UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

"BASES DE GRÖBNER, SICIGIAS Y POLINOMIO DE HILBERT"

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A :

JOSE DE JESUS MALAGON LOPEZ

DIRECTOR DE TESIS: DR. ENRIQUE JAVIER ELIZONDO HUERTA

VNIVERSIDAD NACIONAL
AVTNOMA DE
MEXICO

MAT. MARGARITA ELVIRA CHÁVEZ CANO
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo de Tesis.

Bases de Gröbner, sicigias y polinomio de Hilbert.

realizado por José de Jesús Malagón López

con número de cuenta 9115120 - 1 , pasante de la carrera de Matemáticas.

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. Enrique Javier Elizondo Huerta.	Javier Elizondo
Propietario	Dr. Herbert Kanarek Blando.	H Kanarek
Propietario	M. en C. Emigdio Martínez Ojeda.	
Suplente	Dr. Rodolfo San Agustín Chi.	Rodolfo
Suplente	Dr. Oscar Alfredo Palmas Velasco.	

Consejo Departamental de Matématicas.

Héctor Méndez L.

Dr. Héctor Méndez Lango.

"BASES DE GRÖBNER, SICIGIAS Y POLINOMIO DE HILBERT"

A ***Trinidad López Jiménez***, mi madre.

Agradecimientos.

Quiero agradecer a todos aquellos que influyerón en este trabajo. A los míos: mis padres *Trinidad López y Agustín Malagón*, a mis hermanas *María de los Angeles, Rosa Martha, Guadalupe y Lilia*, mi hermano *Agustín* y mi tío *Rafael,* quienes siempre me han apoyado, no sólo en la carrera. Con especial cariño, este trabajo es también para mis sobrinos: *Emmanuel, Mariana, Josué, Hugo, Emiliano y Oliver.*

Quiero agradecer a todos mis sinodales por sus aportaciones y tiempo dedicado a este trabajo. En especial le agradesco al *Dr. Javier Elizondo*, por su apoyo, paciencia y la libertad de trabajo que me ha dado, permitiéndome cometer mis propios errores, que son de los cuales se aprende.

Finamente le agradesco a la banda del Instituto y de la Facultad, con los cuales he logrado un buen ambiente de trabajo.

Índice General

Introducción 5

1 Módulos 9

1.1 Nociones Básicas 9

1.1.1 Módulos Noetherianos 11

1.1.2 Módulos Graduados 13

1.2 Generadores y Relaciones 16

1.3 Caracterización de las Sicigias 18

1.4 Resoluciones Libres, Graduadas y Presentaciones de Módulos 19

2 Bases de Gröbner 29

2.1 Submódulos y Ordenes Monomiales 29

2.1.1 Ideales y Submódulos Monomiales 30

2.1.2 Ordenes Monomiales 35

2.2 Bases de Gröbner 40

2.3 Algoritmo de la División Multivariado 42

2.4 Algoritmo de Buchberger 47

2.4.1 S-Vectores 47

2.4.2 Algoritmo de Buchberger 53

2.4.3 Bases de Gröbner Reducidas 57

3 Sicigias 63

3.1 Cálculo del Submódulo de Sicigias 63

3.1.1 Sicigias de Submódulos Monomiales 63
3.1.2 Sicigias de Bases de Gröbner 68
3.1.3 Sicigias de Conjuntos Generadores 72
3.2 Teorema de Sicigias de Hilbert 78

4 Polinomio de Hilbert **81**
4.1 Función de Hilbert 81
4.2 Polinomio de Hilbert 86

A **89**
A.1 Algoritmo de la División 89
A.2 Teorema de la Base de Hilbert 90

Bibliografía **92**

Introducción

Podemos decir, a grandes rasgos, que el objeto de estudio en gemetría algebraica es el conjunto de las soluciones de sistemas finitos de ecuaciones algebraicas. Así, un problema básico de la geometría algebraica se puede plantear en la siguiente pregunta: ¿Cómo es la estructura del conjunto de soluciones de un número finito de ecuaciones polinomiales en varias variables?

Buscando dar cada vez una mejor respuesta, un medio muy importante en los últimos años ha sido la computación, que ha influido a que se de una tendencia a formular de forma más constructiva a la geometría algebraica. Una herramienta importantísima ha sido la teoría de bases de Gröbner, teoría en la cual se basan la mayoría de las herramientas computacionales desarrolladas para la geometría algebraica. El concepto de base de Gröbner y su algoritmo de obtención en forma explícita fueron introducidos por Bruno Buchberger en su tesis doctoral [1965; Universidad de Innsbruck], la cual fue dirigida por Wolfgang Gröbner, y refinadas en dos artículos posteriores (1970,1976) por el mismo Buchberger Aunque las ideas detrás de las bases de Gröbner ya habían sido dadas por Gordan (1900), Macaulay (1927) y Hironaka (1964), la contribución de Buchberger fue haberle dado forma y sentido propio, además de dar resultados explícitos.

Con el uso de las computadoras adquirió auge una vieja rama de las matemáticas, la teoría de invariantes. La teoría de invariantes clásica llegó a su fin a finales del siglo XIX, en dos artículos de Hilbert (1890,1893), en el cual aparecen ideas y resultados que tuvieron gran impacto en el desarrollo del álgebra moderna y de la geometría algebraica. Algunos de los resultados que aparecieron son: teorema de la base, teorema de sicigias (caso graduado), existencia del polinomio del Hilbert, Nullstellensatz y teorema de finitud para invariantes (objetivo de ambos artículos)

El objetivo de esta tesis es dar un método de obtención del polinomio de Hilbert y de las sicigias de un conjunto generador de elementos homogéneos de un $k[x_1, \ldots, x_r]$-módulo. El

camino a seguir es usando resultados de Macaulay (1927) y Schreyer (1980). El objetivo del trabajo de Macaulay era caracterizar las posibles funciones de Hilbert de ideales graduados, comparándolos con las funciones de Hilbert de ideales monomiales. La aportación de Schreyer fue dar un algoritmo para calcular las sicigias de un conjunto generador, de forma matemática bien detallada. Su obtención se basó en dar una forma más refinada del teorema de sicigias de Hilbert y dar una demostración constructiva.

Consideremos el siguiente problema: dado $I \subset k[_1, \ldots, x_r]$ un ideal, determinar cuando un polinomio cualquiera pertenece a I. Este problema se conoce como el *problema de la membresía*, cuya solución juega un papel muy importante en la obtención de los algoritmos que buscamos. La solución del problema de la membrresía envuelve al siguiente problema: aún cuando contemos con un conjunto generador para el ideal, expresiones distintas que estén en función del conjunto generador pueden definir al mismo elemento. Problema que se resume en la pregunta: ¿Qué tan "independientes" son los generadores de un ideal? De la necesidad de dar respuesta a esta pregunta da lugar al concepto de sicigia. Una interpretación geométrica directa de las sicigias no es muy clara, pero lo cierto es que sus propiedades tiene importantes consecuencias geométricas.

En la presente tesis procuré dar las definiciones y resultados conforme se van requiriendo, esto con la idea de ir motivando la necesidad de tal definición o resultado. La tesis está estructurada de la siguiente manera: en el capítulo uno tratamos el concepto de módulo, comenzando con las nociones básicas. Después estudiaremos a los $k[x_1, \ldots, x_n]$-módulos, prestando especial atención en las relaciones de los conjuntos generadores, para después dar algunas de sus caracterizaciones. Acabamos el capítulo estudiando a los módulos con métodos de álgebra homológica, las resoluciones libres y graduadas.

En el capítulo dos tratamos el tema de las bases de Gröbner, comenzando a desarrollar la herramienta necesaria para obtener los algoritmos deseados. Un estudio comprensivo de las teoría de bases de Gröbner resulta ser muy amplio, debido en gran parte a sus numerosas aplicaciones, pero para la finalidad de este trabajo sólo presento las ideas importantes que dan valor a la teoría de bases de Gröbner, que es más o menos el material al que Sturmfels llama "Gröbner basics". En este capítulo se tratará el tema de submódulos monomiales y ordenes monomiales. También se demostrará la existencia de las bases de Gröbner, y haciendo uso de la generalización del algoritmo de la división, y de una caracterización de las bases de Gröbner dada por Buchberger, se obtendrá un algoritmo para calcularlas.

El capítulo tres también tratará el tema de las sicigias, dando un método de obtención

acompañado de ejemplos no triviales, para después enunciar el teorema de sicigias de Hilbert, cuya demostración será haciendo uso de las bases de Gröbner, método utilizado por Schreyer.

En el último capítulo haremos un pequeño estudio de la función y polinomio de Hilbert, cuya demostración de la existencia del polinomio hace uso del teorema de sicigias. Después, haciendo uso nuevamente de un resultado de Macaulay (1927), daremos la forma de obtener un polinomio de Hilbert mediante resoluciones graduadas

Hay un apéndice donde se enuncian dos resultados, que aunque son de importancia en el texto, no encajan en el seguimiento de ideas que se pretende en el presente trabajo. El primer resultado es el algoritmo de la división, el cual, además de motivar el algoritmo de la división multivariado dado en el capítulo dos, da como resultado la observación que todo generador de grado mínimo de un ideal de $k[x_1]$, resulta ser base de Gröbner. En la segunda parte del apéndice demostraremos el teorema de la base, que es usado durante todo el texto al garantizarnos que todo submódulo de los que vamos a considerar están finitamente generados, además de ayudar a garantizar la culminación, en un número finito de pasos, de los algoritmos a presentar.

Capítulo 1

Módulos

Módulos son la generalización de espacios vectoriales, son grupos abelianos con una acción de un anillo S (si S es campo, el S-módulo sería S-espacio vectorial). En este capítulo daremos las nociones básicas sobre módulos para pasar después al estudio de R-módulos, donde R es el anillo de polinomios sobre un campo k. En la sección *1.2* definiremos lo que es una sicigia, concepto que surge al no haber necesariamente independencia lineal entre generadores de un módulo, para después dar algunas formas de caracterizarlas. Acabamos este capítulo con resoluciones libres de R-módulos, que a diferencia de espacios vectoriales muchas propiedades de módulos se pueden establecer en términos de resoluciones libres.

1.1 Nociones Básicas

Definición 1.1.1. Un *módulo* sobre un anillo S (o *S-módulo*) es un grupo abeliano M junto con una acción de S sobre M, que es, un mapeo

$$\begin{aligned} S \times M &\longrightarrow M \\ (s, m) &\longmapsto sm, \end{aligned}$$

satisfaciendo para todo $r, s \in S$ y $m, n \in M$:

$$\begin{aligned} r(sm) &= (rs)m && \text{(asociatividad)} \\ r(m+n) &= rm + rn \\ (r+s)m &= rm + sm && \text{(distributividad)} \end{aligned}$$

Si además cumple con

$$em = m \qquad \text{(identidad)}$$

decimos que es un *módulo unitario*. La acción de S sobre M es llamada *multiplicación por escalar*.

En lo que resta del presente trabajo, la palabra módulo significara módulo unitario.

Ejemplo 1.1.2. 1. Todo anillo S es un S-módulo. Más aún, el anillo $\bigoplus_{i\in I} Se_i$, para algún conjunto de índices I, es un S-módulo, donde $\{e_i\}_{i\in I}$ es la base canónica.

2. Todo ideal $I \subset S$ y su anillo cociente S/I son ejemplos de S-módulos.

Definición 1.1.3. Un morfismo $\varphi : M \to M'$ de grupos abelianos es un *morfismo* de S-módulos si para todo $m \in M$, $s \in S$, se cumple que

$$\varphi(sm) = s\,\varphi(m)$$

Un morfismo $\varphi : M \to M$ se dice que es un *endomorfismo*. Decimos que un morfismo es un *monomorfismo* (o *epimorfismo* o *isomorfismo*) si viéndolo como mapeo entre conjuntos es un mapeo inyectivo (o sobreyectivo o biyectivo).

Definición 1.1.4. Sea M un S-módulo, y sea N un subgrupo aditivo de M. Decimos que $N \subset M$ es un *submódulo* si N es cerrado bajo la acción de S. El subgrupo abeliano M/N hereda una estructura de S-módulo, definida por $s(m + N) = sm + N$, llamado *módulo cociente*.

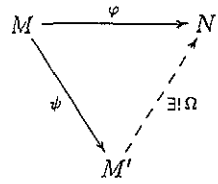
Se tiene un morfismo natural sobre el módulo cociente

$$\begin{aligned} \nu : M &\longrightarrow M/N \\ m &\longmapsto [m] = m + N \end{aligned}$$

Si $\varphi : M \to M'$ es un morfismo de S-módulos, el núcleo de φ, $Ker(\varphi) := \{m \in M |\ \varphi(m) = 0\}$ es un submódulo de M: la imagen de M bajo φ, $Im(\varphi)$, es un submódulo de M'. Así, el módulo cociente $M'/Im(\varphi)$ es un submódulo. Dicho submódulo es llamado *conúcleo* y es denotado por $Coker(\varphi)$.

Teorema 1.1.5. Sean M, M' y N S-módulos. Sea $\varphi : M \to N$ un morfismo de S-módulos. Si $\psi : M \to M'$ es un epimorfismo con $Ker(\psi) \subseteq Ker(\varphi)$, entonces existe un único morfismo $\Omega : M' \to N$ tal que

$$\varphi = \Omega \circ \psi.$$



Más aún, Ω es monomorfismo si, y sólo si, $Ker(\psi) = Ker(\varphi)$ y Ω es epimorfismo si, y sólo si, φ es epimorfismo.

Demostración. Véase Wisbauer ([Wis91], pag 37). □

Para todo subconjunto B de M, existe un único submódulo $N \subseteq M$ que contiene a B como subconjunto y tal que para todo submódulo $N' \subseteq M$ que contenga a B, se tiene que $N \subseteq N'$. Tal submódulo N, consiste de todas las combinaciones S-lineales

$$\sum_{i=1}^{n} s_i m_i, \qquad s_i \in S,\ m_i \in B.$$

El submódulo N es llamado el *submódulo generado por B en M*, y denotado por $\langle B \rangle$. Un conjunto generador para M es un subconjunto $B \subset M$ tal que $M = \langle B \rangle$. Se dice que M es *finitamente generado* si tiene un conjunto finito de generadores.

1.1.1 Módulos Noetherianos

Definición 1.1.6. Un S-módulo M es *Noetheriano* si todo submódulo de M es finitamente generado.

Proposición 1.1.7. *Sea M un S-módulo. Entonces M es Noetheriano si, y sólo si, cada cadena ascendente de submódulos de M se estaciona.*

Demostración. Véase Wisbauer ([Wis91], pag. 59) □

Proposición 1.1.8. i) *Sea $\varphi : M \to M'$ un epimorfismo de S-módulos, y asumamos que M es Noetheriano. Entonces M' es Noetheriano.*

ii) *Sea M un S-módulo. Sea N un submódulo de M. Entonces M es Noetheriano si, y sólo si, N y M/N son Noetherianos.*

Demostración. Véase Wisbauer ([Wis91], pag. 60). □

Proposición 1.1.9. *Si S es anillo noetheriano y M un S-módulo finitamente generado, entonces M es Noetheriano.*

Demostración. Véase Eisenbud ([Eis95], pag. 28). □

Como en el caso de espacios vectoriales, un subconjunto $B \subseteq M$ de un S-módulo se dice que es *linealmente independiente* si la combinación lineal

$$\sum_{i=1}^{n} \alpha_i m_i = 0 \qquad \alpha_i \in S,\ m_i \in B,$$

unicamente se cumple con $\alpha_i = 0$, para toda i.

Se dice que B es *linealmente dependiente* en caso contrario. Decimos que B es *base* de M si es linealmente independiente y es un conjunto generador de M.

Observación 1.1.10. Notemos que cualquier ideal $I \subset S$ que no sea principal, no puede ser generado por un conjunto linealmente independiente.

Ejemplo 1.1.11. Sea S un anillo. Sea $I = \langle f_1, f_2 | \, f_1, f_2 \in S \backslash \{0\} \rangle$ un ideal, entonces ambos elementos generadores satisfacen una relación de dependencia lineal, la cual es $f_1 f_2 - f_2 f_1 = 0$.

Los módulos que tienen base reciben un nombre especial.

Definición 1.1.12. Sea M un S-módulo. Decimos que M es *libre* si tiene una base.

Ejemplo 1.1.13. Sea S un anillo. El S-módulo

$$S^m = \bigoplus_{i=1}^{m} S e_i,$$

donde $\{e_i | i = 1, \ldots, m\}$ es la base canónica, es un S-módulo libre.

Observación 1.1.14. En el caso de que S sea un campo, todo S^m módulo libre es un espacio vectorial de dimensión m.

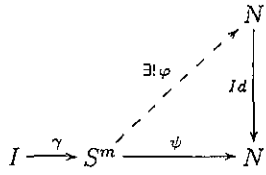
Sea $I = \{1, \ldots, m\}$ el conjunto de índices de una base $\{s_i\}$, para el S-módulo libre S^m. Consideremos al mapeo

$$\begin{aligned} \gamma : I &\longrightarrow S^m \\ i &\longmapsto s_i \end{aligned}$$

Este mapeo tiene la siguiente propiedad universal.

Teorema 1.1.15 (Propiedad Universal de las Bases). Sea N un S-módulo. Entonces para cada mapeo $\psi : S^m \to N$, existe un único morfismo de S-módulos $\varphi : S^m \to N$ tal que

$$\gamma\varphi = \psi.$$



Demostración. Véase Wisbauer ([Wis91], pag. 23). □

1.1.2 Módulos Graduados

Definición 1.1.16. Si $S = \bigoplus_{i \in I} S_i$ es un anillo graduado, entonces un *S-módulo graduado* es un S-módulo M con una descomposición en suma directa

$$M = \bigoplus_{-\infty}^{\infty} M_i$$

como grupo abeliano, tal que $S_i M_j \subset M_{i+j}$, para todo i, j. Los elementos $f \in M$ tales que $f \in M_i$, para alguna i, son llamados *homogéneos de grado i.*

Todo elemento $f \in M$ se escribe de forma única como suma de elementos homogéneos pertenecientes a M, es decir,

$$f = \sum_{i=1}^{m} f_i \qquad\qquad f_i \in M_i.$$

Si $N \subset M$ es un submódulo del módulo graduado M, decimos que N es un *submódulo graduado* si los subgrupos aditivos $N_i = M_i \cap N$, para $i \in \mathbb{Z}$, define una estructura de módulo graduado sobre N.

Lema 1.1.17. *Sean $M_1, \ldots, M_n$ módulos graduados. Entonces*

$$N = \bigoplus_{i=1}^{n} M_i$$

es un módulo gradudo, cuya graduación está dada por

$$N_d = \bigoplus_{i=1}^{n} (M_i)_d.$$

Demostración. Se sigue de

$$\bigoplus_{-\infty}^{\infty} N_d = \bigoplus_{-\infty}^{\infty} \bigoplus_{i=1}^{n} (M_i)_d = \bigoplus_{i=1}^{n} \bigoplus_{-\infty}^{\infty} (M_i)_d = \bigoplus_{i=1}^{n} M_i = N.$$

□

Lema 1.1.18. *Sea $N \subset M$ un submódulo graduado de un módulo graduado. Entonces el módulo cociente M/N tiene estructura de módulo graduado, dada por*

$$(M/N)_d = M_d/N_d = M_d/(M_d \cap N).$$

Demostración. Como la sucesión

$$0 \longrightarrow N_d \longrightarrow M_d \longrightarrow M_d/N_d \longrightarrow 0$$

es exacta para todo $d \in \mathbb{Z}$, tenemos que la sucesión

$$0 \longrightarrow \bigoplus_{-\infty}^{\infty} N_d \longrightarrow \bigoplus_{-\infty}^{\infty} M_d \longrightarrow \bigoplus_{-\infty}^{\infty} M_d / \bigoplus_{-\infty}^{\infty} N_d \longrightarrow 0$$

es exacta. Entonces se tiene que

$$\bigoplus_{-\infty}^{\infty} (M/N)_d = \bigoplus_{-\infty}^{\infty} (M_d/N_d) = \bigoplus_{-\infty}^{\infty} M_d / \bigoplus_{-\infty}^{\infty} N_d = M/N.$$

□

Ahora sólo considaremos R-módulos, donde $R = k[x_1, \ldots, x_r]$.

Sea $M = \bigoplus_{-\infty}^{\infty} M_i$ un R-módulo graduado, y notemos que toda componente graduada M_i es un R_0-módulo, donde $R_0 = k \subset R$. Al ser k campo, tenemos que M_i es un k-espacio

vectorial. Así, si M es graduado, entonces es un k-espacio vectorial. Ejemplos de este estilo son los ideales homogéneos.

Notemos que los módulos libres R^m son ejemplos de R-módulos graduados, haciendo $(R^m)_d = (R_d)^m$, es decir,

$$R^m = \bigoplus_{-\infty}^{\infty} (R^m)_d = \bigoplus_{-\infty}^{\infty} (R_d)^m$$

Llamaremos a los componentes graduados $(R_d)^m$ la *estructura estándar de módulo graduado* sobre R^m.

Lema 1.1.19. *Sea $M \subset R^m$ un R-módulo graduado finitamente generado. Entonces*

$$dim_k(M_i) < \infty$$

para toda i.

Demostración. Si M_i no fuera finitamente generado, el R-módulo

$$\bigoplus_{k=i}^{\infty} M_k \subset M$$

no sería finitamente generado, contradiciendo a la proposición (1.1.9). Por lo tanto,

$$dim_k(M_i) < \infty.$$

□

Sea M un R-módulo graduado y d un número entero. Definimos

$$M(d) = \bigoplus_{k \in \mathbb{Z}} M(d)_k$$

donde $M(d)_k = M_{d+k}$. El módulo graduado $M(d)$ es llamado el *d-Módulo Graduado Deslizado*. De hecho, la igualdad $M(d)_k = M_{d+k}$ nos da un isomorfismo entre M y $M(d)$.

Si $M = R^m$, notemos que los elementos de la base canónica $\{e_i\}$ siguen siendo base para $R(d)^m$, sólo que ahora son elementos homogéneos de grado $-d$, ya que $R_0 = R(d)_{-d}$.

Más aún, por el lema (1.1.17) podemos considerar R-módulos graduados libres de la forma

$$\bigoplus_{i=1}^{m} R(d_i)$$

para cualesquiera enteros $d_1, \ldots, d_m$. Su base es e_i, de grado $-d_i$ para toda i.

Los módulos que consideraremos son del tipo de

$$\bigoplus_{i=1}^{m} R(-d_i)$$

donde ahora los elementos base e_i son de grado d_i.

Definición 1.1.20. Sean M y N R-módulos graduados. Decimos que un morfismo de R-módulos $\varphi : M \to N$ es un *morfismo graduado de grado* d si $\varphi(M_i) \subset N_{i+d}$, para toda $i \in \mathbb{Z}$.

Supongamos que M es un R-módulo graduado generado por elementos homogéneos $f_1, \ldots, f_t$ de grado $d_1, \ldots, d_t$ respectivamente. Entonces tenemos un morfismo

$$\varphi : \bigoplus_{i=1}^{t} R(-d_i) \longrightarrow M$$
$$e_i \longmapsto f_i.$$

Por 3) de la proposición (1.4.4), φ es un epimorfismo. Además, al tener que e_i es de grado d_i al igual que f_i, tenemos que φ es un morfismo graduado de grado cero.

1.2 Generadores y Relaciones

En lo que resta del presente trabajo sólo consideraremos R-módulos finitamente generados.

Consideremos al R-módulo libre R^m, que aunque cuenta con base, sus submódulos se comportan muy contrariamente a subespacios vectoriales no importando que sean generados por un conjunto mínimo. Esto se debe a que tal conjunto generador no es necesariamente linealmente independiente.

Ejemplo 1.2.1. Sea $M = \langle f_1, f_2, f_3 \rangle \subset k[x, y, z]^3$ un submódulo, donde $f_1 = (y, -x, 0)$, $f_2 = (z, 0, -x)$ y $f_3 = (0, z, -y)$. Notemos que $M \neq \langle f_i, f_j \rangle$, para todo $1 \leq i, j \leq 3$. En efecto, ya que si $f_1 = pf_2 + qf_3$, con $p, q \in R$, tendríamos que

$$y = pz$$
$$-x = qz$$
$$0 = -qy - pz$$

entonces $pz - y = 0$, es decir, las variables y y z serían linealmente dependientes, contradiciendo el hecho que y y z son elementos de la base para $k[x, y, z]$ como k-espacio vectorial. Análogamente las otras dos posibilidades no son ciertas. Por lo tanto, $\{f_1, f_2, f_3\}$ es un conjunto generador mínimo. Más sin embargo, son un conjunto linealmente dependiente, al cumplir la relación

$$zf_1 - yf_2 + xf_3 = 0.$$

Observación 1.2.2. Como consecuencia de esto, cuando expresemos a un elemento $f \in \langle f_1, \ldots, f_t \rangle$ como:

$$f = \sum_{i=1}^{t} h_i f_i, \qquad h_i \in R,$$

sus coeficientes h_i no serán únicos necesariamente, es decir, un mismo elemento puede tener expresiones distintas en términos del conjunto generador.

Ejemplo 1.2.3. Sea $M \subset k[x, y, z]^3$ como en el ejemplo anterior. Las siguientes expresiones definen al mismo elemento:

$$\begin{aligned} h &= f_1(z + y) + f_2(y + x) + f_3(x + z) \\ &= f_1(y) + f_2(2y + x) + f_3(z) \end{aligned}$$

Esto no ocurre si el conjunto generador es base.

Proposición 1.2.4. *Sea M un R-módulo. Un conjunto $B \subset M$ es base de M si, y sólo si, todo elemento $f \in M$ puede ser escrito en forma única como una combinación R-lineal*

$$f = \sum_{i=1}^{n} p_i f_i, \qquad p_i \in R,\ f_i \in B.$$

Demostración. Véase Cox, Little y O'Shea ([CLO98], pag.186). □

El hecho que algunos módulos no tengan base (o no sepamos como encontrarla) es un problema al momento de hacer cálculos en dichos módulos, ya que necesitamos saber cuando dos combinaciones lineales de un conjunto generador representan a un mismo elemento, es decir, si $\{g_1, \ldots, g_t\}$ es un conjunto generador y dados los elementos $\sum_{i=1}^{t} p_i g_i$ y $\sum_{i=1}^{t} p'_i g_i$, saber si

$$\sum_{i=1}^{t} p_i g_i - \sum_{i=1}^{t} p'_i g_i = \sum_{i=1}^{t} (p_i - p'_i) g_i = 0. \tag{1.1}$$

Tales diferencias son llamadas las *relaciones algebraicas* entre los g_i.

Observación 1.2.5. Puesto que una relación sobre un conjunto generador $G = \{g_1, \ldots, g_t\}$ de un submódulo M, es una combinación R-lineal de los g_i que es igual a cero:

$$\sum_{i=1}^{t} h_i g_i = 0 \qquad \in M,$$

podemos pensar a una relación sobre el conjunto generador G formado por t elementos, como una t-upla $(h_1, \ldots, h_t)$ de elementos de R, es decir, podemos pensar a una relación como un elemento del módulo libre R^t.

Definición 1.2.6. A las relaciones vistas como t-uplas se les dice las *sicigias* del conjunto generador.

Proposición 1.2.7. *Sea M un R-módulo. Sea $G = \{g_1, \ldots, g_t\}$ una colección de t elementos de M. El conjunto de todos los elementos $(h_1, \ldots, h_t) \in R^t$ tales que $\sum_{i=1}^{t} h_i g_i = 0$, es un submódulo de R^t.*

Definición 1.2.8. Al submódulo de R^t dado por las relaciones de G como en la proposición anterior es llamado el *(primer) módulo de sicigias de* $\{g_1, \ldots, g_t\}$, el cual es denotado por $Syz(g_1, \ldots, g_t)$.

Corolario 1.2.9. *El (primer) módulo de sicigias de un conjunto $\{g_1, \ldots, g_t\}$ es finitamente generado.*

Corolario 1.2.10. *Sea M un R-módulo. Un conjunto B es base de M si, y sólo si, $Syz(B) = \{0\}$.*

1.3 Caracterización de las Sicigias

Estaremos trabajando sobre los R-módulos libres finitamente generados. Consideremos al conjunto $G = \{g_1, \ldots, g_t | g_i \in R^m\}$.

1. Puesto que $Syz(g_1, \ldots, g_t)$ es el conjunto de todos los elementos $h = (h_1, \ldots, h_t) \in R^t$ tales que $\sum_{i=1}^{t} h_i g_t = 0$, podemos pensar a $Syz(g_1, \ldots, g_t)$ como el conjunto de todas las soluciones polinomiales $h \in R^t$ de el sistema de ecuaciones lineales homogéneas $Gh = 0$ con coeficientes polinomiales. Es decir, si $g_1 = (g_{11}, \ldots, g_{m1}), \ldots, g_t = (g_{1t}, \ldots, g_{mt})$,

entonces $Syz(g_1,\ldots,g_t)$ es el conjunto de todas las soluciones polinomiales simultáneas $\chi_1,\ldots,\chi_t$ del sistema

$$\begin{aligned} g_{11}\chi_1 &+ \ldots + g_{1t}\chi_t = 0 \\ g_{21}\chi_1 &+ \ldots + g_{2t}\chi_t = 0 \\ &\vdots \\ g_{m1}\chi_1 &+ \ldots + g_{mt}\chi_t = 0 \end{aligned}$$

2. Consideremos el morfismo de R-módulos libres

$$\pi : R^t \longrightarrow R^m$$

$$(h_1,\ldots,h_t) \longmapsto \sum_{i=1}^{t} h_i g_i,$$

teniendo que $Im(\pi) = M = \langle g_1,\ldots,g_t\rangle$.

Por como definimos al morfismo π, es claro que

$$Syz(g_1,\ldots,g_t) = Ker(\pi).$$

1.4 Resoluciones Libres, Graduadas y Presentaciones de Módulos

Dado un R-módulo M, una resolución libre de M nos sirve para *"medir"* que tan lejos está M de ser un R-módulo libre, además de dar algunos invariantes importantes del módulo M. Comenzaremos con una definición muy importante

Definición 1.4.1. Consideremos una sucesión de R-módulos y morfismos

$$\cdots \longrightarrow M_{j+1} \xrightarrow{\varphi_{j+1}} M_j \xrightarrow{\varphi_j} M_{j-1} \longrightarrow \cdots$$

1. Decimos que la sucesión es *exacta en* M_j si $Im(\varphi_{j+1}) = Ker(\varphi_j)$
2. La sucesión se dice que es *exacta* si es exacta en cada M_j.

La importancia de trabajar con sucesiones exactas es que podemos expresar en términos de éstas a algunas propiedades de R-módulos o de morfismos de R-módulos.

Lema 1.4.2. *Sean φ y ψ morfismos de R-módulos. Entonces*

1. *La sucesión*

$$M \xrightarrow{\varphi} M' \longrightarrow 0$$

es exacta si, y sólo si, φ es epimorfismo.

2. *La sucesión*

$$0 \longrightarrow M \xrightarrow{\varphi} M'$$

es exacta si, y sólo si, φ es monomorfismo.

3. *La sucesión*

$$0 \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow 0$$

es exacta si, y sólo si, φ es isomorfismo.

4. *La sucesión*

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

es exacta si, y sólo si, φ es monomorfismo, ψ es epimorfismo e $Im(\varphi) = Ker(\psi)$.

Demostración. Se sigue inmediatamente de la definición. □

Ejemplo 1.4.3. 1. Sea $\varphi : M \to M'$ un morfismo de R-módulos, la sucesión

$$0 \longrightarrow Ker(\varphi) \xrightarrow{i} M \xrightarrow{\varphi} M' \xrightarrow{\nu} Coker(\varphi) \longrightarrow 0$$

es exacta, donde i es el morfismo inclusión, y ν es el morfismo natural sobre su cociente.

2. Sea N un submódulo de un R-módulo M. la sucesión

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\nu} M/N \longrightarrow 0$$

es exacta, donde i es el morfismo inclusión, y ν es el morfismo natural sobre su cociente.

Proposición 1.4.4. *Sea M un R-módulo. Entonces*

1. *Escoger un elemento de M es equivalente a escoger un morfismo de R- módulos*

$$R \longrightarrow M$$

2. *Escoger t elementos de M es equivalente a escoger un morfismo de R-módulos*

$$R^t \longrightarrow M$$

3. *Escoger un conjunto $\{m_1, \ldots, m_t\} \subset M$ que sea generador de M es equivalente a escoger un epimorfismo de R-módulos*

$$R^t \longrightarrow M$$

4. *Si M es libre, escoger una base de t elementos es equivalente a escoger un isomorfismo*

$$R^t \longrightarrow M$$

Demostración. 1. Sea $f \in M$ un elemento dado. Sea

$$\begin{aligned} \varphi : R &\longrightarrow M \\ 1 &\longmapsto f \end{aligned}$$

Así, para todo $r \in R$,

$$\varphi(r) = \varphi(1 \cdot r) = r\varphi(1) = rf$$

Por el teorema (1.1.15), φ es morfismo.

2. Sea $\{f_1, \ldots, f_t\} \subset M$ un conjunto dado. Para todo i, sea

$$\begin{aligned} \varphi_i : R &\longrightarrow M \\ 1 &\longmapsto f_i \end{aligned}$$

Definamos

$$\varphi := \sum_{i=1}^{t} \varphi_i : R^t \longrightarrow M$$

Es decir, si $(r_1, \ldots, r_t) \in R^t$, entonces

$$\varphi(r_1, \ldots, r_t) = \sum_{i=1}^{t} \varphi_i(r_i) = \sum_{i=1}^{t} \varphi_i(1 \cdot r_i) = \sum_{i=1}^{t} r_i\varphi_i(1) = \sum_{i=1}^{t} r_i f_i.$$

Por el teorema (1.1.15), φ es morfismo.

3. Sea $\{e_i\}$ la base estándar de R^t, y sea $\{m_1, \ldots, m_t\}$ un conjunto generador de M. Consideremos

$$\begin{aligned} \varphi : R^t &\longrightarrow M \\ e_i &\longmapsto m_i \end{aligned}$$

Si $(r_1, \ldots, r_t) \in R^t$, entonces

$$\varphi(r_1, \ldots, r_t) = \varphi\left(\sum_{i=1}^{t} e_i r_i\right) = \sum_{i=1}^{t} r_i m_i$$

el cual por el teorema (1.1.15) es morfismo, teniendo que $Im(\varphi) = \langle m_1, \ldots, m_t \rangle$. Pero suposimos que $M = \langle m_1, \ldots, m_t \rangle$. Así, la sucesión

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

es exacta. Pero por *1)* del lema (1.4.2), φ es epimorfismo.

4. Por parte *3)* de esta proposición, tenemos que el morfismo

$$\varphi : R^t \longrightarrow M,$$

es epimorfismo. Sea $(r_1, \ldots, r_t) \in R^t$, y supongamos que $\varphi(r_1, \ldots, r_t) = 0$, teniendo que

$$0 = \varphi(r_1, \ldots, r_t) = \sum_{i=1}^{t} r_i m_i,$$

donde el conjunto de los m_i son linealmente independientes al ser una base para M. Por lo tanto, $m_i = 0$, para todo i. Así, φ es isomorfismo.

□

Proposición 1.4.5. *Sea M un R-módulo finitamente generado, y sea $F = \{f_1, \ldots, f_t\}$ un conjunto generador. Entonces*

1. *Existe una sucesión exacta de la forma:*

$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0 \tag{1.2}$$

para algunos $s, t \in \mathbb{N}$, con φ y ψ epimorfismos.

2 *El módulo M es de la forma*

$$M \cong R^t/Syz(f_1, \ldots, f_t),$$

donde $Syz(f_1, \ldots, f_t) = Ker(\varphi)$.

Definición 1.4.6. A la sucesión (1.2) se le llama la *presentación libre* de M, y al cociente $R^t/Syz(f_1, \ldots, f_t)$ se le dice una *presentación* de M.

Demostración de la proposición (1.4.5). 1. Por *3)* de la proposición (1.4.4), el conjunto generador F da un epimorfismo

$$\varphi : R^t \longrightarrow M,$$

es decir, la sucesión

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

es exacta. Pero φ es el mismo morfismo dado en la Sección 1.3, donde se tenía que

$$Ker(\varphi) = Syz(f_1, \ldots, f_t).$$

Ahora, nuevamente por *3)* de la proposición (1.4.4), dado un conjunto $\{\tau_1, \ldots, \tau_s\}$ que sea generador de $Syz(f_1, \ldots, f_t)$, se tiene un epimorfismo

$$\psi : R^s \longrightarrow Syz(f_1, \ldots, f_t) \subset R^t.$$

Es decir, $Im(\psi) = Syz(f_1, \ldots, f_t) = Ker(\varphi)$, implicando que tenemos la sucesión exacta

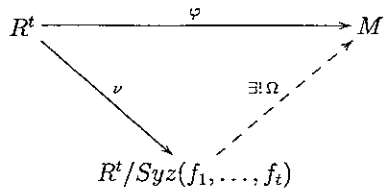
$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0$$

2. Sea $\nu : R^t \to R^t/Syz(f_1, \ldots, f_t)$. Como

$$Syz(f_1, \ldots, f_t) = Ker(\varphi) = Ker(\nu), \tag{1.3}$$

por el teorema (1.1.5), existe un único morfismo $\Omega : R^t/Syz(f_1, \ldots, f_t) \to M$, tal que cumple con

$$\varphi = \Omega \circ \nu$$



Sabemos que φ es epimorfismo, y considerando a la igualdad (1.3) junto con el teorema (1.1.5), tenemos que Ω es un isomorfismo único.

□

Sea $M \subset R^m$ un submódulo, y $F = \{f_1, \ldots, f_{t_0}\}$ un conjunto generador para M. Sea $\mathcal{S}_0 = \{\tau_1^{(0)}, \ldots, \tau_{t_1}^{(0)}\}$ un conjunto generador para $Syz(f_1, \ldots, f_{t_0}) \subset R^{t_0}$. Así, la proposición anterior nos dice que el submódulo M es de la forma

$$M \cong R^{t_0}/\langle \mathcal{S}_0 \rangle.$$

Pero esto nos da una sucesión exacta de la forma

$$0 \longrightarrow \langle \mathcal{S}_0 \rangle \xrightarrow{i_0} R^{t_0} \xrightarrow{\pi_0} M \longrightarrow 0 \tag{1.4}$$

Siendo $i_0 : \langle \mathcal{S}_0 \rangle \to R^{t_0}$ el mapeo inclusión, y $\pi_0 : R^{t_0} \to M$ el mapeo definido al final de la Sección 1.3.

Al ser $\langle \mathcal{S}_0 \rangle$ un módulo, su conjunto generador cuenta también con un módulo de sicigias. Sea $\mathcal{S}_1 = \{\tau_1^{(1)}, \ldots, \tau_{t_2}^{(1)}\}$ el conjunto generador para $Syz(\tau_1^{(0)}, \ldots, \tau_{t_1}^{(0)}) \subset R^{t_1}$, el cual tiene una representación de la forma

$$\langle \mathcal{S}_0 \rangle \cong R^{t_1}/\langle \mathcal{S}_1 \rangle$$

además de contar con la sucesión exacta

$$0 \longrightarrow \langle \mathcal{S}_1 \rangle \xrightarrow{i_1} R^{t_1} \xrightarrow{\pi_1} \langle \mathcal{S}_0 \rangle \longrightarrow 0 \tag{1.5}$$

El submódulo $\langle \mathcal{S}_1 \rangle \subset R^{t_1}$ es llamado el *segundo módulo de sicigias de* M. Continuando con este proceso recursivamente, tenemos en el $j+1$ paso la presentación

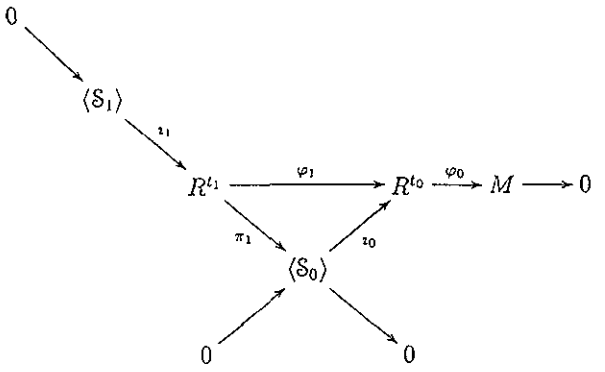
$$\langle \mathcal{S}_{j-1} \rangle \cong R^{t_j}/\langle \mathcal{S}_j \rangle$$

con la sucesión exacta corta

$$0 \longrightarrow \langle \mathcal{S}_j \rangle \xrightarrow{i_{j-1}} R^{t_{j-1}} \xrightarrow{\pi_{j-1}} \langle \mathcal{S}_{j-1} \rangle \longrightarrow 0$$

El submódulo $\langle S_j \rangle$ es el *j-ésimo módulo de sicigias de* M.

De las sucesiones exactas (1.4) y (1.5) tenemos el siguiente diagrama



Donde $\varphi_0 = \pi_0$, y $\varphi_1 = \pi_1 \circ i_0$. Teniendo en particular la sucesión de R-módulos libres

$$\longrightarrow R^{t_1} \xrightarrow{\varphi_1} R^{t_0} \xrightarrow{\varphi_0} M \longrightarrow 0$$

Análogamente, para toda j tenemos

$$\cdots \longrightarrow R^{t_{j+1}} \xrightarrow{\varphi_{j+1}} R^{t_j} \xrightarrow{\varphi_j} R^{t_{j-1}} \longrightarrow \cdots$$

De esta forma, le hemos asociado a M una sucesión de la forma:

$$\cdots \longrightarrow R^{t_{j+1}} \xrightarrow{\varphi_{j+1}} R^{t_j} \xrightarrow{\varphi_j} R^{t_{j-1}} \xrightarrow{\varphi_{j-1}} \cdots \xrightarrow{\varphi_2} R^{t_1} \xrightarrow{\varphi_1} R^{t_0} \xrightarrow{\varphi_0} M \longrightarrow 0 \qquad (1.6)$$

Esta nueva sucesión da pie a la siguiente definición.

Definición 1.4.7. Sea M un R-módulo. Una *resolución libre* M° para el módulo M es una sucesión exacta de la forma

$$\cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

donde F_j es un R-módulo libre, es decir, $F_j \cong R^{m_j}$ para toda j. Si existe $n \in \mathbb{N}$ tal que $F_{n+1} = F_{n+2} = \ldots = 0$, con $F_n \neq 0$, decimos que la resolución es *finita de longitud* n.

A las resoluciones de longitud n las escribiremos de la forma

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

Proposición 1.4.8. *Sea M un R-módulo finitamente generado. Entonces M tiene una resolución libre.*

Demostración. En la discusión anterior encontramos la sucesión de R-módulos libres (1.6) para M, restándonos mostrar que tal sucesión es exacta.

Observemos que el morfismo $i_j : \langle S_j \rangle \to R^{t_j}$ es un encaje, y como $\varphi_j = i_{j-1} \circ \pi_j$, tenemos que $Im(\pi_j) = Im(\varphi_j)$. Pero recordemos que $Im(\pi_j) = \langle S_{j-1} \rangle = Ker(\varphi_{j-1})$, es decir, $Im(\pi_j) = Ker(\varphi_{j-1})$, esto para toda $j = 1, 2, \ldots$ □

Proposición 1.4.9. *En una resolución libre finita*

$$0 \longrightarrow F_l \xrightarrow{\varphi_l} F_{l-1} \xrightarrow{\varphi_{l-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0 \tag{1.7}$$

$Ker(\varphi_{l-1})$ es un R-módulo libre. Conversamente, si M tiene una resolución libre en la cual $Ker(\varphi_{l-1})$ es un R-módulo libre para algún l, entonces M tiene una resolución libre finita de longitud l.

Demostración. Si (1.7) es una resolución libre de longitud l, entonces φ_l es monomorfismo al ser exacta en F_l, así su imagen es isomorfa a F_l, que es R-módulo libre.

Conversamente, consideremos la resolución libre

$$F_{l-1} \xrightarrow{\varphi_{l-1}} F_{l-2} \xrightarrow{\varphi_{l-2}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

Sea $F_l = Ker(\varphi_{l-1})$ y $\varphi_l : F_l \to F_{l-1}$ el morfismo inclusión. Así,

$$0 \longrightarrow F_l \xrightarrow{\varphi_l} F_{l-1} \xrightarrow{\varphi_{l-1}} F_{l-2} \xrightarrow{\varphi_{l-2}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

es resolución libre, ya que por definición φ_l es monomorfismo, y también por definición $Im(\varphi_l) \cong F_l = Ker(\varphi_{l-1})$. □

Vimos al principio de este capítulo que todo R-módulo libre es un R-módulo graduado, así la siguiente definición es de esperarse.

Definición 1.4.10. Una *resolución graduada* $M^\bullet$ para el R-módulo M es una sucesión exacta de la forma

$$\cdots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

donde cada F_j es un R-módulo libre graduado deslizado $\bigoplus_{i=1}^{m} R(-d_i)$ y cada morfismo φ_i es un morfismo graduado de grado cero. Si existe $n \in \mathbb{N}$ tal que $F_{n+1} = F_{n+2} = \ldots = 0$, con $F_n \neq 0$, decimos que la resolución es *finita de longitud n.*

Acabamos con un resultado que nos será de gran utilidad en el último capítulo.

Lema 1.4.11. *Sea $\{V_i\}_{i=0}^n$ un conjunto de k-espacios vectoriales de dimensión finita. Consideremos a la sucesión exacta*

$$0 \longrightarrow V_n \xrightarrow{\varphi_n} V_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_2} V_1 \xrightarrow{\varphi_1} V_0 \longrightarrow 0. \tag{1.8}$$

Entonces

$$\sum_{i=0}^{n}(-1)^i dim_k(V_i) = 0.$$

Demostración. Como (1.8) es una sucesión exacta tenemos que

$$Im(\varphi_{i+1}) = Ker(\varphi_i)$$

para $i = 0, \ldots, n-1$. Al ser los V_i k-espacios vectoriales de dimensión finita, tenemos que

$$dim_k(V_i) = dim_k(Ker(\varphi_i)) + dim_k(Im(\varphi_i)) \tag{1.9}$$

Así

$$\begin{aligned} dim_k(V_1) &= dim_k(Ker(\varphi_1)) + dim_k(Im(\varphi_1)) \\ &= dim_k(Ker(\varphi_1)) + dim_k(V_0). \end{aligned}$$

Lo que implica que

$$dim_k(V_0) - dim_k(V_1) + dim_k(Ker(\varphi_1)) = 0. \tag{1.10}$$

Ahora, por (1.9)

$$dim_k(Ker(\varphi_1)) = dim_k(Im(\varphi_2)) = dim_k(V_2) - dim_k(Ker(\varphi_2)).$$

Sustituyendo en (1.10) obtenemos

$$dim_k(V_0) - dim_k(V_1) + dim_k(V_2) - dim_k(Ker(\varphi_2)) = 0$$

donde, análogamente

$$dim_k(Ker(\varphi_2)) = dim_k(V_3) - dim_k(Ker(\varphi_3))$$

y sustituyendo tenemos que

$$dim_k(V_0) - dim_k(V_1) + dim_k(V_2) - dim_k(V_3) + dim_k(Ker(\varphi_3)) = 0.$$

Repitiendo el proceso hasta considerar al morfismo φ_n, tenemos que

$$dim_k(V_0) - dim_k(V_1) + \ldots + (-1)^n dim_k(V_n) + (-1)^{n+1} dim_k(Ker(\varphi_n)) = 0.$$

Pero $Ker(\varphi_n) = 0$ al ser (1.8) exacta en V_n. Por lo tanto

$$\sum_{i=0}^{n} (-1)^i dim_k(V_i) = 0.$$

□

Capítulo 2

Bases de Gröbner

Una herramienta importante al momento de hacer cálculos en módulos sobre el anillo de polinomios son las bases de Gröbner. En la primera sección estudiaremos a los submódulos monomiales, resolviendo el problema de la membresía en este caso, para después motivar y tratar el concepto de orden monomial. Todo esto para poder llegar al concepto de bases de Gröbner y así comenzar su estudio y poder resolver el problema de membresía para un submódulo arbitrario. Para este propósito también estudiamos una versión generalizada del algoritmo de división. En la última sección veremos los S-vectores, con los cuales podremos caracterizar a las bases de Gröbner, caracterización que da a lugar a un algoritmo de obtención de bases de Gröbner, el algoritmo de Buchberger, así como un método de obtención de bases de Gröbner únicas.

En este capítulo denotaremos por $R = k[x_1, \ldots, x_r]$ al anillo de polinomios en r variables con coeficientes en el campo k. Podemos pensar al campo k como $\mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$. Al conjunto de todos los monomios en R lo denotaremos por $\mathbb{M}_R$.

En lo que resta del presente trabajo, todos los R-módulos que consideremos serán finitamente generados.

2.1 Submódulos y Ordenes Monomiales

Para simplificar la escritura de monomios haremos uso de multi-índices. Si $a = (a_1, \ldots, a_r)$ con $a_i \in \mathbb{N}$, entonces un monomio se escribirá como $x^a = x_1^{a_1} x_2^{a_2}, \cdots, x_r^{a_r}$.

2.1.1 Ideales y Submódulos Monomiales

La importancia de trabajar con ideales monomiales radica en el hecho de que el problema de la membresía es facilmente resuelto en esta clase de ideales, como los lemas a continuación lo demuestran. Pero antes daremos algunas definiciones.

Definición 2.1.1. Sean $a, b, c \in \mathbb{N}^r$, diremos que el monomio x^a *divide* al monomio x^b (denotándolo por $x^a | x^b$) si existe un monomio x^c tal que $x^a x^c = x^b$.

Definición 2.1.2. Dado un subconjunto $A \subseteq \mathbb{N}^r$ (posiblemente infinito), un ideal $J \subseteq R$ es llamado *ideal monomial* si es de la forma

$$J = \langle x^a | a \in A \rangle,$$

es decir, es generado por un conjunto (posiblemente infinito) de monomios.

Primero caracterizaremos a todos los elementos pertenecientes a dichos ideales.

Lema 2.1.3. *Sea $J = \langle x^a | a \in A \subset \mathbb{N}^r \rangle$ un ideal monomial. Entonces un monomio $x^b \in R$ está en J si, y sólo si, x^b es divisible por x^a, para alguna $a \in A$.*

Demostración. Sea $x^b \in J$, entonces podemos escribir

$$x^b = \sum_{i=1}^{k} p_i x^{a(i)} \quad \text{donde} \quad p_i \in R,\ a(i) \in A.$$

Desarrollando la parte derecha de la igualdad obtenemos una suma de términos donde cada uno es divisible por algún $x^{a(i)}$. En tal desarrollo habrá términos que se eliminen entre sí, los términos que no se eliminaron contienen al mismo monomio, justamente x^b. Esto debido a que dicha suma de términos es igual a un monomio y, que toda suma de monomios es linealmente independiente. Así x^b es divisible por algún elemento generador de J. Conversamente, si x^b es múltiplo de x^a, para alguna $a \in A$, entonces $x^b \in J$ por definición de ideal. □

Con el siguiente lema queda resuelto el problema de la membresía en un ideal monomial.

Lema 2.1.4. *Sea $J = \langle x^a | a \in A \subset \mathbb{N}^r \rangle$ un ideal monomial, y $f \in R$. Entonces $f \in J$ si, y sólo si, cada uno de los términos de f pertenecen a J.*

Demostración Sea $f \in J$ y tomemos la descomposición de f en sus términos,

$$f = \sum_{i=1}^{k} \alpha_i x^{b(i)} \qquad \text{donde} \quad x^{b(i)} \in R,\ \alpha_i \in k. \tag{2.1}$$

Por otro lado, como $f \in J$,

$$f = \sum_{j=1}^{n} p_j x^{a(j)} \qquad \text{donde} \quad p_j \in R,\ a(j) \in A. \tag{2.2}$$

Desarrollando la ecuación (2.2) obtenemos una suma de términos, donde cada término es divisible por algún $x^{a(j)}$. Pero como R es un k-espacio vectorial teniendo como base al conjunto $\mathbb{M}_R$, el desarrollo en sus términos de la ecuación (2.2) coincide con la ecuación (2.1), así todo término de f es divisible por algún $x^{a(j)}$. Conversamente, si cada término de f pertenece a J, por definición de ideal tenemos que $f \in J$.

□

Hasta el momento hemos resuelto el problema de la membresía en ideales monomiales, pero en realidad lo que buscamos es poder hacer cálculos en dichos ideales monomiales, y una base infinita no nos sirve de mucho. El siguiente teorema nos soluciona este problema.

Teorema 2.1.5. Todo ideal monomial $J = \langle x^a | a \in A \in \mathbb{N}^r \rangle$ es de la forma

$$J = \langle x^{a(1)}, \ldots, x^{a(s)} \rangle, \qquad a(i) \in A.$$

Demostración. Por el teorema de la base de Hilbert tenemos que el ideal monomial tiene la forma

$$J = \langle f_1, \ldots, f_n \rangle,$$

donde cada $f_i \in R$ es un polinomio. Sea G el conjunto de todos los monomios de los polinomios generadores del ideal monomial J, es decir, $G = \{x^a | x^a$ es monomio de algún f_i, $i = 1, \ldots, n\}$. Consideremos al ideal $\langle G \rangle$, si demostramos que $\langle G \rangle = \langle f_1, \ldots, f_n \rangle$ habremos acabado, ya que G es un conjunto finito de monomios. Como cada f_i es combinación lineal del conjunto de monomios G, sólo nos basta ver que todo monomio de G esta dado por una combinación lineal de los f_i. Sabemos que para toda i, $f_i \in J$, entonces por el lema (2.1.4) cada monomio de los f_i pertenece a J. Teniendo así una combinación lineal

$$x^a = \sum_{i=1}^{s} g_i f_i \ \in G, \qquad g_i \in R.$$

□

Lo siguiente es definir un par de objetos que nos serán de gran utilidad.

Definición 2.1.6. El *máximo común divisor* de 2 monomios $x^a, x^b \in R$, es un monomio denotado por $mcd(x^a, x^b)$, que está dado de la siguiente manera:

$$mcd(x^a, x^b) = x_1^{min(a_1,b_1)} x_2^{min(a_2,b_2)} \cdots x_r^{min(a_r,b_r)}.$$

Definición 2.1.7. El *mínimo común múltiplo* de 2 monomios $x^a, x^b \in R$, es un monomio denotado por $mcm[x^a, x^b]$. que esta dado de la siguiente manera:

$$mcm[x^a, x^b] = x_1^{max(a_1,b_1)} x_2^{max(a_2,b_2)} \cdots x_r^{max(a_r,b_r)}.$$

Lema 2.1.8. *Sean $x^a, x^b \in R$ monomios. Entonces*

$$x^a x^b = mcd(x^a, x^b) \cdot mcm[x^a, x^b]$$

□

Extendemos estas definiciones y resultados a cualquier R-módulo libre R^m de manera inmediata. Sólo basta recordar que todo R-módulo libre R^m es finitamente generado y es de la forma $\bigoplus_{i=1}^m Re_i$, donde usamos la base canónica $\{e_i\}$.

Definición 2.1.9. Un *monomio* m en R^m es un elemento de la forma $x^a e_i$ para alguna i. En este caso diremos que m *contiene* al vector base estándar e_i.

Comentario 2.1.10. Cada elemento $f \in R^m$ puede ser escrito en forma única como una combinación k-lineal de monomios $m_i \in R^m$

$$f = \sum_{i=1}^{n} \alpha_i m_{i_i} \qquad \alpha_i \in k\backslash\{0\}. \tag{2.3}$$

Lo que estamos diciendo es que, como R es un k-espacio vectorial teniendo como base al conjunto de monomios $\mathbb{M}_R$ en R, el módulo libre R^m es también un k-espacio vectorial teniendo como base al conjunto de monomios $\mathbb{M}$ en R^m.

Ejemplo 2.1.11. Sea $R^3 = k[x_1, x_2]^3$, y notemos que

$$\begin{aligned} f &= (5xy^2 - y^{10} + 3\,,\, 4x^3 + 2y\,,\, 16x) \\ &= 5(xy^2, 0, 0) - (y^{10}, 0, 0) + 3(1, 0, 0) + 4(0, x^3, 0) + 2(0, y, 0) + 16(0, 0, x) \\ &= 5xy^2 e_1 - y^{10} e_1 + 3e_1 + 4x^3 e_2 + 2ye_2 + 16xe_3. \end{aligned}$$

Definición 2.1.12. Al producto αm, de un monomio $m \in R^m$ por un escalar $\alpha \in k$ se le llama *término*. Diremos que los términos $\alpha_i m_i$ y los monomios m_i correspondientes en la descomposición (2.3) de $f \in R^m$, *pertenecen* a f.

Sean $m, n \in R^m$ monomios, $m = x^a e_i$ y $n = x^b e_j$, entonces decimos que n *divide* a m (o m es *divisible* por n) si, y sólo si, $i = j$ y x^b divide a x^a en R. El *cociente* será $x^a/x^b \in R$, es decir, $m/n = x^{a-b} \in R$.

Si m y n son monomios que contienen al mismo elemento base e_i, podemos definir el *máximo común divisor* y el *mínimo común múltiplo* de m y n como:

1. $mcd(m, n) = mcd(x^a, x^b)e_i$
2. $mcm[m, n] = mcm(x^a, x^b)e_i$,

respectivamente.

Nota 2.1.13. Si m y n son monomios que no contienen al mismo elemento base de R^m, podemos definir al mínimo común múltiplo como:

$$mcm[m, n] = 0.$$

Lema 2.1.14. *Sean $m, n \in R^m$ monomios. Entonces*

$$m\, n = mcd(m, n) \cdot mcm[m, n].$$

□

Definición 2.1.15. Decimos que un submódulo $M \subset R^m$ es un *submódulo monomial* si M es generado por una colección de monomios.

Lema 2.1.16. *Todo submódulo monomial $M \subset R^m$, es suma directa de módulos de la forma $J_i e_i$, con $J_i \in R$ ideal monomial.*

Demostración. Sea $G = \{m_i\}_{i \in I}$ el conjunto generador de M, con $I \subset \mathbb{N}$, entonces $m_i = x^a e_j$, para alguna j. Sea $M_j = J_j e_j$ el submódulo generado por todos los monomios en G que contienen al elemento base e_j, esto para cada j. Entonces tenemos que $M = \bigoplus_{j=1}^{m} M_j = \bigoplus_{j=1}^{m} J_j e_j$, que es justamente lo que queríamos demostrar.

□

Ahora damos los resultados para submódulos monomiales análogos a los que se dieron para ideales monomiales.

Lema 2.1.17. *Sea $M \subset R^m$ un submódulo monomial. Entonces un monomio $x^a e_i$ está en M si, y sólo si, $x^a e_i$ es divisible por alguno de los monomios generadores de M.*

Demostración. Sea $M = \bigoplus_{i=1}^m J_i e_i$. Si $x^a e_i \in M$ entonces $x^a e_i \in J_i e_i$. Así, el problema se reduce a demostrar que x^a es divisible por alguno de los generadores de J, pero por el lema (2.1.3) esto sucede. Conversamente, si $x^a e_i$ es divisible por alguno de los generadores de M, por definición de submódulo $x^a e_i \in M$.

□

Lema 2.1.18. *Sea $M \subset R^m$ submódulo monomial, y sea $f \in R^m$. Entonces $f \in M$ si, y sólo si, cada uno de los términos de f pertenece a M.*

Demostración. Tomando en cuenta el Comentario (2.1.10), la demostración es completamente análoga a la del lema (2.1.4). □

Teorema 2.1.19. Todo submódulo monomial $M \subset R^m$, es de la forma $M = \langle m_1, \ldots, m_t \rangle$.

Demostración. Sea $M = \bigoplus_{i=1}^m M_i = \bigoplus_{i=1}^m J_i e_i$. Por el teorema (2.1.5) tenemos que $J_i = \langle x^{a(i1)}, \ldots, x^{a(ik_i)} \rangle$, entonces el conjunto de monomios

$$\begin{array}{ccc} x^{a(11)}e_1, & \ldots & , x^{a(1k_1)}e_1 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ x^{a(m1)}e_m, & \ldots & , x^{a(mk_m)}e_m \end{array}$$

generan M.

□

Dado cualquier conjunto de monomios generadores de M, podemos eliminar aquellos que sean divisibles por otros monomios del conjunto y tener todavía un conjunto generador de M. De esta forma obtenemos un conjunto mínimo de monomios generadores de M, mínimo respecto al orden parcial dado por la divisibilidad de monomios en R^m. A este conjunto lo llamaremos *generadores mínimos de M*.

2.1.2 Ordenes Monomiales

Con lo visto en la sección anterior tenemos que si $J \subset R$ es un ideal monomial, el conjunto B de todos los monomios que no están en J forman una base de k-espacio vectorial para R/J, lo cual hace más accesible el poder hacer cálculos en R/J. Para el caso con I un ideal arbitrario, nos gustaría tener una situación igual de simple para R/I. Para esto, como los monomios de R forman una base de k-espacio vectorial, sus imagenes en R/I generan R/I, así, un subconjunto máximo linealmente independiente será una base, llamada *base monomial.*

Si además, podemos escoger a B como el complemento del conjunto de monomios de algún ideal monomial J, tendremos una gran ventaja, principalmente en el problema de la membresía. Se probará más adelante, en el teorema de Macaulay, que tal base monomial B existe para R/I, con I un ideal arbitrario. Antes haremos algunas observaciones y definiciones.

Definición 2.1.20. Sea M un submódulo de R^m, y sea B un conjunto de monomios. Decimos que los elementos $\{m_i\}_{i=1}^{s} \subset B$ son *linealmente dependientes módulo* M, si existe una relación de la forma.

$$p = \sum_{i=1}^{s} \alpha_i m_i \in M, \qquad \alpha_i \in k\backslash\{0\}.$$

En caso contrario, diremos que son *linealmente independientes módulo* M.

Lo que estamos diciendo es que B es linealmente independiente módulo M si ningún elemento de M se puede escribir como suma de elementos de B.

Con estas nociones, sea J un ideal monomial y B el conjunto de monomios que no están en J. Los elementos de B, por como los tomamos, son linealmente independientes módulo el ideal J, y si queremos que los elementos de B permanezcan linealmente independientes módulo un ideal arbitrario I, ningún elemento de I deberá poder escribirse como suma de elementos de B, es decir, para cada elemento $f \in I$ hay al menos un monomio de f que no pertenece a B.

En otras palabras, los elementos de B son linealmente independientes módulo el ideal I, *si el ideal monomial J contiene al menos un monomio de cada elemento de I.* El inverso también es válido, si *el ideal monomial J contiene al menos un monomio de cada elemento de I*, al momento de tomar a B como el conjunto de monomios que no están en J, no hay elemento de I que pueda ser escrito por monomios de B, es decir, los monomios de B son

linealmente independientes módulo el ideal I. Así, tenemos el siguiente lema:

Lema 2.1.21. *Sea I un ideal arbitrario. Sea J un ideal monomial, B el complemento de J en $\mathbb{M}_R$. Los monomios de B son linealmente independientes módulo el ideal I si, y sólo si, J contiene al menos un monomio de cada polinomio en I.*

De esta forma ya hemos asociado a los elementos de un ideal I (no necesariamente monomial) con los de algún ideal monomial J, bastándonos escoger un monomio de cada elemento de I. Como queremos que los elementos de B sean base para R/I, necesitamos que sea máximo, en el sentido de contener al mayor número de monomios posibles, lo que significa que debemos buscar hacer a J lo más pequeño posible. Para lograr esto necesitamos un método de elección que tome en cuenta algunas consideraciones.

Supongamos por ejemplo que x^a, x^b, x^c son monomios distintos de grado d, y consideremos al ideal

$$I = \langle x^a + x^b, x^b + x^c \rangle.$$

Supongamos que elegimos a x^a de $x^a + x^b$ y, a x^b de $x^b + x^c$ para ponerlos en J. Notemos que el ideal I también contiene al polinomio

$$(x^a + x^b) - (x^b + x^c) = x^a - x^c.$$

Si elegimos a x^c para J, tendríamos que J no es mínimo, así que nuestra elección debe ser x^a.

En la relación del ejemplo anterior: el monomio $x^{a(i)}$ es elegido sobre el monomio $x^{a(j)}$, denotando esta elección por $x^{a(i)} > x^{a(j)}$, tenemos que la relación $>$ debe satisfacer el axioma para una relación de orden. Si $x^a > x^b > x^c \Rightarrow x^a > x^c$. Así que una forma de seleccionar a los monomios es dándoles un orden y posteriormente tomar el monomio más grande de cada polinomio en I y ponerlo en J.

Teniendo presente que J es ideal, el orden $>$ debe satisfacer dos requerimientos más. *Primero*, el orden debe ser congruente con la operación con que hemos estado trabajando, divisibilidad. Así, si x^b es divisible por x^a, debemos tener que $x^b > x^a$. *Segundo*, el orden debe preservarse bajo el producto. Supongamos que $I = \langle x^a + x^b \rangle$ con $x^a > x^b$ y tal que $x^b \nmid x^a$, teniendo entonces que $x^a \in J$. Sea $x^c \in R$ un monomio, así $x^c x^a + x^c x^b \in I$, donde $x^c x^a \in J$, al ser J un ideal. Tomando $x^c x^b > x^c x^a$ tendríamos que J no sería mínimo, pero tomando $x^c x^a > x^c x^b$, J sería mínimo. Teniendo esto en consideración, llegamos a la siguiente definición.

Definición 2.1.22. Sea R^m un R-módulo libre. Un *orden monomial*, $>$, sobre R^m es un orden total sobre los monomios de R^m tal que si m_1, m_2 son monomios de R^m y $x^a \neq 1$ es monomio de R, entonces

$$m_1 > m_2 \qquad \text{implica} \qquad x^a m_1 > x^a m_2 > m_2.$$

Proposición 2.1.23. *Sean $m, n \in R^m$ monomios distintos. Si $m|n$, entonces $n > m$.*

Demostración. Sean $m = x^a e_i$ y $n = x^b e_i$. Como $m|n$, tenemos que $x^a|x^b$, existiendo un monomio $x^c \in R$, con $x^c \neq 1$, tal que $x^c m = n$. Por definición de orden monomial tenemos que

$$n = x^c m > m$$

□

Esta proposición nos dice que nuestra definición de orden monomial cumple con todo lo deseado. Ahora demostraremos un lema de gran utilidad.

Lema 2.1.24. *Sea R^m un R-módulo libre. Cualquier orden monomial sobre R^m es un* buen orden, *es decir, para cada subconjunto $A \subset \mathbb{M}$, existe un monomio $m \in A$ tal que para todo $m' \in A$, $m \leq m'$ (cada subconjunto tiene un último elemento)*

Demostración Sea $A \subset \mathbb{M}$ un subconjunto de monomios de R^m. Por el teorema (2.1.19), el submódulo monomial $\langle A \rangle \subset R^m$ es generado por un número finito de monomios pertenecientes al subconjunto A. Sea $X = \{m_1, \ldots, m_n\}$ tal conjunto generador. En particular, los elementos de X están ordenados, donde al ser un número finito tienen un último elemento. Sin pérdida de generalidad, sea m_n el elemento más pequeño de X. Como todo monomio en $\langle A \rangle$ es de la forma $x^a m_i$, tenemos por definición de orden monomial que

$$x^a m_i > x^a m_n > m_n.$$

Esto para todo monomio en A.

□

Extenderemos la noción de orden a términos. Si αm y βn son términos de R^m, con $\alpha, \beta \in k \backslash \{0\}$ escalares distintos de cero, $m, n \in R^m$ monomios con $m > n$ (respectivamente, $m \geq n$), entonces tendremos $\alpha m > \beta n$ (respectivamente, $\alpha m \geq \beta n$).

Observación 2.1.25. Notemos que esto no es un orden parcial sobre los términos de R^m, ya que si tomamos $m = n$ y $\alpha \neq \beta$, tenemos que $\alpha m \geq \beta m$ y $\beta m \geq \alpha m$.

Definición 2.1.26. Sea $>$ un orden monomial sobre R^m. Para cualquier elemento $f \in R^m$ definimos el *monomio inicial de* f, denotado por $lm_>(f)$, como el monomio más grande con respecto al orden $>$. Al coeficiente del monomio inicial lo llamaremos *coeficiente inicial de* f, y lo denotaremos por $lc_>(f)$. Definimos el *término inicial de* f con respecto al orden $>$, denotado por $in_>(f)$, como el producto $lc_>(f)lm_>(f)$. Si M es un submódulo de R^m, definimos el *submódulo inicial de* M, denotado por $in_>(M)$, como el submódulo monomial generado por los elementos $in_>(f)$ para todo $f \in M$.

Observación 2.1.27. Es claro de la definición anterior que, si M es submódulo monomial, entonces $in_>(M) = M$, lo que es congruente con lo deseado.

Ahora ya estamos en posición de dar el resultado más importante de esta sección.

Teorema 2.1.28 (Macaulay). Sea R^m un R-módulo, y sea $M \subset R^m$ un submódulo arbitrario. Para cada orden monomial $>$ sobre R^m, el conjunto B de todos los monomios que no están en $in_>(M)$ forman una base para R^m/M.

Demostración. Veamos primero que los elementos de B son linealmente independientes. Supongamos que no ocurre así, que tenemos una relación de dependencia

$$p = \sum_{i=1}^{n} \alpha_i m_i \in M, \qquad m_i \in B,\ \alpha_i \in k\backslash\{0\}.$$

Lo que implica que $in_>(p) \in in_>(M)$. Al ser $in_>(p)$ alguno de los $\alpha_i m_i$, tenemos una contradicción a la pertenencia de los m_i al conjunto B. Por lo tanto, los elementos de B son linealmente independientes.

Ahora veamos que B genera al módulo R^m/M. De entre todos los elementos de $R^m\backslash M$, por el lema (2.1.24), podemos escoger a un elemento con término inicial mínimo. Sea f dicho elemento. Para el término $in_>(f)$ tenemos dos opciones.

i) $in_>(f) \in in_>(M)$. Tomemos al elemento $f' = f - g$, donde $g \in M$ y es tal que $in_>(f) = in_>(g)$. Como $in_>(f) > in_>(f')$, tenemos que $f' \in M$. Así, $f = f' + g \in M$ (contrario a la suposición de que $f \in R^m\backslash M$). Por lo tanto, $in_>(f) \notin in_>(M)$, quedándonos sólo una opción.

ii) $in_>(f) \in B$. Tomemos al elemento $f' = f - in_>(f)$, con lo cual $in_>(f) > in_>(f')$, por lo que $f' \in M$. Así, $f = f' + in_>(f)$ es la suma de un elemento que vive en $\langle B \rangle$ ($in_>(f)$) más un elemento de M (el cual es f'), es decir, en R^m/M el elemento f vive en el generado por B. Por lo tanto, R^m/M es generado por B. □

Lo siguiente es un lema que nos será de gran utilidad en el próximo capítulo.

Lema 2.1.29. *Si $N \subseteq M \subseteq R^m$ son submódulos finitamente generados y $in_>(N) = in_>(M)$ con respecto a un mismo orden monomial $>$, entonces $N = M$.*

Demostración. Supongamos que $N \subsetneq M$. Por el lema (2.1.24) existe $f \in M \backslash N$ con término inicial mínimo de entre todos los elementos de $M \backslash N$. Como $in_>(f) \in in_>(M) = in_>(N)$, existe $g \in N$ tal que $in_>(g) = in_>(f)$. El elemento $f' = f - g \in M$ es tal que $in_>(f') < in_>(f)$, teniendo que $f' \in N$. Pero entonces $f = f' + g \in N$, contradiciendo la elección de f Por lo tanto, $N = M$.

□

Se pueden dar ordenes monomiales sobre un módulo libre R^m con base $\{e_i\}$ a partir de ordenes monomiales sobre R. En todo orden monomial que demos sobre R^m tendremos a la base ordenada mediante $e_i > e_j$ si, y sólo si, $i < j$

Definición 2.1.30. Sea $>_i$ un orden monomial sobre R.

1.-Decimos que $x^a e_i >_{TOP} x^b e_j$ si $x^a >_i x^b$ o, si $x^a = x^b$ y $j > i$

2.-Decimos que $x^a e_i >_{POT} x^b e_j$ si $j > i$ o, si $i = j$ y $x^a >_i x^b$.

Sólo nos basta dar ejemplos de ordenes monomiales en R. Siempre tendremos numeradas a las variables con $x_1 > x_2 > \ldots > x_r$, y sólo describiremos ordenes con esta propiedad.

Ejemplo 2.1.31. Sea $R^m = k[x]$ el anillo de polinomios en una variable El único orden monomial sobre R^m es el orden dado por el grado Para notar esto, sea $>$ un orden sobre R^m. Sean $x^a, x^b \in R^m$ monomios tales que $x^a > x^b$ Al ser R^m un Anillo Euclideano y por la proposición (2.1.23), tenemos que $x^b | x^a$. Entonces existe $c \in \mathbb{N}$ tal que $x^b x^c = x^a$, es decir, $b < a$. Así, el orden $>$ coincide con el orden dado por el grado.

Ejemplo 2.1.32. Sea $R^m = k[x_1, x_2]$. En este caso, sólo hay un orden monomial sobre R^m que refina el orden dado por el grado y que satisface la convención $x_1 > x_2$. Para ver esto,

sean $x^a = x_1^{a_1}x_2^{a_2}$ y $x^b = x_1^{b_1}x_2^{b_2}$ monomios con $a_1+a_2 = b_1+b_2$. Si $a_1 > b_1$, sea $\varepsilon = a_1 - b_1 > 0$. Denotando por $p = x_1^{b_1}x_2^{a_2}$, al máximo común divisor de x^a y x^b, tenemos que

$$x^a = x_1^{\varepsilon}p \qquad y \qquad x^b = x_2^{\varepsilon}p.$$

Al ser $x_1 > x_2$, se cumple que $x_1^{\varepsilon} > x_1^{\varepsilon-1}x_2 > x_2^{\varepsilon}$. Pero lo anterior por definición de orden monomial nos dice que $x^a > x^b$, así, el único orden que refina el orden dado por el grado es el orden dado por comparar el grado en x_1.

Los siguientes tres ejemplos de ordenes monomiales son los más importantes en la literatura.

ORDEN LEXICOGRAFICO (OL). Decimos que $x^a >_l x^b$ si, y sólo si, $a_i > b_i$ para el primer índice i con $a_i \neq b_i$.

ORDEN LEXICOGRAFICO HOMOGÉNEO (OLH). Decimos que $x^a >_h x^b$ si, y sólo si, $deg(x^a) > deg(x^b)$ ó, $deg(x^a) = deg(x^b)$ y $a_i > b_i$ para el primer índice i con $a_i \neq b_i$.

ORDEN LEXICOGRAFICO INVERSO (OLI). Decimos que $x^a >_r x^b$ si, y sólo si, $deg(x^a) > deg(x^b)$ ó, $deg(x^a) = deg(x^b)$ y $a_i < b_i$ para el último índice i con $a_i \neq b_i$.

Es claro que a diferentes ordenes monomiales corresponden diferentes términos iniciales.

Ejemplo 2.1.33. **a)** Sea $R^m = \mathbb{Q}[x, y, z]$.

Sea $f = 3x^4z - 2x^3y^4 + 7x^2y^2z^3 \in R^m$. Entonces

$$in_{>_l}(f) = 3x^4z, \qquad in_{>_h}(f) = -2x^3y^4, \qquad in_{>_r}(f) = -2x^3y^4$$

b) Sea $R^m = k[x, y]^3$.

Sea f como en el ejemplo (2.1.11).Con OL tenemos

$$in_{>_{TOP}} = 4x^3e_2, \qquad in_{>_{POT}} = 5xy^2.$$

Con OLH y OLI tenemos

$$in_{>_{TOP}} = -y^{10}e_1, \qquad in_{>_{POT}} = -y^{10}e_1.$$

2.2 Bases de Gröbner

En esta sección consideraremos un orden monomial siempre fijo sobre R^m, el cual denotaremos por $>$.

En la sección anterior vimos que el ideal monomial $in_>(M)$ es el ideal que buscamos, y en el lema (2.1.29) que cualquier conjunto de elementos de M cuyos términos iniciales generen $in_>(M)$, generan a M. Este conjunto distinguido de elementos de M que se definen más explícitamente a continuación, son el concepto más importante del capítulo.

Definición 2.2.1. Una *Base de Gröbner* con respecto a un orden $>$ sobre un módulo libre R^m, es un conjunto de elementos $\mathcal{G} = \{g_1, \ldots, g_t\} \subset R^m$ tal que si M es el submódulo de R^m generado por $g_1, \ldots, g_t$, entonces $\langle in_>(g_1), \ldots, in_>(g_t)\rangle = in_>(M)$. Decimos entonces que $\mathcal{G}$ son una *base de Gröbner para* M.

Observación 2.2.2. No necesariamente una base de Gröbner es base para M como R-módulo. Una base de Gröbner es un conjunto generador del submódulo M, pero no es un conjunto linealmente independiente sobre R necesariamente.

Ejemplo 2.2.3. Por la observación (2.1.27), una base de Gröbner para un submódulo monomial es cualquier conjunto generador.

Ejemplo 2.2.4. Sea $R^m = k[x]$, por el ejemplo (2.1.31) sabemos que el único orden monomial sobre R^m es el orden dado por el grado. Por la observación (A.1.3), todos los submódulos $M \subset R^m$ son ideales de la forma $M = \langle p(x)\rangle$, con $p(x)$ un polinomio de grado mínimo en M. Para todo polinomio $g(x) \in M$, sabemos que $in_>(p(x)) < in_>(g(x))$, teniendo que $in_>(p(x)) | in_>(g(x))$, es decir, $\langle in_>(p(x))\rangle = in_>(M)$. Con esto, una base de Gröbner para un ideal $M \subset k[x]$ es cualquier polinomio de grado mínimo en M.

Corolario 2.2.5. *Todo submódulo $M \subset R^m$ tiene base de Gröbner.*

Demostración. Por el teorema (2.1.19) sabemos que el submódulo inicial de M es de la forma $in_>(M) = \langle in_>(g_1), \ldots, in_>(g_t)\rangle$, $g_i \in M$. Sea $N = \langle g_1, \ldots, g_t\rangle$. Por el lema (2.1.29) tenemos que $N = M$, concluyendo que $g_1, \ldots, g_t$ es base de Gröbner para M. □

Definición 2.2.6. Una base de Gröbner $g_1, \ldots, g_t$ es llamada *mínima* si para toda i, $lc_>(g_i) = 1$ y, para todo $i \neq j$, $lm_>(g_i) \nmid lm_>(g_j)$.

Lema 2.2.7. *Sea $M \subset R^m$ un submódulo. Sea $\mathcal{G} = \{g_1, \ldots, g_t\}$ una base de Gröbner para M. Si $lm_>(g_i) | lm_>(g_j)$, con $i \neq j$, entonces $\mathcal{G}' = \{g_1, \ldots, g_{j-1}, g_{j+1}, \ldots, g_t\}$ es también base de Gröbner para M.*

Corolario 2.2.8. *Todo submódulo $M \subset R^m$ tiene base de Gröbner mínima.*

Proposición 2.2.9. *Sea $M \subset R^m$ un submódulo. Si $\mathcal{G} = \{g_1, \ldots, g_t\}$ y $\mathcal{F} = \{f_1, \ldots, f_s\}$ son bases de Gröbner mínimas para M, entonces $s = t$ y, después de renumerar en caso de ser necesario, $in_>(f_i) = in_>(g_i)$, $i = 1, \ldots, t$.*

Demostración. Como $f_1 \in M$ y $\mathcal{G}$ es base de Gröbner para M, existe $g_i \in \mathcal{G}$ tal que $lm(g_i)|lm(f_1)$. Renumerando de ser necesario, podemos asumir que $g_i = g_1$. Pero $g_1 \in M$ y $\mathcal{F}$ es base de Gröbner para M, entonces existe $f_j \in \mathcal{F}$ tal que $lm_>(f_j)|lm_>(g_1)$. Concluyendo entonces que $lm_>(f_j)|lm_>(f_1)$. Como $\mathcal{F}$ es mínima, $j = 1$. Por lo tanto, $lm_>(f_1) = lm_>(g_1)$.

Ahora, $f_2 \in M$ existiendo $g_i \in \mathcal{G}$ tal que $lm_>(g_i)|lm_>(f_2)$. Como $\mathcal{F}$ es mínima y $lm_>(g_1) = lm_>(f_1)$ tenemos que $g_i \neq g_1$ y, renumerando de ser necesario, podemos asumir que $g_i = g_2$. Análogamente a arriba, $lm_>(f_2) = lm_>(g_2)$. Continuando el proceso, obtenemos que $s = t$ y que $lm_>(f_i) = lm_>(g_i)$, $i = 1, \ldots, t$. □

Definición 2.2.10. Una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_t\}$ es llamada *reducida* si para todo i, $lc_>(g_i) = 1$ y ningún término distinto de cero en g_i es divisible por algún $lm_>(g_j)$, para todo $j \neq i$.

Observación 2.2.11. En particular notamos que una base de Gröbner reducida es también mínima.

2.3 Algoritmo de la División Multivariado

En esta sección desarrollaremos una herramienta que junto con bases de Gröbner nos ayudará a resolver el problema de la membresía para un submódulo $M \subset R^m$ dado. Para esto, notemos que en el caso del anillo de polinomios $k[x_1]$, el problema de la membresía está resulto debido a que $k[x_1]$ es un anillo euclideano y un dominio de ideales principales. Si $\langle g \rangle = I$, entonces $f \in k[x_1]$ pertenece a I si, y sólo si, el residuo r que se obtiene al aplicar a f el *algoritmo de la división* respecto a g es igual a cero.

Extenderemos este proceso al caso general para obtener un algoritmo análogo al algoritmo de la división. Para obtener este nuevo algoritmo, que llamaremos *"algoritmo de la división multivariado"*, necesitamos replantear las condiciones sobre el algoritmo de la división dadas en (A.1.1) con las nociones que hemos desarrollado hasta el momento.

Considerando al anillo $k[x_1]$ con su orden monomial, podemos reestablecer las condiciones sobre $t(x)$ y $r(x)$ dadas en el algoritmo (A.1.1) de la siguiente manera: $deg(r(x)) <$

$deg(q(x))$, diciendo que $r(x)$ no tenga ningún término que sea divisible por $in_>(q(x))$; y $deg(t(x)q(x)) = deg(p(x))$, diciendo que $in_>(p(x)) = in_>(t(x)q(x))$ (en particular podemos decir que $in_>(p(x)) \geq in_>(t(x)q(x))$, siendo está última relación la que utilizaremos). Antes de dar el algoritmo, necesitamos dar algunas definiciones.

Definición 2.3.1. Sean $f, g, h \in R^m$, $g \neq 0$. Decimos que f se *reduce a* h *módulo* g *en un paso*, denotado por

$$f \longrightarrow_g h,$$

si, y sólo si, $in_>(g)$ divide al término αm perteneciente a f, y

$$h = f - \frac{\alpha m}{in_>(g)} g = f - \mu g.$$

Observación 2.3.2. Notemos que a f le hemos sustraido el término αm y lo hemos reemplazado por términos estrictamente más pequeños. Así, podemos pensar en h como el residuo en un paso de la división de f por g.

Este proceso lo podemos continuar hasta sustraerle a f todos los términos que sean divisibles por $in_>(g)$. El proceso de continuar reduciendo acabará tras un número finito de pasos, esto debido a que $>$ es un buen orden, existiendo un último término divisible por $in_>(g)$, llegando en algún momento a dicho término.

Este proceso lo aplicaremos al caso en que ambos elementos son homogéneos en R^m.

Lema 2.3.3. *Sea $>$ un orden monomial sobre R^m. Sean $f \in (R_d)^m$ y $g \in (R_{d'})^m$. Si h es la reducción de f módulo g en un paso, entonces $h \in (R_d)^m$.*

Demostración. Sea αm un término de f divisible por g, así $deg(\alpha m) = d$. Entonces

$$deg\left(\frac{\alpha m}{in_>(g)}\right) = deg(\alpha m) - deg(in_>(g)) = d - d'.$$

Si $g = (g_1, \ldots, g_m)$, tenemos que

$$\frac{\alpha m}{in_>(g)} g = \left(\frac{\alpha m}{in_>(g)} g_1, \ldots, \frac{\alpha m}{in_>(g)} g_m\right).$$

Como $g_i \in R_{d'}$, entonces para cualquier término βn de g_i

$$deg\left(\frac{\alpha m}{in_>(g)} \beta n\right) = deg\left(\frac{\alpha m}{in_>(g)}\right) + deg(\beta n) = d - d' + d' = d$$

Por lo tanto

$$\frac{\alpha m}{in_>(g)} g \in (R_d)^m,$$

lo que implica que $h \in (R_d)^m$. □

Observación 2.3.4. Siguiendo la notación de la definición (2.3.1), $\frac{\alpha m}{in_>(g)} \in R_{d-d'}$.

Definición 2.3.5. Sean $f, f_1, \ldots, f_t, r \in R^m$, $f_i \neq 0$, para todo i. Sea $F = \{f_1, \ldots, f_t\}$. Decimos que f *se reduce a* r *módulo* F, denotado por

$$f \longrightarrow_F r$$

si, y sólo si, existe una sucesión de índices $i_1, \ldots, i_s \in \{1, \ldots, t\}$, y una sucesión de elementos $r_1, \ldots, r_{s-1} \in R^m$ tales que

$$f \longrightarrow_{f_{i_1}} r_1 \longrightarrow_{f_{i_2}} r_2 \cdots \longrightarrow_{f_{i_{s-1}}} r_{s-1} \longrightarrow_{f_{i_s}} r.$$

Lema 2.3.6. *Sea* $>$ *un orden monomial sobre* R^m. *Sea* $F = \{f_1, \ldots, f_k\} \subset R^m$. *Para todo* $m, f \in R^m$, m *monomio, si* $f \longrightarrow_F 0$, *entonces* $mf \longrightarrow_F 0$.

□

Definición 2.3.7. Un elemento $r \in R^m$ es llamado *reducido* con respecto a un conjunto $F = \{f_1, \ldots, f_t | \, f_i \in R^m \backslash \{0\}\}$, si $r = 0$ ó ningún término perteneciente a r es divisible por algún $in_>(f_i)$.

Definición 2.3.8. Sean F y r como en la definición anterior, y sea $f \in R^m$. Si $f \longrightarrow_F r$ y r es reducido con respecto a F, entonces llamamos a r el *residuo* para f con respecto a F.

Teorema 2.3.9. Sea $>$ un orden monomial sobre R^m. Consideremos al conjunto $F = \{f_1, \ldots, f_t | \, f_i \in R^m \backslash \{0\}\}$. Entonces todo elemento $f \in R^m$ tiene una expresión de la forma

$$f = \sum_{i=1}^{t} f_i h_i + r \qquad r \in R^m, \; h_i \in R, \tag{2.4}$$

cumpliendo con $in_>(f) = max\{in_>(f_i h_i), in_>(r) | i = 1, \ldots, t\}$, y que r sea reducido con respecto a F.

La demostración del teorema se basa en el siguiente algoritmo.

Algoritmo de la División Multivariado 2.3.10. *Sea $>$ un orden monomial sobre R^m. Sea $F = \{f_1, \ldots, f_t | f_i \in R\backslash\{0\}; in_>(f_i) > in_>(f_j) \Leftrightarrow i < j\}$. Sea $f \in R^m$. Denotemos por $\alpha_1 m_1$ al máximo término de f que sea divisible por algún $in_>(f_i)$ Sea $s_1 = i$ el índice más pequeño para el cual $in_>(f_i)|\alpha_1 m_1$. Definamos al elemento f_1' como*

$$f \longrightarrow_{f_{s_1}} f_1'$$

donde

$$f_1' = f - \frac{\alpha_1 m_1}{in_>(f_{s_1})} f_{s_1} = f - \mu_1 f_{s_1}.$$

Si $f' \neq 0$, sea ahora $\alpha_2 m_2$ el máximo término de f_1' que sea divisible por algún $in_>(f_j)$. Sea $s_2 = j$ el índice más pequeño para el cual $in_>(f_j)|\alpha_2 m_2$. Definamos al elemento $f_2' = f_1' - \mu_2 f_{s_2}$ mediante la reducción de f_1' módulo f_{s_2}

$$f_1' \longrightarrow_{f_{s_2}} f_2'.$$

Si $f_2' \neq 0$, repitamos este proceso definiendo elementos f_u' y μ_u hasta que para alguna p, f_p' sea reducido con respecto a F.

Lema 2.3.11. *El algoritmo de la división multivariado es un proceso finito.*

Demostración. Al ser $>$ un buen orden, el conjunto de términos de f_1' que son divisibles por algún $in_>(f_i)$ tiene elemento mínimo. Como vimos en la observación (2.3.2), en el proceso de reducción para f con respecto a F se tiene que $in_>(f_i') > in_>(f_{i+1}')$. Por lo tanto, en algún momento del proceso de reducción será alcanzado dicho elemento, acabando al algoritmo después de un número finito de pasos. □

Demostración del teorema (2.3.9). Se sigue directamente del algoritmo de la división multivariado y del lema anterior, tomando como h_i a la suma de todos los μ_u tales que $s_u = i$ y siendo $r = f_p'$ Notando que si el elemento $\alpha_1 m_1$ definido en el algoritmo no es $in_>(f)$, entonces $in_>(f)$ pertenece al residuo r, que por su construcción, todos sus demás términos son menores a $in_>(f)$. □

Definición 2.3.12. A la expresión (2.4) de f se le dice *expresión estándar para f* en términos de los f_i.

Corolario 2.3.13. *Sea $F = \{f_1, \ldots, f_m | f_i \in (R_{d_i})^m \backslash \{0\}\}$, y $f \in (R_d)^m$. Entonces*

$$f = \sum_{i=1}^{t} f_i h_i + r \qquad r \in (R_d)^m,\ h_i \in R_{d-d_i},$$

Demostración. Se sigue inmediatamente del lema (2.3.3), observación (2.3.4) y del algoritmo de la división multivariado. □

Observación 2.3.14. En las condiciones para f dadas en (2.4), notemos que si F es base de Gröbner para $\langle F\rangle$, entonces r es la expresión para f módulo M en términos de la base para R^m/M dada en el teorema de Macaulay (2.1.28).

Observación 2.3.15. En la situación del teorema (2.3.9) tenemos que $f - r \in \langle F\rangle$, donde si $r = 0$, entonces $f \in \langle F\rangle$.

El inverso no es cierto necesariamente, puede ocurrir que $f \in \langle F\rangle$, pero reduciendo a f módulo F mediante el algoritmo de la división el residuo puede resultar ser distinto de cero.

Ejemplo 2.3.16. Sea $I = \langle f_1, f_2\rangle \subset \mathbb{Q}[x, y]$, donde $f_1 = yx - y$ y $f_2 = y^2 - x$. Sean $F = \{f_1, f_2\}$, $f = y^2x - x$. Considerando al orden $>_h$ con la convención $x > y$, tenemos en la situación del algoritmo (2.3.10) que $in_>(f_1) = yx$ y $in_>(f_2) = y^2$. Así, $f \longrightarrow_F r$ está dado como

$$f \longrightarrow_{f_1} y^2 - x \longrightarrow_{f_2} 0,$$

es decir, $r = 0$. Y ciertamente tenemos que

$$f = yf_1 + f_2.$$

Pero repitiendo el proceso ahora con $>_h$ y la convención $y > x$, tenemos que el proceso de reducción está dado como

$$f \longrightarrow_{f_2} x^2 - x,$$

siendo $x^2 - x$ reducido con respecto a F. Así,

$$f = xf_2 + r, \qquad r \neq 0,$$

aunque f pertenece a I.

Observación 2.3.17. Notemos que en el caso de $k[x_1] = R^m$, si no tomáramos al conjunto generador de I como aquel dado por un elemento único de grado mínimo en I, tendríamos el mismo problema.

Ejemplo 2.3.18. Sea $I = \langle f_1, f_2\rangle \subset k[x]$, donde $f_1 = x^2$ y $f_2 = x^2 - x$. Sean $F = \{f_1, f_2\}$ y $f = x$. El elemento f es reducido con respecto a F, sin embargo $f = f_2 - f_1 \in I$.

La observación (2.3.17) nos prepara para el siguiente resultado.

Teorema 2.3.19. Sea $>$ un orden monomial sobre R^m. Sea $M \subset R^m$ un submódulo con $\mathcal{G} = \{g_1, \ldots, g_t\}$ una base de Gröbner para M. Entonces $f \in R^m$ pertenece a M si, y sólo si, $f \longrightarrow_{\mathcal{G}} 0$.

Demostración. Sea $f \in M$, siendo su expresión estándar

$$f = \sum_{i=1}^{t} h_i g_i + r. \tag{2.5}$$

Supongamos que $r \neq 0$. Como $r = f - \sum_{i=1}^{t} h_i g_i$, tenemos que $r \in M$. Al ser $\mathcal{G}$ base de Gröbner, $in_>(r)$ es divisible por algún $in_>(g_i)$ Pero esto es una contradicción a que r sea reducido con respecto a $\mathcal{G}$. Por lo tanto, $r = 0$. La parte inversa es precisamente la observación (2.3.15). □

Con este teorema ya casi hemos resuelto el problema de la membresía para algún submódulo $M \subset R^m$, bastándonos dar un método para cálcular bases de Gröbner a partir de un conjunto generador

2.4 Algoritmo de Buchberger

En esta sección daremos la teoría necesaria para poder cálcular bases de Gröbner, para después proceder a obtenerlas mediante un algoritmo, el cual es llamado *"algoritmo de Buchberger"*. Una vez hecho esto, retomaremos el estudio hecho en la Sección (1.2) para dar bases de Gröbner únicas y caracterizar a las bases de Gröbner reducidas de submódulos graduados.

2.4.1 S-Vectores

Sea $>$ un orden monomial sobre R^m. Sea $\mathcal{G} = \{g_1, \ldots, g_t | g_i \in R^m \backslash \{0\}\}$, y consideremos al submódulo $M = \langle \mathcal{G} \rangle$. Sabemos que $\mathcal{G}$ es base de Gröbner para M si, y sólo si, para todo $f \in M$, tenemos que $in_>(g_i) | in_>(f)$ para alguna i. El problema para que $\mathcal{G}$ sea base de Gröbner se presenta cuando existen elementos pertenecientes a M cuyos términos iniciales no son divisibles por algún $in_>(g_i)$.

Ejemplo 2.4.1. Un ejemplo donde esto ocurre, está dado en el ejemplo (2.3.16).

La siguiente definición servirá para ayudar a solucionar este problema.

Definición 2.4.2. Sea $>$ un orden monomial sobre R^m. Sean $f, g \in R^m$ tales que sus términos iniciales contengan al mismo elemento base de R^m. Definimos al *S-vector* de f y g, denotado por $S(f,g)$, como

$$S(f,g) = \frac{mcm[lm_>(f), lm_>(g)]}{in_>(f)} f - \frac{mcm[lm_>(f), lm_>(g)]}{in_>(g)} g.$$

el cual pertenece a R^m.

Observación 2.4.3. Notemos que por definición, $S(f,g) = -S(g,f)$.

Nota 2.4.4. Si los términos iniciales de f y g no contienen al mismo elemento base de R^m, por la nota (2.1.13), podemos definir a su S-vector como $S(f,g) = 0$.

Ejemplo 2.4.5. Sea $R^m = k[x,y]^2$. Sea $f = (xy - x, x^3 + y)$ y $g = (x^2 + 2y^2, x^2 - y^2)$. Usando $>_{POT}$ con $>_l$ y la convención $x > y$, tenemos que

$$S(f,g) = \frac{x^2y}{xy} f - \frac{x^2y}{x^2} g = xf - yg = (-x^2 - 2y^3, x^4 - x^2y + xy + y^3).$$

Pero con $>_{TOP}$ y $>_l$, tenemos que

$$S(f,g) = 0.$$

Lema 2.4.6. *Sea $>$ un orden monomial sobre R^m. Sean $f \in (R_d)^m$ y $g \in (R_{d'})^m$. Entonces $S(f,g) \in (R_t)^m$, donde $t = deg(mcm[in_>(f), in_>(g)])$.*

Demostración. Observemos que

$$deg\left(\frac{mcm[in_>(f), in_>(g)]}{in_>(f)}\right) = t - d$$
$$deg\left(\frac{mcm[in_>(f), in_>(g)]}{in_>(g)}\right) = t - d'.$$

Sea αm un término cualquiera de f, entonces

$$deg\left(\frac{mcm[in_>(f), in_>(g)]}{in_>(f)} \alpha m\right) = deg\left(\frac{mcm[in_>(f), in_>(g)]}{in_>(f)}\right) + deg(\alpha m) = t - d + d = t.$$

Análogamente, para cualquier término βn de g

$$deg\left(\frac{mcm[in_>(f), in_>(g)]}{in_>(g)}\beta n\right) = t.$$

Por lo tanto, $S(f,g) \in (R_t)^m$. □

Ahora daremos un criterio para decir cuando un conjunto generador de un submódulo es base de Gröbner, del cual obtendremos un método para poder cálcular bases de Gröbner.

Teorema 2.4.7 (Criterio de Buchberger). Sea $>$ un orden monomial sobre R^m. Sea $\mathcal{G} = \{g_1, \ldots, g_t | g_i \in R^m \backslash \{0\}\}$. El conjunto $\mathcal{G}$ es base de Gröbner para $\langle \mathcal{G} \rangle = M$ si, y sólo si,

$$S(g_i, g_j) \longrightarrow_{\mathcal{G}} 0 \qquad \forall i, j.$$

Demostración. De la definición de S-vectores notamos que para toda $i \neq j$ se cumple que $S(g_i, g_j) \in M$, así por el teorema (2.3.19) tenemos que

$$S(g_i, g_j) \longrightarrow_{\mathcal{G}} 0\,, \qquad \forall i \neq j$$

Conversamente, sea $f \in M$. Como $\mathcal{G}$ es conjunto generador, tenemos que f se puede expresar como combinación lineal de los g_i, combinación que no necesariamente es única (debido a la observación (1.2.2)). Dichas expresiones son de la forma

$$f = \sum_{j=1}^{t} h_j g_j\,, \qquad h_j \in R. \tag{2.6}$$

De entre todas las expresiones para f, podemos escoger aquella con monomio inicial más pequeño, ya que todo orden monomial es un buen orden. Sea m tal monomio inicial y supongamos que (2.6) es tal expresión, notando que

$$\begin{aligned} m &= lm_>\left(\sum_{i=1}^{t} h_j g_j\right) \\ &= max\{lm_>(h_j g_j) | j = 1, \ldots, t\} = max\{lm_>(h_j) lm_>(g_j) | j = 1, \ldots, t\} \end{aligned}$$

Si $m = lm_>(f)$, tenemos que $\mathcal{G}$ es base de Gröbner para M. Supongamos que no es así, que $\mathcal{G}$ no es base de Gröbner para M, lo que implica que todos los $lm_>(h_i g_i) = m$ se anulan entre sí, es decir, $m > lm_>(f)$. El objetivo siguiente de la demostración es construir una expresión para f con término inicial menor a m, lo cual será una contradicción. Sea

$I = \{i | lm_>(h_i g_i) = m\}$. Denotemos a los términos iniciales de los h_i, con $i \in I$, como $in_>(h_i) = \alpha_i m_i$. Sea g el siguiente elemento:

$$g := \sum_{i \in I} \alpha_i m_i g_i \qquad \in M.$$

Por construcción, $lm_>(m_i g_i) = m$, $\forall i \in I$. Pero la suma de todos los $lm_>(m_i g_i) = m$ es igual a cero, es decir. $\sum_{i \in I} \alpha_i \beta_i = 0$, donde $\beta_i = lc_>(g_i)$, $\forall i \in I$. Por lo tanto, $lm_>(g) < m$.

Notemos que como $m = lm_>(m_i g_i)$ $\forall i \in I$,

$$m = mcm[lm_>(m_i g_i), lm_>(m_j g_j)],$$

teniendo que

$$S(m_i g_i, m_j g_j) = \frac{mcm[lm_>(m_i g_i), lm_>(m_j g_j)]}{in_>(m_i g_i)} m_i g_i - \frac{mcm[lm_>(m_i g_i), lm_>(m_j g_j)]}{in_>(m_j g_j)} m_j g_j$$

$$= \frac{m}{in_>(m_i g_i)} m_i g_i - \frac{m}{in_>(m_j g_j)} m_j g_j = \frac{m}{m_i in_>(g_i)} m_i g_i - \frac{m}{m_j in_>(g_j)} m_j g_j$$

$$= \frac{m}{\beta_i m} m_i g_i - \frac{m}{\beta_j m} m_j g_j = \frac{m_i g_i}{\beta_i} - \frac{m_j g_j}{\beta_j}.$$

Sea $s := max\{i | i \in I\}$, entonces

$$
\begin{aligned}
g = \sum_{i=1}^{s} \alpha_i m_i g_i &= \alpha_1 m_1 g_1 + \ldots \alpha_s m_s g_s = \alpha_1\beta_1 \frac{m_1 g_1}{\beta_1} + \ldots + \alpha_s\beta_s \frac{m_s g_s}{\beta_s} \\
&= \alpha_1\beta_1 \frac{m_1 g_1}{\beta_1} + (\alpha_1\beta_1 - \alpha_1\beta_1 + \alpha_2\beta_2)\frac{m_2 g_2}{\beta_2} + \ldots \\
&\quad + (\alpha_1\beta_1 - \alpha_1\beta_1 + \ldots + \alpha_{s-2}\beta_{s-2} - \alpha_{s-2}\beta_{s-2} + \alpha_{s-1}\beta_{s-1})\frac{m_{s-1} g_{s-1}}{\beta_{s-1}} \\
&\quad + (\alpha_1\beta_1 - \alpha_1\beta_1 + \ldots + \alpha_{s-1}\beta_{s-1} - \alpha_{s-1}\beta_{s-1} + \alpha_s\beta_s)\frac{m_s g_s}{\beta_s} \\
&= \alpha_1\beta_1 \frac{m_1 g_1}{\beta_1} + (\alpha_1\beta_1 + \alpha_2\beta_2)\frac{m_2 g_2}{\beta_2} - \alpha_1\beta_1 \frac{m_2 g_2}{\beta_2} + \ldots \\
&\quad + (\alpha_1\beta_1 + \ldots + \alpha_{s-1}\beta_{s-1})\frac{m_{s-1} g_{s-1}}{\beta_{s-1}} - (\alpha_1\beta_1 + \ldots + \alpha_{s-2}\beta_{s-2})\frac{m_{s-1} g_{s-1}}{\beta_{s-1}} \\
&\quad + (\alpha_1\beta_1 + \ldots + \alpha_s\beta_s)\frac{m_s g_s}{\beta_s} - (\alpha_1\beta_1 + \ldots + \alpha_{s-1}\beta_{s-1})\frac{m_s g_s}{\beta_s} \\
&= (\alpha_1\beta_1)\left(\frac{m_1 g_1}{\beta_1} - \frac{m_2 g_2}{\beta_2}\right) + \ldots + (\alpha_1\beta_1 + \ldots + \alpha_{s-1}\beta_{s-1})\left(\frac{m_{s-1} g_{s-1}}{\beta_{s-1}} - \frac{m_s g_s}{\beta_s}\right) \\
&\quad + (\alpha_1\beta_1 + \ldots + \alpha_s\beta_s)\frac{m_s g_s}{\beta_s} \\
&= (\alpha_1\beta_1)\left(\frac{m_1 g_1}{\beta_1} - \frac{m_2 g_2}{\beta_2}\right) + \ldots + (\alpha_1\beta_1 + \ldots + \alpha_{s-1}\beta_{s-1})\left(\frac{m_{s-1} g_{s-1}}{\beta_{s-1}} - \frac{m_s g_s}{\beta_s}\right)
\end{aligned}
$$

debiéndose la última igualdad a que $\sum_{i=1}^{s} \alpha_i\beta_i = 0$.

Nombrando $\gamma_{ij} = \sum_{u=1}^{i} \alpha_u\beta_u$, tenemos que

$$g = \sum_{\substack{i<j \\ i,j \in I}} \gamma_{ij} S(m_i g_i, m_j g_j).$$

Pero

$$S(m_ig_i, m_jg_j) = \frac{mcm[lm_>(m_ig_i), lm_>(m_jg_j)]}{in_>(m_ig_i)}m_ig_i - \frac{mcm[lm_>(m_ig_i), lm_>(m_jg_j)]}{in_>(m_jg_j)}m_jg_j$$

$$= \frac{m}{m_iin_>(g_i)}m_ig_i - \frac{m}{m_jin_>(g_j)}m_jg_j$$

$$= \frac{m}{in_>(g_i)}g_i - \frac{m}{in_>(g_j)}g_j$$

$$= \left(\frac{mcm[lm_>(g_i), lm_>(g_j)]}{mcm[lm_>(g_i), lm_>(g_j)]}\right)\left(\frac{m}{in_>(g_i)}g_i - \frac{m}{in_>(g_j)}g_j\right)$$

$$= \frac{m}{mcm[lm_>(g_i), lm_>(g_j)]}S(g_i, g_j).$$

Por hipótesis $S(g_i, g_j) \longrightarrow_{\mathcal{G}} 0$, pero por el lema (2.3.6), $S(m_ig_i, m_jg_j) \longrightarrow_{\mathcal{G}} 0$. Por lo tanto, tenemos que

$$S(m_ig_i, m_jg_j) = \sum_{u=1}^{s} h_u^{ij}g_u, \qquad h_u^{ij} \in R. \tag{2.7}$$

Concluyendo por el teorema (2.3.9) que

$$max\{lm_>(h_u^{ij}g_u)|u = 1, \ldots, s\} = lm_>(S(m_ig_i, m_jg_j)).$$

Pero

$$S(m_ig_i, m_jg_j) = \frac{m_ig_i}{\beta_i} - \frac{m_jg_j}{\beta_j}$$
$$= m + \text{términos menores} - m + \text{términos menores}.$$

Es decir,

$$lm_>(S(m_ig_i, m_jg_j)) < m.$$

Sustituyendo en g a los S-vectores mediante las expresiones (2.7) y, posteriormente sustituyendo a g en f, obtenemos una expresión para f de la forma

$$f = \sum_{i=1}^{t} h_i'g_i. \qquad h_i' \in R,$$

donde $max\{lm_>(h_i^t)lm_>(g_i)|i = 1,\ldots,t\} < m$ Así, tenemos una expresión para f con monomio inicial menor a m, contradiciendo la elección de m. Por lo tanto, $\mathcal{G}$ es base de Gröbner. □

Ejemplo 2.4.8. Sea $M = \langle g_1, g_2, g_3, g_4\rangle \subset \mathbb{Q}[x,y]^3$, donde

$$g_1 = (x-y, x, x) \qquad g_3 = (y, x, x)$$
$$g_2 = (xy, y, y) \qquad g_4 = (y, x, 0)$$

Sea $>$ sobre $\mathbb{Q}[x,y]^3$ dado por TOP con $>_h$ sobre $\mathbb{Q}[x,y]$ con la convención $x > y$. Siendo $\mathcal{G} = \{g_1, g_2, g_3, g_4\}$, obtenemos

$$in_>(g_1) = xe_1 \qquad in_>(g_3) = xe_2$$
$$in_>(g_2) = xye_1 \qquad in_>(g_4) = xe_2$$

Con esto, tenemos que $\mathcal{G}$ no es base de Gröbner, ya que

$$\begin{aligned} S(g_3, g_4) &= \frac{x}{x}g_3 - \frac{x}{x}g_4 = g_3 - g_4 = (y,x,x) - (y,x,0) \\ &= (0,0,x), \end{aligned}$$

el cual es de entrada reducido con respecto a $\mathcal{G}$.

2.4.2 Algoritmo de Buchberger

El teorema (2.4.7) nos da una forma de cálcular bases de Gröbner.

Algoritmo de Buchberger 2.4.9. *Sea $>$ un orden monomial sobre R^m. Consideremos al conjunto $\mathcal{G} = \{g_1, \ldots, g_t | g_i \in R^m \backslash \{0\}\}$ Reduscamos a los $S(g_i, g_j)$, $\forall i \neq j$ con respecto a $\mathcal{G}$. Si $S(g_i, g_j) \longrightarrow_{\mathcal{G}} 0 \forall i \neq i$, entonces $\mathcal{G}$ es base de Gröbner. Si la reducción de algún S-vector es distinta de cero, agreguemos a $\mathcal{G}$ dicha reducción. Repetir el proceso, ahora con $\mathcal{G}_1 = \{g_1, \ldots, g_s, g^{ij}\}$, donde g^{ij} es la reducción distinta de cero de $S(g_i, g_j)$. Si las reducciones con respecto a $\mathcal{G}_1$ no son todas cero, seguir repitiendo el proceso de agregar las reducciones distintas de cero y volver a reducir hasta que todas las reducciones sean iguales a cero.*

Teorema 2.4.10. Sea $\mathcal{G} = \{g_1, \ldots, g_t | g_i \in R^m \backslash \{0\}\}$. El algoritmo de Buchberger produce una base de Gröbner para el submódulo $M = \langle \mathcal{G} \rangle$.

Demostración. Basta demostrar que el proceso es finito. Supongamos que esto no ocurre, que el proceso es infinito.

Sea $in_>(\mathcal{G}_1) = \langle in_>(g_1), \ldots, in_>(g_t), in_>(g_1^{ij})\rangle$, donde g_1^{ij} es la primer reducción de algún S-vector en el algoritmo de Buchberger distinta de cero. Al ir agregando g_u^{ij}. vamos creando una cadena de submodulos monomiales

$$in_>(\mathcal{G}) \subseteq in_>(\mathcal{G}_1) \subseteq in_>(\mathcal{G}_2) \subseteq \ldots \tag{2.8}$$

Pero en cada caso, si g_u^{ij} es la reducción a agregar a $\mathcal{G}_{u-1}$ obteniendo $\mathcal{G}_u$, al ser g_u^{ij} reducido con respecto a $in_>(\mathcal{G}_{u-1})$, la cadena (2.8) es de la forma

$$in_>(\mathcal{G}) \subsetneq in_>(\mathcal{G}_1) \subsetneq in_>(\mathcal{G}_2) \subsetneq \ldots$$

que al ir agregando términos indefinidamente se vuelve infinita. Pero esto es una contradicción, ya que por la proposición (1.1.9), el submódulo R^m es Noetheriano. Por lo tanto, el algoritmo de Buchberger es finito. □

Ejemplo 2.4.11. Consideremos el caso del ejemplo (2.4.8). Los únicos mínimos comunes múltiplos distintos de cero son:

$$mcm[lm_>(g_1), lm_>(g_2)] = xye_1$$
$$mcm[lm_>(g_3), lm_>(g_4)] = x\,e_2$$

Por lo tanto, sólo consideraremos a los S-vectores de $\{g_1, g_2\}$ y $\{g_3, g_4\}$. que son

$$\begin{aligned} S(g_1, g_2) &= \frac{xy}{x}g_1 - \frac{xy}{xy}g_2 = yg_1 - g_2 \\ &= y(x-y, x, x) - (xy, y, y) = (xy - y^2, xy, xy) - (xy, y, y) \\ &= (-y^2, xy - y, xy - y) \end{aligned}$$

$$S(g_3, g_4) = (0, 0, x)$$

Así, reduciendo obtenemos

$$S(g_1, g_2) \longrightarrow_{g_3} (-2y^2, -y, -y)$$

el cual es reducido con respecto a $\mathcal{G}$. En el ejemplo (2.4.8) vimos que $S(g_3, g_4)$ es reducido con respecto a $\mathcal{G}$. Por lo tanto, debemos agregar los vectores $g_5 = (-2y^2, -y, -y)$ y $g_6 = (0, 0, x)$

a $\mathcal{G}$, con

$$in_>(g_5) = -2y^2e_1$$
$$in_>(g_6) = x\,e_3$$

Sea $\mathcal{G}_1 = \{g_1, \ldots, g_6\}$. Los nuevos mínimos comunes múltiplos a considerar son

$$mcm[lm_>(g_1), lm_>(g_5)] = xy^2e_1$$
$$mcm[lm_>(g_2), lm_>(g_5)] = xy^2e_1$$

Con esto, hay que cálcular a los S-vectores de $\{g_1, g_5\}$ y $\{g_2, g_5\}$, obteniendo

$$\begin{aligned} S(g_1, g_5) &= \frac{xy^2}{x}g_1 - \frac{xy^2}{-2y^2}g_5 = y^2g_1 + \frac{x}{2}g_5 \\ &= y^2(x-y, x, x) + \frac{x}{2}(-2y^2, -y, -y) \\ &= (xy^2 - y^3, xy^2, xy^2) + \left(-xy^2, \frac{-xy}{2}, \frac{-xy}{2}\right) \\ &= \left(-y^3, xy^2 - \frac{xy}{2}, xy^2 - \frac{xy}{2}\right) \end{aligned}$$

$$\begin{aligned} S(g_2, g_5) &= \frac{xy^2}{xy}g_2 - \frac{xy^2}{-2y^2}g_5 = yg_2 + \frac{x}{2}g_5 \\ &= y(xy, y, y) + \frac{x}{2}(-2y^2, -y, -y) \\ &= (xy^2, y^2, y^2) + \left(-xy^2, \frac{-xy}{2}, \frac{-xy}{2}\right) \\ &= \left(0, y^2 - \frac{xy}{2}, y^2 - \frac{xy}{2}\right) \end{aligned}$$

Así,

$$\begin{aligned} S(g_1, g_5) &\longrightarrow_{g_3} \left(-2y^3, \frac{-xy}{2}, \frac{-xy}{2}\right) \longrightarrow_{g_5} \left(0, y^2 - \frac{xy}{2}, y^2 - \frac{xy}{2}\right) \\ &\longrightarrow_{g_3} \left(\frac{y^2}{2}, y^2, y^2\right) \longrightarrow_{g_5} \left(0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4}\right) \end{aligned}$$

el cual es reducido con respecto a $\mathcal{G}_1$.

$$S(g_2, g_5) \longrightarrow_{g_3} \left(\frac{y^2}{2}, y^2, y^2\right) \longrightarrow_{g_5} \left(0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4}\right)$$

el cual es reducido con respecto a $\mathcal{G}_1$. Sea $g_7 = (0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4})$, con

$$in_>(g_7) = y^2 e_2$$

Sea $\mathcal{G}_2 = \{g_1, \ldots, g_7\}$. Los nuevos mínimos comunes múltiplos a cálcular son

$$mcm[lm_>(g_3), lm_>(g_7)] = xy^2 e_2$$
$$mcm[lm_>(g_4), lm_>(g_7)] = xy^2 e_2$$

considerando a los S-vectores de $\{g_3, g_7\}$ y $\{g_4, g_7\}$. Así

$$\begin{aligned} S(g_3, g_7) &= \frac{xy^2}{x} g_3 - \frac{xy^2}{y^2} g_7 = y^2 g_3 - x g_7 \\ &= y^2(y, x, x) - x\left(0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4}\right) \\ &= (y^3, xy^2, xy^2) - \left(0, xy^2 - \frac{xy}{4}, xy^2 - \frac{xy}{4}\right) \\ &= \left(y^3, \frac{xy}{4}, \frac{xy}{4}\right) \end{aligned}$$

$$\begin{aligned} S(g_4, g_7) &= \frac{xy^2}{x} g_4 - \frac{xy^2}{y^2} g_7 = y^2 g_4 - x g_7 \\ &= y^2(y, x, 0) - x\left(0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4}\right) \\ &= (y^3, xy^2, 0) - \left(0, xy^2 - \frac{xy}{4}, xy^2 - \frac{xy}{4}\right) \\ &= \left(y^3, \frac{xy}{4}, -xy^2 + \frac{xy}{4}\right) \end{aligned}$$

Entonces

$$\begin{aligned} S(g_3, g_7) &\longrightarrow_{g_5} \left(0, \frac{xy}{4} - \frac{y^2}{2}, \frac{xy}{4} - \frac{y^2}{2}\right) \longrightarrow_{g_3} \left(-\frac{y^2}{4}, \frac{-y^2}{2}, \frac{-y^2}{2}\right) \\ &\longrightarrow_{g_5} \left(0, -\frac{y^2}{2} + \frac{y}{8}, -\frac{y^2}{2} + \frac{y}{8}\right) \longrightarrow_{g_7} 0 \end{aligned}$$

$$\begin{aligned} S(g_4, g_7) &\longrightarrow_{g_6} \left(y^3, \frac{xy}{4}, \frac{xy}{4}\right) \longrightarrow_{g_5} \left(0, \frac{xy}{4} - \frac{y^2}{2}, \frac{xy}{4} - \frac{y^2}{2}\right) \\ &\longrightarrow_{g_3} \left(\frac{-y^2}{4}, \frac{-y^2}{2}, \frac{-y^2}{2}\right) \longrightarrow_{g_5} \left(0, -\frac{y^2}{2} + \frac{y}{8}, -\frac{y^2}{2} + \frac{y}{8}\right) \\ &\longrightarrow_{g_7} 0 \end{aligned}$$

Por lo tanto, el conjunto $\{g_1, \ldots, g_7\}$ es base de Gröbner para M.

Corolario 2.4.12. *Sea* $G = \{g_1, \ldots, g_t | g_i \in (R_{d_i})^m \backslash \{0\}\}$. *Entonces* G *tiene una base de Gröbner homogénea.*

Demostración. Si $in_>(G) \neq \langle in_>(g_1), \ldots, in_>(g_t)\rangle$, entonces por el lema (2.4.6) el algoritmo de Buchberger produce la base de Gröbner deseada. □

2.4.3 Bases de Gröbner Reducidas

En la Sección (1.2) vimos el concepto de base de Gröbner reducida, sin embargo no se demostró su existencia. A continuación se demostrará que existe y que es única.

Corolario 2.4.13. *Todo submódulo* $M \subset R^m$ *tiene base de Gröbner reducida.*

Demostración. Sabemos por el corolario (2.2.8) que todo submódulo $M \subset R^m$ tiene base de Gröbner mínima. Sea $\mathcal{G} = \{g_1, \ldots, g_t\}$ tal base para algún submódulo M. La demostración consistirá en dar un proceso de obtención.

Sea $\mathcal{H}_1 = \{g_2, \ldots, g_t\}$ y consideremos al elemento

$$g_1 \longrightarrow_{\mathcal{H}_1} \hbar_1,$$

donde $\hbar_1$ es reducido con respecto a $\mathcal{H}_1$ y es distinto de cero, ya que $\mathcal{G}$ es mínima. Sea ahora $\mathcal{H}_2 = \{\hbar_1, g_3, \ldots, g_t\}$ y consideremos al elemento

$$g_2 \longrightarrow_{\mathcal{H}_2} \hbar_2,$$

donde análogamente $\hbar_2$ es reducido con respecto a $\mathcal{H}_2$ y distinto de cero. Análogamente definimos a los elementos $\hbar_3, \ldots, \hbar_t$, que serán reducidos con respecto a $\mathcal{H}_3 = \{\hbar_1, \hbar_2, g_4, \ldots, g_t\}$, $\ldots, \mathcal{H}_t = \{\hbar_1, \ldots, \hbar_{t-1}\}$.

Notemos que al ser $\mathcal{G}$ base de Gröbner mínima, tenemos que $in_>(g_i) = in_>(\hbar_i)$, $\forall i$. Por lo tanto $\mathcal{H} = \{\hbar_1, \ldots, \hbar_t\}$ es también base de Gröbner para M. Además que en el momento de reducir g_i con respecto a $\mathcal{H}_i$, lo que realmente estamos haciendo es eliminar a los términos de g_i que sean divisibles por $in_>(\hbar_1)$, $\ldots, in_>(\hbar_{i-1}), in_>(g_{i+1}) = in_>(\hbar_{i+1}), \ldots, in_>(g_t) = in_>(\hbar_t)$, esto para toda i. Es decir, $\mathcal{H}$ es una base de Gröbner reducida para M. □

Corolario 2.4.14. *Sea* $G = \{g_1, \ldots, g_t | g_i \in (R_{d_i})^m \backslash \{0\}\}$ *Entonces* G *tiene una base de Gröbner reducida* $\mathcal{H} = \{h_1, \ldots, h_{t_0}\}$ *donde* $h_i \in (R_{d_i})^m$ *para toda* i.

Demostración. Por los corolarios (2.4.12) y (2.2.8) tenemos que G tiene una base de Gröbner mínima dada por elementos homogéneos. Hecho esto, es inmediato del lema (2.3.3) y la construcción de la base de Gröbner reducida dada en la demostración del corolario anterior. □

Teorema 2.4.15 (Buchberger). Sea $>$ un orden monomial sobre R^m. Entonces cada submódulo $M \subset R^m$ tiene una única base de Gröbner reducida con respecto al orden $>$.

Demostración. Sean $\mathcal{G} = \{g_1, \ldots, g_t\}$ y $\mathcal{H} = \{h_1, \ldots, h_s\}$ dos bases de Gröbner reducidas para M. Como en particular $\mathcal{G}$ y $\mathcal{H}$ son bases de Gröbner mínimas, por la proposición (2.2.9) tenemos que $s = t$ y renumerando en caso de ser necesario, $in_>(h_i) = in_>(g_i)$, $\forall i$. Para cada i notemos que si $h_i \neq g_i$, entonces $g_i - h_i \in M\backslash\{0\}$, existiendo un índice j tal que $in_>(h_j)|in_>(g_i - h_i)$. Como $in_>(g_i - h_i) < in_>(h_i)$, tenemos que $i \neq j$. Entonces $in_>(h_j) = in_>(g_j)$ divide algún término de h_i o g_i, contradiciendo el hecho de que $\mathcal{G}$ y $\mathcal{H}$ son bases de Gröbner reducidas. Por lo tanto, $g_i = h_i \, \forall i$. □

Ejemplo 2.4.16. Retomando al ejemplo (2.4.11), consideremos a la base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_7\}$ para el submódulo $M = \langle g_1, g_2, g_3, g_4 \rangle$, recordando que

$$g_1 = (x - y, x, x) \qquad g_3 = (y, x, x) \qquad g_6 = (0, 0, x)$$
$$g_2 = (xy, y, y) \qquad g_4 = (y, x, 0) \qquad g_7 = \left(0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4}\right)$$
$$g_5 = (-2y^2, -y, -y)$$

Teniendo además

$$in_>(g_1) = xe_1 \qquad in_>(g_3) = xe_2 \qquad in_>(g_6) = xe_3$$
$$in_>(g_2) = xye_1 \qquad in_>(g_4) = xe_2 \qquad in_>(g_7) = y^2e_2$$
$$in_>(g_5) = -2y^2e_1$$

Con lo que $lm_>(g_1)|lm_>(g_2)$ y $lm_>(g_3) = lm_>(g_4)$. Consideremos al conjunto

$$\mathcal{H} = \left\{ h_1 = g_1, h_2 = g_3, h_3 = \frac{g_5}{-2}, h_4 = g_6, h_5 = g_7 \right\},$$

el cual es base de Gröbner mínima para M. Sea $\mathcal{H}_1 = \{h_2, h_3, h_4, h_5\}$, y calculemos la reducción de h_1 con respecto a este conjunto, obteniendo

$$h_1 \longrightarrow_{h_2} (x - 2y, 0, 0),$$

el cual es reducido con respecto a $\mathcal{H}_1$. Sea $h_1 = (x - 2y, 0, 0)$. Sea $\mathcal{H}_2 = \{h_1, h_3, h_4, h_5\}$, obteniendo

$$h_2 \longrightarrow_{h_4} (y, x, 0),$$

el cual es reducido con respecto a $\mathcal{H}_2$. Sea $h_2 = (y, x, 0)$. Sea $\mathcal{H}_3 = \{h_1, h_2, h_4, h_5\}$, y notemos que h_3 es reducido con respecto a $\mathcal{H}_3$, al igual que h_4 y h_5 con sus respectivos conjuntos $\mathcal{H}_4$ y $\mathcal{H}_5$, siendo $h_3 = h_3$, $h_4 = h_4$ y $h_5 = h_5$. Por lo tanto, el nuevo conjunto $\{h_1, h_2, h_3, h_4, h_5\}$ es la base de Gröbner reducida para M. Si quisieramos ver con el criterio dado en el teorema (2.4.7) que el nuevo conjunto es base de Gröbner, notemos que los únicos S-vectores a considerar son los de $\{g_1, g_3\}$ y $\{g_2, g_5\}$, los cuales son

$$\begin{aligned} S(h_1, h_3) &= \frac{xy^2}{x}h_1 - \frac{xy^2}{y^2}h_3 = y^2h_1 - xh_3 \\ &= y^2(x - 2y, 0, 0) - x\left(y^2, \frac{y}{2}, \frac{y}{2}\right)(xy^2 - 2y^3, 0, 0) - \left(xy^2, \frac{xy}{2}, \frac{xy}{2}\right) \\ &= \left(-2y^3, -\frac{xy}{2}, -\frac{xy}{2}\right) \end{aligned}$$

$$\begin{aligned} S(h_2, h_5) &= \frac{xy^2}{x}h_2 - \frac{xy^2}{y^2}h_5 = y^2h_2 - xh_5 \\ &= y^2(y, x, 0) - x\left(0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4}\right)(y^3, xy^2, 0) - \left(0.xy^2 - \frac{xy}{4}, xy^2 - \frac{xy}{4}\right) \\ &= \left(y^3, \frac{xy}{4}, -xy^2 + \frac{xy}{4}\right) \end{aligned}$$

Reduciendo obtenemos

$$\begin{aligned} S(h_1, h_3) &\longrightarrow_{h_3} \left(0, -\frac{xy}{2} + y^2, -\frac{xy}{2} + y^2\right) \longrightarrow_{h_2} \left(\frac{y^2}{2}, y^2, -\frac{xy}{2} + y^2\right) \\ &\longrightarrow_{h_4} \left(\frac{y^2}{2}, y^2, y^2\right) \longrightarrow_{h_3} \left(0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4}\right) \\ &\longrightarrow_{h_5} 0 \end{aligned}$$

$$\begin{aligned} S(h_2, h_5) &\longrightarrow_{h_3} \left(0, \frac{xy}{4} - \frac{y^2}{2}, -xy^2 + \frac{xy}{4} - \frac{y^2}{2}\right) \longrightarrow_{h_4} \left(0, \frac{xy}{4} - \frac{y^2}{2}, \frac{xy}{4} - \frac{y^2}{2}\right) \\ &\longrightarrow_{h_2} \left(-\frac{y^2}{4}, -\frac{y^2}{2}, \frac{xy}{4} - \frac{y^2}{2}\right) \longrightarrow_{h_4} \left(-\frac{y^2}{4}, -\frac{y^2}{2} - \frac{y^2}{2}\right) \\ &\longrightarrow_{h_3} \left(0, -\frac{y^2}{2} + \frac{y}{8}, -\frac{y^2}{2} + \frac{y}{8}\right) \longrightarrow_{h_5} 0 \end{aligned}$$

Acabamos esta sección con un resultado que será de gran importancia en el capítulo del Polinomio de Hilbert.

Proposición 2.4.17. *Sea $>$ un orden monomial sobre R^m. Sea $M \subset R^m$ un submódulo finitamente generado. Entonces las siguientes condiciones son equivalentes:*

1. *La graduación estándar sobre R^m induce una estructura de módulo graduado sobre M, dada por*
$$M_d = (R_d)^m \cap M.$$
2. *$M = \langle f_1, \ldots, f_t \rangle$ en R^m, donde cada $f_i \in (R_{d_i})^m$.*
3. *La base de Gröbner reducida con respecto al orden $>$ consiste de elementos g_i tales que $g_i \in (R_{d_i})^m$.*

Demostración. 1. 1) $\Rightarrow$ 3) Al ser M finitamente generado existe un conjunto generador $\{h_1, \ldots, h_t\}$ de M. Por ser M graduado
$$h_i = \sum_{k=1}^{n} h_{ik} \qquad h_{ik} \in (R_{d_k})^m.$$
Así, el conjunto $\{h_{ik} | \, i = 1, \ldots, t;\ k = 1, \ldots, n\}$ es un conjunto generador de M. Por el corolario (2.4.14) existe una base de Gröbner reducida $\mathcal{H} = \{h_1, \ldots, h_{t_0}\}$ para M, donde $h_i \in (R_{d_i})^m$.

2. 3) $\Rightarrow$ 2) Por definición de base de Gröbner.

3. 2) $\Rightarrow$ 1) Sea $\{f_1, \ldots, f_t | \, f_i \in (R_{d_i})^m\}$ un conjunto generador de M. Notemos que
$$M_d = (R_d)^m \cap M = \{f = (f_1, \ldots, f_t) \in M | \, f_i \in R_d \, \forall \, i\}$$
Es claro que la suma directa de los M_d
$$\bigoplus_{-\infty}^{\infty} M_d \subset M$$
es un R-módulo graduado. Sólo hace falta ver que todo elemento de M pertenece a $\bigoplus_{-\infty}^{\infty} M_d$. Sea $f \in M$, entonces por hipótesis
$$f = \sum_{i=1}^{t} p_i f_i \qquad p_i \in R.$$

Sea αm un término cualquiera de p_i, de grado t_i. Entonces $\alpha m f_i \in R_{t_i+d_i}$, y esto para cualquier término de p_i, y para toda $i = 1, \ldots, t$. Por lo tanto $f \in \bigoplus_{-\infty}^{\infty} M_d$.

□

Capítulo 3

Sicigias

Este capítulo se divide en dos partes. En la primera vemos la forma de cálcular el submódulo de sicigias para un conjunto generador arbitrario. En la segunda parte damos un importante teorema sobre sicigias debido a Hilbert, donde para demostrarlo hacemos uso de la parte final del capítulo 1 y de la teoría desarrollada en el capítulo anterior.

Durante todo el capítulo sólo consideraremos R-módulos libres finitamente generados, donde $R = k[x_1, \ldots, x_r]$ es el anillo de polinomios sobre el campo k.

Toda base de Gröbner que consideremos será reducida.

3.1 Cálculo del Submódulo de Sicigias

En esta sección desarrollaremos la teoría necesaria para cálcular a los generadores del submódulo de sicigias de un conjunto generador dado. Para esto, comenzaremos con el caso más simple, que es cuando el conjunto generador está formado unicamente por monomios, continuando con el caso en el que estemos considerando bases de Gröbner. Ambos métodos serán utilizados para el caso más general, es decir cuando el conjunto generador no necesariamente es una base de Gröbner.

3.1.1 Sicigias de Submódulos Monomiales

El cálculo de sicigias de submódulos monomiales es fácil de realizar Antes, definiremos una clase especial de sicigias.

Definición 3.1.1. Sea $G = \{\alpha_1 m_1, \ldots, \alpha_t m_t\} \subset R^m$, donde $m_i = x^{a(i)} e_j$, $a(i) \in \mathbb{N}^r$, para alguna j. Una sicigia $h \in R^t$ sobre G, se llama *sicigia homogénea*, si es de la forma

$$h = (\beta_1 x^{a-a_{(1)}}, \ldots, \beta_t x^{a-a_{(t)}}), \qquad \beta_i \in k,\ a \in \mathbb{N}^r,$$

donde decimos que $a(i)$ es el *multigrado* de m_i.

Sea $M \subset R^m$ el submódulo generado por los monomios $\{m_1, \ldots, m_t\}$. Sea $\bigoplus_{i=1}^t R\varepsilon_i$ un R-módulo libre con base $\{\varepsilon_i\}$. Recordemos que el módulo $Syz(m_1, \ldots, m_t) \subset \bigoplus_{i=1}^t R\varepsilon_i$ se puede ver como el núcleo de un morfismo de R-módulos libres. Sea

$$\begin{aligned} \varphi : \bigoplus_{i=1}^{t} R\varepsilon_i &\longrightarrow R^m \\ \varepsilon_i &\longrightarrow m_i \end{aligned}$$

tal morfismo. Así, $Im(\varphi) = M$.

Para cada par de índices i, j tales que m_i y m_j contengan al mismo elemento base e_u de R^m, definimos a los elementos

$$m_{ij} = \frac{mcm[m_i, m_j]}{m_j} \in R$$

y

$$\sigma_{ij} = m_{ji}\varepsilon_i - m_{ij}\varepsilon_j \in \bigoplus_{i=1}^{t} R\varepsilon_i$$

Observación 3.1.2. Por el lema (2.1.14), tenemos que

$$m_{ij} = \frac{m_i}{mcd(m_i, m_j)}$$

Observación 3.1.3. Es claro de la definición que $\sigma_{ij} \in Ker(\varphi)$.

Observación 3.1.4. Notemos que $\varphi(\sigma_{ij})$ es precisamente $S(m_i, m_j)$.

Comentario 3.1.5. Si m_i y m_j no contienen al mismo elemento base, definimos $m_{ij} = 0$.

Proposición 3.1.6. *Considerando la notación anterior, $Syz(m_1, \ldots, m_t)$ es generado por la colección $\{\sigma_{ij} | 1 \leq i, j \leq t\}$.*

Demostración. Como $\sigma_{ij} = -\sigma_{ji}$, nos basta considerar a los σ_{ij} con $i < j$. Sea $h = (h_1, \ldots, h_t) \in R^t$ una sicigia sobre $\{m_1, \ldots, m_t\}$. Así,

$$\varphi(h) = \sum_{i=1}^{t} h_i m_i = 0 \qquad \in R^m,$$

siendo posible reescribirlo en términos de la base $\{e_i\}$

$$0 = \sum_{i=1}^{t} h_i m_i = \sum_{i=1}^{m} f_i e_i, \qquad f_i \in R,$$

implicando que $f_i = 0$, para toda i. Ahora, renombrando en caso de ser necesario, sea $G_i = \{m_1 = x^{a_{(1)}} e_i, \ldots, m_s = x^{a_{(s)}} e_i\}$ la colección de monomios que contienen al elemento base e_i. Así, $f_i e_i = \sum_{j=1}^{s} h_j m_j$, donde $m_j \in G_i$. Pero esto lo que nos dice es que podemos pensar a la sicigia h como una suma de sicigias sobre los subconjuntos de los m_i que contengan al mismo elemento base, bastándonos estudiar a una de tales sicigias. Sea $(h'_1, \ldots, h'_s) \in Syz(m_1, \ldots, m_s)$, entonces

$$\sum_{i=1}^{s} h'_i x^{a_{(i)}} = 0 \qquad \in R. \tag{3.1}$$

A la expresión (3.1) la podemos separar en distintas colecciones de sumas de términos del mismo multigrado, sumas que cada una debe ser cero. Sean $\{\alpha_1 x^a, \ldots, \alpha_k x^a\} \subset R$ los sumandos de una de tales colecciones, donde $\alpha_i x^a = \alpha_i x^{a - a_{(i)}} \cdot x^{a_{(i)}}$, con $\alpha_i x^{a-a_{(i)}}$ término de h', $\alpha_i \in k$, $i = 1, \ldots, k$. Con esta notación se tiene que

$$\sum_{i=1}^{k} \alpha_i x^a = \sum_{i=1}^{k} \alpha_i x^{a - a_{(i)}} x^{a_{(i)}} = 0.$$

implicando que

$$\sum_{i=1}^{k} \alpha_i = 0. \tag{3.2}$$

Notemos que el elemento $\hbar_a = (\alpha_1 x^{a-a_{(1)}}, \ldots, \alpha_k x^{a-a_{(k)}})$ es una sicigia homogénea. Así, hemos mostrado que toda sicigia sobre algún subconjunto de los m_i que contienen el mismo elemento base, se descompone como suma de sicigias homogéneas, bastándonos mostrar que toda sicigia homogénea se puede ver como una combinación R-lineal de los σ_{ij}.

Viendo a $\hbar_a$ como un elemento de $\bigoplus_{i=1}^{k} R\varepsilon_i$, tenemos que

$$\begin{aligned}
\hbar_a =&(\alpha_1 x^{a-a_{(1)}}, \ldots, \alpha_k x^{a-a_{(k)}})\\
=&(\alpha_1 x^{a-a_{(1)}}, (\alpha_1 - \alpha_1 + \alpha_2)x^{a-a_{(2)}}, \ldots, (\alpha_1 - \alpha_1 + \ldots + \alpha_{k-1} - \alpha_{k-1} + \alpha_k)x^{a-a_{(k)}})\\
=&(\alpha_1 x^{a-a_{(1)}}, -\alpha_1 x^{a-a_{(2)}}, 0. \ldots, 0) + \ldots\\
&+ (0, \ldots, 0, (\alpha_1 + \ldots + \alpha_{k-1})x^{a-a_{(k-1)}}, -(\alpha_1 + \ldots + \alpha_{k-1})x^{a-a_{(k)}})\\
&+ (0, \ldots, 0, (\alpha_1 + \ldots + \alpha_k)x^{a-a_{(k)}})\\
=&(\alpha_1 x^{a-a_{(1)}}, -\alpha_1 x^{a-a_{(2)}}, 0, \ldots, 0) + \ldots\\
&+ (0, \ldots, 0, (\alpha_1 + \ldots + \alpha_{k-1})x^{a-a_{(k-1)}}, -(\alpha_1 + \ldots + \alpha_{k-1})x^{a-a_{(k)}}).
\end{aligned}$$

Debiendose la última igualdad a (3.2).

Notemos que para toda i, al ser x^a divisible por $x^{a-a_{(i)}}$ y $x^{a-a_{(i+1)}}$, se tiene entonces que $mcm[x^{a-a_{(i)}}, x^{a-a_{(i+1)}}] | x^a$. Sea $x^a = \mu_i \cdot mcm[x^{a-a_{(i)}}, x^{a-a_{(i+1)}}]$, con $\mu_i \in R$ monomio. Entonces

$$\begin{aligned}
\hbar_a &= \sum_{i=1}^{k-1}(0, \ldots, 0, (\alpha_1 + \ldots + \alpha_i)x^{a-a_i}, -(\alpha_1 + \ldots + \alpha_i)x^{a-a_{i+1}}, 0, \ldots, 0)\\
&= \sum_{i=1}^{k-1}(0, \ldots, 0, \left(\sum_{u=1}^{i}\alpha_u\right)\frac{x^a}{x^{a_i}}, -\left(\sum_{u=1}^{i}\alpha_u\right)\frac{x^a}{x^{a_{i+1}}}, 0, \ldots, 0)\\
&= \sum_{i=1}^{k-1}(0, \ldots, 0, \left(\sum_{u=1}^{i}\alpha_u\right)\frac{\mu_i\, mcm[x^{a_i}, x^{a_{i+1}}]}{x^{a_i}}, -\left(\sum_{u=1}^{i}\alpha_u\right)\frac{\mu_i\, mcm[x^{a_i}, x^{a_{i+1}}]}{x^{a_{i+1}}}, 0, \ldots, 0)\\
&= \sum_{i=1}^{k-1}\left(\mu_i\sum_{u=1}^{i}\alpha_u\right)\left(0, \ldots, 0, \frac{mcm[x^{a_i}, x^{a_{i+1}}]}{x^{a_i}}, -\frac{mcm[x^{a_i}, x^{a_{i+1}}]}{x^{a_{i+1}}}, 0, \ldots, 0\right)\\
&= \sum_{i=1}^{k-1}\left(\mu_i\sum_{u=1}^{i}\alpha_u\right)\sigma_{i\,i+1}
\end{aligned}$$

□

Ejemplo 3.1.7. Sea $R^m = k[x, y, z]^3$. Consideremos al submódulo monomial $M \subset R^m$ generado por los monomios

$$\begin{aligned}
m_1 &= x^{34}y^7 e_1 & m_5 &= ze_2\\
m_2 &= x^{23}y^{19}e_1 & m_6 &= xye_3\\
m_3 &= xe_2 & m_7 &= xze_3\\
m_4 &= ye_2 & m_8 &= yze_3
\end{aligned}$$

Calculemos los máximos comunes divisores

$$mcm[m_1, m_2] = x^{34}y^{19}e_1 \qquad mcm[m_6, m_7] = xyze_3$$
$$mcm[m_3, m_4] = xye_2 \qquad mcm[m_6, m_8] = xyze_3$$
$$mcm[m_3, m_5] = xze_2 \qquad mcm[m_7, m_8] = xyze_3$$
$$mcm[m_4, m_5] = yze_2$$

Ahora, los elementos $m_{ij} \neq 0$ son

$$m_{12} = x^{11} \qquad m_{53} = z \qquad m_{68} = x$$
$$m_{21} = y^{12} \qquad m_{45} = y \qquad m_{86} = z$$
$$m_{34} = x \qquad m_{54} = z \qquad m_{78} = x$$
$$m_{43} = y \qquad m_{67} = y \qquad m_{87} = y$$
$$m_{35} = x \qquad m_{76} = z$$

Procediendo ahora a calcular las sicigias generadoras

$$\sigma_{12} = y^{12}\varepsilon_1 - x^{11}\varepsilon_2 \qquad \sigma_{67} = z\varepsilon_6 - y\varepsilon_7$$
$$\sigma_{34} = y\varepsilon_3 - x\varepsilon_4 \qquad \sigma_{68} = z\varepsilon_6 - x\varepsilon_8$$
$$\sigma_{45} = z\varepsilon_4 - y\varepsilon_5 \qquad \sigma_{78} = y\varepsilon_7 - x\varepsilon_8$$
$$\sigma_{35} = z\varepsilon_3 - x\varepsilon_5$$

Ejemplo 3.1.8. Consideremos el caso de los términos iniciales de la base de Gröbner reducida obtenida en el ejemplo (2.4.16), siendo el siguiente conjunto de monomios

$$m_1 = xe_1 \qquad m_3 = y^2e_1 \qquad m_4 = xe_3$$
$$m_2 = xe_2 \qquad\qquad m_5 = y^2e_2$$

Los únicos mínimos comunes múltiplos a considerar son

$$mcm[m_1, m_3] = xy^2e_1$$
$$mcm[m_2, m_5] = xy^2e_2$$

Así, los m_{ij} distintos de cero son

$$m_{13} = x \qquad m_{25} = x$$
$$m_{31} = y^2 \qquad m_{52} = y^2$$

Por lo tanto, los generadores de $Syz(m_1, \ldots, m_5)$ son

$$\sigma_{13} = y^2\varepsilon_1 - x\varepsilon_3$$
$$\sigma_{25} = y^2\varepsilon_2 - x\varepsilon_5$$

3.1.2 Sicigias de Bases de Gröbner

La forma de obtener las sicigias sobre una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_t\}$ es utilizando el algoritmo de Buchberger. Denotemos por r_{ij} al residuo del S-vector $S(g_i, g_j)$, que es de la forma:

$$\begin{aligned} r_{ij} &= S(g_i, g_j) - \sum_{u=1}^{t} h_u g_u \\ &= \frac{mcm[lm_>(g_i), lm_>(g_j)]}{in_>(g_i)} g_i - \frac{mcm[lm_>(g_i), lm_>(g_j)]}{in_>(g_j)} g_j - \sum_{u=1}^{t} h_u g_u \\ &= \frac{mcm[lm_>(g_i), lm_>(g_j)]}{lm_>(g_i)} g_i - \frac{mcm[lm_>(g_i), lm_>(g_j)]}{lm_>(g_j)} g_j - \sum_{u=1}^{t} h_u g_u \end{aligned}$$

donde al ser $\mathcal{G}$ una base de Gröbner, $r_{ij} = 0$, es decir, r_{ij} es una sicigia sobre $\mathcal{G}$. Demostraremos que las sicigias de esta forma son un conjunto generador para el submódulo $Syz(g_1, \ldots, g_t)$.

Para demostrar esto, reescribamos la notación de la sección anterior al caso general.

Sea $>$ un orden monomial sobre R^m. Sea $\mathcal{G} = \{g_1, \ldots, g_t\} \in R^m$ una base de Gröbner para el submódulo M. Sea $\bigoplus_{i=1}^{t} R\varepsilon_i$ un R-módulo libre con base $\{\varepsilon_i\}$. Sea φ el mapeo de R-módulos libres

$$\begin{aligned} \varphi : \bigoplus_{i=1}^{t} R\varepsilon_i &\longrightarrow R^m \\ \varepsilon_i &\longrightarrow g_i. \end{aligned}$$

Para cada par de índices i, j tales que los términos $in_>(g_i)$ y $in_>(g_j)$ contengan al mismo

elemento base e_i de R^m, definimos a los elementos

$$m_{ij} = \frac{mcm[lm_>(g_i), lm_>(g_j)]}{in_>(g_j)} \qquad \in R$$

y

$$\sigma_{ij} = m_{ji}\varepsilon_i - m_{ij}\varepsilon_j, \qquad \in \bigoplus_{i=1}^{t} R\varepsilon_i,$$

donde el conjunto de los σ_{ij} por la proposición (3.1.6) generan $Syz(in_>(g_1), \ldots, in_>(g_t))$. Notemos que bajo φ tenemos que

$$\varphi(\sigma_{ij}) = S(g_i, g_j).$$

Análogamente, si $in_>(g_i)$ y $in_>(g_j)$ no contienen al mismo elemento base, entonces $m_{ij} = 0$. Adicionalmente, para cada par de índices i, j que contengan al mismo elemento base e_i, consideremos a la expresión estándar

$$S(g_i, g_j) = \sum_{i=1}^{t} h_i g_i, h_i \in R,$$

y consideremos al elemento

$$\sum_{i=1}^{t} h_i\varepsilon_i \in \bigoplus_{i=1}^{t} R\varepsilon_i.$$

Definamos al elemento $\tau_{ij} \in \bigoplus_{i=1}^{t} R\varepsilon_i$, como

$$\tau_{ij} = \sigma_{ij} - \sum_{i=1}^{t} h_i\varepsilon_i.$$

Observación 3.1.9. Es claro de la definición que $\tau_{ij} \in Ker(\varphi)$.

Observación 3.1.10. Consideremos al conjunto $\{g_1, \ldots, g_{t_0} | g_i \in (R_{d_i})^m\}$. Entonces el elemento τ_{ij} es graduado en algún R-módulo graduado deslizado. En efecto, por el lema (2.4.6) tenemos que $S(g_i, g_j) \in (R_t)^m$, donde $t = mcm[in_>(g_i), in_>(g_j)]$ Notando que los elementos $\{\varepsilon_i\}$ de la base de $\bigoplus_{i=1}^{t_0} R\varepsilon_i$ son de grado d_i en $\bigoplus_{i=1}^{t_0} R(-d_i)$, tenemos que

$$deg(\sigma_{ij}) = deg(S(g_i, g_j)) = t. \tag{3.3}$$

Si $S(g_i, g_j) = \sum_{i=1}^{t_0} h_i g_i$, por (3.3) $deg(h_i g_i) = t$. Por lo tanto

$$deg(\tau_{ij}) = deg\left(\sigma_{ij} - \sum_{i=1}^{t_0} h_i\varepsilon_i\right) = t$$

para todo i, j.

Finalmente, definamos un orden monomial sobre $\bigoplus_{i=1}^{t} R\varepsilon_i$ a partir del orden $>$ sobre R^m. Sea $>_{(>)}$ un orden monomial sobre $\bigoplus_{i=1}^{t} R\varepsilon_i$ definido como: $m\varepsilon_u >_{(>)} n\varepsilon_v$ si, y sólo si,

$$in_>(mg_u) > in_>(ng_v),$$

con respecto a $>$, o

$$lm_>(mg_u) = lm_>(ng_v),$$

pero $u < v$.

Teorema 3.1.11 (Schreyer). Considerando la notación anterior, sea $\mathcal{G} = \{g_1, \ldots, g_t\}$ una base de Gröbner. Entonces la colección $\{\tau_{ij} | 1 \leq i, j \leq t\}$ es una base de Gröbner para $Syz(g_1, \ldots, g_t)$ con respecto al orden $>_{(>)}$. Además $in_{>_{(>)}}(\tau_{ij}) = m_{ji}\varepsilon_i$.

Demostración. Primero mostraremos que $in_{>_{(>)}}(\tau_{ij}) = m_{ji}\varepsilon_i$. Observemos que

$$in_>(m_{ji}g_i) = mcm[lm_>(g_i), lm_>(g_j)] = in_>(m_{ij}g_j), \tag{3.4}$$

pero $i < j$, por lo que $m_{ji}\varepsilon_i >_{(>)} m_{ij}\varepsilon_j$. Sea $\alpha m\varepsilon_u$ un término de $\sum_{i=1}^{t} h_i\varepsilon_i$, entonces por el teorema (2.3.9), $in_>(\alpha m g_u) \leqslant in_>(S(g_i, g_j))$. Pero por (3.4), $in_>(S(g_i, g_j)) \neq in_>(m_{ji}g_i)$, por lo que $in_>(S(g_i, g_j))$ es alguno de los términos restantes. el cual es menor a $in_>(m_{ji}g_i)$. Por lo tanto, $m_{ji}\varepsilon_i >_{(>)} \alpha m\varepsilon_u$.

Ahora mostraremos que la colección $\{\tau_{ij} | 1 \leqslant i < j \leqslant t\}$ es base de Gröbner para $Syz(g_1, \ldots, g_t)$ con respecto a $>_{(>)}$. Como vimos en la observación (3.1.9), tenemos que $\tau_{ij} \in Ker(\varphi)$. Así, por el lema (2.1.29), nos basta demostrar que para toda sicigia $\tau \in Syz(g_1, \ldots, g_t)$, se cumple que $in_{>_{(>)}}(\tau)$ es divisible por algún $m_{ji}\varepsilon_i$. con $i < j$.

Escribamos a la sicigia τ como combinación R-lineal de los ε_i, obteniendo

$$\tau = \sum_{i=1}^{t} f_i\varepsilon_i.$$

Para todo índice $j \in \{1, \ldots, t\}$, sea $n_j\varepsilon_j = in_{>_{(>)}}(f_j\varepsilon_j)$. obteniendo entonces que

$$in_{>_{(>)}}(\tau) = in_{>_{(>)}}(\sum_{j=1}^{t} f_j\varepsilon_j) = n_i\varepsilon_i.$$

para alguna i. Sea $I = \{j \in \{1, \ldots, t\} | lm_>(n_i g_i) = lm_>(n_j g_j)\}$. Como $in_{>_{(>)}}(\tau) = n_i\varepsilon_i$, debemos tener que $i < j$, para todo $j \in I$. Sea $\sigma = \sum_{j \in I} n_j\varepsilon_j$. observando que

$$in_{>_{(>)}}(\sigma) = n_i\varepsilon_i = in_{>_{(>)}}(\tau) \tag{3.5}$$

Como $\varphi(\tau) = 0$, toda colección de términos de $\varphi(\tau)$ que difieran por un escalar se deben eliminar entre si, es decir,

$$\varphi(\sigma) = \sum_{j \in I} n_j in_>(g_j) = 0,$$

concluyendo que $\sigma \in Syz(in_>(g_1), \ldots, in_>(g_t))$. Por la proposición (3.1.6),

$$\sigma = \sum_{\substack{j,k \in I \\ j<k}} h_{jk}\sigma_{jk}, \tag{3.6}$$

donde $h_{jk} \in R$. Así, σ pertenece al submódulo monomial generado por los σ_{jk} de la expresión (3.6). Por (3.5) y (3.6), tenemos que

$$\begin{aligned} in_{>_{(>)}}(\tau) &= in_{>_{(>)}}(\sigma) = n_i\varepsilon_i \\ &= in_{>_{(>)}}\left(\sum_{\substack{j,k \in I \\ j<k}} h_{jk}\sigma_{jk}\right) \\ &= \sum_{j \in I} in_{>_{(>)}}(h_{ij}m_{ji}\varepsilon_i). \end{aligned}$$

Por lo tanto, n_i pertenece al ideal generado por los m_{ji}, con $i < j$. Por lo tanto, $m_{ji}|n_i$, para alguna j. Concluyendo que $in_{>_{(>)}}(\tau) = n_i\varepsilon_i$ es divisible por $m_{ji}\varepsilon_i = in_{>_{(>)}}(\tau_{ij})$. □

Corolario 3.1.12. *Considerando la notación del teorema anterior, $Syz(g_1, \ldots, g_t)$ es generado por la colección $\{\tau_{ij} | 1 \leq i, j \leq t\}$.*

Corolario 3.1.13. *Si $\mathcal{G} = \{g_1, \ldots, g_{t_0} | g_i \in (R_{d_i})^m\}$ es base de Gröbner, entonces el conjunto generador $\{\tau_{ij} | 1 \leq i, j \leq t_0\}$ de las sicigias de $\mathcal{G}$ es homogéneo, viviendo en $\bigoplus_{i=1}^{t_0} R(-d_i)$.*

Demostración. Se sigue inmediatamente de la observación (3.1 10) y del teorema de Schreyer. □

Ejemplo 3.1.14. Consideremos al ejemplo (2.4.16). De los resultados del ejemplo (3.1.8) y los dados en la parte final del ejemplo (2.4.16) obtenemos que $Syz(g_1, g_2, g_3, g_4, g_5)$ está generado por

$$\begin{aligned} \tau_{13} &= y^2\varepsilon_1 - x\varepsilon_3 - \left(-\frac{y}{2}\varepsilon_2 + \left(\frac{1}{2} - 2y\right)\varepsilon_3 - \frac{y}{2}\varepsilon_4 + \varepsilon_5\right) \\ &= y^2\varepsilon_1 - x\varepsilon_3 + \frac{y}{2}\varepsilon_2 - \left(\frac{1}{2} - 2y\right)\varepsilon_3 + \frac{y}{2}\varepsilon_4 - \varepsilon_5 \\ &= y^2\varepsilon_1 + \frac{y}{2}\varepsilon_2 + \left(2y - x - \frac{1}{2}\right)\varepsilon_3 + \frac{y}{2}\varepsilon_4 - \varepsilon_5 \end{aligned}$$

$$\begin{aligned}\tau_{25} &= y^2\varepsilon_2 - x\varepsilon_5 - \left(\frac{y}{4}\varepsilon_2 + \left(y - \frac{1}{4}\right)\varepsilon_3 + \left(\frac{y}{4} - y^2\right)\varepsilon_4 - \frac{1}{2}\varepsilon_5\right) \\ &= y^2\varepsilon_2 - x\varepsilon_5 - \frac{y}{4}\varepsilon_2 - \left(y - \frac{1}{4}\right)\varepsilon_3 - \left(\frac{y}{4} - y^2\right)\varepsilon_4 + \left(\frac{1}{2} - x\right)\varepsilon_5 \\ &= \left(y^2 - \frac{y}{4}\right)\varepsilon_2 + \left(\frac{1}{4} - y\right)\varepsilon_3 + \left(y^2 - \frac{y}{4}\right)\varepsilon_4 + \left(\frac{1}{2} - x\right)\varepsilon_5\end{aligned}$$

Hasta el momento solo hemos resuelto el problema de cálcular el conjunto generador de las sicigias sobre un conjunto $\mathcal{G} \subset R^m$, que es base de Gröbner. Restándonos encontrar las sicigias sobre un conjunto $F \subset R^m$ que no sea base de Gröbner.

3.1.3 Sicigias de Conjuntos Generadores

Consideremos en lo que resta de la presente sección un orden monomial $>$ fijo sobre R^m. Para el caso general, donde nos ocuparemos de un conjunto de elementos cualesquiera $F = \{f_1, \ldots, f_t\} \subset R^m$, necesitamos primero cálcular una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_s\} \subset R^m$ para $M = \langle F \rangle = \langle \mathcal{G} \rangle$. Así, consideremos a las matrices

$$\mathcal{M}_F = (f_1 \cdots f_t)$$

y

$$\mathcal{M}_\mathcal{G} = (g_1 \cdots g_s)$$

de $m \times t$ y $m \times s$, donde los f_i y g_i son las columnas, respectivamente. Al ser $\mathcal{M}_F$ y $\mathcal{M}_\mathcal{G}$ representaciones matriciales de M con respecto a los conjuntos generadores F y $\mathcal{G}$, existen matrices $\mathcal{A}$ y $\mathcal{B}$, de $t \times s$ y $s \times t$ respectivamente, ambas con entradas en R que cumplen ser las matrices de cambio, es decir,

$$\mathcal{M}_\mathcal{G} = \mathcal{M}_F\mathcal{A} \tag{3.7}$$

y

$$\mathcal{M}_F = \mathcal{M}_\mathcal{G}\mathcal{B} \tag{3.8}$$

La teoría necesaria para obtener estas matrices se desarrollo en el capítulo anterior.

Para obtener la matriz $\mathcal{A}$ hay que encontrar los coeficientes necesarios para expresar a los g_i en función de los f_i, coeficientes que serán las columnas de la matriz $\mathcal{A}$. Los coeficientes se obtienen aplicando el algoritmo de Buchberger, ya que la base de Gröbner se obtiene al ir agregando los nuevos elementos que salen del algoritmo, elementos que construimos en función de los f_i.

Ejemplo 3.1.15. Retomemos el ejemplo manejado en el capítulo anterior. Recordando que el conjunto generador a considerar es $F = \{f_1, f_2, f_3, f_4\}$, donde

$$f_1 = (x - y, x, x) \qquad f_3 = (y, x, x)$$
$$f_2 = (xy, y, y) \qquad f_4 = (y, x, 0)$$

y la base de Gröbner es $\mathcal{G} = \{g_1, g_2, g_3, g_4, g_5\}$, donde

$$g_1 = (x - 2y, 0, 0) \qquad g_3 = \left(y^2, \frac{y}{2}, \frac{y}{2}\right) \qquad g_4 = (0, 0, x)$$
$$g_2 = (y, x, 0) \qquad g_5 = \left(0, y^2 - \frac{y}{4}, y^2 - \frac{y}{4}\right)$$

Los términos iniciales de los elementos del conjunto generador, considerando el mismo orden con que se les manejo son:

$$in_>(f_1) = xe_1 \qquad in_>(f_3) = xe_2$$
$$in_>(f_2) = xe_1 \qquad in_>(f_4) = xe_2$$

y en el caso de los elementos de la base de Gröbner son:

$$in_>(g_1) = xe_1 \qquad in_>(g_3) = y^2e_1 \qquad in_>(g_4) = xe_3$$
$$in_>(g_2) = xe_2 \qquad in_>(g_5) = y^2e_2$$

Ahora, los resultados de los ejemplos (2.4.11) y (2.4.16) que requerimos son

$$\begin{aligned}
g_1 &= f_1 - f_3 \\
g_2 &= f_4 \\
g_3 &= -\frac{1}{2}(yf_1 - f_2 - yf_3) \\
&= -\frac{y}{2}f_1 + \frac{1}{2}f_2 + \frac{y}{2}f_3 \\
g_4 &= f_3 - f_4 \\
g_5 &= yf_2 - yf_3 - \left(\frac{x+1}{4}\right)(yf_1 - f_2 - yf_3) \\
&= \left(\frac{xy}{2} + \frac{y}{4}\right)f_1 + \left(y - \frac{x}{2} - \frac{1}{4}\right)f_2 + \left(\frac{y}{2} - \frac{xy}{2} - \frac{y}{4}\right)f_3
\end{aligned}$$

Así, tenemos que

$$\mathcal{M}_{\mathcal{G}} = \begin{pmatrix} x - 2y & y & y^2 & 0 & 0 \\ 0 & x & \frac{y}{2} & 0 & y^2 - \frac{y}{4} \\ 0 & 0 & \frac{y}{2} & x & y^2 - \frac{y}{4} \end{pmatrix}$$

$$= \begin{pmatrix} x-y & xy & y & y \\ x & y & x & x \\ x & y & x & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -\frac{y}{2} & 0 & \frac{xy}{2}+\frac{y}{4} \\ 0 & 0 & \frac{1}{2} & 0 & y-\frac{x}{2}-\frac{1}{4} \\ -1 & 0 & \frac{y}{2} & 1 & \frac{y}{2}-\frac{xy}{2}-\frac{y}{4} \\ 0 & 1 & 0 & -1 & 0 \end{pmatrix} = \mathcal{M}_F\mathcal{A}$$

La matriz $\mathcal{B}$ es obtenida aplicando el algoritmo de la división multivariado, dando en cada paso los valores en R que necesitamos para poner al conjunto generador en función de los elementos de la base de Gröbner, valores que serán las columnas de la matriz $\mathcal{A}$.

Ejemplo 3.1.16. Consideremos el caso del ejemplo anterior. Aplicando el algoritmo de la división multivariado obtenemos los siguientes resultados:

$$\begin{aligned} f_1 &\longrightarrow_{g_1} (y,x,x) \longrightarrow_{g_2} (0,0,x) \longrightarrow_{g_4} 0 \\ f_2 &\longrightarrow_{g_1} (2y^2,y,y) \longrightarrow_{g_3} \left(y^2,\frac{y}{2},\frac{y}{2}\right) \longrightarrow_{g_3} 0 \\ f_3 &\longrightarrow_{g_2} (0,0,x) \longrightarrow_{g_4} 0 \\ f_4 &\longrightarrow_{g_2} 0 \end{aligned}$$

Así, tenemos que

$$\mathcal{M}_F = \begin{pmatrix} x-y & xy & y & y \\ x & y & x & x \\ x & y & x & 0 \end{pmatrix}$$

$$= \begin{pmatrix} x-2y & y & y^2 & 0 & 0 \\ 0 & x & \frac{y}{2} & 0 & y^2-\frac{y}{4} \\ 0 & 0 & \frac{y}{2} & x & y^2-\frac{y}{4} \end{pmatrix} \begin{pmatrix} 1 & y & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \mathcal{M}_\mathcal{G}\mathcal{B}$$

Al ser $\mathcal{A}$ y $\mathcal{B}$ matrices de cambio de $\mathcal{M}_F$ a $\mathcal{M}_\mathcal{G}$ y de $\mathcal{M}_\mathcal{G}$ a $\mathcal{M}_F$, respectivamente, se cumple que

$$\mathcal{M}_F = \mathcal{M}_F\mathcal{A}\mathcal{B} \tag{3.9}$$

$$\mathcal{M}_\mathcal{G} = \mathcal{M}_\mathcal{G}\mathcal{B}\mathcal{A} \tag{3.10}$$

Si M fuera espacio vectorial, adicionalmente tendríamos que las matrices de cambio cumplen con $\mathcal{A}\mathcal{B} = \mathbb{I}_t$ y $\mathcal{B}\mathcal{A} = \mathbb{I}_s$, donde $\mathbb{I}_t$ e $\mathbb{I}_s$ son las matrices identidad en las matrices

de $t \times t$ y $s \times s$, respectivamente. Esto último no ocurre necesariamente en el caso en que M es R-módulo.

Ejemplo 3.1.17. Si consideramos las matrices $\mathcal{A}$ y $\mathcal{B}$ obtenidas en los ejemplos (3.1.15) y (3.1.16), tenemos que

$$\mathcal{AB} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathcal{BA} = \begin{pmatrix} 1 & 0 & 0 & 0 & y^2 \\ 0 & 1 & 0 & 0 & \frac{y}{2} \\ 0 & 0 & 1 & 0 & 2y - x - \frac{1}{2} \\ 0 & 0 & 0 & 1 & \frac{y}{2} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Comentario 3.1.18. En este ejemplo resultó que un producto de las matrices de cambio sí fue la matriz identidad, pero esto en general no sucede.

Las matrices $\mathcal{A}$ y $\mathcal{B}$ además de relacionar a los conjuntos generadores F y $\mathcal{G}$, relacionan a las sicigias sobre F y $\mathcal{G}$.

Lema 3.1.19. *Considerando la notación anterior, afirmamos lo siguiente:*

1. *Sea $\tau_{\mathcal{G}} \in Syz(g_1, \ldots, g_s)$, entonces la matriz producto (viéndo a $\tau_{\mathcal{G}}$ como vector columna) $\mathcal{A} \cdot \tau_{\mathcal{G}}$ es un elemento de $Syz(f_1, \ldots, f_t)$.*

2. *Sea $\tau_F \in Syz(f_1, \ldots, f_t)$, entonces la matriz producto (viéndo a τ_F como vector columna) $\mathcal{B} \cdot \tau_F$ es un elemento de $Syz(g_1, \ldots, g_s)$.*

3. *Cada columna de la matriz $\mathfrak{I}_t - \mathcal{AB}$ es un elemento de $Syz(f_1, \ldots, f_t)$.*

Demostración. 1. Considerando a la igualdad (3 7) tenemos que

$$0 = \mathcal{M}_{\mathcal{G}} \cdot \tau_{\mathcal{G}} = (\mathcal{M}_F \mathcal{A})\, \tau_{\mathcal{G}} = \mathcal{M}_F\, (\mathcal{A} \cdot \tau_{\mathcal{G}})$$

Por lo tanto $\mathcal{A} \cdot \tau_{\mathcal{G}} \in Syz(f_1, \ldots, f_t)$.

2. Considerando la igualdad (3.8) tenemos que

$$0 = \mathcal{M}_F \cdot \tau_F = (\mathcal{M}_\mathcal{G}\mathcal{B})\,\tau_F = \mathcal{M}_\mathcal{G}\,(\mathcal{B} \cdot \tau_F)$$

Por lo tanto $\mathcal{B} \cdot \tau_F \in Syz(g_1, \ldots, g_s)$.

3. De la igualdad (3.9) se sigue que

$$\mathcal{M}_F\,(\mathcal{I}_t - \mathcal{A}\mathcal{B}) = \mathcal{M}_F\mathcal{I}_t - \mathcal{M}_f\mathcal{A}\mathcal{B} = \mathcal{M}_F - \mathcal{M}_F = 0$$

Por definición de producto de matrices se tiene el resultado deseado.

□

Ahora ya estamos en posición de dar el resultado importante de esta sección, que es dar la forma de cálcular las sicigias sobre un conjunto generador (no necesariamente base de Gröbner) $F = \{f_1, \ldots, f_t\}$.

Teorema 3.1.20. Sea $F = \{f_1, \ldots, f_t\} \subset R^m$ un conjunto, y sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ una base de Gröbner para $M = \langle F \rangle$. Sean $\mathcal{A}$ y $\mathcal{B}$ las matrices de cambio de $\mathcal{M}_F$ a $\mathcal{M}_\mathcal{G}$ y de $\mathcal{M}_\mathcal{G}$ a $\mathcal{M}_F$, respectivamente. Sea $\{\tau_1, \ldots, \tau_k\}$ el conjunto generador para $Syz(g_1, \ldots, g_s)$ como el dado en el corolario (3.1.12). Sean $c_1, \ldots, c_t$ las columnas de la matriz $\mathcal{I}_t - \mathcal{A}\mathcal{B}$. Entonces

$$Syz(f_1, \ldots, f_t) = \langle \mathcal{A} \cdot \tau_1, \ldots, \mathcal{A} \cdot \tau_k, c_1, \ldots, c_t \rangle$$

Demostración. Observemos que por el lema anterior se tiene que

$$\langle \mathcal{A} \cdot \tau_1, \ldots, \mathcal{A} \cdot \tau_k, c_1, \ldots c_t \rangle \subset Syz(f_1, \ldots, f_t)$$

restándonos mostrar que toda sicigia sobre F se puede expresar como una combinación R-lineal de los $\mathcal{A} \cdot \tau_i$ y c_j. Sea $\tau \in Syz(f_1, \ldots, f_t)$, por el inciso b) del lema anterior tenemos que $\mathcal{B} \cdot \tau \in Syz(g_1, \ldots, g_s)$, lo que implica que se tiene una expresión para $\mathcal{B} \cdot \tau$ de la forma

$$\mathcal{B} \cdot \tau = \sum_{i=1}^{k} h_i \tau_i \tag{3.11}$$

Multiplicando por $\mathcal{A}$ a la expresión (3.11) por la izquierda, obtenemos

$$\mathcal{A}\mathcal{B} \cdot \tau = \mathcal{A} \sum_{i=1}^{k} h_i \tau_i = \sum_{i=1}^{k} h_i \mathcal{A} \cdot \tau_i \tag{3.12}$$

Pero notemos que

$$\tau = ((\mathcal{I}_t - \mathcal{AB}) + \mathcal{AB})\tau = (\mathcal{I}_t - \mathcal{AB})\tau + \mathcal{AB}\cdot\tau \tag{3.13}$$

Así, de las expresiones (3.12) y (3.13) tenemos que

$$\begin{aligned}\tau &= (\mathcal{I}_t - \mathcal{AB})\tau + \sum_{i=1}^{k} h_i \mathcal{A}\cdot\tau_i \\ &= \sum_{i=1}^{t} h_i' c_i + \sum_{i=1}^{k} h_i \mathcal{A}\cdot\tau_i\end{aligned}$$

con $h_i' \in R$, para toda i. La última igualdad se sigue de la definición de las columnas c_i Pero la última expresión nos dice que $\tau \in \langle \mathcal{A}\cdot\tau_1, \ldots, \mathcal{A}\cdot\tau_k, c_1, \ldots, c_t\rangle$. □

Ejemplo 3.1.21. Retomemos el ejemplo que hemos manejado hasta el momento. De los resultados del ejemplo (3.1.17) tenemos que

$$\begin{pmatrix} c_1 & c_2 & c_3 & c_4 \end{pmatrix} = \mathcal{I}_4 - \mathcal{AB}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

En este caso en particular, $c_i = (0,0,0,0)$, para toda i. Tenemos del ejemplo (3.1.14) que $Syz(g_1, g_2, g_3, g_4, g_5) = \langle \tau_{13}, \tau_{25}\rangle$ Así, $Syz(f_1, f_2, f_3, f_4) = \langle \mathcal{A}\cdot\tau_{13}, \mathcal{A}\cdot\tau_{25}\rangle$, donde

$$\mathcal{A}\cdot\tau_{13} = (0,0,0,0)$$

$$\begin{aligned}\mathcal{A}\cdot\tau_{25} &= \left(\frac{y^2}{2} - \frac{x^2y}{2}, \frac{x^2}{2} - xy, \frac{y^2}{2} + \frac{x^2y}{2} - \frac{xy}{2}, 0\right) \\ &= \left(\frac{y^2 - x^2y}{2}\right)\varepsilon_1 + \left(\frac{x^2}{2} - xy\right)\varepsilon_2 + \left(\frac{y^2 + x^2y - xy}{2}\right)\varepsilon_3\end{aligned}$$

En este caso, el submódulo de sicigias sobre F tiene un solo generador.

3.2 Teorema de Sicigias de Hilbert

En el Capítulo 1 vimos que todo R-módulo tiene una resolución libre dada a partir de su presentación, pero no que tiene una graduada. En esta sección procederemos a probar que todo R-módulo finitamente generado tiene una resolución graduada finita, resultado conocido como el *"teorema de Sicigias de Hilbert"*,

Para demostrar el teorema hay que hacer uso del siguiente lema.

Lema 3.2.1. *Sea $>$ un orden monomial sobre R^m. Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ una base de Gröbner para el submódulo $M \subset R^m$. Reordenemos a los elementos de $\mathcal{G}$ en un vector $G = (g_1, \ldots, g_s)$ de tal forma que si $in_>(g_i)$ y $in_>(g_j)$ contienen al mismo elemento base e_u e $i < j$. entonces $lm_>(g_i) >_l lm_>(g_j)$, con $>_l$ el orden lexicográfico considerando $x_1 > x_2 > \cdots > x_r$. Si las variables $x_1, \ldots, x_i$ no aparecen en $lm_>(g_u)$, para alguna $u \in \{1, \ldots, s\}$, entonces las variables $x_1, \ldots, x_i, x_{i+1}$ no aparecen en $lm_{>(>)}(\tau_{uv})$, donde τ_{uv} es un elemento del conjunto generador de $Syz(g_1, \ldots, g_s)$ (como los obtenidos en la sección anterior), para toda u tal que $u < v \leq s$. Así, si las variables $x_1, \ldots, x_i$ no aparecen en ningún $lm_>(g_u)$ para $u = 1, \ldots, s$, entonces las variables $x_1, \ldots, x_i, x_{i+1}$ no aparecen en ningún $lm_{>(>)}(\tau_{uv})$ para $1 \leq u < v \leq s$.*

Demostración. En vista de que si $lm_>(g_u)$ y $lm_>(g_v)$ no contienen al mismo elemento base, entonces $\tau_{uv} = 0$, y de que $\tau_{uv} = -\tau_{vu}$, nos bastará considerar el caso en que ambos monomios contengan al mismo elemento base con $u < v$.

Ahora, al no aparecer $x_1, \ldots, x_i$ en $lm_>(g_u)$, tenemos que

$$lm_>(g_u) = x_{i+1}^{\alpha} + n_u$$

con $\alpha \in \mathbb{N}$, $n_u \in R$ monomio conteniendo unicamente a las variables $x_{i+2}, \ldots, x_r$. Por la forma en que ordenamos al vector G, tenemos que $lm_>(g_u) >_l lm_>(g_v)$. Con esto, las variables $x_1, \ldots, x_i$ no pueden aparecer en $lm_>(g_v)$, teniendo que

$$lm_>(g_v) = x_{i+1}^{\beta} + n_v$$

con $\beta \in \mathbb{N}$, $n_v \in R$ monomio conteniendo unicamente a las variables $x_{i+2}, \ldots, x_r$, donde $\alpha \geq \beta$. Así,

$$mcm[lm_>(g_u), lm_>(g_v)] = x_{i+1}^{\alpha} n_{uv}$$

con $n_{uv} \in R$ monomio conteniendo unicamente a las variables $x_{i+2}, \ldots, x_r$. El teorema

(3.1.11) nos dice que

$$in_{>_{(>)}}(\tau_{uv}) = \frac{mcm[lm_>(g_u), lm_>(g_v)]}{in_>(g_u)}\varepsilon_u = \frac{x_{i+1}^{\alpha} n_{uv}}{x_{i+1}^{\alpha} n_u}\varepsilon_u$$
$$= \frac{n_{uv}}{n_u}\varepsilon_u$$

es decir, $in_{>_{(>)}}(\tau_{uv})$ no contiene a las variables $x_1, \ldots, x_i, x_{i+1}$. Por lo tanto, si no aparecen en cualquier $lm_>(g_u)$, $u = 1, \ldots, s$, entonces $x_1, \ldots, x_i, x_{i+1}$ no pueden aparecer en cualquier $lm_{>_{(>)}}(\tau_{uv})$, para $1 \leq u < v \leq s$. □

Teorema 3.2.2 (Graduado de las Sicigias de Hilbert). Todo R-módulo M finitamente generado tiene una resolución graduada de longitud a lo más r.

Demostración. En la Sección 1.4 vimos como obtener una resolución libre para todo R-módulo finitamente generado, obteniendo la proposición (1.4.8). Ahora repetiremos el proceso, sólo que esta vez utilizaremos la herramienta desarrollada hasta el momento y notando que la resolución obtenida es graduada.

Por la proposición (2.4.17), al ser M graduado podemos considerar una base de Gröbner reducida $\{g_1, \ldots, g_{t_0} | \, g_i \in (R_{d_i})^m\}$ para M. Por el corolario (3.1.13) y la proposición (2.4.17), $Syz(g_1, \ldots, g_{t_0})$ es graduado. Así, su base de Gröbner reducida $\mathcal{T}_0 = \{\tau_1^{(0)}, \ldots, \tau_{t_1}^{(0)} | \, deg(\tau_j^{(0)}) = d_{1,j}\}$, con respecto a algún orden monomial $>$ en $R(-d_i)$, es homogénea. La presentación para M

$$\bigoplus_{1,j=1}^{t_1} R(-d_{1,j}) \xrightarrow{\varphi_1} \bigoplus_{i=1}^{t_0} R(-d_i) \xrightarrow{\varphi_0} M \longrightarrow 0$$

está dada por morfismos φ_0, φ_1 que por construcción son graduados de grado cero, y cumpliendo $Im(\varphi_1) = Syz(g_1, \ldots, g_{t_0}) = Ker(\varphi_0)$. Ordenemos a los elementos de $\mathcal{T}_0$ para obtener un vector T_0 como el que pide el lema anterior. Análogamente $Syz(\mathcal{T}_0)$ es módulo graduado, con una base de Gröbner reducida para $Syz(\mathcal{T}_0) \subset \bigoplus_{1,j=1}^{t_1} R(-d_{1,j})$ con respecto al orden monomial asociado a $\bigoplus_{1,j=1}^{t_1} R(-d_{1,j})$ como en el teorema de Schreyer, el cual denotaremos por $>_{t_1}$.

Por el lema anterior, al menos para la variable x_1 tenemos que $x_1 \notin in_{>_{t_1}}(\mathcal{T}_1)$. Además tenemos la sucesión exacta

$$\bigoplus_{2,j=1}^{t_2} R(-d_{2,j}) \xrightarrow{\varphi_2} \bigoplus_{1,j=1}^{t_1} R(-d_{1,j}) \xrightarrow{\varphi_1} \bigoplus_{i=1}^{t_0} R(-d_i) \xrightarrow{\varphi_0} M \longrightarrow 0$$

con el morfismo φ_2 graduado de grado cero y cumpliendo que $Im(\varphi_2) = Syz(\mathcal{T}_1) = Ker(\varphi_1)$.

Continuando con este proceso obtenemos morfismos de graduados de grado cero

$$\varphi_k : \bigoplus_{k,j=1}^{t_k} R(-d_{k,j}) \longrightarrow \bigoplus_{k-1,j=1}^{t_{k-1}} R(-d_{k-1,j})$$

donde $Im(\varphi_k) = Syz(\mathcal{T}_{k-1}) = Ker(\varphi_{k-1})$, con $\mathcal{T}_{kj}$ base de Gröbner reducida para $Syz(\mathcal{T}_{k-1})$, ordenando en cada paso k a los elementos de $\mathcal{T}_k$ para obtener los vectores T_k como se pide en el lema anterior.

Por el lema anterior, en cada paso decrese el número de variables pertenecientes a los τ_k, donde al tener un número finito de variables (más precisamente r), después de $l \leq r$ pasos tendremos que

$$x_i \notin in_{>_{t_l}}(\mathcal{T}_l), \tag{3.14}$$

esto para toda $i = 1, \ldots, r$. Así, hemos obtenido una sucesión exacta

$$\bigoplus_{l,j=1}^{t_l} R(-d_{l,j}) \xrightarrow{\varphi_l} \cdots \xrightarrow{\varphi_2} \bigoplus_{1,j=1}^{t_1} R(-d_{1,j}) \xrightarrow{\varphi_1} \bigoplus_{i=1}^{t_0} R(-d_i) \xrightarrow{\varphi_0} M \longrightarrow 0 \tag{3.15}$$

Por (3.14), $in_{>_{t_l}}(\mathcal{T}_l)$ esta formado de elementos de la forma $\alpha_u \varepsilon_u$, con $\alpha_u \in K$, ε_u elemento de la base estándar de $\bigoplus_{l,j=1}^{t_l} R(-d_{l,j})$. Sea $G = \{\alpha_1\varepsilon_1, \ldots, \alpha_k\varepsilon_k | k \leq l\}$ el conjunto generador para $in_{>_{t_l}}(\mathcal{T}_l)$. Al ser $\mathcal{T}_l$ base de Grōbner reducida, $\alpha_i\varepsilon_i \neq \alpha_j\varepsilon_j$, para todo $i \neq j$. Por lo tanto, todos los S-vectores de los generadores de $\mathcal{T}_l$ son cero, lo que implica que

$$Syz(\mathcal{T}_l) = \{0\}$$

Así, por el corolario (1.2.10) tenemos que $\mathcal{T}_l$ es base de $Syz(\mathcal{T}_{l-1})$, es decir, $\mathcal{T}_{l-1}$ es libre. Por la proposición (1.4.9), podemos extender la sucesión (3.15) a otra sucesión exacta agregando un cero por la izquierda, obteniendo

$$0 \longrightarrow \bigoplus_{l,j=1}^{t_l} R(-d_{l,j}) \xrightarrow{\varphi_l} \cdots \xrightarrow{\varphi_2} \bigoplus_{1,j=1}^{t_1} R(-d_{1,j}) \xrightarrow{\varphi_1} \bigoplus_{i=1}^{t_0} R(-d_i) \xrightarrow{\varphi_0} M \longrightarrow 0$$

la cual es una resolución graduada finita de longitud $l \leq r$. □

Observación 3.2.3. Notemos que la demostración es constructiva, es decir, nos da explícitamente la forma de obtener la resolución graduada de un R-módulo graduado finitamente generado. Más aún, al ser únicas las base de Grōbner reducidas, mediante este método la resolución obtenida es única.

Capítulo 4

Polinomio de Hilbert

En este capítulo calcularemos las funciones y polinomios de Hilbert de R-módulos graduados finitamente generados, usados en el estudio de variedades proyectivas. En esta ocasión R es de la forma

$$R = k[x_0, \ldots, x_r],$$

es decir, el anillo de polinomios en $r+1$ variables.

4.1 Función de Hilbert

Definición 4.1.1. Sea $M \subset R^m$ un R módulo graduado finitamente generado. La función

$$\begin{aligned} H_M : \mathbb{Z} &\longrightarrow \mathbb{N} \\ i &\longmapsto dim_k(M_i) \end{aligned}$$

es llamada la *función de Hilbert* de M.

Nota 4.1.2. La dimensión que estamos considerando es la dimensión como k-espacio vectorial.

Observación 4.1.3. Por el lema (1.1.19), la función de Hilbert está bien definida.

A contiuación daremos un lema que nos ayudará a encontrar ejemplos de la función de Hilbert, además de ser de gran utilidad para desarrolar un método de obtención del polinomio de Hilbert.

Lema 4.1.4. *El número de monomios de grado d en $r+1$ variables es* $\binom{d+r}{r}$.

Demostración. Recordemos que

$$\binom{d+r}{r} = \frac{(d+1)\cdots(d+r)}{r!}$$

Sea $F(d,r)$ el número de monomios de grado d en $r+1$ variables. Lo haremos por inducción sobre r.

1. $r = 0$ El número de monomios de grado d en una variable son d, que es precesimente $\binom{d}{0}$.

2. $r = k$ Supongamos que es válido para $k-1$. Denotemos por $f^{(d)}$ a los monomios de grado d, donde dichos monomios se pueden ver como

$$f^{(d)} = x_k^d f^{(0)} + x_k^{d-1} f^{(1)} + \cdots + x_k^0 f^{(d)}.$$

Por lo tanto

$$F(d,k) = F(0,k-1) + F(1,k-1) + \cdots F(d,k-1),$$

y de igual manera tenemos que

$$F(d-1,k) = F(0,k-1) + \cdots + F(d-1,k-1).$$

Así

$$F(d,k) - F(d-1,k) = F(d,k-1),$$

y por lo tanto

$$F(d,k) = F(d,k-1) + F(d-1,k).$$

Sea $\Upsilon(d,k) = F(d,k) - \binom{d+k}{k}$, y consideremos

$$\begin{aligned}
\Upsilon(d,k) - \Upsilon(d-1,k) &= F(d,k) - \binom{d+k}{k} - F(d-1,k) + \binom{d-1+k}{k} \\
&= F(d,k-1) - \frac{(d+1)\cdots(d+k)}{k!} + \frac{(d)\cdots(d-1+k)}{k!} \\
&= F(d,k-1) \\
&+ \frac{[(d+1)\cdots(d-1+k)]d - [(d+1)\cdots(d-1+k)](d+k)}{k!} \\
&= F(d,k-1) + \frac{[(d+1)\cdots(d-1+k)](d-d+k)}{k!} \\
&= F(d,k-1) + \frac{[(d+1)\cdots(d-1+k)](-k)}{k!} \\
&= F(d,k-1) - \frac{(d+1)\cdots(d-1+k)}{(k-1)!} \\
&= F(d,k-1) - F(d,k-1) = 0.
\end{aligned}$$

La penúltima igualdad por hipótesis de inducción. Repitiendo el desarrollo anterior tenemos

$$\Upsilon(d,k) = \Upsilon(d-1,k) = \cdots = \Upsilon(1,k)$$

Entonces

$$\Upsilon(d,k) = \Upsilon(1,k) = F(1,k) - \binom{1+k}{k!} = (k+1) - (k+1) = 0$$

y por lo tanto

$$F(d,k) = \binom{d+k}{k}$$

□

El lema a continuación nos ayudará a dar una clase importante de ejemplos de funciones de Hilbert.

Lema 4.1.5. *Considerando a R como un R-módulo graduado finitamente generado, tenemos que*

$$H_R(i) = dim_k(R_i) = \binom{i+r}{r},$$

para toda $i \in \mathbb{N}$.

Demostración. La base de R_i como k-espacio vectorial son los monomios de grado i. Pero el lema (4.1.4) nos dice que el número de monomios de grado i en $r+1$ variables es precisamente $\binom{i+r}{r}$. □

Observación 4.1.6. Aplicando la convención de $\binom{a}{b} = 0$ si $a < b$, el lema anterior es cierto para toda $i \in \mathbb{Z}$.

Lema 4.1.7. *Sea $M \subset R^m$ un R-módulo graduado finitamente generado y $M(d)$ el módulo deslizado. Entonces*

$$H_{M(d)}(i) = H_M(i+d),$$

para toda $i \in \mathbb{Z}$.

Demostración. Es claro, ya que

$$\begin{aligned} H_{M(d)}(i) &= dim_k(M(d)_i) = dim_k(M_{d+i}) \\ &= H_M(d+i). \end{aligned}$$

□

Corolario 4.1.8. *Considerando a R como un R-módulo graduado finitamente generado, tenemos que*

$$H_{R(d)}(i) = \binom{i+d+r}{r}$$

para toda $i \in \mathbb{Z}$.

Lema 4.1.9. *Sean $M, N \subset R^m$ R-módulos graduados finitamente generados. Si la sucesión*

$$0 \longrightarrow M \xrightarrow{\varphi} P \xrightarrow{\psi} N \longrightarrow 0$$

es exacta con φ, ψ morfismos graduados de grado cero, entonces

$$H_P = H_M + H_N.$$

Demostración. Al ser φ y ψ morfismos de grado cero, la sucesión

$$M_i \xrightarrow{\varphi_i} P_i \xrightarrow{\psi_i} N_i.$$

con $\varphi_i = \varphi|_{M_i}$ y $\psi_i = \psi|_{P_i}$, es exacta, es decir, tenemos que

$$0 \longrightarrow M_i \xrightarrow{\varphi_i} P_i \xrightarrow{\psi_i} N_i \longrightarrow 0 \tag{4.1}$$

para cada i.

Pero M_i, P_i y N_i son k-espacios vectoriales, así, la sucesión (4.1) es una sucesión exacta de k-espacios vectoriales. Entonces

$$dim_k(M_i) = dim_k(Ker(\varphi_i)) + dim_k(Im(\varphi_i))$$
$$dim_k(P_i) = dim_k(Ker(\psi_i)) + dim_k(Im(\psi_i))$$

Como (4.1) es exacta, tenemos que

$$\begin{aligned} dim_k(M_i) &= 0 + dim_k(Im(\varphi_i)) \\ &= dim_k(Ker(\psi_i)). \end{aligned}$$

Así,

$$\begin{aligned} dim_k(P_i) &= dim_k(M_i) + dim_k(Im(\psi_i)) \\ &= dim_k(M_i) + dim_k(N_i) \end{aligned}$$

debiéndose la última igualdad a que ψ_i es sobreyectivo. □

Corolario 4.1.10. *Sean $M, N \subset R^m$ R-módulos graduados finitamente generados. Entonces*

$$H_{M \oplus N} = H_M + H_N.$$

Teorema 4.1.11. Sea M un R-módulo graduado finitamente generado. Entonces para cualquier resolución graduada finita $M^\bullet$ de M

$$0 \longrightarrow F_k \xrightarrow{\varphi_k} F_{k-1} \xrightarrow{\varphi_{k-1}} \cdots F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

tenemos que

$$H_M(i) = dim_k(M_i) = \sum_{j=0}^{k} (-1)^j dim_k(F_j)_i = \sum_{j=0}^{k} (-1)^j H_{F_j}(i).$$

Demostración. La resolución graduada $M^\bullet$ es de la forma

$$0 \longrightarrow \bigoplus_{i=1}^{m_k} (F_k)_i \xrightarrow{\varphi_k} \bigoplus_{i=1}^{m_{k-1}} (F_{k-1})_i \xrightarrow{\varphi_{k-1}} \cdots \xrightarrow{\varphi_1} \bigoplus_{i=1}^{m_0} (F_0)_i \xrightarrow{\varphi_0} \bigoplus_{i=1}^{m} M_i \longrightarrow 0$$

con φ_j morfismo graduado de grado cero. Así, si $\varphi_{j,i} = \varphi_j|_{(F_j)_i}$ obtenemos una sucesión exacta de k-espacios vectoriales de dimensión finita

$$0 \longrightarrow (F_k)_i \xrightarrow{\varphi_{k,i}} (F_{k-1})_i \xrightarrow{\varphi_{k-1,i}} \cdots \xrightarrow{\varphi_{1,i}} (F_0)_i \xrightarrow{\varphi_{0,i}} M_i \longrightarrow 0$$

Por el lema (1.4.11) tenemos que

$$dim_k(M_i) - \sum_{j=0}^{k}(-1)^j dim_k(F_j)_i = 0$$

Por lo tanto,

$$dim_k(M_i) = \sum_{j=0}^{k}(-1)^j dim_k(F_j)_i = 0$$

□

Haremos uso de este teorema para cálcular las funciones de Hilbert.

4.2 Polinomio de Hilbert

Supongamos por el momento que el R-módulo a considerar es $R = k[x_0, \ldots, x_r]$.

Observación 4.2.1. Para cada r fijo, con $i, r \in \mathbb{N}$, el coeficiente binomial $\binom{i+r}{r}$ es un polinomio de grado r en i. En efecto,

$$\begin{aligned}\binom{i+r}{r} &= \frac{(i+r)!}{i!\,r!} = \frac{(i+r)(i+r-1)\cdots(i+1)}{r!} \\ &= (i+r)\cdots(i+1)\cdot\frac{1}{r!} \\ &= \frac{i^r + i^{r-1}a_{r-1} + \cdots + ia_1 + r!}{r!}\end{aligned}$$

con $a_i \in k$.

Observación 4.2.2. Del corolario (4.1.8) tenemos que la función de Hilbert para R coincide con un polinomio, para todo $i \in \mathbb{N}$.

Observación 4.2.3. El corolario (4.1.10) nos dice que para un R-módulo libre deslizado

$$F = \bigoplus_{i=1}^{m} R(-d_i)$$

su función de Hilbert es de la forma

$$H_F(i) = H_{\oplus R(-d_i)}(i) = \sum_{i=1}^{m} H_{R(-d_i)} = \sum_{i=1}^{m} \binom{i - d_i + r}{r},$$

y por lo tanto coindide con un polinomio en i, con $i \geq max(d_1, \ldots, d_m)$

La última observación es solo un caso particular del siguiente teorema de Hilbert.

Teorema 4.2.4 (De Hilbert). Sea $M \subset R^m$ un R-módulo graduado finitamente generado. Entonces existe un único polinomio HP_M tal que

$$H_M(i) = HP_M(i),$$

para i suficientemente grande.

Definición 4.2.5. El polinomio HP_M del teorema anterior es llamado el *polinomio de Hilbert* de M.

Demostración del Teorema (4.2.4). Sea M un R-módulo graduado finitamente generado. Por el teorema de Sicigias de Hilbert podemos considerar una resolución graduada finita $M^\bullet$ de M

$$0 \longrightarrow F_k \longrightarrow F_{k-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

Por el teotema (4.1.11) tenemos que

$$H_M(i) = \sum_{j=0}^{k} (-1)^j H_{F_j}(i).$$

La observación anterior nos dice que cada $H_{F_j}(i)$ del sumando coincide con un polinomio para i suficientemente grande. Por lo tanto, al ser $H_M(i)$ suma finita de polinomios, $H_M(i)$ es un polinomio para i suficientemente grande. □

Para facilitarnos el proceso de cálcular el polinomio de Hilbert de algún cociente de módulos graduados, tenemos el siguiente teorema.

Teorema 4.2.6. Sea M un R-módulo graduado finitamente generado, teniendo una presentación de la forma $M = F/N$, donde F es un R-módulo libre con base homogénea y N un submódulo generado por elementos homogéneos. Entonces

$$H_M = H_{F/N} = H_{F/in_>(N)}$$

para cualquier orden monomial $>$ sobre F.

Demostración. Sea B el conjunto de monomios que no están en $in_>(N)$. Sean

$$F_d = \{f \in F | \, deg(f) = d\}$$
$$N_d = \{f \in N | \, deg(f) = d\}$$
$$M_d = \{f \in M \, deg(f) = d\}$$
$$B_d = \{m \in B | \, deg(m) = d\}$$

Al ser graduado $M = \bigoplus_{-\infty}^{\infty} M_d$, y por el lema (1.1.18), $M_d = F_d/N_d$.

Por el teorema de Macaulay, la imagen de B en el cociente F/N da una base de k-espacio vectorial para M, implicando que la imagen de B_d es una base para M_d. Por lo tanto, $dim_k(M_d)$ es igual al número de elementos de B_d, que son los elementos de F_d que no están en $in_>(N_d)$, es decir,

$$dim_k(M_d) = dim_k(F_d/in_>(N_d)).$$

□

Apéndice A

A.1 Algoritmo de la División

Algoritmo de la División A.1.1. *Dados dos polinomios* $p(x)$ *y* $q(x) \in k[x]$, *con* $q(x) \neq 0$, *entonces existen dos polinomios* $t(x)$ *y* $r(x) \in k[x]$ *tales que*

$$p(x) = t(x)q(x) + r(x),$$

con $r(x) = 0$ *ó* $deg(r(x)) < deg(q(x))$, $deg(t(x)q(x)) = deg(p(x))$.

Demostración. Véase Hungerford ([Hun74], pag. 158). □

De este algoritmo se sigue la siguiente proposición.

Proposición A.1.2. *El anillo de polinomios* $k[x]$ *es un Dominio Entero, Dominio Euclideano y Dominio de Ideales Principales.*

Observación A.1.3. Por la proposición (A.1.2), todo ideal $I \subset k[x]$ es de la forma $I = \langle p(x) \rangle$, con $p(x)$ polinomio de grado mínimo entre todos los polinomios pertenecientes a I

A.2 Teorema de la Base de Hilbert

Teorema A.2.1 (De la Base de Hilbert). Si S es un anillo noetheriano, entonces $S[x]$ es noetheriano.

Demostración. Sea $I \subset S[x]$ un ideal. Probaremos que I es finitamente generado. Definimos para cada $n \in \mathbb{N}$ al conjunto $I_n = \{r \in S | \, lc(h) = r$ para algún $h \in S$; con $deg(h) = n\} \cup \{0\}$, el cual claramente, para cada $n \in \mathbb{N}$, es un ideal de S. Notando que $I_n \subseteq I_{n+1}$ y que S es noetheriano, tenemos que existe $N \in \mathbb{N}$ tal que

$$I_n = I_N \tag{A.1}$$

para todo $n \geq N$, y que además los ideales I_n son de la forma

$$I_n = \langle r_{n1}, \ldots, r_{nt_n} \rangle \tag{A.2}$$

es decir, son finitamente generados.

Para $i = 1, \ldots, N$ y $j = 1, \ldots, t_n$, sea $f_{ij} \in I$ un polinomio tal que $lc(f_{ij}) = r_{ij}$ y $deg(f_{ij}) = i$. Renumeremos a los índices ij para obtener al conjunto

$$\{f_1, \ldots, l_m\} = \{f_{ij} | \, i = 1, \ldots, N; \; j = 1, \ldots, t_i\}$$

y considerar al ideal $\langle f_1, \ldots, f_m \rangle$.

Podemos suponer que todo polinomio de I de grado menor a N pertenece a $\langle f_1, \ldots, f_m \rangle$. Afirmamos que

$$I = \langle f_1, \ldots, f_m \rangle$$

Supongamos lo contrario, que existe $f \in I$ tal que $f \notin \langle f_1, \ldots, f_m \rangle$. Por (A.1) y (A.2) tenemos que $lc(f) = \sum_{k=1}^{m} s_k r_k$, donde $s_k \in S$. Como $deg(f) > deg(f_k)$, para todo k, podemos considerar al elemento

$$g = \sum_{k=1}^{m} s_k \, f_k \, x^{deg(f) - deg(f_k)} \quad \in \langle f_1, \ldots, f_m \rangle$$

Así el elemento $f - g$ que pertenece a I, no pertenece al ideal $\langle f_1, \ldots, f_m \rangle$ y es tal que $deg(f - g) \leq N$, lo cual no puede ser cierto. Por lo tanto

$$I = \langle f_1, \ldots, f_m \rangle$$

□

Corolario A.2.2. *El anillo $k[x_1, \ldots, x_r]$ es noetheriano.*

Bibliografía

[Buc70] B. Buchberger. An algorithmic criterion for the solvability of algebraic systems of equations. *Aequationes Math.*, 4:374–383, 1970.

[Buc76] B. Buchberger. A theorical basis for the reduction of polynomials to canonical forms *ACM SIGSAM Bull.*, 39:19–29, 1976.

[CLO98] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Text in Mathematics* Springer-Verlag, 1998

[Eis95] David Eisenbud. *Commutative Algebra· with a view toward algebraic geometry*, volume 150 of *Graduate Text in Mathematics.* Springer-Verlag, New York, First Edition 1995. Corrected Second Printing, 1996

[Gor00] P Gordan. Les invariants des formes binaires. *Journal de Mathématiques Pures et Appliqués*, 6:141–156, 1900

[Hil90] David Hilbert. Über die theorie von algebraischen formen. *Math. Ann.*, 36:473–534, 1890.

[Hil93] David Hilbert. Über die vollen invariantensysteme. *Math. Ann.*, 42·313–373, 1893.

[Hun74] T. Hungerford. *Algebra*, volume 73 of *Graduate Text in Mathematics.* Springer-Verlag, 1974.

[Mac27] F S Macaulay. Some properties of enumeration in the theory of modular systems. *Proc. London Math. Soc.*, 26:531–555, 1927.

[Sch80] F.-O. Schreyer. *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionssatz.* PhD thesis, Universidad de Hamburgo, Alemania, 1980.

[Wis91] R. Wisbauer. *Foundations of Module and Ring Theory.* Gordon and Breach Science Publishers, 1991.