulo graduado finitamente generado y no nulo, y $\mathbf{f} = (f_1, ..., f_q)$ una sucesión M-regular de elementos homogéneos de R de grados positivos. Entonces:*

1. *Toda permutación de los elementos $f_1, ..., f_q$ también es M-regular.*
2. *Si existen $m_1, ..., m_q \in M$ tales que $f_1 m_1 + ... + f_q m_q = 0$, entonces $m_1, ..., m_q \in \mathbf{f}M$.*

Demostración. 1. Dada $\mathbf{f}_\sigma = (f_{\sigma(1)}, ..., f_{\sigma(q)})$, con $\sigma \in S_q$, se tiene que $(\mathbf{K}(\mathbf{f}_\sigma; M), d \otimes \mathrm{Id})$ tiene la misma homología que $(\mathbf{K}(\mathbf{f}; M), d \otimes \mathrm{Id})$, por lo que aplicando alguna de las equivalencias del teorema anterior, obtenemos el resultado (para más detalles, ver [**Pee**]).

2. Tenemos que

$$(d_1 \otimes \mathrm{Id})(\mathbf{e}_1 \otimes m_1 + ... + \mathbf{e}_q \otimes m_q) = f_1 \otimes m_1 + ... + f_q \otimes m_q =$$

$$= 1 \otimes (f_1 m_1 + ... + f_q m_q) = 1 \otimes 0 = 0.$$

Por tanto, por ser $(\mathbf{K}(\mathbf{f}; M), d \otimes \mathrm{Id})$ exacto, se tiene que

$$\mathbf{e}_1 \otimes m_1 + ... + \mathbf{e}_q \otimes m_q = d_2 \left(\sum_{i,j} (\mathbf{e}_i \wedge \mathbf{e}_j) \otimes m_{i,j} \right) =$$

$$= \sum_{r,s} \mathbf{e}_r \otimes (f_s n_{r,s}) \in R^q \otimes \mathbf{f}M \cong (R \otimes \mathbf{f}M)^q,$$

de donde se deduce que $\mathbf{e}_j \otimes m_i \in R \otimes \mathbf{f}M$, es decir, $m_i \in \mathbf{f}M$.

□

Finalmente, damos la resolución libre minimal graduada de k sobre S:

Teorema 2.32. *Considerando $k = S/\mathfrak{m}$ como S-módulo graduado, con $\mathfrak{m} = \langle x_1, ..., x_n \rangle$, se tiene que $\mathbf{K}(x_1, ..., x_n)$ es su resolución libre minimal graduada sobre S, donde en K_i definimos la graduación dada por $\deg(\mathbf{e}_{j_1} \wedge ... \wedge \mathbf{e}_{j_i}) = i$.*

Demostración. Claramente, $(x_1, ..., x_n)$ es S-regular. Aplicamos entonces el teorema 2.30 a $\mathbf{K}((x_1, ..., x_n); S)$, y obtenemos que el complejo siguiente es exacto:

$$0 \longrightarrow K_q \otimes S \xrightarrow{d_q \otimes \mathrm{Id}} K_{q-1} \otimes S \longrightarrow ... \longrightarrow K_1 \otimes S \xrightarrow{d_1 \otimes \mathrm{Id}} S \otimes S \xrightarrow{\epsilon \otimes \mathrm{Id}} k \otimes S \longrightarrow 0,$$

donde $\epsilon : S \longrightarrow k$ es la aplicación de paso al cociente. Como $M \otimes_S S \cong M$ para todo módulo M, donde el isomorfismo se define como $m \otimes a = (am) \otimes 1 \longmapsto am$, tenemos una resolución libre de k sobre S dada simplemente por $\mathbf{K}(x_1, ..., x_n)$:

$$0 \longrightarrow K_q \xrightarrow{d_q} K_{q-1} \longrightarrow ... \longrightarrow K_1 \xrightarrow{d_1} S \xrightarrow{\epsilon} k \longrightarrow 0.$$

Dicha resolución es graduada, ya que por cómo hemos definido la graduación de K_i, es inmediato comprobar que d_i es graduada de grado 0.

Finalmente, $\mathrm{Im}(d_{i+1}) = d_{i+1}(K_{i+1}) \subset \langle x_1, ..., x_n \rangle K_i$, por la definición de d_i, por lo que la resolución es minimal. □

Observemos que la graduación que hemos definido en K_i es $R(-i)^{\binom{n}{i}}$. En particular, obtenemos los números de Betti y la dimensión proyectiva de k sobre S,

$$b_i^S(k) = \binom{n}{i} \quad \text{y} \quad \mathrm{dp}_S(k) = n.$$

Observemos también que, por la proposición 1.39, también hemos obtenido la resolución libre minimal graduada del ideal $\mathfrak{m}$, que es:

$$0 \longrightarrow K_q \xrightarrow{d_q} K_{q-1} \longrightarrow ... \longrightarrow K_1 \xrightarrow{d_1} \mathfrak{m} \longrightarrow 0.$$

Ahora, finalmente, obtenemos la demostración del Teorema de las Sicigias de Hilbert:

Teorema 2.33 (**De las Sicigias de Hilbert, versión graduada**). *Tomando $S = k[x_1, ..., x_n]$, y M un S-módulo graduado finitamente generado, se verifica que*

$$\mathrm{dp}_S(M) \leq n.$$

Demostración. Primero, por 2.14, tenemos que $b_i^S(M) = \dim_k(\mathrm{Tor}_i^S(M, k))$.

Segundo, por 2.13, tenemos que $\dim_k(\mathrm{Tor}_i^S(M, k)) = \dim_k(\mathrm{Tor}_i^S(k, M))$.

Ahora bien, por el teorema anterior, como $\mathbf{K}(x_1, ..., x_n)$ es la resolución libre minimal graduada de k sobre S, por la definición de Tor, se tiene que $\mathrm{Tor}_i^S(k, M) = H_i(\mathbf{K}(x_1, ..., x_n) \otimes M)$. Pero $K_i = 0$, si $i > n$, por lo que $\mathrm{Tor}_i^S(k, M) = 0$ para $i > n$. Es decir, $b_i^S(M) = 0$ para $i > n$, como queríamos demostrar. □

Capítulo 3

Una demostración constructiva del Teorema de las Sicigias

En este tercer capítulo daremos una prueba del Teorema de las Sicigias de Hilbert en la que, en contraste con la demostración anterior, se hace una construcción explícita de una resolución libre cuya longitud será a lo sumo n, como indica el teorema. Además, veremos también la demostración del teorema en su versión no graduada.

Dicha demostración se debe a Schreyer y hace uso de las bases de Groebner, que son una herramienta fundamental en el Álgebra Computacional. Aunque se puede desarrollar dicha teoría primero para ideales y después para módulos, como se hace en [**CLO1**] y [**CLO2**], nosotros comenzaremos directamente con módulos. Para no extendernos demasiado, omitiremos algunas demostraciones, que se pueden encontrar en los libros anteriores. Otras buenas referencias para todo el capítulo son [**Eis1**, Chapter 15] y [**EH**].

3.1. Módulos monomiales

Esta primera sección es un preámbulo para introducir los ideales y módulos monomiales, que son una clase de ideales y módulos homogéneos especial que juega un papel muy importante en Álgebra Conmutativa (son homogéneos para graduaciones del tipo 1.12). Una razón es que permiten generalizar el algoritmo de división euclídea de $k[x]$ al anillo $S = k[x_1, ..., x_n]$

y al módulo S^m, a pesar de que S no sea un dominio euclídeo si $n \geq 2$. Sin embargo, dicho algoritmo existirá gracias a que también tenemos monomios tanto en S como en S^m.

A lo largo de este capítulo, consideraremos siempre el anillo $R = S$, y de hecho, todos los S-módulos que consideraremos serán submódulos de S^m para algún m.

Definición 3.1. Definimos los **monomios** de S^m como los elementos de la forma $\mathbf{m} = \underline{\mathrm{x}}^{\alpha}\mathbf{e}_i$, con $\alpha \in \mathbb{N}^m$. Decimos que $\mathbf{n} = \underline{\mathrm{x}}^{\beta}\mathbf{e}_j$ **divide** a $\mathbf{m} = \underline{\mathrm{x}}^{\alpha}\mathbf{e}_i$, y escribimos $\mathbf{n}|\mathbf{m}$, si $i = j$ y $\underline{\mathrm{x}}^{\beta}|\underline{\mathrm{x}}^{\alpha}$, es decir, $\beta_k \leq \alpha_k$, para $k = 1, ..., n$. Se define en ese caso el **cociente** de $\mathbf{m}$ por $\mathbf{n}$ como $\mathbf{m}/\mathbf{n} = \underline{\mathrm{x}}^{\alpha-\beta} \in S$.

Por otro, lado, dados $\mathbf{m}$ y $\mathbf{n}$ como antes, se definen su:

1. **Máximo comúm divisor**: Es $\mathrm{mcd}(\mathbf{m}, \mathbf{n}) = \underline{\mathrm{x}}^{\gamma}\mathbf{e}_i$ si $i = j$, donde $\gamma_k = \mathrm{mín}(\alpha_k, \beta_k)$, y $\mathrm{mcd}(\mathbf{m}, \mathbf{n}) = 0$ si $i \neq j$.
2. **Mínimo comúm múltiplo**: Es $\mathrm{mcm}(\mathbf{m}, \mathbf{n}) = \underline{\mathrm{x}}^{\delta}\mathbf{e}_i$ si $i = j$, donde $\delta_k = \mathrm{máx}(\alpha_k, \beta_k)$, y $\mathrm{mcm}(\mathbf{m}, \mathbf{n}) = 0$ si $i \neq j$.

Antes de continuar, observemos que, al igual que ocurre en S, todo elemento de S^m se puede escribir como una combinación lineal de monomios, $\mathbf{f} = \sum c_\alpha \underline{\mathrm{x}}^{\alpha}\mathbf{e}_{i_\alpha}$, donde $c_\alpha \in k$. De hecho, como en S, los monomios de S^m forman una base como k-espacio vectorial.

Por otro lado, para poder extender el algoritmo de división de $k[x]$, necesitamos ordenar monomios (observemos que en $k[x]$ la propia graduación da un orden total en el conjunto de monomios, lo que no ocurre en $k[x_1, ..., x_n]$).

Definición 3.2. Un **orden monomial** en S^m es una relación de orden $<$ en el conjunto de monomios de S^m tal que:

1. Es total,
2. si $\mathbf{n} < \mathbf{m}$, entonces $\underline{\mathrm{x}}^{\alpha}\mathbf{n} < \underline{\mathrm{x}}^{\alpha}\mathbf{m}$, para todo $\alpha \in \mathbb{N}^n$, y
3. es un buen orden, es decir, todo conjunto de monomios admite uno mínimo.

Observación 3.3. En el caso $m = 1$, es decir, si consideramos monomios de $S = k[x_1, ..., x_n]$, dar un orden monomial equivale a dar un orden en $\mathbb{N}^n$ que verifique 1 y 3 de la definición anterior, pero cambiando la propiedad 2 por:

Si $\beta < \alpha$, entonces $\beta + \gamma < \alpha + \gamma$, para todo $\gamma \in \mathbb{N}^n$.

Antes de continuar, veamos unos ejemplos de órdenes monomiales, alguno de los cuales usaremos más adelante:

Ejemplo 3.4. En S tenemos los siguientes órdenes monomiales, definidos en $\mathbb{N}^n$:

1. **Lexicográfico**: ó LEX, definido por $\alpha >_{lex} \beta$ si, y sólo si, la componente no nula más a la izquierda de $\alpha - \beta$ es positiva. Lo que hacemos cuando consideramos este orden es mirar qué monomio tiene mayor grado en x_1, en caso de empate, miramos x_2, etc.

2. **Lexicográfico graduado**: ó GRLEX, definido por $\alpha >_{grlex} \beta$ si, y sólo si, $|\alpha| > |\beta|$ ó, si $|\alpha| = |\beta|$, entonces $\alpha >_{lex} \beta$. En este caso, miramos primero el grado del monomio según la graduación estándar de S, y en caso de empate, recurrimos al orden LEX.

3. **Lexicográfico graduado inverso**: ó GREVLEX, definido por $\alpha >_{grevlex} \beta$ si, y sólo si, $|\alpha| > |\beta|$ ó, si $|\alpha| = |\beta|$, entonces la componente no nula más a la derecha de $\alpha - \beta$ es negativa. En este caso, de nuevo miramos los grados, y en caso de empate, miramos qué monomio tiene menor grado en x_n, después en x_{n-1}, etc. Observemos que un orden lexicográfico inverso no graduado no nos proporcionaría un orden monomial, ya que no es un buen orden. La graduación evita esto.

En todos estos casos estamos tomando las indeterminadas en el orden $x_1 > x_2 > ... > x_n$, pero podríamos definir igualmente los órdenes correspondientes tomando otra ordenación de las indeterminadas. Si no se especifica lo contrario, siempre supondremos que $x_1 > x_2 > ... > x_n$.

Por otro lado, órdenes monomiales en S inducen órdenes monomiales en S^m de las dos formas siguientes:

Ejemplo 3.5. Dado un orden monomial $\leq$ en S, podemos definir sus extensiones a órdenes monomiales en S^m:

1. **Extensión TOP**: Está definido por $\underline{\mathrm{x}}^{\alpha}\mathbf{e}_i >_{TOP} \underline{\mathrm{x}}^{\beta}\mathbf{e}_j$ si $\underline{\mathrm{x}}^{\alpha} > \underline{\mathrm{x}}^{\beta}$ ó, en caso de que $\alpha = \beta$, $i < j$. Lo que hacemos es ordenar primero mirando monomios en S y después la posición de dicho monomio en la m-upla. De ahí que su nombre provenga del inglés "term over position".

2. **Extensión POT**: Está definido por $\underline{x}^{\alpha}\mathbf{e}_i >_{POT} \underline{x}^{\beta}\mathbf{e}_j$ si $i < j$ ó, en caso de que $i = j$, $\underline{x}^{\alpha} > \underline{x}^{\beta}$. Ahora, en cambio, miramos primero la posición del monomio en la m-upla y después su orden según $\leq$. En este caso, su nombre proviene del inglés "position over term".

Como ocurría en S, ahora las extensiones TOP y POT dependen del orden que demos a la base canónica de S^m. En este caso hemos considerado que $\mathbf{e}_1 > \mathbf{e}_2 > ... > \mathbf{e}_m$, es decir, $\mathbf{e}_i > \mathbf{e}_j$ si $i < j$. Pero podríamos considerar otro orden. De nuevo, si no especificamos lo contrario, asumiremos que el orden de la base canónica será este.

Un orden monomial nos permite, además de dar un algoritmo de división, ordenar los monomios que componen un elemento de S^m. Esto nos permite dar las siguientes definiciones:

Definición 3.6. Sea $\mathbf{f} \in S^m$ y $<$ un orden monomial, donde $\mathbf{f} = \sum_i c_i\mathbf{m}_i$ ($c_i \in k$), los $\mathbf{m}_i$ son monomios y $\mathbf{m}_j = \max_i \mathbf{m}_i$. Se definen:

1. El **multigrado** de $\mathbf{f}$ como $\mathrm{mdeg}(\mathbf{f}) = \mathrm{mdeg}(\mathbf{m}_j)$, donde $\mathrm{mdeg}(\underline{x}^{\alpha}\mathbf{e}_k) = \alpha$.

2. El **término inicial** (o monomio inicial) de $\mathbf{f}$ como $\mathtt{in}(\mathbf{f}) = c_j\mathbf{m}_j$.

Podríamos hacer como en [**CLO1**] y [**CLO2**] y distinguir entre término inicial, monomio inicial y coeficiente inicial. Como resulta muy pesado, consideramos sólo lo que hemos definido por término inicial, que consideraremos también como monomio.

Observemos que en el caso $m = 1$, es decir, en el anillo de polinomios S, definiendo el orden monomial como un orden en $\mathbb{N}^n$, obtenemos que $\mathrm{mdeg}(f) = \max\{\alpha / c_\alpha \neq 0\}$, donde $f = \sum_\alpha c_\alpha \underline{x}^{\alpha}$.

A continuación pasamos a enunciar el algoritmo de división en S^m, que es una extensión natural de la división euclídea para $k[x]$. No daremos la demostración de que el algoritmo termina, básicamente resulta de las propiedades de los órdenes monomiales (ver [**CLO1**, Chapter 2, Section 3]).

Teorema 3.7. *Fijado un orden monomial $<$ en S^m, para todo $\mathbf{f} \in S^m$ y toda s-upla (lista ordenada) $F = (\mathbf{f}_1, ..., \mathbf{f}_s)$ de elementos de S^m, existen $a_1, ..., a_s \in S$ y $\mathbf{r} \in S^m$ tales que*

$$\mathbf{f} = a_1\mathbf{f}_1 + ... + a_s\mathbf{f}_s + \mathbf{r},$$

donde $\mathbf{r} = 0$ *ó ningún monomio de* $\mathbf{r}$ *es divisible por ninguno de los* $\mathtt{in}(\mathbf{f}_i)$.

Algorithm 1 Algoritmo de División

Require: $\mathbf{f}, F = (\mathbf{f}_1, ..., \mathbf{f}_s)$
Ensure: $a_1, ..., a_s, \mathbf{r}$
  $a_1 := 0$, ..., $a_s := 0$, $\mathbf{r} := 0$, $\mathbf{p} := \mathbf{f}$
  while $\mathbf{p} \neq 0$ **do**
    $i := 1$
    division := false
    while $i \leq s$ **and** *division* = false **do**
      if $\mathtt{in}(\mathbf{f}_i)|\mathtt{in}(\mathbf{p})$ **then**
        $a_i := a_i + \mathtt{in}(\mathbf{p})/\mathtt{in}(\mathbf{f}_i)$
        $\mathbf{p} := \mathbf{p} - (\mathtt{in}(\mathbf{p})/\mathtt{in}(\mathbf{f}_i))\mathbf{f}_i$
        division := true
      else
        $i := i + 1$
      end if
    end while
    if *division* = false **then**
      $\mathbf{r} := \mathbf{r} + \mathtt{in}(\mathbf{p})$, $\mathbf{p} := \mathbf{p} - \mathtt{in}(\mathbf{p})$
    end if
  end while

Básicamente, lo que vamos haciendo es ordenar los monomios de $\mathbf{f}$ e intentar dividir cada uno por los monomios iniciales de $\mathbf{f}_1, ..., \mathbf{f}_s$, en ese orden (por eso pedimos que la lista F sea ordenada). Si el monomio se puede dividir por un $\mathtt{in}(\mathbf{f}_j)$, dicho cociente lo guardamos en a_j y a $\mathbf{f}$ le restamos el cociente multiplicado por $\mathbf{f}_j$. Y si no se puede dividir, guardamos dicho monomio en el resto, $\mathbf{r}$, y lo quitamos de $\mathbf{f}$.

La segunda propiedad del orden monomial nos garantiza que el grado de $\mathbf{f}$ va descendiendo en cada paso, y la tercera propiedad, el buen orden, nos garantiza que el algoritmo termina, ya que en todo conjunto bien ordenado, una sucesión descendente se estabiliza.

Observemos que tanto el resto, $\mathbf{r}$, como los coeficientes, $a_1, ..., a_s$, dependen tanto del orden monomial elegido (ya que depende de cómo ordenemos los monomios de $\mathbf{f}$ y de $\mathbf{f}_1, ..., \mathbf{f}_s$) y del orden de los $\mathbf{f}_j$ elegido. Por tanto,

no hay unicidad en el resto y los coeficientes, al contrario que en la división euclídea en $k[x]$.

Por otro lado, a continuación pasamos a trabajar por fin con ideales y módulos monomiales, que en particular son ideales homogéneos (utilizando graduaciones del tipo $S^m = S(-p_1) \oplus ... \oplus S(-p_m)$).

Definición 3.8. Sea $M \subset S^m$ un submódulo. Decimos que es **monomial** si está generado por monomios.

Un par de propiedades interesantes de los módulos monomiales son las siguientes:

Lema 3.9. *Sea $M \subset S^m$ un submódulo monomial generado por monomios $\{\mathbf{n}_i\}_{i\in I}$, y sea $\mathbf{m} \in S^m$ un monomio. Entonces, $\mathbf{m} \in M$ si, y sólo si, $\mathbf{n}_j|\mathbf{m}$ para algún $j \in I$.*

Demostración. Por un lado, si $\mathbf{m} \in M$, entonces $\mathbf{m} = \sum_i g_i\mathbf{n}_i$, con $g_i \in S$. Como cada término de la derecha es divisible por un $\mathbf{n}_j$ y el conjunto de monomios de S^m forman una base como k-espacio vectorial, se deduce que alguno de los $\mathbf{n}_j$ divide a $\mathbf{m}$. El recíproco del lema es trivial. □

Lema 3.10. *Sea $M \subset S^m$ un submódulo monomial y $\mathbf{f} \in S^m$. Son equivalentes:*

1. $\mathbf{f} \in M$.
2. *Todo término de* $\mathbf{f}$ *está en* M.
3. $\mathbf{f} = \sum_i c_i\mathbf{m}_i$, *donde* $c_i \in k$ *y los* $\mathbf{m}_i$ *son monomios de* M.

Demostración. Claramente 2 implica 3 y 3 implica 1. Veamos que 1 implica 2. Por estar M generado por monomios, $\mathbf{f}$ es combinación lineal (con coeficientes en S) de monomios de M. Ahora bien, expandiendo los polinomios de S de dicha combinación lineal, obtenemos una combinación lineal con coeficientes en k de monomios de M, de donde se deduce 2. □

Y obtenemos como corolario el siguiente resultado, similar a 1.18:

Corolario 3.11. *Sea $M \subset S^m$ un submódulo monomial. Entonces existe un único sistema minimal de generadores formado por monomios.*

Demostración. Si tenemos dos sistemas de generadores formados por monomios, por 3.9, los elementos de uno dividen a los del otro, por lo que por minimalidad, deben coincidir. □

A continuación, obtenemos un refinamiento del teorema de la base de Hilbert, del cual se puede deducir fácilmente dicho teorema (cuando el anillo de polinomios es sobre un cuerpo k). Lo que nos dice es que todo módulo monomial admite un sistema de generadores finito pero formado por monomios, que además se pueden extraer de un sistema dado.

Teorema 3.12 (**Lema de Dickson**). *Sea $M \subset S^m$ un submódulo monomial generado por monomios $\{\boldsymbol{n}_i\}_{i\in I}$. Entonces, existen $j_1, ..., j_s \in I$ tales que $\boldsymbol{n}_{j_1}, ..., \boldsymbol{n}_{j_s}$ generan M.*

Demostración. Veámoslo primero para $m = 1$, es decir, en $S = k[x_1, ..., x_n]$, y lo haremos por inducción en n. Para $n = 1$ es bien conocido que $k[x]$ es un dominio de ideales principales, de donde se deduce el resultado.

Supongamos que es cierto para $n \geq 1$, y veamos que se cumple para $n+1$. Pongamos $S = k[x_1, ..., x_n, y]$ y $\underline{x}^\alpha y^r$ para los monomios de S, y nuestro submódulo será el ideal I.

Sea $J = \langle\{\underline{x}^\alpha / \exists r \text{ tal que } \underline{x}^\alpha y^r \in I\}\rangle$, ideal de $k[x_1, ..., x_n]$. Por hipótesis de inducción, existen $\alpha^{(1)}, ..., \alpha^{(s)} \in \mathbb{N}^n$ tales que $J = \langle \underline{x}^{\alpha^{(1)}}, ..., \underline{x}^{\alpha^{(s)}}\rangle$. Sea r el máximo de los r_i tales que $\underline{x}^{\alpha^{(i)}} y^{r_i} \in I$.

Para cada $0 \leq k \leq r-1$, sea $J_k = \langle\{\underline{x}^\alpha / \underline{x}^\alpha y^k \in I\}\rangle$, de nuevo un ideal de $k[x_1, ..., x_n]$. Por tanto, de nuevo existen $\alpha_k^{(1)}, ..., \alpha_k^{(s_k)} \in \mathbb{N}^n$ tales que $J_k = \langle \underline{x}^{\alpha_k^{(1)}}, ..., \underline{x}^{\alpha_k^{(s_k)}}\rangle$.

Ahora es sencillo comprobar que I está generado por los siguientes monomios:

$$\underline{x}^{\alpha^{(1)}} y^r, ..., \underline{x}^{\alpha^{(s)}} y^r; \quad \underline{x}^{\alpha_k^{(1)}} y^k, ..., \underline{x}^{\alpha_k^{(s_k)}} y^k; \quad 0 \leq k \leq r-1.$$

Por último, en el caso general de un submódulo monomial M de S^m, hacemos lo siguiente. Se verifica que $M = (M \cap \langle \mathbf{e}_1\rangle) \oplus ... \oplus (M \cap \langle \mathbf{e}_m\rangle)$. Ahora bien, $M \cap \langle \mathbf{e}_j\rangle = I_j \langle e_j\rangle$, con $I_j \subset S$ un ideal monomial. Como cada I_j está finitamente generado, se concluye que M también.

Para tomar los monomios entre los generadores dados, por el lema 3.9, cada uno de los monomios anteriores es dividido por uno de los monomios del sistema de generadores dado. □

Un corolario importante es el siguiente:

Corolario 3.13. *Sea $<$ un orden en el conjunto de monomios de S^m que verifica las propiedades 1 y 2 de la definición 3.2. Entonces, $<$ es un buen orden si, y sólo si, $\underline{x}^\alpha \mathbf{m} \geq \mathbf{m}$ para todo $\alpha \in \mathbb{N}^n$ y todo monomio $\mathbf{m}$ de S^m.*

Demostración. Supongamos que $\underline{x}^\alpha \mathbf{m} < \mathbf{m}$, para ciertos α y $\mathbf{m}$. Entonces, recursivamente, obtenemos la sucesión $\mathbf{m} > \underline{x}^\alpha \mathbf{m} > \underline{x}^{2\alpha} \mathbf{m} > \underline{x}^{3\alpha} \mathbf{m} > ...$ que no se estabiliza, por lo que $\leq$ no es un buen orden.

Supongamos ahora que $\underline{x}^\alpha \mathbf{m} \geq \mathbf{m}$ para todo $\alpha \in \mathbb{N}^n$ y todo monomio $\mathbf{m}$ de S^m. Sea $\{\mathbf{n}_i\}_{i \in I}$ un conjunto de monomios de S^m. Consideremos $M = \langle \{\mathbf{n}_i\}_{i \in I} \rangle$, módulo monomial. Por el lema de Dickson, existen $j_1, ..., j_s \in I$ tales que $M = \langle \mathbf{n}_{j_1}, ..., \mathbf{n}_{j_s} \rangle$. Cojamos j tal que $\mathbf{n}_j$ es el mínimo de $\{\mathbf{n}_{j_1}, ..., \mathbf{n}_{j_s}\}$. Ahora, cogiendo un $i \in I$ cualquiera, por el lema 3.9, $\mathbf{n}_i$ es dividido por algún $\mathbf{n}_{j_k}$. Por tanto, $\mathbf{n}_j \leq \mathbf{n}_{j_k} \leq \mathbf{n}_i$, de donde se deduce que $\{\mathbf{n}_i\}_{i \in I}$ tiene mínimo, $\mathbf{n}_j$, por lo que el orden es un buen orden. □

Observación 3.14. En el caso $m = 1$, es decir, en S, podemos sustituir la condición "$\underline{x}^\alpha \mathbf{m} \geq \mathbf{m}$ para todo $\alpha \in \mathbb{N}^n$ y todo monomio $\mathbf{m}$ de S" por "$\alpha \geq 0$ para todo $\alpha \in \mathbb{N}^n$", considerando el orden en $\mathbb{N}^n$.

3.2. Bases de Groebner

Las bases de Groebner son una herramienta decisiva en Álgebra Conmutativa para multitud de problemas computacionales, ya que dan respuestas constructivas. El primer ejemplo que surge es el problema de saber si, dado un ideal $I \subset S$, un elemento $f \in S$ pertenece o no a dicho ideal. Una base de Groebner de dicho ideal constituirá a posteriori un sistema de generadores suyo que permitirá, de forma algorítmica, contestar a esta pregunta.

Aunque lo expongamos de forma separada, esta sección es una continuación natural de la sección anterior. La clave de las bases de Groebner es que relacionan un ideal cualquiera con otro que es monomial y aprovechan las propiedades de este:

Definición 3.15. Dado un subconjunto $A \subset S^m$, definimos su **conjunto de monomios iniciales** como $\mathtt{in}(A) = \{\mathtt{in}(\mathbf{f}) / \mathbf{f} \in A\}$, y su **ideal de monomios iniciales** como $\langle \mathtt{in}(A) \rangle$.

El lema de Dickson proporciona de inmediato el siguiente resultado:

Proposición 3.16. *Sea $M \subset S^m$ un submódulo. Entonces, existen $\mathbf{f}_1, ..., \mathbf{f}_s \in M$ tales que $\langle \mathtt{in}(M) \rangle = \langle \mathtt{in}(\mathbf{f}_1), ..., \mathtt{in}(\mathbf{f}_s) \rangle$.*

Además, obtenemos lo siguiente:

Proposición 3.17. *Sean $M \subset S^m$ un submódulo y $\mathbf{f}_1, ..., \mathbf{f}_s \in M$ tales que $\langle \mathtt{in}(M) \rangle = \langle \mathtt{in}(\mathbf{f}_1), ..., \mathtt{in}(\mathbf{f}_s) \rangle$. Entonces, $M = \langle \mathbf{f}_1, ..., \mathbf{f}_s \rangle$.*

Demostración. Sea $\mathbf{f} \in M$ y dividámoslo según el algoritmo de división 3.7 por $F = (\mathbf{f}_1, ..., \mathbf{f}_s)$. Entonces, podemos escribir $\mathbf{f} = a_1\mathbf{f}_1 + ... + a_s\mathbf{f}_s + \mathbf{r}$, donde $\mathbf{r} = 0$ ó ningún monomio suyo es divisible por ningún $\mathtt{in}(\mathbf{f}_j)$.

Si siempre ocurre lo primero, $\mathbf{f} \in \langle \mathbf{f}_1, ..., \mathbf{f}_s \rangle$, $\forall \mathbf{f} \in M$, por lo que $M \subset \langle \mathbf{f}_1, ..., \mathbf{f}_s \rangle$ y como la otra contención es obvia, habríamos acabado. Si ocurriese lo contrario, vemos que $\mathbf{r} = \mathbf{f} - a_1\mathbf{f}_1 - ... - a_s\mathbf{f}_s \in M$, por lo que $\mathtt{in}(\mathbf{r}) \in \langle \mathtt{in}(\mathbf{f}_1), ..., \mathtt{in}(\mathbf{f}_s) \rangle$. Por el lema 3.9, llegamos a la contradicción de que algún $\mathtt{in}(\mathbf{f}_j)$ divide a $\mathtt{in}(\mathbf{r})$. □

Si nos fijamos, juntando las dos proposiciones anteriores obtenemos de inmediato el Teorema de la Base de Hilbert para el anillo noetheriano k, y también obtenemos de inmediato que S^m es un S-módulo noetheriano.

A continuación pasamos a trabajar ya con bases de Groebner:

Definición 3.18. Sea $M \subset S^m$ un submódulo, $\mathbf{g}_1, ..., \mathbf{g}_s \in M$ y $<$ un orden monomial. Decimos que $G = \{\mathbf{g}_1, ..., \mathbf{g}_s\}$ es una **base de Groebner** de M para el orden $<$ si $\langle \mathtt{in}(M) \rangle = \langle \mathtt{in}(\mathbf{g}_1), ..., \mathtt{in}(\mathbf{g}_s) \rangle$.

La última proposición nos dice, por tanto, que una base de Groebner de un submódulo de S^m es, en particular, un sistema de generadores suyo. La siguiente proposición es otra interpretación del lema de Dickson:

Proposición 3.19. *Todo submódulo $M \subset S^m$ admite una base de Groebner.*

Veamos ahora una propiedad clave de estas bases, que además resuelve el problema planteado al principio sobre si un elemento pertenece o no a un módulo:

Teorema 3.20. *Sean $M \subset S^m$ un submódulo, $G = \{\mathbf{g}_1, ..., \mathbf{g}_s\}$ una base de Groebner suya y $\mathbf{f} \in S^m$. Entonces, existe un único $\mathbf{r} \in S^m$ que cumple:*

1. $\mathbf{r} = 0$ *ó ningún monomio suyo es divisible por ningún* $\mathtt{in}(\mathbf{g}_j)$.

2. *Existe un* $\mathbf{g} \in M$ *tal que* $\mathbf{f} = \mathbf{g} + \mathbf{r}$.

En particular, $\mathbf{r}$ *es el resto de la división de* $\mathbf{f}$ *por* $(\mathbf{g}_1, ..., \mathbf{g}_s)$ *sin importar el orden de estos.*

Demostración. La existencia se deduce del propio algoritmo de división 3.7. Ahora supongamos que existen $\mathbf{r}, \mathbf{r}' \in S^m$ y $\mathbf{g}, \mathbf{g}' \in M$ tales que $\mathbf{f} = \mathbf{g} + \mathbf{r} = \mathbf{g}' + \mathbf{r}'$ y cumpliendo 1. Entonces, $\mathbf{r} - \mathbf{r}' = \mathbf{g}' - \mathbf{g} \in M$, por lo que, si no es nulo, cada monomio de $\mathbf{r} - \mathbf{r}'$ es divisible por algún $\mathbf{g}_j$. Como ninguno monomio de $\mathbf{r}$ ni de $\mathbf{r}'$ cumple esto, deducimos que debe ser $\mathbf{r} - \mathbf{r}' = 0$, de donde obtenemos la unicidad. □

Corolario 3.21. *En la situación del teorema anterior,* $\mathbf{f} \in M$ *si, y sólo si,* $\mathbf{r} = 0$.

Finalmente, pasamos a dar algunas definiciones y el criterio y el algoritmo de Buchberger, que nos permitirán saber si un sistema de generadores dado es una base de Groebner, cómo construir una a partir de él si no lo es y cómo obtener una base que sea única en cierto sentido que definiremos al final.

Definición 3.22. Dados elementos $\mathbf{f}, \mathbf{f}_1, ..., \mathbf{f}_s \in S^m$, denotaremos al resto de la división de $\mathbf{f}$ por $F = (\mathbf{f}_1, ..., \mathbf{f}_s)$ mediante $\overline{\mathbf{f}}^F$.

Por otro lado, dados dos elementos $\mathbf{f}, \mathbf{g} \in S^m$, definimos su **S-vector** (**S-polinomio** si estamos en S) como

$$S(\mathbf{f}, \mathbf{g}) = \frac{\mathbf{m}}{\mathtt{in}(\mathbf{f})}\mathbf{f} - \frac{\mathbf{m}}{\mathtt{in}(\mathbf{g})}\mathbf{g},$$

donde $\mathbf{m} = \mathrm{mcm}(\mathtt{in}(\mathbf{f}), \mathtt{in}(\mathbf{g}))$.

Los S-vectores serán la clave para saber si un sistema de generadores es una base de Groebner y para construir una. Aunque no damos la demostración de los dos siguientes teoremas (para ideales pueden encontrarse en [**CLO1**, Chapter 2, sections 6 and 7], aunque no hay problemas para adaptar las demostraciones para módulos), diremos que se basan en el hecho de que en un S-vector tomamos los monomios de los dos elementos elegidos salvo sus monomios iniciales.

Teorema 3.23 (**Criterio de Buchberger**). *Sea $M \subset S^m$ un submódulo y $G = \{\mathbf{g}_1, ..., \mathbf{g}_s\}$ un sistema de generadores suyo. Entonces, G es una base de Groebner de M si, y sólo si, $\overline{S(\mathbf{g}_i, \mathbf{g}_j)}^G = 0$, si $1 \leq i < j \leq s$.*

Teorema 3.24 (**Algoritmo de Buchberger**). *Sea $M \subset S^m$ un submódulo y $F = \{\mathbf{f}_1, ..., \mathbf{f}_s\}$ un sistema de generadores suyo. La salida del siguiente algoritmo proporciona una base de Groebner de M.*

Algorithm 2 Algoritmo de Buchberger

Require: $F = \{\mathbf{f}_1, ..., \mathbf{f}_s\}$
Ensure: $G = \{\mathbf{g}_1, ..., \mathbf{g}_s\}$
  $G := F$
  repeat
    $G' := G$
    for $\{\mathbf{p}, \mathbf{q}\} \subset G' / \mathbf{p} \neq \mathbf{q}$ **do**
      $S := \overline{S(\mathbf{p}, \mathbf{q})}^{G'}$
      if $S \neq 0$ **then**
        $G := G \cup \{S\}$
      end if
    end for
  until $G = G'$

Y ahora veremos que, exigiendo algunas condiciones más a las bases de Groebner, obtenemos una que será única:

Definición 3.25. Sea $M \subset S^m$ un submódulo y $G = \{\mathbf{g}_1, ..., \mathbf{g}_s\}$ una base de Groebner suya formada por elementos mónicos, es decir, tales que el coeficiente de $\mathtt{in}(\mathbf{g}_i)$ es 1, para $1 \leq i \leq s$. Decimos que G es:

1. **Minimal**: Si $\mathtt{in}(\mathbf{g}_i) \notin \langle \mathtt{in}(\mathbf{g}_1), ..., \widehat{\mathtt{in}(\mathbf{g}_i)}, ..., \mathtt{in}(\mathbf{g}_s) \rangle$, para $1 \leq i \leq s$. Es decir, si $\{\mathtt{in}(\mathbf{g}_1), ..., \mathtt{in}(\mathbf{g}_s)\}$ es sistema de generadores minimal de $\langle \mathtt{in}(M) \rangle$.

2. **Reducida**: Si ningún monomio de $\mathbf{g}_i$ está en $\langle \mathtt{in}(\mathbf{g}_1), ..., \widehat{\mathtt{in}(\mathbf{g}_i)}, ..., \mathtt{in}(\mathbf{g}_s) \rangle$, para $1 \leq i \leq s$.

Observamos que, en particular, las bases de Groebner reducidas son minimales. Lo importante es que un módulo dado $M \subset S^m$ tendrá una única base

de Groebner reducida, que además se puede obtener de forma algorítmica, como veremos en la demostración del siguiente teorema:

Teorema 3.26. *Sea $M \subset S^m$ un submódulo. Entonces, admite una única base de Groebner reducida para un orden monomial dado.*

Demostración. Veamos primero la existencia: Tomamos una base de Groebner cualquiera $G = \{\mathbf{g}_1, ..., \mathbf{g}_s\}$ de M. Primero, es inmediato comprobar que si vamos quitando aquellos $\mathbf{g}_i$ tales que $\mathtt{in}(\mathbf{g}_i) \in \langle \mathtt{in}(\mathbf{g}_1), ..., \widehat{\mathtt{in}(\mathbf{g}_i)}, ..., \mathtt{in}(\mathbf{g}_s)\rangle$ hasta que no quede ninguno con esta propiedad, obtenemos una base minimal. Podemos suponer entonces que $G = \{\mathbf{g}_1, ..., \mathbf{g}_s\}$ es una base de Groebner minimal.

A continuación, tomamos $\mathbf{g}'_i = \overline{\mathbf{g}_i}^{G-\{\mathbf{g}_i\}}$ y $G' = \{\mathbf{g}'_1, ..., \mathbf{g}'_s\}$. Por las propiedades del algoritmo de división y por ser G minimal, obtenemos que G' ya es reducida.

Veamos ahora la unicidad: Sean $G = \{\mathbf{g}_1, ..., \mathbf{g}_s\}$ y $G' = \{\mathbf{g}'_1, ..., \mathbf{g}'_t\}$ dos bases de Groebner reducidas. Observamos primero que $\mathtt{in}(G) = \mathtt{in}(G')$ por 3.11, ya que por ser reducidas, $\mathtt{in}(G)$ e $\mathtt{in}(G')$ son sistemas minimales de generadores del mismo ideal monomial.

Pero por otra parte, si $\mathtt{in}(\mathbf{g}) = \mathtt{in}(\mathbf{g}')$, entonces $\mathbf{g} = \mathbf{g}'$, ya que en caso de no ser nulo, ningún monomio de $\mathbf{g} - \mathbf{g}'$ sería divisible por alguno de los $\mathtt{in}(G) = \mathtt{in}(G')$, por ser dichas bases reducidas. Esto concluye la demostración. □

3.3. El Teorema de Schreyer y las sicigias

En esta última sección del capítulo 3 veremos cómo las bases de Groebner nos proporcionan la demostración constructiva del Teorema de las Sicigias de Hilbert que estamos buscando. La idea se debe al matemático Frank-Olaf Schreyer y la clave está en definir un orden monomial, llamado orden de Schreyer, que va cambiando en cada módulo de sicigias de la resolución libre que estemos considerando. Una vez vistas las propiedades de este orden monomial, el Teorema de las Sicigias será sencillo de demostrar.

Como la mayor parte del tiempo estaremos considerando dos bases canónicas, una en S^m y otra en S^r, denotaremos la primera por $\{\mathbf{e}_1, ..., \mathbf{e}_m\}$ y la segunda por $\{\mathbf{e}'_1, ..., \mathbf{e}'_r\}$.

Definición 3.27. Sea $M \subset S^m$ un submódulo y sea $G = \{\mathbf{g}_1, ..., \mathbf{g}_r\}$ una base de Groebner suya respecto de un orden monomial dado $<$. Definimos el **orden de Schreyer** en S^r respecto de G de la siguiente forma:

$$\underline{\mathrm{x}}^{\alpha}\mathbf{e}'_i >_G \underline{\mathrm{x}}^{\beta}\mathbf{e}'_j \iff \begin{cases} \mathtt{in}(\underline{\mathrm{x}}^{\alpha}\mathbf{g}_i) > \mathtt{in}(\underline{\mathrm{x}}^{\beta}\mathbf{g}_j) \\ \text{ó} \\ \mathtt{in}(\underline{\mathrm{x}}^{\alpha}\mathbf{g}_i) = \mathtt{in}(\underline{\mathrm{x}}^{\beta}\mathbf{g}_j) \quad \text{e} \quad i < j. \end{cases}$$

Proposición 3.28. *El orden de Schreyer definido antes es un orden monomial en S^r.*

Demostración. Lo primero, por cómo está definido, es un orden total debido a que el orden $<$ era un orden total.

Por otro lado, sean $\underline{\mathrm{x}}^{\alpha}\mathbf{e}'_i, \underline{\mathrm{x}}^{\beta}\mathbf{e}'_j \in S^r$ dos monomios tales que $\underline{\mathrm{x}}^{\alpha}\mathbf{e}'_i <_G \underline{\mathrm{x}}^{\beta}\mathbf{e}'_j$, y sea $\gamma \in \mathbb{N}$. Supongamos que $\mathtt{in}(\underline{\mathrm{x}}^{\alpha}\mathbf{g}_i) < \mathtt{in}(\underline{\mathrm{x}}^{\beta}\mathbf{g}_j)$, entonces $\mathtt{in}(\underline{\mathrm{x}}^{\alpha+\gamma}\mathbf{g}_i) < \mathtt{in}(\underline{\mathrm{x}}^{\beta+\gamma}\mathbf{g}_j)$, por lo que $\underline{\mathrm{x}}^{\alpha+\gamma}\mathbf{e}'_i <_G \underline{\mathrm{x}}^{\beta+\gamma}\mathbf{e}'_j$. La otra posibilidad es que $\mathtt{in}(\underline{\mathrm{x}}^{\alpha}\mathbf{g}_i) = \mathtt{in}(\underline{\mathrm{x}}^{\beta}\mathbf{g}_j)$ e $i < j$, de donde resulta inmediato que $\underline{\mathrm{x}}^{\alpha+\gamma}\mathbf{e}'_i <_G \underline{\mathrm{x}}^{\beta+\gamma}\mathbf{e}'_j$.

Finalmente, para ver que es un buen orden aplicamos el corolario 3.13. □

A continuación demostraremos el teorema de Schreyer cuando $M \subset S^m$ es un submódulo monomial. Observemos antes que cualquier sistema de generadores de M formado por monomios es una base de Groebner suya.

Lema 3.29. *Sea $M \subset S^m$ un submódulo monomial generado por los monomios $\{\mathbf{m}_1, ..., \mathbf{m}_r\}$, y sean $\mathbf{m}_{ij} = \mathrm{mcm}(\mathbf{m}_i, \mathbf{m}_j)$ y*

$$\sigma_{ij} = \frac{\mathbf{m}_{ij}}{\mathbf{m}_i}\mathbf{e}'_i - \frac{\mathbf{m}_{ij}}{\mathbf{m}_j}\mathbf{e}'_j.$$

Entonces, $\{\sigma_{ij}/1 \leq i < j \leq r\}$ es una base de Groebner de $\mathrm{Sic}(\mathbf{m}_1, ..., \mathbf{m}_r)$ para el orden de Schreyer inducido por $G = \{\mathbf{m}_1, ..., \mathbf{m}_r\}$.

Demostración. Primero veamos que los σ_{ij} generan $\mathrm{Sic}(\mathbf{m}_1, ..., \mathbf{m}_r)$, donde es obvio que $\sigma_{ij} \in \mathrm{Sic}(\mathbf{m}_1, ..., \mathbf{m}_r)$. Pongamos $\mathbf{m}_j = \underline{\mathrm{x}}^{\alpha_j}\mathbf{e}_{i_j}$ y sea $(a_1, ..., a_r) \in \mathrm{Sic}(\mathbf{m}_1, ..., \mathbf{m}_r)$, es decir,

$$a_1\mathbf{m}_1 + ... + a_r\mathbf{m}_r = f_1\mathbf{e}_1 + ... + f_m\mathbf{e}_m = 0,$$

donde f_i es la suma de los $a_j \underline{\mathrm{x}}^{\alpha_j}$ correspondientes a $\mathbf{e}_i$. Como cada $f_i = 0$, por aliviar la notación, podemos suponer que todos los $\mathbf{m}_j$ se corresponden al mismo $\mathbf{e}_i$ y por tanto, $\sum_{j=1}^{r} a_j \underline{\mathrm{x}}^{\alpha_j} = 0$.

Por tanto, $(a_1, ..., a_r)$ es suma de elementos de la forma $(c_1 \underline{\mathrm{x}}^{\alpha-\alpha_1}, ..., c_r \underline{\mathrm{x}}^{\alpha-\alpha_r})$, donde $c_l \in k$ y $\sum_{l=1}^{r} c_l = 0$. Observemos además que no importa que $\alpha - \alpha_j$ tenga una componente negativa si $c_j = 0$. Si suponemos que $c_1 = ... = c_{j-1} = 0$ y $c_j \neq 0$, entonces:

$$(c_1 \underline{\mathrm{x}}^{\alpha-\alpha_1}, ..., c_r \underline{\mathrm{x}}^{\alpha-\alpha_r}) =$$

$$= c_{j+1}(0, ..., 0, -\underline{\mathrm{x}}^{\alpha-\alpha_j}, \underline{\mathrm{x}}^{\alpha-\alpha_{j+1}}, 0, ..., 0) + ... + c_r(0, ..., 0, -\underline{\mathrm{x}}^{\alpha-\alpha_j}, 0, ..., 0, \underline{\mathrm{x}}^{\alpha-\alpha_r})$$

y por otro lado,

$$(0, ..., 0, -\underline{\mathrm{x}}^{\alpha-\alpha_j}, 0, ..., 0, \underline{\mathrm{x}}^{\alpha-\alpha_l}, 0, ..., 0) = -\underline{\mathrm{x}}^{\alpha-\alpha_j}\mathbf{e}'_j + \underline{\mathrm{x}}^{\alpha-\alpha_l}\mathbf{e}'_l = -\underline{\mathrm{x}}^{\gamma}\sigma_{jl},$$

para cierto $\gamma \in \mathbb{N}^n$, si $c_l \neq 0$, de donde deducimos que los σ_{ij} son generadores.

Ahora veamos que forman una base de Groebner para $<_G$. Como se verifica que $(\mathbf{m}_{ij}/\mathbf{m}_i)\mathbf{m}_i = (\mathbf{m}_{ij}/\mathbf{m}_j)\mathbf{m}_j$, tenemos que, si $i < j$, entonces $\mathtt{in}(\sigma_{ij}) = (\mathbf{m}_{ij}/\mathbf{m}_i)\mathbf{e}'_i$ para el orden $<_G$.

Por otra parte, si suponemos que $c_1 = ... = c_{j-1} = 0$ y $c_j \neq 0$, el monomio inicial de un elemento de la forma

$$(c_1 \underline{\mathrm{x}}^{\alpha-\alpha_1}, ..., c_r \underline{\mathrm{x}}^{\alpha-\alpha_r})$$

es $\underline{\mathrm{x}}^{\alpha-\alpha_j}\mathbf{e}'_j$. Por lo tanto, el monomio inicial de un $(a_1, ..., a_r) \in \mathrm{Sic}(\mathbf{m}_1, ..., \mathbf{m}_r)$ será un múltiplo de algún $\mathtt{in}(\sigma_{ij}) = (\mathbf{m}_{ij}/\mathbf{m}_i)\mathbf{e}'_i$. □

Si nos fijamos, lo que hemos hecho es tomar los S-vectores de los $\mathbf{m}_i$ para formar a partir de ellos unos generadores del módulo de sicigias. Esto será lo que haremos a continuación en módulos que no tienen por qué ser monomiales.

Lema 3.30. *Sea $M \subset S^m$ un submódulo y $G = \{\mathbf{g}_1, ..., \mathbf{g}_r\}$ una base de Groebner suya. Entonces, existen $a_{ijk} \in S$ tales que $S(\mathbf{g}_i, \mathbf{g}_j) = \sum_{k=1}^{r} a_{ijk}\mathbf{g}_k$, donde además, $\mathtt{in}(a_{ijk}\mathbf{g}_k) \leq \mathtt{in}(S(\mathbf{g}_i, \mathbf{g}_j))$.*

Demostración. La existencia de los $a_{ijk} \in S$ se deduce del algoritmo de división en S^m y del criterio de Buchberger. El hecho de que $\mathtt{in}(a_{ijk}\mathbf{g}_k) \leq \mathtt{in}(S(\mathbf{g}_i, \mathbf{g}_j))$ es consecuencia de las propiedades del algoritmo de división. □

Notación. En las condiciones anteriores, denotamos $\mathbf{a}_{ij} = (a_{ij1}, ..., a_{ijr})$ y

$$\mathbf{s}_{ij} = \frac{\mathbf{m}_{ij}}{\mathtt{in}(\mathbf{g}_i)}\mathbf{e}'_i - \frac{\mathbf{m}_{ij}}{\mathtt{in}(\mathbf{g}_j)}\mathbf{e}'_j - \mathbf{a}_{ij} \in S^r,$$

donde $\mathbf{m}_{ij} = \text{mcm}(\mathtt{in}(\mathbf{g}_i), \mathtt{in}(\mathbf{g}_j))$.

Si nos fijamos, lo que acabamos de definir es una generalización de los σ_{ij} para el caso no monomial. Esto es así porque el S-vector de dos monomios es obviamente nulo y, por tanto, los a_{ijk} de la división son obviamente nulos en ese caso.

Ahora llegamos ya al Teorema de Schreyer, que es la generalización que habíamos anunciado del lema 3.29 anterior:

Teorema 3.31 (de Schreyer). *Sea $M \in S^m$ un submódulo y $G = \{\mathbf{g}_1, ..., \mathbf{g}_r\}$ una base de Groebner suya. Entonces, $\{\mathbf{s}_{ij}/1 \leq i < j \leq r\}$ es una base de Groebner de* $\text{Sic}(\mathbf{g}_1, ..., \mathbf{g}_r)$ *para el orden de Schreyer inducido por* $G = \{\mathbf{g}_1, ..., \mathbf{g}_r\}$.

Demostración. Como hicimos con σ_{ij}, observamos que $\mathtt{in}(\mathbf{s}_{ij}) = (\mathbf{m}_{ij}/\mathtt{in}(\mathbf{g}_i))\mathbf{e}'_i$, si $i < j$, por el mismo razonamiento que en 3.29, usando en este caso que $\mathtt{in}(a_{ijk}\mathbf{g}_k) \leq \mathtt{in}(S(\mathbf{g}_i, \mathbf{g}_j))$. Ahora escribimos $\sigma_{ij} = (\mathbf{m}_{ij}/\mathtt{in}(\mathbf{g}_i))\mathbf{e}'_i - (\mathbf{m}_{ij}/\mathtt{in}(\mathbf{g}_j))\mathbf{e}'_j$, que son los σ_{ij} anteriores con respecto a $\mathbf{m}_i = \mathtt{in}(\mathbf{g}_i)$. Por lo tanto, de 3.29 deducimos que:

$$\langle \mathtt{in}(\text{Sic}(\mathtt{in}(\mathbf{g}_1), ..., \mathtt{in}(\mathbf{g}_r)))\rangle = \langle \mathtt{in}(\sigma_{ij})\rangle = \langle \mathtt{in}(\mathbf{s}_{ij})\rangle \subset \langle \mathtt{in}(\text{Sic}(\mathbf{g}_1, ..., \mathbf{g}_r))\rangle.$$

Por otro lado, sea $\mathbf{b} \in \text{Sic}(\mathbf{g}_1, ..., \mathbf{g}_r)$. Entonces, tomando los mayores monomios en $b_1\mathbf{g}_1 + ... + b_r\mathbf{g}_r = 0$, obtenemos que $b'_{i_1}\mathtt{in}(\mathbf{g}_{i_1}) + ... + b'_{i_t}\mathtt{in}(\mathbf{g}_{i_t}) = 0$, donde $1 \leq i_1 < ... < i_t \leq r$ y b'_{i_j} es un término de b_{i_j}. Es decir, $b'_{i_1}\mathbf{e}'_{i_1} + ... + b'_{i_t}\mathbf{e}'_{i_t} \in \text{Sic}(\mathtt{in}(\mathbf{g}_1), ..., \mathtt{in}(\mathbf{g}_r))$.

Ahora, como $\mathtt{in}(\mathbf{b}) = b'_{i_1}\mathbf{e}'_{i_1}$ para el orden $<_G$, deducimos que $\mathtt{in}(\mathbf{b}) \in \langle \mathtt{in}(\text{Sic}(\mathtt{in}(\mathbf{g}_1), ..., \mathtt{in}(\mathbf{g}_r)))\rangle$, por lo que obtenemos la otra contención, es decir:

$$\langle \mathtt{in}(\text{Sic}(\mathbf{g}_1, ..., \mathbf{g}_r))\rangle = \langle \mathtt{in}(\text{Sic}(\mathtt{in}(\mathbf{g}_1), ..., \mathtt{in}(\mathbf{g}_r)))\rangle = \langle \mathtt{in}(\mathbf{s}_{ij})\rangle,$$

lo que demuestra que $\{\mathbf{s}_{ij}/1 \leq i < j \leq r\}$ es una base de Groebner de $\text{Sic}(\mathbf{g}_1, ..., \mathbf{g}_r)$. □

Observación 3.32. Dentro de la demostración anterior hemos obtenido que:

$$\langle \mathtt{in}(\mathrm{Sic}(\mathtt{in}(\mathbf{g}_1), ..., \mathtt{in}(\mathbf{g}_r)))\rangle = \langle \mathtt{in}(\mathrm{Sic}(\mathbf{g}_1, ..., \mathbf{g}_r))\rangle,$$

lo cual implica que $\mathrm{Sic}(\mathtt{in}(\mathbf{g}_1), ..., \mathtt{in}(\mathbf{g}_r)) = 0$ si, y sólo si, $\mathrm{Sic}(\mathbf{g}_1, ..., \mathbf{g}_r) = 0$.

Lo que hemos conseguido hasta ahora, con el Teorema de Schreyer, es obtener unos generadores del módulo de sicigias de una base de Groebner, que además forman también una base de Groebner, respecto al orden de Schreyer. Lo que haremos ahora será ver cómo podemos obtener generadores de las sicigias de un sistema de generadores cualquiera a partir de las sicigias de una base de Groebner. Un primer resultado al respecto sería 1.24.

Por su sencillez, omitimos las demostraciones de los resultados siguientes para no alargarnos:

Lema 3.33. *Sea $M \subset S^m$ un submódulo, y sean $\mathbf{f}_1, ..., \mathbf{f}_r \in S^m$ y $\mathbf{g}_1, ..., \mathbf{g}_t \in S^m$ dos sistemas de generadores suyos. Escribamos $F = (\mathbf{f}_1, ..., \mathbf{f}_r)$ y $G = (\mathbf{g}_1, ..., \mathbf{g}_t)$ como matrices cuyas columnas son los vectores $\mathbf{f}_i$ y $\mathbf{g}_j$, respectivamente. Entonces existen matrices A y B con coeficientes en S, de tamaños $r \times t$ y $t \times r$, respectivamente, tales que $G = FA$ y $F = GB$, y que verifican:*

1. *$A\mathbf{s} \in \mathrm{Sic}(\mathbf{f}_1, ..., \mathbf{f}_r)$ si $\mathbf{s} \in \mathrm{Sic}(\mathbf{g}_1, ..., \mathbf{g}_t)$.*
2. *Las columnas de $I - AB$ están en $\mathrm{Sic}(\mathbf{f}_1, ..., \mathbf{f}_r)$.*

Además observemos que, si G es una base de Groebner de M, entonces podemos hallar B mediante el algoritmo de división.

Lema 3.34. *En las mismas condiciones,*

1. *Si $G = \{\mathbf{g}_1, ..., \mathbf{g}_t\}$ es una base de Groebner, $\mathbf{s}_{ij} = (\mathbf{m}_{ij}/\mathtt{in}(\mathbf{g}_i))\mathbf{e}'_i - (\mathbf{m}_{ij}/\mathtt{in}(\mathbf{g}_j))\mathbf{e}'_j$ y S_l son las columnas de $I - AB$, entonces*

   $$\{A\mathbf{s}_{ij}, S_l / 1 \leq i < j \leq t, 1 \leq l \leq r\}$$

   generan $\mathrm{Sic}(\mathbf{f}_1, ..., \mathbf{f}_r)$.

2. *En general (si G es una base de Groebner o no), si D es una matriz de presentación de M respecto de $\{\mathbf{g}_1, ..., \mathbf{g}_t\}$, entonces las columnas de la matriz concatenada $(AD|I - AB)$ generan $\mathrm{Sic}(\mathbf{f}_1, ..., \mathbf{f}_r)$.*

Finalmente, llegamos al Teorema de las Sicigias de Hilbert, para el cual necesitamos un par de lemas previos:

Lema 3.35. *Sea M un S-módulo cualquiera, $(\mathbf{F}, d)$ una resolución libre suya y $N \in \mathbb{N}$. Entonces,* $\ker(d_{N-1})$ *es libre si $F_i = 0$ para $i > N$. Recíprocamente, si* $\ker(d_{N-1})$ *es libre, entonces M admite una resolución libre $(\mathbf{G}, \partial)$ tal que $G_i = 0$ si $i > N$.*

Demostración. Si $F_i = 0$ para $i > N$, entonces d_N es inyectiva, y por tanto, $F_N \cong \mathrm{Im}(d_N) = \ker(d_{N-1})$, de donde se deduce el resultado. Recíprocamente, si $\ker(d_{N-1})$ es libre, basta sustituir F_N por $\mathrm{Im}(d_N)$ para obtener una resolución libre como en el enunciado. □

Lema 3.36. *Sea $M \subset S^m$ un submódulo y $G = \{\mathbf{g}_1, ..., \mathbf{g}_r\}$ una base de Groebner suya que verifica: si $\mathtt{in}(\mathbf{g}_i)$ y $\mathtt{in}(\mathbf{g}_j)$ contienen el mismo vector $\mathbf{e}_l$ e $i < j$, entonces $(\mathtt{in}(\mathbf{g}_i)/\mathtt{in}(\mathbf{e}_l)) >_{lex} (\mathtt{in}(\mathbf{g}_j)/\mathtt{in}(\mathbf{e}_l))$. Si $0 \leq q \leq n-1$ y $x_1, ..., x_q$ no aparecen en $\mathtt{in}(G)$, entonces $x_1, ..., x_{q+1}$ no aparecen en los $\mathtt{in}(\mathbf{s}_{ij})$, para el orden de Schreyer.*

Demostración. Sabemos que, si $\mathbf{s}_{ij} = (\mathbf{m}_{ij}/\mathtt{in}(\mathbf{g}_i))\mathbf{e}'_i - (\mathbf{m}_{ij}/\mathtt{in}(\mathbf{g}_j))\mathbf{e}'_j - \mathbf{a}_{ij}$, entonces $\mathtt{in}(\mathbf{s}_{ij}) = (\mathbf{m}_{ij}/\mathtt{in}(\mathbf{g}_i))\mathbf{e}'_i$ si $i < j$. Como $\mathbf{m}_{ij} = 0$ si $\mathbf{g}_i$ y $\mathbf{g}_j$ contienen a distintos e_l, supongamos que contienen al mismo.

Entonces, por la hipótesis del enunciado, $\mathbf{m}_{ij} = \underline{\mathrm{x}}^{\gamma_{ij}}\mathbf{e}_l$, con $\gamma_{ijk} = 0$, si $k = 1, ..., q$, y $\gamma_{ij,q+1} = \alpha_{i,q+1}$, si $\mathtt{in}(\mathbf{g}_i) = \underline{\mathrm{x}}^{\alpha_i}\mathbf{e}_l$. Por tanto, $\mathtt{in}(\mathbf{s}_{ij}) = \underline{\mathrm{x}}^{\gamma_{ij}-\alpha_i}\mathbf{e}'_i$, pero en $\underline{\mathrm{x}}^{\gamma_{ij}-\alpha_i}$ no aparecen $x_1, ..., x_q, x_{q+1}$. □

Observación 3.37. Una base de Groebner cualquiera siempre se puede reordenar de forma que cumpla la hipótesis del lema anterior. Basta agrupar los elementos que contienen al mismo vector de la base canónica y ordenarlos según el enunciado del lema.

A continuación, primero veremos la demostración del Teorema de las Sicigias de Hilbert en su versión no graduada, que aún no habíamos demostrado:

Teorema 3.38 (De las Sicigias de Hilbert). *Tomando $S = k[x_1, ..., x_n]$, todo S-módulo finitamente generado M admite una resolución libre finita de longitud a lo sumo n.*

Demostración. Como habíamos anunciado, haremos una demostración constructiva. Primero, tomamos unos generadores de M y consideramos la aplicación $d_0 : F_0 \longrightarrow M$, con $F_0 = R^s$, que lleve la base canónica en dichos generadores. Obtenemos una base de Groebner de F_0, que sabemos que podemos obtenerla reducida y cumpliendo la hipótesis del lema. La denotamos por G_0 y construimos a partir de ella una presentación de M:

$$F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0.$$

Ahora, por el Teorema de Schreyer obtenemos una base de Groebner G_1 de $\ker(d_1) = \mathrm{Sic}(G_0)$, que por el lema anterior además cumple que x_1 no aparece en $\mathtt{in}(G_1)$. De nuevo podemos hacer que sea reducida y cumpliendo la hipótesis del lema anterior. Construimos el siguiente paso en la resolución:

$$F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0.$$

Vemos que podemos iterar el proceso, donde en cada $\ker(d_i) \subset F_i$ obtenemos una base de Groebner G_i cumpliendo lo anterior, y donde en $\mathtt{in}(G_i)$ no aparecen $x_1, ..., x_{i+1}$. Llegamos así hasta $\ker(d_{n-1}) \subset F_{n-1}$,

$$F_{n-1} \xrightarrow{d_{n-1}} F_{n-2} \longrightarrow ... \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \longrightarrow 0,$$

donde en $\mathtt{in}(G_{n-1})$ no aparecen $x_1, ..., x_{n-1}$. Veamos que entonces G_{n-1} de hecho es una base de $\mathrm{Sic}(G_{n-2}) = \ker(d_{n-1})$, es decir, sus elementos son libres. En ese caso, definiendo $F_n = \mathrm{Sic}(G_{n-2}) = \ker(d_{n-1})$ y d_n la inclusión, ya obtenemos, como vimos en el lema 3.35, una resolución libre de M de longitud n.

Para ello, utilizamos la observación 3.32, gracias a la cual basta ver que los elementos de $\mathtt{in}(G_{n-1})$ son libres. Ahora bien, como dichos términos iniciales están en $k[x_n]^q$ para cierto $q \in \mathbb{N}$, si no fueran libres, no formarían un sistema minimal de generadores, lo cual contradice que G_{n-1} sea una base de Groebner reducida. □

Lo que haremos a continuación será modificar dicha prueba para obtener el teorema en su versión graduada. Para ello, necesitamos un lema previo que relaciona bases de Groebner con los módulos homogéneos:

Lema 3.39. *Consideremos una graduación del tipo $S^m = S(-p_1) \oplus ... \oplus S(-p_m)$. Entonces, un submódulo $M \subset S^m$ es homogéneo si, y sólo si, su base de Groebner reducida G está formada por elementos homogéneos (fijado siempre un orden monomial $<$).*

Demostración. Obviamente, si G contiene sólo elementos homogéneos, entonces M es homogéneo. Recíprocamente, si M es homogéneo, tomemos $\{\mathbf{f}_1, ..., \mathbf{f}_t\}$ unos generadores homogéneos suyos, y utilicemos el algoritmo de Buchberger para obtener una base de Groebner a partir de ellos, $G = \{\mathbf{g}_1, ..., \mathbf{g}_r\}$. Los S-vectores de los f_i tienen la forma:

$$S(\mathbf{f}_i, \mathbf{f}_j) = \frac{\mathbf{m}_{ij}}{\mathtt{in}(\mathbf{f}_i)}\mathbf{f}_i - \frac{\mathbf{m}_{ij}}{\mathtt{in}(\mathbf{f}_j)}\mathbf{f}_j,$$

donde $\mathbf{m}_{ij} = \text{mcm}(\mathtt{in}(\mathbf{f}_i), \mathtt{in}(\mathbf{f}_j))$. Con la graduación que estamos considerando, los monomios son homogéneos. Por tanto, observamos que los S-vectores también son homogéneos, ya que, salvo que sean nulos por cancelaciones o por la característica de k, obtenemos que:

$$\deg\left(\frac{\mathbf{m}_{ij}}{\mathtt{in}(\mathbf{f}_i)}\mathbf{f}_i\right) = \deg(\mathbf{m}_{ij}) - \deg(\mathbf{f}_i) + \deg(\mathbf{f}_i) = \deg(\mathbf{m}_{ij}) =$$

$$= \deg(\mathbf{m}_{ij}) - \deg(\mathbf{f}_j) + \deg(\mathbf{f}_j) = \deg\left(\frac{\mathbf{m}_{ij}}{\mathtt{in}(\mathbf{f}_j)}\mathbf{f}_j\right).$$

Por tanto, los restos de los S-vectores que se obtienen en el algoritmo de Buchberger también son homogéneos, por las propiedades del algoritmo de división. Además, al reducir la base, como sólo estamos quitando monomios, obtenemos que la base reducida G está formada por elementos homogéneos. □

Teorema 3.40 (**De las Sicigias de Hilbert, versión graduada**). *Tomando $S = k[x_1, ..., x_n]$, y M un S-módulo graduado finitamente generado, se verifica que*

$$\text{dp}_S(M) \leq n.$$

Demostración. La demostración es esencialmente la misma que en el caso no graduado. La única diferencia es que, como el módulo de sicigias de un sistema de generadores homogéneos es homogéneo (como vimos en el comienzo de la sección 1.3), en cada paso obtenemos una base de Groebner reducida de un módulo homogéneo, que por el lema anterior, está formada por elementos homogéneos. Por tanto, la resolución libre que obtenemos es una resolución graduada de longitud a lo sumo n. Como la resolución libre minimal graduada es la de menor longitud, llegamos a que tiene longitud a lo sumo n. □

Capítulo 4

La Función de Hilbert

Llegados a este punto, nos podemos preguntar cuál era la motivación de Hilbert para hacer todo este estudio de las sicigias y de las resoluciones libres de un módulo graduado, y por qué resulta clave su Teorema de las Sicigias. La respuesta es la función de Hilbert, que tiene múltiples aplicaciones, de las cuales mencionaremos al final, y como conclusión, algunas relativas a la Geometría Algebraica.

Este capítulo tiene una estructura diferente a los anteriores. Para empezar, es claramente más corto, y no está dividido en secciones. La razón es que resulta como conclusión y aplicación de todo lo visto en los tres capítulos anteriores. Extendernos en dichas aplicaciones nos llevaría a comenzar otro proyecto entero, pues a partir de aquí, el estudio de resoluciones, funciones de Hilbert, invariantes, etc. diverge en múltiples ramas del Álgebra Conmutativa, cada una de las cuales tiene como base teórica lo expuesto en estos capítulos.

Empezamos con algunas definiciones, donde haremos la misma consideración que en capítulos anteriores, tomando R como un anillo graduado, cociente de S por un ideal homogéneo. Observemos que si M es un R-módulo graduado cuya graduación está dada por $M = \bigoplus_{i\in\mathbb{N}} M_i$, y es finitamente generado como R-módulo, entonces cada M_i es un k-espacio vectorial de dimensión finita.

Definición 4.1. Sea M un R-módulo graduado finitamente generado. Definimos:

1. **Función de Hilbert**: de M es la función $\mathrm{Hilb}_M : \mathbb{N} \longrightarrow \mathbb{Z}$ definida por $\mathrm{Hilb}_M(i) = \dim_k(M_i)$.
2. **Serie de Hilbert**: es la función generatriz de la sucesión $\dim_k(M_i)$, es decir, es la serie $\mathrm{H}_M(t) = \sum_{i=0}^{\infty} \dim_k(M_i)t^i \in \mathbb{Z}[[t]]$.

(De aquí en adelante, como la dimensión la tomamos siempre sobre el cuerpo k, escribiremos dim en lugar de $\dim_k$.)

Nuestro objetivo (y el de Hilbert) es probar que la función de Hilbert de un S-módulo graduado (finitamente generado) es en realidad un polinomio, a partir de un cierto número natural. Para ello, veremos antes las propiedades de "aditividad" y "desfase" de la serie y la función de Hilbert:

Lema 4.2. *Sean U, V, W, $V_1, ..., V_r$ varios k-espacios vectoriales.*

1. *Si $0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$ es exacta, entonces*
$$\dim(V) = \dim(U) + \dim(W).$$
2. *Si $0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow ... \longrightarrow V_r \longrightarrow 0$ es exacta, entonces*
$$\sum_{i=0}^{r} (-1)^i \dim(V_i) = 0.$$

Demostración. Lo primero es inmediato teniendo en cuenta que la exactitud de dicha sucesión de espacios vectoriales equivale a que $V \cong U \oplus W$. Lo segundo es consecuencia directa de lo primero, teniendo en cuenta que en el siguiente diagrama las columnas son exactas y la imagen de una aplicación es el núcleo de la siguiente:

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & & & 0 & & \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \\
 & & 0 & & \ker(f_2) & & & & \ker(0) & & \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \\
0 & \longrightarrow & V_1 & \xrightarrow{f_1} & V_2 & \xrightarrow{f_2} & ... & \xrightarrow{f_{r-1}} & V_r & \longrightarrow & 0. \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \\
 & & \mathrm{Im}(f_1) & & \mathrm{Im}(f_2) & & & & 0 & & \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \\
 & & 0 & & 0 & & & & 0 & &
\end{array}$$

□

Para funciones de la forma $\lambda : C \longrightarrow \mathbb{Z}$ que parten de una colección de R-módulos C, las condiciones 1 y 2 anteriores son equivalentes (sustituyendo dim por λ), y en caso de cumplirse, se dice que λ es una **función aditiva**. Para más información sobre esto, ver [**AM**, página 27]. Lo que nos interesa a nosotros es el siguiente corolario:

Corolario 4.3. *Sean M, M', M'' y $N_1, ..., N_r$ varios R-módulos graduados finitamente generados.*

1. *Si $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ es exacta, entonces*

$$\mathrm{H}_M(t) = \mathrm{H}_{M'}(t) + \mathrm{H}_{M''}(t).$$

2. *Si $0 \longrightarrow N_1 \longrightarrow ... \longrightarrow N_r \longrightarrow 0$ es exacta, entonces*

$$\sum_{i=0}^{r} (-1)^i \mathrm{H}_{N_i}(t) = 0.$$

Por otro lado, ya podemos obtener las series de Hilbert más sencillas, que son las siguientes:

Proposición 4.4. *Si $R = S/I$ y M es un R-módulo graduado finitamente generado, se verifica:*

1. $\mathrm{H}_{M(-p)}(t) = t^p \mathrm{H}_M$, *si* $p > 0$.

2. $$\mathrm{H}_S(t) = \frac{1}{(1-t)^n} \quad y \quad \mathrm{Hilb}_S(i) = \binom{n+i-1}{i}.$$

3. $\mathrm{H}_R(t) = \mathrm{H}_S(t) - \mathrm{H}_I(t)$.

Demostración. 1 es inmediato y 3 es un caso particular del corolario anterior. Para 2, es sencillo comprobar que $\dim(S_i) = \binom{n+i-1}{i}$, ya que es el número de monomios de grado i, que se corresponde con el cardinal del conjunto $\{\alpha \in \mathbb{N}^n / |\alpha| = i\}$. Por tanto,

$$\mathrm{H}_S(t) = \sum_{i=0}^{\infty} \binom{n+i-1}{i} t^i.$$

Para ver que dicha serie es $(1-t)^{-n}$ (dentro del cuerpo $\mathbb{Z}((t))$), podemos razonar por inducción derivando series. Para $n = 1$ el resultado es bien conocido, $(1-t)^{-1} = \sum_{i=0}^{\infty} t^i$. Supongamos ahora que es cierto para algún $n \geq 1$ y veámoslo para $n+1$. Escribamos $f_n(t) = \sum_{i=0}^{\infty} \binom{n+i-1}{i} t^i$. Entonces, utilizando ambas expresiones de f_n, por hipótesis de inducción:

$$\frac{n}{(1-t)^{n+1}} = f_n'(t) = \sum_{i=1}^{\infty} i \frac{(n+i-1)!}{i!(n-1)!} t^{i-1} = n \sum_{i=0}^{\infty} \frac{(n+i)!}{i!n!} t^i = n f_{n+1}(t),$$

de donde se deduce el resultado. □

El resultado que afirma que la función de Hilbert de un S-módulo graduado finitamente generado es un polinomio, a partir de cierto natural, es consecuencia del teorema siguiente. Aunque lo que buscaba Hilbert era su consecuencia, este teorema se suele denominar en la literatura como Teorema de Hilbert:

Teorema 4.5 (de Hilbert). *Sea M un R-módulo graduado finitamente generado y $(\mathbf{F}, d)$ una resolución libre graduada suya tal que: Para todo $p \geq 0$, existe un $N_p \in \mathbb{N}$ tal que $c_{ip} = 0$, si $i > N_p$, donde $F_i = \bigoplus_{p \geq 0} R(-p)^{c_{ip}}$. Entonces:*

$$\mathrm{H}_M(t) = \mathrm{H}_R(t) \sum_{p=0}^{\infty} \left(\sum_{i=0}^{N_p} (-1)^i c_{ip} \right) t^p.$$

Demostración. Vamos a dividir la demostración en dos casos:

Caso 1: Si la resolución tiene longitud finita N, entonces por el último corolario:

$$\mathrm{H}_M(t) = \sum_{i=0}^{N} (-1)^i \mathrm{H}_{F_i}(t).$$

Ahora bien,

$$\mathrm{H}_{F_i}(t) = \sum_{j=0}^{\infty} \left(\sum_{p=0}^{j} c_{ip} \dim(R_{j-p}) \right) t^j = \mathrm{H}_R(t) \sum_{p=0}^{\infty} c_{ip} t^p,$$

de donde se deduce el resultado, ya que en este caso particular podemos tomar $N_p = N$, para todo $p \geq 0$.

Caso 2: Veamos el caso general. Si fijamos un grado $j \geq 0$, observamos que existirá un $i_0 \geq 0$ tal que $F_{i,j} = 0$, si $i > i_0$, por la condición que hemos impuesto a la resolución. Por tanto, obtenemos la sucesión exacta siguiente:

$$0 \longrightarrow F_{i_0,j} \longrightarrow ... \longrightarrow F_{1,j} \longrightarrow F_{0,j} \longrightarrow M_j \longrightarrow 0.$$

Por tanto, tenemos que

$$\dim(M_j) = \sum_{i=0}^{i_0} (-1)^i \dim(F_{i,j}) = \sum_{i=0}^{i_0} (-1)^i \left(\sum_{p=0}^{j} c_{ip} \dim(R_{j-p}) \right),$$

que es una expresión análoga a la del caso anterior. De ella se deduce el resultado. □

Antes de ver las consecuencias de este teorema, podríamos pensar en qué situaciones podemos obtener una resolución que cumpla las hipótesis anteriores. Como hemos visto en el caso 1, si la resolución es finita, entonces lo cumple. Por el Teorema de las Sicigias, sabemos que si $R = S$, entonces podemos obtener una resolución finita. Para el caso general, la resolución libre minimal graduada también nos sirve, debido a la proposición 1.45.

Y a continuación veamos el resultado que estábamos buscando. Observemos antes que, en el caso $R = S$, en el teorema anterior obtenemos un polinomio $f \in \mathbb{Z}[t]$ tal que:

$$\mathrm{H}_M(t) = \frac{f(t)}{(1-t)^n}.$$

Despejando, vemos que es único. Ahora, si lo dividimos por su factor irreducible $(1-t)$ elevado a la potencia máxima, y llamamos $h \in \mathbb{Z}[t]$ al cociente, obtenemos que:

$$\mathrm{H}_M(t) = \frac{h(t)}{(1-t)^d},$$

donde $0 \leq d \leq n$, y $h(1) \neq 0$.

Corolario 4.6. *En la situación descrita antes ($R = S$), se verifica que:*

1. *Existe un único polinomio* $\mathrm{HP}_M(i) \in \mathbb{Q}[i]$ *tal que existe un* $N \in \mathbb{N}$ *a partir del cual* $\mathrm{Hilb}_M(i) = \mathrm{HP}_M(i)$. *De hecho, lo verifica para todo* $i \geq \deg(h)$.

2. $\mathrm{HP}_M(i) = \sum_{j=0}^{\deg(h)} h_j \binom{d-1+i-j}{d-1}$, *donde* h_j *es el coeficiente que acompaña a* t^j *en* h.

3. $\deg(\mathrm{HP}_M) = d-1$.

4. *El coeficiente principal de* HP_M *es*

$$\frac{h(1)}{(d-1)!}.$$

Al polinomio HP_M *se le denomina* ***polinomio de Hilbert*** *de* M*, a* $h(1)$*,* ***multiplicidad*** *de* M*, y a* d*,* ***dimensión de Krull*** *de* M.

Demostración. En la expresión que habíamos obtenido antes, tenemos que:

$$\sum_{i=0}^{\infty} \dim(M_i)t^i = (h_0 + h_1 t + ... + h_r t^r) \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} t^i,$$

donde $r = \deg(h)$. Si $i \geq r$, observamos que:

$$\mathrm{Hilb}_M(i) = \dim(M_i) = \binom{n+i-1}{n-1} h_0 + ... + \binom{n+i-r-1}{n-1} h_r$$

y, por tanto, nuestro polinomio HP_M será:

$$\mathrm{HP}_M(i) = \binom{n+i-1}{n-1} h_0 + ... + \binom{n+i-r-1}{n-1} h_r,$$

que es la expresión en 2. Para terminar de probar 1, si otro polinomio coincidiera con este en todo número natural a partir de uno dado, su diferencia tendría infinitas raíces, por lo que deben ser iguales.

Por otro lado, tenemos que:

$$h_j \binom{d-1+i-j}{d-1} = h_j \frac{(d-1+i-j)\cdots(i-j+1)}{(d-1)!} = \frac{h_j}{(d-1)!} i^{d-1} + ...,$$

donde los puntos suspensivos indican términos de menor grado en i. De ahí se obtiene 3 y 4 sumando en j. □

Este corolario podría deducirse también directamente de la aditividad de la función $\dim_k$, utilizando una resolución finita. Sin embargo, el teorema 4.5 abre las puertas a estudiar resoluciones infinitas, tema que genera una gran actividad investigadora en la actualidad, como podemos observar en un artículo reciente de Eisenbud y Peeva, titulado "Matrix Factorizations for Complete Intersections and Minimal Free Resolutions", [**EP**].

Finalmente, veamos una aplicación de estos resultados a la Geometría Algebraica.

Tomando $\mathbb{P}^n$ como el espacio proyectivo de dimensión n sobre k, es decir, $\mathbb{P}^n = \mathbb{P}(k^{n+1})$, podemos definir conjuntos algebraicos como conjuntos de ceros de polinomios, al igual que se hace en el espacio afín. Sin embargo, en el caso proyectivo, necesitamos considerar polinomios homogéneos para que el concepto de "cero" de dichos polinomios no dependa del representante del punto.

Más concretamente, denotemos por $[x_0, x_1, ..., x_n] \in \mathbb{P}^n$ a los puntos de $\mathbb{P}^n$, donde $(x_0, ..., x_n) \in k^{n+1} - \{0\}$ es un representante suyo. Si $f \in k[x_0, ..., x_n]$ es un polinomio cualquiera y $\lambda \in k^*$, entonces $[x_0, ..., x_n] = [\lambda x_0, ..., \lambda x_n]$, pero no tiene por qué verificarse que:

$$f(x_0, ..., x_n) = 0 \quad \Longrightarrow \quad f(\lambda x_0, ..., \lambda x_n) = 0.$$

Sin embargo, si f es homogéneo, se verifica que

$$f(\lambda x_0, ..., \lambda x_n) = \lambda^{\deg(f)} f(x_0, ..., x_n),$$

por lo que en este caso sí que se cumple la implicación anterior. Por lo tanto, si tenemos un ideal homogéneo $I \subset k[x_0, ..., x_n]$, y $f_1, ..., f_r \in I$ son generadores homogéneos suyos, entonces podemos definir la variedad proyectiva asociada a I como:

$$\mathrm{V}(I) = \{[x_0, x_1, ..., x_n] \in \mathbb{P}^n / f_i(x_0, ..., x_n) = 0, \quad i = 1, ..., r\},$$

donde es sencillo comprobar que dicho conjunto no depende del sistema de generadores homogéneos elegido.

Dichas variedades proyectivas tienen asociados dos números, su **dimensión** y su **grado**. Sobre la dimensión, se puede probar que existe una proyectividad que lleva $\mathrm{V}(I)$ en $\mathrm{V}(x_{m+1}, ..., x_n)$, y que dicho m es independiente de

la proyectividad escogida, al cual se le denomina **dimensión** de $\mathrm{V}(I)$. Sobre el **grado**, se define como el máximo número de puntos de $\mathrm{V}(I)$ que pueden cortar a un subespacio proyectivo de dimensión $n-d$, con d la dimensión de $\mathrm{V}(I)$.

Lo importante es que, si $S = k[x_0, ..., x_n]$, h es el polinomio anterior correspondiente a S/I y $c \in k$ es el coeficiente principal de $\mathrm{HP}_{S/I}$, entonces se puede demostrar que:

1. La **dimensión** de $\mathrm{V}(I)$ es $d - 1 = \deg(\mathrm{HP}_{S/I})$.
2. El **grado** de $\mathrm{V}(I)$ es $h(1) = c(\deg(\mathrm{HP}_{S/I})!)$.

De hecho, estas son las definiciones que se dan en [**CLO1**]. Observemos también que no sólo hemos encontrado una definición alternativa de dichos conceptos, sino que todo lo expuesto en estos capítulos proporciona un método constructivo para hallarlos, ya que el polinomio de Hilbert se halla a partir de la serie de Hilbert, según el último corolario, y ésta se puede hallar a partir de la resolución libre minimal graduada de S/I, la cual podemos hallar utilizando bases de Groebner, según el capítulo 3.

A partir de aquí, se puede hacer un estudio de las relaciones que hay entre la Geometría Algebraica y la Teoría de las Sicigias. Una referencia importante sería [**Eis2**], donde el objeto central de todo el libro es precisamente estudiar los aspectos geométricos de las sicigias. De hecho, el primer capítulo repasa los conceptos vistos en esta memoria, viendo que la función de Hilbert es un polinomio a partir de cierto natural (página 4), y viendo la información geométrica que encierra.

Bibliografía

[**AM**] M. F. Atiyah & I. G. Macdonald, *Introducción al Álgebra Conmutativa*, Reverté Barcelona Buenos Aires Caracas, 1973

[**CLO1**] D. Cox , J. Little & D. O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, Springer Berlin Heidelberg New York, 1997

[**CLO2**] D. Cox , J. Little & D. O'Shea, *Using algebraic Geometry*, Graduate Texts in Mathematics **185**, Springer Berlin Heidelberg New York, 1998

[**DFX**] F. Delgado , C. Fuertes & S. Xambó, *Introducción al Álgebra. Anillos, Factorización y Teoría de Cuerpos*, Universidad de Valladolid, 1998

[**EH**] V. Ene & J. Herzog , *Gröbner Bases in Commutative Algebra*, Graduate Studies in Mathematics **130**, American Mathematical Society, 2012

[**Eis1**] D. Eisenbud, *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer Berlin Heidelberg New York, 1995

[**Eis2**] D. Eisenbud, *The Geometry of Syzygies*, Graduate Texts in Mathematics **229**, Springer Berlin Heidelberg New York, 2005

[**EP**] D. Eisenbud, I. Peeva, *Matrix Factorizations for Complete Intersections and Minimal Free Resolutions*, arXiv: 1306.2615v2, Preprint 17 June 2013

[**Pee**] I. Peeva, *Graded Syzygies*, Algebra and Applications Volume **14**, Springer Berlin Heidelberg New York, 2011

[**Wei**] C. Weibel, *An introduction to homological algebra*, Cambridge studies in advanced mathematics **38**, Cambridge University Press, 1994