UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

POSGRADO EN CIENCIAS MATEMATICAS

FACULTAD DE CIENCIAS

OPTIMIZACION DEL ALGORITMO DE BUCHBERGER POR MEDIO DE RESOLICIONES PLANAS

TESIS

QUE PARA OBTENER EL GRADO ACADEMICO DE
MAESTRO ENCIENCIAS

PRESENTA
ABRAHAM MARTIN DEL CAMPO SANCHEZ

DIRECTOR DE TESIS: **DR. ENRIQUE JAVIER ELIZONDO HUERTA**

Índice general

Introducción

En geometría algebraica computacional, y en álgebra conmutativa computacional el algoritmo de Buchberger constituye una pieza fundamental puesto que dicho algoritmo ha revolucionado los métodos algorítmicos así como las aplicaciones de la geometría algebraica, y es un área de investigación actual. Este algoritmo fue creado por el matemático austriaco Bruno Buchberger y presentado en su tesis doctoral [4].

El algoritmo de Buchberger nos permite hacer cálculos sobre el anillo de polinomios. Para poder trabajar con polinomios necesitamos poder saber cuándo un polinomio dado pertenece o no a un ideal fijo. En el caso de $[x]$ el problema es resuelto fácilmente por el algoritmo de la división que se tiene gracias a que $[x]$ es un anillo Euclidiano. Lo que hace que en el caso de una variable las cosas funcionen, es que tenemos un invariante (el grado) y un proceso que reduce el invariante. En este algoritmo de la división para una variable, lo que hacemos es dividir el polinomio entre el término inicial, por lo que para el caso de varias variables, lo que necesitamos es una noción de término inicial, por ejemplo, ¿cuál es el término inicial de $x^2y + y^2x$?. Resulta que esto significa que debemos ordenar los monomios de $[x_1, \ldots, x_n]$, esto es casi inmediato. Desafortunadamente nos encontraremos que aunque hayamos encontrado un algoritmo de la división aún no podremos resolver el problema de pertenencia planteado previamente. La pieza faltante es un análogo al algoritmo Euclidiano para el caso de varias variables que nos produzca un buen conjunto de generadores (uno en el caso de una variable). Pero hay una simple y bella solución para nuestro obstáculo; el algoritmo de Buchberger es una manera sistemática de producir un conjunto de generadores (una base de Gröbner) para un ideal de tal manera que el algoritmo de la división funcione.

El algoritmo dado originalmente por el matemático austriaco resulta muchas veces ser ineficiente y, para implementarlo en un sistema computacional resulta vital tener procesos lo más eficientes posibles. El mismo B. Buchberger dio un criterio para eliminar términos redundantes dentro del algoritmo y así obtener un proceso mejorado. La base de esta optimización es saber qué se debe agregar al conjunto de generadores del ideal en cuestión para obtener de ahí una base de Gröbner. Estos elementos que se deben agregar son un subconjunto de sizigias particulares, así es que, estudiando dichas sizigias se puede dar una optimización del algoritmo.

El objetivo de este trabajo de tesis es presentar una optimización de dicho algoritmo

restringido sólo para el caso en que se considere el anillo de polinomios en 3 variables $[x, y, z]$. Nuestro proceso consistirá en asociar una gráfica plana a un ideal monomial dado, la cual nos permitirá leer toda la información contenida en el ideal, y necesaria para dicha optimización.

El material principal en que se basa esta tesis esta contenido en el libro *Combinatorial Commutative Algebra, E. Miller, B. Sturmfels* [14] el cual presenta una compilación de los resultados mas importantes del tema en la época.

Durante el primer capítulo de esta tesis se presenta el problema de pertenencia y se provee una introducción a todo lo necesario para hablar de bases de Gröbner, además de presentar a detalle el algoritmo de Buchberger. El segundo capítulo está dedicado al estudio del módulo de sizigias, la relación que tienen con las bases de Gröbner y con la optimización dada por Bruno Buchberger. Por último, en el tercer capítulo damos la definición de la gráfica de Buchberger asociada a cualquier ideal monomial y estudiamos un algoritmo que nos permite encontrar, a partir de dicha gráfica, los generadores de los módulos de sizigias y esto se puede implementar en el algoritmo de Buchberger para encontrar, de manera eficiente, una base de Gröbner.

Esta tesis presenta una relación (la gráfica de Buchberger) entre la geometría algebraica computacional y la teoría de gráficas, esta relación resulta tan natural que pareciera como si estas dos áreas no fueran tan distantes como se podría creer. Dicha relación esta basada en presentar con ideas sencillas y claras, provistas por la combinatoria, resultados que suelen ser mas complejos sin esta herramienta. Parece lamentable que dicha relación solo se encuentre en el anillo de polinomios en no mas de tres variables por lo que en este trabajo se proveen las herramientas necesarias para atacar el problema para el caso de cuatro o mas variables.

Capítulo 1

Bases de Gröbner

1.1. Ideales monomiales

Sea un campo, y $S =$ $[x_1, \ldots, x_r]$ el anillo de polinomios en r indeterminadas, con coeficientes en .

Definición 1.1.1. Un *monomio* en S es un producto $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}$ para un vector $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{N}^r$ de enteros no negativos. Un ideal $I \subset S$ es llamado *ideal monomial* si es generado por monomios.

Observación 1.1.1. *Como espacio vectorial sobre , el anillo de polinomios S es una suma directa*

$$S = \bigoplus_{\mathbf{a} \in \mathbb{N}^r} S_{\mathbf{a}}$$

donde $S_{\mathbf{a}} =$ $\{\mathbf{x}^{\mathbf{a}}\}$ es el subespacio de S generado por el monomio $\mathbf{x}^{\mathbf{a}}$. Como el producto de componentes graduadas $S_{\mathbf{a}} \cdot S_{\mathbf{b}}$ es igual a la componente $S_{\mathbf{a}+\mathbf{b}}$ de grado $\mathbf{a} + \mathbf{b}$, decimos entonces que S es una $-$álgebra $\mathbb{N}^r-$graduada.

Los ideales monomiales son los ideales $\mathbb{N}^r-$graduados de S, lo que por la definición significa que I puede ser expresado como una suma directa

$$I = \bigoplus_{\mathbf{x}^{\mathbf{a}} \in I} \{\mathbf{x}^{\mathbf{a}}\}$$

Lema 1.1.1. *Todo ideal monomial tiene un único conjunto mínimo de monomios generadores, y este conjunto es finito.*

Demostración. El Teorema de la Base de Hilbert nos dice que cada ideal en S es finitamente generado. Esto implica que si I es un ideal monomial, entonces $I = \langle \mathbf{x}_1^{\mathbf{a}}, \ldots, \mathbf{x}_n^{\mathbf{a}} \rangle$. La condición de la suma directa nos dice que un polinomio f está en I si y sólo si cada término de f es divisible por uno de los generadores dados $\mathbf{x}^{\mathbf{a}_i}$. ■

Ahora haremos una definición más general.

Definición 1.1.2. Si F es un $S-$módulo libre finitamente generado, con base $\{\mathbf{e}_i\}$, entonces un *monomio en* F, o un *elemento monomial de* F, es un elemento de la forma $m = \mathbf{x}^{\mathbf{a}}\mathbf{e}_i$ para alguna i. Decimos que un *submódulo monomial de* F es un submódulo generado por elementos monomiales.

De esta definición podemos observar que cualquier submódulo monomial M de F puede ser escrito como

$$M = \bigoplus I_j\mathbf{e}_j \subset \bigoplus S\mathbf{e}_j = F$$

con I_j el ideal monomial generado por aquellos elementos monomiales m de F, tales que $m\mathbf{e}_j \in M$.

Definición 1.1.3. Un *término* en F es un elemento monomial multiplicado por un escalar.

Todas estas definiciones dependen de la elección de la base $\{\mathbf{e}_i\}$ de F. Cuando sea posible y claro, suprimiremos la notación de la base $\{\mathbf{e}_i\}$ y nos referiremos a F simplemente como un *módulo libre con base*.

Definición 1.1.4. Si $m, n \in S$ son monomios, y $u, v \in$ con $v \neq 0$, entonces decimos el término $um\mathbf{e}_i$ es *divisible* por el término $vn\mathbf{e}_j$, si $i = j$ y si m es divisible por n en S; denotamos a esto por $vn\mathbf{e}_j \mid um\mathbf{e}_i$. El *cociente* es entonces $um/vn \in S$.

Es claro que podemos realizar algunas operaciones más fácilmente para monomios que para polinomios en general, por ejemplo, el máximo común divisor y el mínimo común múltiplo de dos monomios de S es obtenido componente a componente, es decir, si $\mathbf{x}^{\mathbf{a}}$, $\mathbf{x}^{\mathbf{b}} \in S$ dos monomios, entonces

$$\text{MCD}(\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}}) = x_1^{\text{mín}(a_1,b_1)} x_2^{\text{mín}(a_2,b2)} \cdots x_r^{\text{mín}(a_r,b_r)},$$

$$\text{MCM}(\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}}) = x_1^{\text{máx}(a_1,b_1)} x_2^{\text{máx}(a_2,b_2)} \cdots x_r^{\text{máx}(a_r,b_r)}.$$

Extendemos estas operaciones a términos de cualquier módulo libre con base F: Si $m, n \in F$ son términos que involucran al mismo elemento de la base $\mathbf{e}_i$ de F, entonces el MCD de m y n es el más grande elemento monomial de F que puede dividir tanto a m como a n, y de manera análoga definimos el mcm.

Lema 1.1.2. *Sea* $I = \langle \mathbf{x}^{\mathbf{a}} \rangle_{\mathbf{a} \in A \subset \mathbb{N}^n}$ *un ideal monomial. Entonces un monomio* $\mathbf{x}^{\mathbf{b}} \in I$ *si y sólo si* $\mathbf{x}^{\mathbf{b}}$ *es divisible por* $\mathbf{x}^{\mathbf{a}}$ *para alguna* $\mathbf{a} \in A$*, i. e., Existe* $\mathbf{a} \in A$ *tal que* $\mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{b}}$.

Demostración. Si $\mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{b}}$ entonces $\mathbf{x}^{\mathbf{a}} \cdot \mathbf{x}^{\mathbf{c}} = \mathbf{x}^{\mathbf{b}}$, con $\mathbf{x}^{\mathbf{c}} \in [x_1, \ldots, x_n]$ un monomio, por lo que $\mathbf{x}^{\mathbf{b}} \in I$ de la definición de ideal.

Supongamos pues que $\mathbf{x}^{\mathbf{b}} \in I$, entonces $\mathbf{x}^{\mathbf{b}} = \sum_{i=1}^{s} h_i \, \mathbf{x}^{\mathbf{a}_i}$, donde $h_i \in [x_1, \ldots, x_n]$, y $\mathbf{a}_i \in A$. Si expandimos cada h_i como combinación lineal de monomios, entonces es claro que cada término de la suma es divisible por algún $\mathbf{x}^{\mathbf{a}_i}$, entonces también pasa que $\mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{b}}$. ■

Observemos que $\mathbf{x^a} \mid \mathbf{x^b}$ significa que $\mathbf{x^b} = \mathbf{x^a} \cdot \mathbf{x^c}$ para alguna $\mathbf{c} \in \mathbb{N}^n$. Esto es equivalente a decir que $\mathbf{b} = \mathbf{a} + \mathbf{c}$. Con esto, el conjunto

$$\mathbf{a} + \mathbb{N}^n = \{\mathbf{a} + \mathbf{c} \mid \mathbf{c} \in \mathbb{N}^n\}$$

consiste de los exponentes de todos los monomios divisibles por $\mathbf{x^a}$. Esta observación, junto con el lema anterior nos permite obtener una imagen de los monomios contenidos en un ideal monomial dado.

Abundaremos más en esta idea más adelante.

Definición 1.1.5. Decimos que un ideal I de un anillo R es *artiniano* si y sólo si R/I es un anillo artiniano.

El siguiente resultado nos da caracterización de los ideales artinianos en para el caso de ideales monomiales.

Proposición 1.1.1. *Sea $I = \langle m_1, \ldots, m_r \rangle$ un ideal monomial del anillo de polinomios $S = [x_1, \ldots, x_n]$. Entonces I es artiniano si y sólo si $\{x_1^{a_1}, \ldots, x_n^{a_n}\} \subseteq \{m_1, \ldots, m_r\}$, con $a_i \in \mathbb{N} - \{0\}$.*

Demostración. $\Leftarrow$: Si $\{x_1^{a_1}, \ldots, x_n^{a_n}\} \subseteq \{m_1, \ldots, m_r\}$, entonces S/I es un anillo finito y por tanto artiniano.

$\Rightarrow$: Supongamos que $\{x_1^{a_1}, \ldots, x_n^{a_n}\} \nsubseteq \{m_1, \ldots, m_r\}$, entonces hay una potencia pura de una de las variables que no está en I, digamos $x_1^n \notin I$ para ninguna $n \in \mathbb{N}^*$. La cadena de ideales

$$\langle x_1 \rangle \supset \langle x_1^2 \rangle \supset \langle x_1^3 \rangle \supset \cdots$$

que nunca se estaciona en S/I, por lo tanto, I no es artiniano.

■

Lema 1.1.3. *Sea I un ideal monomial, y sea $f \in [x_1, \ldots, x_n]$. Entonces las siguientes son equivalentes:*

(i) $f \in I$.

(ii) *Cada término de f está en I.*

(iii) *f es una combinación $-$lineal de monomios en I.*

Demostración. Las implicaciones $(iii) \Rightarrow (ii) \Rightarrow (i)$ son obvias. La prueba de que $(i) \Rightarrow (iii)$ es muy similar a lo que se hizo para probar el Lema 1.1.2. Supongamos que $I = \langle m_1, \ldots, m_s \rangle$ con m_i monomios. Entonces, si $f \in I$, se tiene que $f = \sum_{i=1}^{s} h_i m_i$. Si expandimos cada h_i como combinación lineal de monomios, entonces es claro que cada término de la suma $\sum_{i=1}^{s} h_i m_i$ es un monomio en I, multiplicado por un escalar, puesto que cada término es un monomio multiplicado por algún m_i. Esto demuestra $(i) \Rightarrow (iii)$. ■

Una consecuencia inmediata de la parte (*iii*) del lema, es que un ideal monomial queda únicamente determinado por sus monomios. Por lo que tenemos el siguiente corolario.

Corolario 1.1.1. *Dos ideales monomiales son iguales si y sólo si ambos contienen los mismos monomios.*

1.2. Orden de monomios en $[x_1, \ldots, x_n]$.

Para esta sección vamos a dar un orden a los términos de un polinomio. El caso para una variable es sencillo, pues tenemos el siguiente:

$$1 < x < x^2 < \ldots < x^m < x^{m+1} < \ldots$$

Si asumimos que hay un orden entre las variables, digamos que para n variables se tiene $x_1 > x_2 > \ldots > x_n$, entonces nos reducimos a dar un orden total a $\mathbb{N}^n$ que cumpla:

Si $\mathbf{x^a} \in [x_1, \ldots, x_n]$, entonces $1 < \mathbf{x^a}$ para todo monomio no constante, y que $\mathbf{x^b} > \mathbf{x^c}$ si y sólo si $\mathbf{x^{b+a}} > \mathbf{x^{c+a}}$ para toda $\mathbf{a} \in \mathbb{N}^n$.

Definición 1.2.1. Un *orden monomial* en $[x_1, \ldots, x_n]$ es una relación $>$ sobre $\mathbb{N}^n$, o equivalentemente una relación sobre el conjunto de monomios $\mathbf{x^a}$, con $\mathbf{a} \in \mathbb{N}^n$, que satisface:

(i) $>$ es un orden total sobre $\mathbb{N}^n$.

(ii) Si $\mathbf{a} > \mathbf{b}$ y $\mathbf{c} \in \mathbb{N}^n$, entonces $\mathbf{a} + \mathbf{c} > \mathbf{b} + \mathbf{c}$.

(iii) $>$ es un buen orden sobre $\mathbb{N}^n$. Esto es, cada subconjunto no vacío de $\mathbb{N}^n$ tiene un elemento mínimo bajo la relación de orden $>$.

El siguiente lema nos va ser de ayuda para entender el verdadero significado de la condición (iii) del buen orden.

Lema 1.2.1. *Una relación de orden $>$ sobre $\mathbb{N}^n$ es un buen orden si y sólo si cada sucesión estrictamente decreciente en $\mathbb{N}^n$*

$$\mathbf{a}_1 > \mathbf{a}_2 > \mathbf{a}_3 > \cdots$$

eventualmente termina.

Demostración. La prueba será por contrapositiva: $>$ no es un buen orden si y sólo si existe una sucesión infinita estrictamente decreciente en $\mathbb{N}^n$.

Si $>$ no es un buen orden, entonces algún subconjunto no vacío $N \subset \mathbb{N}^n$ no tiene elemento mínimo. Escójase $\mathbf{a}_1 \in N$, como $\mathbf{a}_1$ no es el elemento mínimo, podemos encontrar $\mathbf{a}_1 > \mathbf{a}_2$ en N. Ahora, como $\mathbf{a}_2$ tampoco es el elemento mínimo de N, entonces hay un $\mathbf{a}_2 > \mathbf{a}_3$ en N. Continuando de esta manera obtenemos una sucesión infinita estrictamente decreciente

$$\mathbf{a}_1 > \mathbf{a}_2 > \mathbf{a}_3 > \cdots .$$

Análogamente, dada una sucesión infinita como esta última, el conjunto formado por los elementos de la sucesión $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \ldots\}$ es un subconjunto no vacío de $\mathbb{N}^n$ sin elemento mínimo, y con esto $>$ no es un buen orden. ■

Observemos que el orden numérico usual

$$\cdots > m+1 > m > \cdots > 3 > 2 > 1 > 0$$

sobre elementos de $\mathbb{N}$, satisface las tres condiciones de la Definición 1.2.1; por lo que ordenar un polinomio en el anillo de polinomios $[x]$ por el grado, el cual mencionamos como ejemplo al principio de esta sección, constituye un orden monomial como era de esperarse.

Nuestro primer ejemplo de un orden para $n-$adas será el orden lexicográfico.

Definición 1.2.2 (Orden Lexicográfico). Sean $\mathbf{a} = (a_1, \ldots, a_n)$ y $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$. Decimos que $\mathbf{a} >_{lex} \mathbf{b}$ si, en la diferencia vectorial $\mathbf{a} - \mathbf{b} \in \mathbb{Z}^n$, la primer entrada no cero de la izquierda, es positiva. Escribiremos $\mathbf{x^a} >_{lex} \mathbf{x^b}$ si $\mathbf{a} >_{lex} \mathbf{b}$.

Ejemplo 1.2.1. Algunos ejemplos del orden lexicográfico recién definido son:

a. $(1,2,0) >_{lex} (0,3,4)$ puesto que $\mathbf{a} - \mathbf{b} = (1,-1,-4)$.

b. $(3,2,4) >_{lex} (3,2,1)$ dado que $\mathbf{a} - \mathbf{b} = (0,0,3)$.

c. Las variables $x_1, \ldots, x_n$ están ordenadas de la forma usual por el orden lexicográfico, puesto que:

$$(1,0,\ldots,0) >_{lex} (0,1,0,\ldots,0) >_{lex} \cdots >_{lex} (0,\ldots,0,1),$$

por lo que $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$.

♢

El nombre y la idea del orden lexicográfico proviene justamente de el orden análogo para las palabras usado por los diccionarios.

Falta aún verificar que el orden lexicográfico satisface las tres condiciones de la Definición 1.2.1.

Proposición 1.2.1. *El orden lexicográfico sobre $\mathbb{N}^n$ es un orden monomial.*

Demostración.

(i) Que $>_{lex}$ es un orden total se sigue directamente de la definición, y del hecho de que el orden numérico usual sobre $\mathbb{N}$ es un orden total.

(ii) Si $\mathbf{a} >_{lex} \mathbf{b}$, entonces tenemos que la entrada no cero más a la izquierda en $\mathbf{a} - \mathbf{b}$, digamos $a_k - b_k$, es positiva. Pero $\mathbf{x^a} \cdot \mathbf{x^c} = \mathbf{x^{a+c}}$, y también $\mathbf{x^b} \cdot \mathbf{x^c} = \mathbf{x^{b+c}}$ para toda $\mathbf{c} \in \mathbb{N}^n$. Entonces en $(\mathbf{a}+\mathbf{c}) - (\mathbf{b}+\mathbf{c}) = \mathbf{a} - \mathbf{b}$, la entrada más a la izquierda distinta de cero es de nuevo $a_k - b_k > 0$.

(iii) Supóngase que $>_{lex}$ no es un buen orden. Entonces según el Lema 1.2.1 debe haber una sucesión infinita estrictamente decreciente

$$\mathbf{a}_1 >_{lex} \mathbf{a}_2 >_{lex} \mathbf{a}_3 >_{lex} \cdots$$

de elementos de $\mathbb{N}^n$.

Consideremos la primer entrada de los vectores $\mathbf{a}_i \in \mathbb{N}^n$. Por definición del orden lexicográfico, estas primeras entradas forman una sucesión no creciente de números naturales no nulos. Dado que $\mathbb{N}$ está bien ordenado, las primeras entradas de las $\mathbf{a}_i$ se deben estacionar eventualmente. Esto es, que existe un k tal que todas las primeras entradas de los $\mathbf{a}_i$ con $i \geq k$ son iguales.

Las segundas entradas de $\mathbf{a}_k$, $\mathbf{a}_{k+1}$, ... forman una sucesión no creciente. Por el argumento anterior, las segundas entradas se estacionan también eventualmente. Continuando de esta manera, vemos que para alguna ℓ, los $\mathbf{a}_\ell$, $\mathbf{a}_{\ell+1}, \ldots$ son iguales, lo que contradice el hecho de que $\mathbf{a}_\ell > \mathbf{a}_{\ell+1}$.

■

Es importante recalcar que hay varios órdenes lexicográficos, dependiendo de cómo estén ordenadas las variables, por ejemplo, nosotros hemos usado el orden lexicográfico con el orden de las variables $x_1 > x_2 > \cdots > x_n$. Pero dado cualquier otro orden en las variables $x_1, \ldots, x_n$, le correspondería un orden lexicográfico. En general, para n variables existen $n!$ órdenes lexicográficos, uno para cada orden posible de las variables.

Observemos que de acuerdo con el orden lexicográfico con $x > y > z$, tenemos que $x >_{lex} y^5 z^3$. Pero en algunas ocasiones nos es importante considerar también el grado total de un monomio al considerar el orden lexicográfico.

Definición 1.2.3 (**Orden Lexicográfico Graduado**). Sean $\mathbf{a} = (a_1, \ldots, a_n)$ y $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$, decimos que $\mathbf{a} >_{grlex} \mathbf{b}$ si

$$|\mathbf{a}| = \sum_{i=1}^{n} a_i \ > \ |\mathbf{b}| = \sum_{i=1}^{n} b_i, \quad \text{o si} \quad |\mathbf{a}| = |\mathbf{b}| \ \text{ y } \ \mathbf{a} >_{lex} \mathbf{b}.$$

De manera análoga escribiremos $\mathbf{x}^{\mathbf{a}} >_{grlex} \mathbf{x}^{\mathbf{b}}$ cuando $\mathbf{a} >_{grlex} \mathbf{b}$.

Ejemplo 1.2.2. Algunos ejemplos del orden lexicográfico graduado recién definido son:

a. $(1,2,3) >_{grlex} (3,2,0)$ puesto que $|(1,2,3)| = 6 > |(3,2,0)| = 5$.

b. $(1,2,4) >_{grlex} (1,1,5)$ dado que $|(1,2,4)| = 7 = |(1,1,5)|$, y $(1,2,4) >_{lex} (1,1,5)$.

c. Las variables $x_1, \ldots, x_n$ están ordenadas de la forma usual por el orden lexicográfico graduado, es decir, $x_1 >_{grlex} x_2 >_{grlex} \cdots >_{grlex} x_n$; puesto que $|x_i| = 1 = |x_j|$ para cualesquiera $i, j \in \{1, \ldots, n\}$, y se tiene que $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$.

♢

Proposición 1.2.2. *El orden lexicográfico graduado sobre $\mathbb{N}^n$ es un orden monomial.*

Otro orden menos intuitivo, pero que se ha mostrado recientemente que es más eficiente para algunos cálculos es el orden lexicográfico graduado inverso.

Definición 1.2.4 (Orden Lexicográfico Graduado Inverso). Sean $\mathbf{a} = (a_1, \ldots, a_n)$ y $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$, decimos que $\mathbf{a} >_{grevlex} \mathbf{b}$ si

$$|\mathbf{a}| = \sum_{i=1}^{n} a_i \ > \ |\mathbf{b}| = \sum_{i=1}^{n} b_i, \quad \text{o si} \quad |\mathbf{a}| = |\mathbf{b}|$$

y, en $\mathbf{a} - \mathbf{b} \in \mathbb{Z}^n$, la entrada no nula más a la derecha es negativa.

De manera análoga escribiremos $\mathbf{x}^{\mathbf{a}} >_{grevlex} \mathbf{x}^{\mathbf{b}}$ cuando $\mathbf{a} >_{grevlex} \mathbf{b}$.

Ejemplo 1.2.3. Algunos ejemplos del orden lexicográfico graduado recién definido son:

a. $(4, 7, 1) >_{grevlex} (4, 2, 3)$ puesto que $|(4, 7, 1)| = 12 > |(4, 2, 3)| = 9$.

b. $(1, 5, 2) >_{grevlex} (4, 1, 3)$ dado que $|(1, 5, 2)| = 8 = |(4, 1, 3)|$, y $\mathbf{a} - \mathbf{b} = (-3, 4, -1)$.

c. Las variables $x_1, \ldots, x_n$ están ordenadas de la forma usual por el orden lexicográfico graduado inverso.

♢

Proposición 1.2.3. *El orden lexicográfico graduado inverso sobre $\mathbb{N}^n$ es un orden monomial.*

Para recalcar un poco las diferencias entre el orden $>_{grlex}$ y el $>_{grevlex}$, consideremos el siguiente ejemplo:

$$x^5yz^2 >_{grlex} x^4y^3z$$

mientras que

$$x^5yz^2 <_{grevlex} x^4y^3z.$$

Concluiremos esta sección con una discusión sobre cómo un orden monomial puede ser aplicado a polinomios.

Si $f = \sum_{\mathbf{a}} \alpha_{\mathbf{a}} \mathbf{x}^{\mathbf{a}} \in \ [x_1, \ldots, x_n]$, y hemos seleccionado previamente un orden monomial $>$, entonces podemos ordenar los monomios de f con respecto a $>$ de una manera precisa.

Por ejemplo, sea $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in \ [x_1, \ldots, x_n]$. Entonces:

a. Con respecto al orden $>_{lex}$, reordenamos los términos de f de manera decreciente:

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2.$$

b. Con respecto al orden $>_{grlex}$, tendríamos:

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2.$$

c. Con respecto al orden $>_{grevlex}$, tendríamos:

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2.$$

Esto nos motiva a dar las siguiente terminología, que nos será de utilidad en adelante.

Definición 1.2.5. Sea $f = \sum_{\mathbf{a}} \alpha_{\mathbf{a}} \mathbf{x}^{\mathbf{a}} \in \ [x_1, \ldots, x_n]$ no nulo, y sea $>$ un orden monomial.

(i) El *multigrado* de f es

$$\text{MGRAD}(f) = \max_{>}\{\mathbf{a} \in \mathbb{N}^n \mid \alpha_{\mathbf{a}} \neq 0\}.$$

(ii) El *monomio inicial* de f es

$$\text{LM}(f) = \mathbf{x}^{\text{MGRAD}(f)}.$$

(iii) El *coeficiente inicial* de f es

$$\text{LC}(f) = \alpha_{\text{MGRAD}(f)}.$$

(iv) El *término inicial* de f es

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

Para ilustrar, considere $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ como antes, y sea $>$ denotando al orden lexicográfico $>_{lex}$. Entonces

$$\begin{aligned} \text{MGRAD}(f) &= (3,0,0), \\ \text{LC}(f) &= -5, \\ \text{LM}(f) &= x^3, \\ \text{LT}(f) &= -5x^3. \end{aligned}$$

Con esto, podemos enunciar el siguiente lema, que establece algunas condiciones familiares sobre el comportamiento de los polinomios.

Lema 1.2.2. *Sean $f, g \in \ [x_1, \ldots, x_n]$ polinomios no nulos. Entonces:*

(i) $\text{MGRAD}(fg) = \text{MGRAD}(f) + \text{MGRAD}(g)$.

(ii) Si $f + g \neq 0$, entonces $\text{MGRAD}(f+g) \leq \max\{\text{MGRAD}(f), \text{MGRAD}(g)\}$. *Si además* $\text{MGRAD}(f) \neq \text{MGRAD}(g)$, *entonces la igualdad se cumple.*

1.3. Algoritmo de la división

Observemos que el anillo de polinomios $[x]$ sobre un campo es de ideales principales, por lo que un ideal $I \subset [x]$ es de la forma $\langle g \rangle$. Ahora, para saber si un polinomio arbitrario $f \in [x]$ está o no en I sólo hay que dividir el polinomio f entre g, si el residuo es cero entonces $f \in I$.

Desgraciadamente el algoritmo de la división para $[x]$ se comporta más bonito que en general para $[x_1, \ldots, x_n]$, pero es posible que alguna información podamos sacar de la generalización de este algoritmo para el caso de n variables.

La generalización del algoritmo de la división para el caso en que estemos trabajando con $[x_1, \ldots, x_n]$ es la siguiente, el objetivo es dividir $f \in [x_1, \ldots, x_n]$ entre $f_1, \ldots, f_s \in [x_1, \ldots, x_n]$, para escribir una expresión para f de la forma

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

donde $a_1, \ldots, a_s, r \in [x_1, \ldots, x_n]$. Debemos tener algún cuidado en la manera en que vamos a caracterizar al residuo, y es aquí donde vamos a utilizar los ordenes monomiales introducidos en la sección anterior.

Antes de enunciar el algoritmo en general, primero veamos el comportamiento que deseamos por medio de unos ejemplos.

Ejemplo 1.3.1. Queremos dividir $f = xy^2 + 1$ entre $f_1 = xy + 1$ y $f_2 = y + 1$, utilizando el orden lexicográfico $>_{lex}$ con $x > y$. Vamos a utilizar el mismo esquema que el de la división en polinomios de una variable, pero con la diferencia de que ahora hay varios divisores y cocientes. Tenemos entonces la siguiente representación:

$$\begin{array}{rl} a_1: & \\ a_2: & \\ xy+1 & \big| \overline{xy^2+1} \\ y+1 & \end{array}$$

Ambos términos iniciales $\text{LT}(f_1) = xy$ y $\text{LT}(f_2) = y$ dividen al término inicial $\text{LT}(f) = xy^2$. Como f_1 está listado primero, es el polinomio que vamos a utilizar. Así que dividimos xy^2 entre xy, y nos da y, y escribimos la resta f menos $y \cdot f_1$:

$$\begin{array}{rl} a_1: & y \\ a_2: & \\ xy+1 & \big| \overline{xy^2+1} \\ y+1 & \\ & xy^2 + y \\ \hline & -y+1 \end{array}$$

Ahora repetimos el mismo proceso para $-y + 1$. Esta vez necesitamos usar a f_2 puesto que

$\text{LT}(f_1) = xy$ no divide a $\text{LT}(-y+1) = -y$. Así obtenemos:

$$\begin{array}{rr|l} a_1: & y & \\ a_2: & -1 & \\ xy+1 & & xy^2+1 \\ y+1 & & \\ \hline & xy^2+y & \\ \hline & -y+1 & \\ & -y-1 & \\ \hline & 2 & \end{array}$$

Como 2 no es divisible entre $\text{LT}(f_1)$, ni entre $\text{LT}(f_2)$, entonces el residuo es $r = 2$ y terminamos. Con esto hemos escrito a $f = xy^2 + 1$ de la forma

$$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2.$$

$\diamondsuit$

En el siguiente ejemplo encontraremos un obstáculo que puede ocurrir al dividir polinomios con más de una variable:

Ejemplo 1.3.2. Utilizando el orden lexicográfico, considérese $f = x^2y + xy^2 + y^2$ y lo dividiremos entre $f_1 = xy - 1$, y $f_2 = y^2 - 1$. Los primeros dos pasos son iguales al ejemplo anterior.

$$\begin{array}{rr|l} a_1: & x+y & \\ a_2: & & \\ xy-1 & & x^2y+xy^2+y^2 \\ y^2-1 & & \\ \hline & x^2y-x & \\ \hline & xy^2+x+y^2 & \\ & xy^2-y & \\ \hline & x+y^2+y & \end{array}$$

Puesto que $\text{LT}(f_1) = xy$ y $\text{LT}(f_2) = y^2$ no dividen a $\text{LT}(x + y^2 + y) = x$ ya no podemos seguir dividiendo. Pero observemos que no podemos escribir a $x+y^2+y$ como residuo, pues $\text{LT}(f_2)$ divide a y^2, así es que si mandamos a x al residuo podremos seguir dividiendo.

Para implementar esta idea vamos a crear una columna r, a la derecha de la división, en donde pondremos los términos que pertenezcan al residuo. Al polinomio bajo el radical lo llamaremos *dividendo intermedio*. Continuamos así dividiendo hasta que el dividendo intermedio sea cero.

A continuación presentamos el paso siguientes, donde mandamos a x a la columna del residuo.

$$\begin{array}{rl} & a_1: \quad x+y \\ & a_2: \\ xy-1 & \Big| \overline{x^2y+xy^2+y^2} \\ y^2-1 & \Big| \\ & \underline{x^2y-x} \\ & \quad xy^2+x+y^2 \\ & \quad \underline{xy^2-y} \\ & \quad\quad x+y^2+y \\ & \quad\quad \underline{y^2+y} \quad \rightarrow \quad x \\ & \quad\quad\quad 0 \end{array} \qquad \overline{\overline{r}}$$

Ahora continuamos dividiendo. Si podemos dividir entre $\text{LT}(f_1)$ o $\text{LT}(f_2)$ continuamos de manera usual, y si ninguno de los dos divide, entonces mandamos el término inicial del dividendo intermedio a la columna de residuo. Presentamos a continuación el resto de la división.

$$\begin{array}{rl} & a_1: \quad x+y \\ & a_2: \quad\quad 1 \\ xy-1 & \Big| \overline{x^2y+xy^2+y^2} \\ y^2-1 & \Big| \\ & \underline{x^2y-x} \\ & \quad xy^2+x+y^2 \\ & \quad \underline{xy^2-y} \\ & \quad\quad x+y^2+y \\ & \quad\quad \underline{y^2+y} \quad \rightarrow \quad\quad x \\ & \quad\quad\quad y^2-1 \\ & \quad\quad\quad \underline{y+1} \\ & \quad\quad\quad\quad 1 \quad \rightarrow \quad x+y \\ & \quad\quad\quad\quad 0 \quad \rightarrow \quad x+y+1 \end{array} \qquad \overline{\overline{r}}$$

Entonces el residuo es $x+y+1$, y así obtenemos

$$x^2y+xy^2+y^2 = (x+y)(xy-1)+1\cdot(y^2-1)+(x+y+1).$$

Obsérvese que el residuo es una suma de monomios, de los cuales ninguno es divisible entre $\text{LT}(f_1)$ ni $\text{LT}(f_2)$.

$\diamondsuit$

Observación 1.3.1. *Note que al invertir f_1 con f_2, muestra que el residuo no es único.*

Observación 1.3.2. *Que se cumpla $r = 0$ es una condición suficiente para que $f \in \langle f_1, \ldots, f_s\rangle$, pero no es necesaria. Tómese $f_1 = xy+1$, $f_2 = y^2-1$ con el orden lexicográfico, y divida $f = xy^2 - x$. Al invertir (f_1, f_2) por (f_2, f_1) vemos que en el primer caso $r = 0$, pero para el segundo $r \neq 0$.*

El ejemplo anterior nos muestra cómo funciona el algoritmo de la división. Inclusive nos muestra que propiedades queremos que tenga el residuo: ninguno de sus términos debe ser divisible por ninguno de los términos iniciales de los polinomios entre los que estamos dividiendo.

Podemos ahora establecer la forma general del algoritmo de la división.

Teorema 1.3.1 (**Algoritmo de la División en** $[x_1, \ldots, x_n]$)**.** *Fije un orden monomial* $>$ *en* $\mathbb{N}^n$*, y sea* $F = (f_1, \ldots, f_s)$ *una* $s-$*ada ordenada de polinomios en* $[x_1, \ldots, x_n]$*. Entonces cada* $f \in [x_1, \ldots, x_n]$ *puede ser escrito como*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

donde a_i, $r \in [x_1, \ldots, x_n]$*, y* $r = 0$*, o bien,* r *es una combinación lineal, con coeficientes en , de monomios tales que ninguno es divisible entre ninguno de los* $\text{LT}(f_1), \ldots, \text{LT}(f_s)$*. Llamaremos a* r *el* residuo *de* f *al dividirlo entre* F*. Más aún, si* $a_i f_i \neq 0$*, entonces tenemos que*

$$\text{MGRAD}(f) \geq \text{MGRAD}(a_i f_i).$$

Demostración. Probaremos la existencia de $a_1, \ldots, a_s$ y r dando un algoritmo explícito para su construcción, y mostrando que opera correctamente con cualquier entrada dada.

Algoritmo 1.1. El siguiente es un algoritmo de la división para polinomios en varias variables.

Input: $f_1, \ldots, f_s, f$
Output: $a_1, \ldots, a_s, r$

$a_1 := 0; \ldots; a_s := 0;\ r := 0$
$p := f$
WHILE $p \neq 0$ DO
    $i := 1$
    divisionoccurred:= false
    WHILE $i \leq s$ AND divisionoccurred = false DO
        IF $\text{LT}(f_i)$ divides $\text{LT}(p)$ THEN
            $a_i := a_i + \text{LT}(p)/\text{LT}(f_i)$
            $p := p - (\text{LT}(p)/\text{LT}(f_i))f_i$
            divisionoccurred := true
        ELSE
            $i := i + 1$
    IF divisionoccurred = false THEN
        $r := r + \text{LT}(p)$
        $p := p - \text{LT}(p)$

Podemos ver que este algoritmo es parecido al utilizado en el ejemplo anterior, pero con la diferencia que agregamos la variable p quien representa el dividendo intermedio en

cada paso, la variable r representa la columna del lado derecho, y las variables $a_1, \ldots, a_s$ representan los cocientes listados encima del símbolo de división.

Por último, la variable "divisionoccurred"nos dice cuando algún $\text{LT}(f_i)$ divide al coeficiente inicial del dividendo intermedio. Es claro que se está dentro del bucle principal WHILE...DO, precisamente cuando una de las dos siguientes cosas pasan:

- (Paso de División) Si algún $\text{LT}(f_i)$ divide a $\text{LT}(p)$, entonces el algoritmo procede como en el caso de una variable.
- (Paso de Residuo) Si ningún $\text{LT}(f_i)$ divide a $\text{LT}(p)$, entonces el algoritmo manda $\text{LT}(p)$ al residuo.

Estos pasos corresponden exactamente a lo que hicimos durante el Ejemplo 1.3.2.

Para mostrar que el Algoritmo 1.1 funciona correctamente, primero vamos a mostrar que la igualdad

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \tag{1.1}$$

se cumple en cada etapa. Esto es claro para los valores iniciales de $a_1, \ldots, a_s, p$ y r. Ahora supóngase que la igualdad (1.1) se cumple en uno de los pasos del algoritmo. Si el siguiente paso es un Paso de División, entonces algún $\text{LT}(f_i)$ divide a $\text{LT}(p)$, y la igualdad

$$a_i f_i + p = (a_i + \text{LT}(p)/\text{LT}(f_i))f_i + (p - (\text{LT}(p)/\text{LT}(f_i))f_i)$$

nos muestra que $a_i f_i + p$ permanece intacto. Dado que las otras variables no son afectadas, (1.1) sigue siendo cierta en este caso. Por otro lado, si el siguiente caso es un Paso de Residuo, entonces p y r serán sustituidos, pero la suma $p+r$ permanece intacta puesto que:

$$p + r = (p - \text{LT}(p)) + (r + \text{LT}(p)).$$

Y como antes, la igualdad (1.1) se preserva.

Ahora obsérvese que el algoritmo se detiene si $p = 0$. En esta situación, (1.1) se convierte en

$$f = a_1 f_1 + \cdots + a_s f_s + r.$$

Dado que se añaden términos a r sólo cuando no son divisibles por ninguno de los $\text{LT}(f_i)$, de aquí se sigue que $a_1, \ldots, a_s$ y r tienen las propiedades que deseamos cuando el algoritmo termina.

Por último debemos mostrar que el algoritmo eventualmente termina. Para esto, obsérvese que cada vez que se redefine la variable p, o se hace 0, o su multigrado disminuye. Para ver esto último, primero supóngase que durante el Paso de División, p es redefinido como

$$p' = p - \frac{\text{LT}(p)}{\text{LT}(f_i)} f_i.$$

Por el Lema 1.2.2, tenemos que

$$\text{MGRAD}\left(\frac{\text{LT}(p)}{\text{LT}(f_i)} f_i\right) = \text{MGRAD}\left(\frac{\text{LT}(p)}{\text{LT}(f_i)}\right) + \text{MGRAD}(f_i),$$

y este se obtiene de fijarse en el multigrado del producto de los dos términos iniciales, de aquí se sigue la siguiente igualdad

$$\text{LT}\left(\frac{\text{LT}(p)}{\text{LT}(f_i)}f_i\right) = \frac{\text{LT}(p)}{\text{LT}(f_i)}\text{LT}(f_i) = \text{LT}(p),$$

con lo que p y $(\text{LT}(p)/\text{LT}(f_i))f_i$ tienen el mismo término inicial. Se sigue entonces que su diferencia, p', cancela el término inicial de p, y por consiguiente p' tiene grado estrictamente menor cuando $p' \neq 0$.

Ahora supóngase que durante el Paso del Residuo, p es redefinido como

$$p' = p - \text{LT}(p).$$

Aquí, es obvio que $\text{MGRAD}(p') < \text{MGRAD}(p)$ cuando $p' \neq 0$. Entonces, en cualquiera de los casos, el multigrado debe disminuir. Si el algoritmo nunca terminara, entonces podríamos encontrar una sucesión decreciente infinita de multigrados. Como el Lema 1.2.1 establece que $<$ es un Buen Orden si y sólo si, toda sucesión decreciente debe terminar, lo que muestra que esta sucesión de multigrados no puede tomarse. Con esto, eventualmente debe pasar que $p = 0$, y así el algoritmo termina después de un número finito de pasos.

Sólo nos resta estudiar la relación entre $\text{MGRAD}(f)$ y $\text{MGRAD}(a_i f_i)$. Todo término en a_i es de la forma $\text{LT}(p)/\text{LT}(f_i)$ para algún valor de la variable p. El algoritmo inicia con $p = f$, y acabamos de mostrar que el multigrado de p decrece. Esto nos muestra que $\text{LT}(p) \leq \text{LT}(f)$, y se sigue fácilmente (usando el inciso (ii) de la Definición 1.2.1) que

$$\text{MGRAD}(a_i f_i) \leq \text{MGRAD}(p) \leq \text{MGRAD}(f)$$

cuando $a_i f_i \neq 0$. ■

1.4. Bases de Gröbner

A través de la siguiente sección vamos a estudiar las bases de Gröbner, que nos van a permitir resolver problemas sobre ideales polinomiales, de una manera algorítmica o computacional. Las bases de Gröbner se usan en muchos sistemas algebraicos computacionales poderosos para estudiar ideas específicas ideas polinomiales que aterrizan en diversas aplicaciones.

Empezaremos por mostrar el Lema de Dickson, que explica una propiedad fundamental de los ideales monomiales, y que nos será de utilidad para probar algunas afirmaciones más adelante.

Teorema 1.4.1 (Lema de Dickson). *Un ideal monomial* $I = \langle \mathbf{x}^{\mathbf{a}} \rangle_{\mathbf{a} \in A} \subset [x_1, \ldots, x_n]$ *puede ser escrito de la forma* $I = \langle \mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_s} \rangle$, *con* $\mathbf{a}_1, \ldots, \mathbf{a}_s \in A$. *En particular,* I *tiene una base finita.*

Demostración. La prueba será por inducción en el número de variables. Si $n = 1$, entonces I está generado por monomios x_1^a con $a \in A \subset \mathbb{N}$. Sea b el primer elemento de A. Entonces $b \leq a$ para todo $a \in A$, por lo que x_1^b divide a todos los generadores x_1^a. Por lo tanto $I = \langle x_1^b \rangle$.

Ahora supóngase que $n > 1$ y que el teorema es cierto para $n - 1$. Vamos a tomar las variables $x_1, \ldots, x_{n-1}, y$, así los monomios en $[x_1, \ldots, x_{n-1}, y]$ pueden ser escritos como $\mathbf{x}^{\mathbf{a}} y^m$, donde $\mathbf{a} = (a_1, \ldots, a_{n-1}) \in \mathbb{N}^{n-1}$ y $m \in \mathbb{N}$.

Supóngase que $I \subset [x_1, \ldots, x_{n-1}, y]$ es un ideal monomial. Para encontrar generadores para I, sea J el ideal en $[x_1, \ldots, x_{n-1}]$ generado por los monomios $\mathbf{x}^{\mathbf{a}}$, para los cuales $\mathbf{x}^{\mathbf{a}} y^m \in I$ para alguna $m \geq 0$. Dado que J es un ideal monomial en $[x_1, \ldots, x_{n-1}]$, por nuestra hipótesis de inducción se implica que un número finito de las $\mathbf{x}^{\mathbf{a}}$ generan J, digamos $J = \langle \mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_s} \rangle$. Podemos entender al ideal J como la "proyección"de I en $[x_1, \ldots, x_{n-1}]$.

Para cada i con $1 \leq i \leq s$, la definición de J nos dice que $\mathbf{x}^{\mathbf{a}_i} y^{m_i} \in I$ para alguna $m_i \geq 0$. Sea m la más grande de las m_i. Entonces, para cada k con $0 \leq k \leq m - 1$, considere el ideal $J_k \subset [x_1, \ldots, x_{n-1}]$ generado por los monomios $\mathbf{x}^{\mathbf{b}}$ tales que $\mathbf{x}^{\mathbf{b}} y^k \in I$. Uno puede pensar a J_k como la "rebanada"de I generada por monomios que contienen la variable y exactamente a la potencia k. Usando nuestra hipótesis inductiva nuevamente, J_k tiene un número finito de monomios generadores, digamos $J_k = \langle \mathbf{x}^{\mathbf{a}_1(k)}, \ldots, \mathbf{x}^{\mathbf{a}_{s_k}(k)} \rangle$.

Afirmamos que I está generado por los monomios de la siguiente lista:

$$\begin{array}{rcl} J & : & \mathbf{x}^{\mathbf{a}_1} y^m, \ldots, \mathbf{x}^{\mathbf{a}_s} y^m, \\ J_0 & : & \mathbf{x}^{\mathbf{a}_1(0)}, \ldots, \mathbf{x}^{\mathbf{a}_{s_0}(0)}, \\ J_1 & : & \mathbf{x}^{\mathbf{a}_1(1)} y, \ldots, \mathbf{x}^{\mathbf{a}_{s_1}(1)} y, \\ & \vdots & \\ J_{m-1} & : & \mathbf{x}^{\mathbf{a}_1(m-1)} y^{m-1}, \ldots, \mathbf{x}^{\mathbf{a}_{s_{m-1}}(m-1)} y^{m-1}. \end{array}$$

Para esto, notemos que cada monomio en I es divisible por algún monomio de esta lista. Para ver por qué, sea $\mathbf{x}^{\mathbf{a}}y^p \in I$. Si $p \geq m$, entonces $\mathbf{x}^{\mathbf{a}}y^p$ es divisible por algún $\mathbf{x}^{\mathbf{a}_i}y^m$ por cómo construimos J. Por otro lado, si $p \leq m-1$, entonces $\mathbf{x}^{\mathbf{a}}y^p$ es divisible por algún $\mathbf{x}^{\mathbf{a}_j(p)}y^p$ por la construcción de J_p. Como consecuencia del Lema 1.1.2, los monomios de arriba generan un ideal que tiene los mismos monomios que I. Gracias al Corolario 1.1.1, los ideales están forzados a ser iguales, y nuestra afirmación está probada.

Para completar la prueba, necesitamos mostrar que un conjunto finito de generadores pueden ser escogidos de un conjunto de generadores dados de un ideal. Si regresamos a escribir las variables como $x_1, \ldots, x_n$, entonces nuestro ideal monomial es $I = \langle \mathbf{x}^{\mathbf{a}} \rangle_{\mathbf{a} \in A} \subset [x_1, \ldots, x_n]$. Necesitamos mostrar que I está generado por un número finito de las $\mathbf{x}^{\mathbf{a}}$, con $\mathbf{a} \in A$. Del párrafo anterior tenemos que $I = \langle \mathbf{x}^{\mathbf{b}_1}, \ldots, \mathbf{x}^{\mathbf{b}_s} \rangle$ para algunos monomios $\mathbf{x}^{\mathbf{b}_i} \in I$. Dado que $\mathbf{x}^{\mathbf{b}_i} \in I = \langle \mathbf{x}^{\mathbf{a}} \rangle_{\mathbf{a} \in A}$, el Lema 1.1.2 nos asegura que cada $\mathbf{x}^{\mathbf{b}_i}$ es divisible por $\mathbf{x}^{\mathbf{a}_i}$ para alguna $\mathbf{a}_i \in A$. De aquí es fácil notar que $I = \langle \mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_s} \rangle$. ■

Definición 1.4.1. Sea $I \subset [x_1, \ldots, x_n]$ un ideal, definimos el *ideal inicial* de I como

$$in(I) = \langle \text{LT}(f) \mid f \in I \rangle$$

Observemos que si I es finitamente generado, digamos $I = \langle g_1, \ldots, g_s \rangle$, entonces el ideal $\langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle \subset in(I)$, puesto que $\text{LT}(g_i) \in in(I)$ por definición, pero ¿qué tan desiguales pueden ser estos ideales? En general $in(I)$ suele ser estrictamente mayor.

Para ver esto, consideremos el siguiente ejemplo.

Ejemplo 1.4.1. Sea $I = \langle f_1, f_2 \rangle$, donde $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$, y utilize el orden $>_{grlex}$ para monomios en $[x, y]$. Entonces

$$x \cdot f_2 - y \cdot f_1 = x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2$$

por lo que $x^2 \in I$. Tenemos que $x^2 = \text{LT}(x^2) \in in(I)$. Sin embargo, x^2 no es divisible entre $\text{LT}(f_1) = x^3$ ni $\text{LT}(f_2) = x^2y$, por lo que $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$ gracias al Lema 1.1.2.

♢

Ahora mostraremos que $in(I)$ es un ideal monomial. De esto se desprenderá que $in(I)$ es generado por un número finito de términos iniciales.

Proposición 1.4.1. *Sea $I \subset [x_1, \ldots, x_n]$ un ideal. Entonces*

(i) $in(I)$ es un ideal monomial.

(ii) Existen $g_1, \ldots, g_s \in I$ tales que $in(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$

Demostración.

(i) Los monomios iniciales $\text{LM}(g)$ de elementos $g \in I - \{0\}$ generan al ideal monomial $\langle \text{LM}(g) \mid g \in I - \{0\} \rangle$. Como $\text{LM}(g)$ y $\text{LT}(g)$ difieren sólo por una constante no nula (que son unidades en $[x_1, \ldots, x_n]$), entonces los ideales que generan son el mismo, esto es, $\langle \text{LM}(g) \mid g \in I - \{0\} \rangle = \langle \text{LT}(g) \mid g \in I - \{0\} \rangle = in(I)$. Por lo que $in(I)$ es un ideal monomial.

(ii) Dado que $in(I)$ está generado por los monomios $\text{LM}(g)$ con $g \in I - \{0\}$, el Lema de Dickson (Teorema 1.4.1) nos dice que $in(I) = \langle \text{LM}(g_1), \ldots, \text{LM}(g_s) \rangle$ para un número finito de $g_1, \ldots, g_s \in I$. Como $\text{LM}(g_i)$ y $\text{LT}(g_i)$ sólo difieren por una constante no cero (una unidad en $[x_1, \ldots, x_n]$), entonces $in(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$, lo que completa la prueba.

■

El siguiente Teorema es un resultado clásico en Geometría Algebraica y en Algebra Conmutativa, y aquí presentamos una prueba utilizando únicamente argumentos de Algebra conmutativa, y la herramienta desarrollada hasta el momento.

Teorema 1.4.2 (Teorema de la Base de Hilbert). *Todo ideal $I \subset [x_1, \ldots, x_n]$ tiene un conjunto finito de generadores. Esto es, $I = \langle g_1, \ldots, g_s \rangle$ para algunos $g_1, \ldots, g_s \in I$.*

Demostración. Si $I = 0$, entonces el conjunto finito $\{0\}$ es un conjunto de generadores. Si I contiene algún polinomio no cero, entonces, gracias a la Proposición 1.4.1, existen $g_1, \ldots, g_s \in I$ tales que $in(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$. Afirmamos que $I = \langle g_1, \ldots, g_s \rangle$.

Es claro que $\langle g_1, \ldots, g_s \rangle \subset I$ puesto que cada $g_i \in I$. Ahora sea $f \in I$ cualquier polinomio. Si aplicamos el algoritmo de la división para dividir f entre $\{g_1, \ldots, g_s\}$, obtenemos una expresión de la forma

$$f = a_1 g_1 + \cdots + a_t g_t + r$$

donde cada término de r no es divisible por ninguno de los $\text{LT}(g_1), \ldots, \text{LT}(g_t)$. Si escribimos

$$r = f - a_1 g_1 - \cdots - a_t g_t \in I$$

y suponemos que $r \neq 0$, entonces $\text{LT}(r) \in in(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$, y por el Lema 1.1.2 se sigue que $\text{LT}(r)$ debe ser divisible por algún $\text{LT}(g_i)$, lo cual contradice el hecho de ser un residuo no cero, y como consecuencia, r debe ser cero.

Con esto tenemos

$$f = a_1 g_1 + \cdots + a_t g_t + 0 \in \langle g_1, \ldots, g_s \rangle,$$

lo que muestra que $I \subset \langle g_1, \ldots, g_s \rangle$. Esto termina la prueba. ■

Obsérvese que la base de I, $\{g_1, \ldots, g_s\}$ usada en la prueba del Teorema 1.4.2 tiene la propiedad de que $in(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle$. Pero en el Ejemplo 1.4.1 vimos que no toda base de un ideal tiene esta propiedad. Es por esto que hacemos la siguiente distinción a este tipo de bases.

Definición 1.4.2. Fíjese un orden monomial. Un conjunto finito de generadores $G = \{g_1, \ldots, g_s\}$ de un ideal I se dice que es *base de Gröbner* si

$$\langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle = in(I).$$

Observemos que con la técnica utilizada en la prueba del Teorema 1.4.2, pudimos haber hecho una definición menos rigurosa de base de Gröbner, definiéndola simplemente como un subconjunto $\{g_1, \ldots, g_s\} \subset I$, que cumpla $\langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle = in(I)$. Y luego se puede demostrar, como hicimos en la prueba del Teorema 1.4.2, que un conjunto que cumpla $\langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle = in(I)$, satisface que $\langle g_1, \ldots, g_s \rangle = I$..

Nótese que la observación anterior nos asegura, junto con la Proposición 1.4.1, que todo ideal $I \subset [x_1, \ldots, x_n]$ posee una base de Gröbner.

Ahora estudiaremos algunas propiedades de las bases de Gröbner, y comenzaremos mostrando que para ellas se cumplen los comportamientos deseados en el algoritmo de la división.

Lo primero que mostraremos es que el residuo está bien determinado cuando se divide entre una base de Gröbner.

Proposición 1.4.2. *Sea $G = \{g_1, \ldots, g_s\}$ una base de Gröbner de un ideal $I \subset [x_1, \ldots, x_n]$, y sea $f \in [x_1, \ldots, x_n]$. Entonces existe un único $r \in [x_1, \ldots, x_n]$ con las siguientes propiedades:*

(i) Ningún término de r es divisible por ninguno de los $\text{LT}(g_1), \ldots, \text{LT}(g_s)$.

(ii) Existe $g \in I$ tal que $f = g + r$.

En particular, r es el residuo al dividir f entre G sin importar cómo estén listados los elementos de G a la hora de usar el algoritmo de la división.

Demostración. El algoritmo de la división nos da $f = a_1 g_1 + \cdots + a_t g_t + r$, donde r satisface la propiedad *(i)*. Para que se satisfaga *(ii)*, simplemente hágase $g = a_1 g_1 + \cdots + a_t g_t \in I$.

Para probar la unicidad, supóngase que $f = g_1 + r_1 = g_2 + r_2$, que satisfacen las condiciones *(i)* y *(ii)*. Entonces $r_2 - r_1 = g_1 - g_2 \in I$, por lo que si $r_1 \neq r_2$, entonces $\text{LT}(r_2 - r_1) \in in(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Por el Lema 1.1.2, se sigue que $\text{LT}(r_2 - r_1)$ es divisible por algún $\text{LT}(g_i)$. Esto no es posible puesto que ninguno de los $\text{LT}(g_i)$ divide a ningún término ni de r_1, ni de r_2. Entonces $r_2 - r_1$ debe ser cero, y esto prueba la unicidad.

La última parte de la proposición se sigue a partir de la unicidad de r. ■

Corolario 1.4.1. *Sea $G = \{g_1, \ldots, g_s\}$ una base de Gröbner para un ideal $I \subset [x_1, \ldots, x_n]$, y sea $f \in [x_1, \ldots, x_n]$. Entonces $f \in I$ si y sólo si el residuo de la división de f entre G es cero.*

Demostración. Si el residuo es cero, por la Observación 1.3.2, tenemos que $f \in I$. Supongamos ahora que $f \in I$ está dado, entonces la expresión $f = f + 0$ satisface las condiciones de la Proposición 1.4.2, y se sigue de aquí que 0 es el residuo al dividir f entre G. ■

La propiedad dada en el Corolario 1.4.1 es muchas veces tomada como la definición de base de Gröbner, puesto que se puede mostrar que la afirmación de el Corolario es cierta si y sólo si $\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle = in(I)$.

Usaremos en adelante la siguiente notación para el residuo.

Definición 1.4.3. Escribiremos $\overline{f}^F$ para denotar el residuo al dividir f entre una $s-$ada ordenada $F = (f_1, \ldots, f_s)$. Si F es una base de Gröbner para $\langle f_1, \ldots, f_s \rangle$, entonces podemos considerar a F simplemente como conjunto (sin considerar ningún orden) gracias a la Proposición 1.4.2.

Un ejemplo de esta notación es el siguiente, sea $F = (x^2y - y^2, x^4y^2 - y^2) \subset \ [x, y]$, usando el orden lexicográfico tenemos

$$\overline{x^5y}^F = xy^3$$

Puesto que el algoritmo de la división nos dice

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3.$$

Ahora trataremos de indicar cuando un conjunto de generadores de un ideal es una base de Gröbner.

Observemos que para que $\{f_1, \ldots, f_s\}$ no sea una base de Gröbner es porque puede haber combinaciones polinomiales de los f_i que produzcan polinomios cuyos términos iniciales no estén generados por los $\text{LT}(f_i)$. Una posibilidad para que esto pase es si una combinación

$$\alpha \mathbf{x^a} f_i - \beta \mathbf{x^b} f_j$$

cancela los términos iniciales, dejando sólo términos más chicos. Por otro lado, $\alpha \mathbf{x^a} f_i - \beta \mathbf{x^b} f_j \in I$, por lo que su término inicial está en $in(I)$.

Para estudiar estas cancelaciones, introducimos las siguientes combinaciones especiales.

Definición 1.4.4. Sean $f, g \in \ [x_1, \ldots, x_n]$ polinomios no cero.

(i) Si llamamos $\mathbf{a} = \text{MGRAD}(f)$ y $\mathbf{b} = \text{MGRAD}(g)$, entonces definimos $\mathbf{c} = (c_1, \ldots, c_n)$ con $c_i = \text{máx}\{a_i, b_i\}$ para cada i. Llamamos al monomio $\mathbf{x^c}$ el *mínimo común múltiplo* de $\text{LM}(f)$ y $\text{LM}(g)$, escrito como $\mathbf{x^c} = \text{MCM}(\text{LM}(f), \text{LM}(g))$.

(ii) Definimos al $\mathcal{S}-$*polinomio* de f y g como la combinación

$$\mathcal{S}(f, g) = \frac{\mathbf{x^c}}{\text{LT}(f)} \cdot f - \frac{\mathbf{x^c}}{\text{LT}(g)} \cdot g.$$

La parte *(i)* de la definición anterior, ya la habíamos hecho debajo de la Definición 1.1.4, pero aquí la recordamos.

Para ilustrar la notación definida en la segunda parte de la definición anterior, tómese $f = x^3y^2 - x^2y^3 + x$ y $g = 3x^4y + y^2$ en $\mathbb{R}[x, y]$ con el orden $>_{grlex}$. Entonces $\mathbf{c} = (4, 2)$ y

$$\begin{aligned} \mathcal{S}(f,g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3. \end{aligned}$$

Un $\mathcal{S}-$polinomio $\mathcal{S}(f, g)$ está diseñado para cancelar los términos iniciales entre f y g. De hecho, el siguiente lema mostrará que cada cancelación de términos iniciales entre polinomios con el mismo multigrado es de esta forma.

Lema 1.4.1. *Supóngase que se tiene* $\sum_{i=1}^{s} c_i f_i$ *con* $c_i \in$ *y* $\text{MGRAD}(f_i) = \mathbf{d} \in \mathbb{N}^n$ *para toda* i. *Si* $\text{MGRAD}(\sum_{i=1}^{s} c_i f_i) < \mathbf{d}$, *entonces* $\sum_{i=1}^{s} c_i f_i$ *es una combinación lineal, con coeficientes en , de los* $\mathcal{S}-$*polinomios* $\mathcal{S}(f_j, f_k)$ *para* $1 \leq j, k \leq s$. *Más aún, cada* $\mathcal{S}(f_i, f_k)$ *tiene multigrado estrictamente menor que* $\mathbf{d}$.

Demostración. Sea $d_i = \text{LC}(f_i)$, por lo que $d_i c_i = \text{LC}(c_i f_i)$. Como $\text{MGRAD}(c_i f_i) = \mathbf{d}$ para cada i, y la suma de todos tiene multigrado menor estrictamente que $\mathbf{d}$, entonces se debe tener una cancelación de los términos iniciales, es decir, se debe tener que $\sum_{i=1}^{s} c_i d_i = 0$.

Definamos $p_i = f_i/d_i$, y consideremos la suma telescópica

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots$$

$$+(c_1 d_1 + \cdots + c_{t-1} d_{t-1})(p_{t-1} - p_t) + (c_1 d_1 + \cdots + c_t d_t) p_t.$$

Por hipótesis, $\text{LT}(f_i) = d_i \mathbf{x}^{\mathbf{d}}$, lo que implica que $\text{MCM}(\text{LM}(f_j), \text{LM}(f_k)) = \mathbf{x}^{\mathbf{d}}$. Entonces se tiene que

$$\mathcal{S}(f_j, f_k) = \frac{\mathbf{x}^{\mathbf{d}}}{\text{LT}(f_j)} f_j - \frac{\mathbf{x}^{\mathbf{d}}}{\text{LT}(f_k)} f_k = \frac{\mathbf{x}^{\mathbf{d}}}{d_j \mathbf{x}^{\mathbf{d}}} f_j - \frac{\mathbf{x}^{\mathbf{d}}}{d_k \mathbf{x}^{\mathbf{d}}} f_k = p_j - p_k. \tag{1.2}$$

Usando el hecho de que $\sum_{i=1}^{s} c_i d_i = 0$, la suma de arriba se convierte en

$$\sum_{i=1}^{s} c_i d_i = c_1 d_1 \mathcal{S}(f_1, f_2) + (c_1 d_1 + c_2 d_2)\mathcal{S}(f_2, f_3) + \cdots$$

$$+(c_1 d_1 + \cdots + c_{t-1} d_{t-1})\mathcal{S}(f_{t-1}, f_t),$$

que es una suma de la forma deseada. Dado que $\text{MGRAD}(p_j) = \text{MGRAD}(p_k) = \mathbf{d}$, y $\text{LC}(p_j) = 1 = \text{LC}(p_k)$, entonces se concluye que $\text{MGRAD}(p_j - p_k) < \mathbf{d}$. Gracias a la ecuación 1.2, lo mismo es cierto para $\mathcal{S}(f_j, f_k)$. ■

Cuando polinomios $f_1, \ldots, f_s$ satisfacen las hipótesis del Lema 1.4.1, obtenemos una ecuación de la forma

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_{jk} \mathcal{S}(f_j, f_k).$$

Vamos a considerar el momento en que sucede la cancelación de términos iniciales. En la suma del lado izquierdo, cada sumando $c_i f_i$ tiene multigrado $\mathbf{d}$, por lo que la cancelación ocurre a la hora de sumarlos todos. Sin embargo, en la suma del lado derecho, cada sumando $c_{jk}\mathcal{S}(f_j, f_k)$ tiene multigrado menor que $\mathbf{d}$, por lo que la cancelación debió ya haber sucedido antes de sumarlos. Intuitivamente, esto significa que todas las cancelaciones pueden expresarse en términos de los $\mathcal{S}-$polinomios.

Usando $\mathcal{S}-$polinomios y el Lema 1.4.1, podemos probar el siguiente Teorema, que sirve para decir cuándo una base de un ideal es una base de Gröbner.

Teorema 1.4.3 (**Criterio de Buchberger**). *Sea I un ideal polinomial. Entonces una base $G = \{g_1, \ldots, g_s\}$ de I es una base de Gröbner si y sólo si para todos los pares $i \neq j$, el residuo en la división de $\mathcal{S}(g_i, g_j)$ entre G es cero.*

Demostración.

$\Rightarrow$: Si G es una base de Gröbner, entonces, puesto que $\mathcal{S}(g_i, g_j) \in I$, el residuo al dividir entre G es cero, gracias al Corolario 1.4.1.

$\Leftarrow$: Sea $f \in I$ un polinomio no nulo. Debemos mostrar que si todos los $\mathcal{S}-$polinomios tienen residuo cero a la hora de dividirlos entre G, entonces $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Primero vamos a esbozar la estrategia para la prueba.

Dado $f \in I = \langle g_1, \ldots, g_s \rangle$, existen polinomios $h_i \in \ [x_1, \ldots, x_n]$ tales que

$$f = \sum_{i=1}^{t} h_i g_i. \tag{1.3}$$

Gracias al Lema 1.2.2, se tiene que

$$\text{MGRAD}(f) \leq \text{máx}\{\text{MGRAD}(h_i g_i)\}. \tag{1.4}$$

Si la igualdad no se cumple, es porque debe haber algunas cancelaciones entre los términos iniciales de (1.3). El Lema 1.4.1 nos permite reescribir esto en términos de $\mathcal{S}-$polinomios. Ahora, nuestra hipótesis de que los $\mathcal{S}-$polinomios tienen residuo cero, nos permite reemplazar los $\mathcal{S}-$polinomios por expresiones que involucran menos cancelaciones. Entonces obtendremos una expresión para f que tiene menos cancelaciones en los términos iniciales. Continuando de éste modo, llegaremos eventualmente a una expresión como (1.3) para f en la que la igualdad se cumpla para (1.4). Entonces $\text{MGRAD}(f) = \text{MGRAD}(h_i g_i)$ para alguna i, y se seguirá que $\text{LT}(f)$ es divisible por

$\text{LT}(g_i)$. Esto mostrará que $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, que es lo que queremos probar.

Ahora daremos los detalles de la prueba. Dada una expresión (1.3) para f, sea $m(i) = \text{MGRAD}(h_i g_i)$, y definamos $\mathbf{d} = \text{máx}\{m(1), \ldots, m(t)\}$. Entonces la desigualdad (1.4) se convierte en

$$\text{MGRAD}(f) \leq \mathbf{d}.$$

Ahora consideremos todas las maneras en que podemos escribir a f de la forma (1.3). Para cada una obtendremos posiblemente diferentes $\mathbf{d}$. Como un orden monomial es un buen orden, podemos escoger una expresión como en (1.3) en la que la $\mathbf{d}$ sea mínima.

Mostraremos que una vez escogida $\mathbf{d}$ mínima, entonces $\text{MGRAD}(f) = \mathbf{d}$. De lo que se obtendrá que la igualdad se cumple en (1.4), y por tanto $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, lo que concluirá la demostración del teorema.

Sólo nos resta probar que $\text{MGRAD}(f) = \mathbf{d}$. Lo haremos por contradicción. Supongamos que $\text{MGRAD}(f) < \mathbf{d}$, y escribamos f de la siguiente forma

$$\begin{aligned} f &= \sum_{m(i)=\mathbf{d}} h_i g_i + \sum_{m(i)<\mathbf{d}} h_i g_i \qquad (1.5) \\ &= \sum_{m(i)=\mathbf{d}} \text{LT}(h_i) g_i + \sum_{m(i)=\mathbf{d}} (h_i - \text{LT}(h_i)) g_i + \sum_{m(i)<\mathbf{d}} h_i g_i. \end{aligned}$$

Todos los monomios que aparecen en el tercer y el segundo sumando del segundo renglón, tienen multigrado $< \mathbf{d}$. Entonces, suponer que $\text{MGRAD}(f) < \mathbf{d}$ significa que el primer sumando también tiene multigrado $< \mathbf{d}$.

Sea $\text{LT}(h_i) = c_i \mathbf{x}^{\mathbf{a}_i}$. Entonces observemos que el primer sumando $\sum_{m(i)=\mathbf{d}} \text{LT}(h_i) g_i = \sum_{m(i)=\mathbf{d}} c_i \mathbf{x}^{\mathbf{a}_i} g_i$ tiene exactamente la forma descrita en el Lema 1.4.1, considerando $f_i = \mathbf{x}^{\mathbf{a}_i} g_i$. Entonces el Lema 1.4.1 implica que esta suma es combinación lineal de los $\mathcal{S}-$polinomios $\mathcal{S}(\mathbf{x}^{\mathbf{a}_j} g_j, \mathbf{x}^{\mathbf{a}_k} g_k)$. De cualquier modo se tiene

$$\begin{aligned} \mathcal{S}(\mathbf{x}^{\mathbf{a}_j} g_j, \mathbf{x}^{\mathbf{a}_k} g_k) &= \frac{\mathbf{x}^{\mathbf{d}}}{\mathbf{x}^{\mathbf{a}_j} \text{LT}(g_j)} \mathbf{x}^{\mathbf{a}_j} g_j - \frac{\mathbf{x}^{\mathbf{d}}}{\mathbf{x}^{\mathbf{a}_k} \text{LT}(g_k)} \mathbf{x}^{\mathbf{a}_k} g_k = \\ &= \mathbf{x}^{\mathbf{d} - \gamma_{jk}} \mathcal{S}(g_j, g_k), \end{aligned}$$

donde $\mathbf{x}^{\gamma_{jk}} = \text{MCM}(\text{LM}(g_i), \text{LM}(g_k))$. Entonces existen constantes $c_{jk} \in$ tales que

$$\sum_{m(i)=\mathbf{d}} \text{LT}(h_i) g_i = \sum_{j,k} c_{jk} \mathbf{x}^{\mathbf{d} - \gamma_{jk}} \mathcal{S}(g_j, g_k). \qquad (1.6)$$

Por hipótesis tenemos que el residuo de $\mathcal{S}(g_j, g_k)$ entre $g_1, \ldots, g_s$ es cero. Usando el algoritmo de la división, esto nos dice que cada $\mathcal{S}-$polinomio puede ser escrito de la

forma

$$\mathcal{S}(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{1.7}$$

con $a_{ijk} \in \ [x_1, \ldots, x_n]$. El algoritmo de la división también nos dice que

$$\text{MGRAD}(a_{ijk} g_i) \leq \text{MGRAD}(\mathcal{S}(g_j, g_k)) \quad \forall\ i,\ j,\ k. \tag{1.8}$$

Intuitivamente esto nos está diciendo que cuando el residuo es cero, podemos encontrar una expresión para $\mathcal{S}(g_j, g_k)$ en términos de G donde no todos los términos iniciales se cancelan.

Para explotar esto, multipliquemos (1.7) por $\mathbf{x}^{\mathbf{d}-\gamma_{jk}}$ para obtener

$$\mathbf{x}^{\mathbf{d}-\gamma_{jk}} \mathcal{S}(g_j,\ g_k) = \sum_{i=1}^{t} b_{ijk} g_i,$$

donde $b_{ijk} = \mathbf{x}^{\mathbf{d}-\gamma_{jk}} a_{ijk}$. Entonces la ecuación (1.8) y el Lema 1.4.1 nos ayudan a deducir que

$$\text{MGRAD}(b_{ijk} g_i) \leq \text{MGRAD}(\mathbf{x}^{\mathbf{d}-\gamma_{jk}} \mathcal{S}(g_j,\ g_k)) < \mathbf{d}. \tag{1.9}$$

Si substituimos la expresión de arriba en (1.6), obtenemos

$$\sum_{m(i)=\mathbf{d}} \text{LT}(h_i) g_i = \sum_{j,k} c_{jk} \mathbf{x}^{\mathbf{d}-\gamma_{jk}} \mathcal{S}(g_j, g_k) = \sum_{j,k} c_{jk} \left(\sum_i b_{ijk} g_i \right) = \sum_i \widetilde{h}_i g_i$$

que por (1.9) tienen la propiedad de que para toda i,

$$\text{MGRAD}(\widetilde{h}_i g_i) < \mathbf{d}.$$

Por último, substituimos

$$\sum_{m(i)=\mathbf{d}} \text{LT}(h_i) g_i = \sum_i \widetilde{h}_i g_i$$

en la ecuación (1.5), y obtenemos una expresión para f en términos de las g_i en la que *todos* los sumandos tienen multigrado $< \mathbf{d}$. Esto contradice la minimalidad de $\mathbf{d}$, y completa nuestra prueba.

■

Para ejemplificar el uso del Teorema 1.4.3, considere el ideal $I = \langle y - x^2, z - x^4 \rangle$ en $\mathbb{R}[x, y, z]$. Afirmamos que $G = \{y - x^2, z - x^3\}$ es una base de Gröbner usando el orden lexicográfico, con $y > z > x$. Para mostrar esto, considere el $\mathcal{S}-$polinomio

$$\mathcal{S}(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Usando el algoritmo de la división, encontramos

$$-zx^2 + yx^3 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0.$$

Así, obtenemos $\overline{\mathcal{S}(y - x^2, z - x^3)}^{G} = 0$, y por el Teorema 1.4.3, G es una base de Gröbner para I. Inclusive no es difícil mostrar que G *no* es una base de Gröbner si usamos el orden lexicográfico con $x > y > z$.

1.5. Algoritmo de Buchberger

En la Sección 1.4 vimos que todo ideal no nulo en $[x_1, \ldots, x_n]$ tiene una base de Gröbner. Desafortunadamente, la prueba de este hecho no fue constructiva, en el sentido de que no nos dice la manera en que podemos calcular una base de Gröbner. Así es que ahora nos planteamos la siguiente pregunta: dado un ideal $I \subset [x_1, \ldots, x_n]$, ¿cómo podemos construir una base de Gröbner para I? Para ver las ideas principales detrás del método al que vamos a recurrir al Ejemplo 1.4.1 visto en la Sección 1.4.

Ejemplo 1.5.1. Considere el anillo $[x, y]$ con el orden $>_{grlex}$, y sea $I = \langle f_1, f_2 \rangle$, donde $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$. Recordemos que $\{f_1, f_2\}$ no es una base de Gröbner para I, puesto que $\text{LT}(\mathcal{S}(f_1, f_2)) = -x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$.

Para producir una base de Gröbner, una idea natural es tratar primero de extender el conjunto original de generadores a una base de Gröbner agregando más polinomios de I.

La pregunta que surge ahora es, ¿cuáles nuevos generadores debemos agregar? Por lo que hemos dicho acerca de $\mathcal{S}-$polinomios en la Sección 1.4, lo siguiente no debe extrañarnos. Tenemos que $\mathcal{S}(f_1, f_2) = -x^2 \in I$, y su residuo al dividirlo entre $F = (f_1, f_2)$ es $-x^2$, que es un monomio no cero. Entonces, debemos incluir el residuo en nuestro conjunto de generadores, como un nuevo generador $f_3 = -x^2$. Si llamamos $F = (f_1, f_2, f_3)$, podemos usar el Teorema 1.4.3 para probar si nuestro nuevo conjunto es una base de Gröbner para I. Así es que calculamos

$$\begin{aligned}
\mathcal{S}(f_1, f_2) &= f_3, \quad \text{así que} \\
\overline{\mathcal{S}(f_1, f_2)}^F &= 0, \\
\mathcal{S}(f_1, f_3) &= (x^3 - 2xy) - (-x)(-x^2) = -2xy, \quad \text{pero} \\
\overline{\mathcal{S}(f_1, f_3)}^F &= -2xy \neq 0.
\end{aligned}$$

Entonces, debemos agregar $f_4 = -2xy$ a nuestro conjunto de generadores. Si hacemos $F = (f_1, f_2, f_3, f_4)$, entonces

$$\begin{aligned}
\overline{\mathcal{S}(f_1, f_2)}^F &= \overline{\mathcal{S}(f_1, f_3)}^F = 0, \\
\mathcal{S}(f_1, f_4) &= y(x^3 - 2xy) - (-1/2)x^2(-2xy) = -2xy = yf_4, \quad \text{así} \\
\overline{\mathcal{S}(f_1, f_4)}^F &= 0, \\
\mathcal{S}(f_2, f_3) &= (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \quad \text{pero} \\
\overline{\mathcal{S}(f_2, f_3)}^F &= -2y^2 + x \neq 0.
\end{aligned}$$

Entonces, también debemos agregar $f_5 = -2y^2 + x$ dentro de nuestro conjunto de generadores. Haciendo $F = (f_1, f_2, f_3, f_4, f_5)$, podemos verificar que

$$\overline{\mathcal{S}(f_i, f_j)}^F = 0 \quad \text{para toda} \quad 1 \leq i \leq j \leq 5.$$

Por el Teorema 1.4.3, se sigue que una base de Gröbner con $>_{grlex}$ para I está dada por

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}. \qquad \diamondsuit$$

El ejemplo previo nos sugiere que, en general, debemos tratar de extender una base F a una base de Gröbner añadiéndole sucesivamente a F los residuos no nulos de la forma $\overline{\mathcal{S}(f_i,\, f_j)}^{F}$. Esta idea es una consecuencia directa del Primer Criterio de Buchberger (Teorema 1.4.3), y nos motiva a definir el siguiente algoritmo creado por Buchberger para calcular bases de Gröbner.

Teorema 1.5.1 (**Algoritmo de Buchberger**). *Sea $I = \langle f_1, \ldots, f_s\rangle \neq \{0\}$ un ideal polinomial. Entonces una base de Gröbner para I puede ser construida en un número finito de pasos por el siguiente algoritmo:*

Algoritmo 1.2. Dado un ideal polinomial I generado por $\{f_1, ldots, f_s\}$, obtenemos una base de Gröbner para I haciendo los siguientes pasos.

Input: $F = (f_1, \ldots,\, f_s)$
Output: una base de Gröbner $G = (g_1, \ldots,\, g_t)$ *para* I, *con* $F \subset G$

$G := F$
REPEAT
  $G' := G$
  FOR each pair $\{p, q\}$, $p \neq q$ *in* G' *DO*
    $S := \overline{\mathcal{S}(p,\, q)}^{G'}$
    IF $S \neq 0$ *THEN* $G := G \cup \{S\}$
UNTIL $G = G'$

Demostración. Comenzaremos por definir una notación usada frecuentemente. Si $G = \{g_1, \ldots, g_s\}$, entonces $\langle G\rangle$ denotará al ideal $\langle g_1, \ldots, g_s\rangle$, y $in(G)$ al ideal $\langle \text{LT}(g_1), \ldots, \text{LT}(g_s)\rangle$.

Ahora, volviendo con la demostración del teorema, primero vamos a mostrar que $G \subset I$ se cumple en todos los pasos del algoritmo. Esto es cierto en un principio, y cada que hacemos crecer a G, lo hacemos añadiendo el residuo $\mathcal{S} = \overline{\mathcal{S}(p,\, q)}^{G'}$ para $p, q \in G$. Así, si $G \subset I$, entonces tanto p, q, como $\mathcal{S}(p,\, q)$ están en I, y dado que estamos dividiendo entre $G' \subset I$, obtenemos que $G \cup \{\mathcal{S}\} \subset I$. También observamos que G contiene a la base dada F de I, por lo que G es también una base de I.

El algoritmo termina cuando $G = G'$, lo que significa que $\overline{\mathcal{S}(p,\, q)}^{G'} = 0$ para toda p, $q \in G$. Entonces G es una base de Gröbner para $\langle G\rangle = I$ por el Teorema 1.4.3.

Sólo nos resta probar que el algoritmo termina. Para esto necesitamos considerar lo que pasa después de cada paso a través del ciclo principal. El conjunto G consiste de G' (el antiguo G) junto con los residuos no cero de $\mathcal{S}-$polinomios de elementos de G'. Entonces

$$in(G') \subset in(G) \tag{1.10}$$

puesto que $G' \subset G$. Más aún, si $G' \neq G$, afirmamos que $in(G')$ está estrictamente contenido en $in(G)$. Para ver esto, supóngase que le hemos agregado a G un residuo no cero r de un $\mathcal{S}-$polinomio. Dado que r es un residuo en la división entre G', entonces $\text{LT}(r)$ no es divisible

entre ninguno de los términos iniciales de los elementos de G', y por tanto $\text{LT}(r) \notin in(G')$. Pero $\text{LT}(r) \in in(G)$, lo que prueba nuestra afirmación.

De la ecuación (1.10), tenemos que los ideales $in(G')$ provenientes de iterar sucesivamente el ciclo, forman una cadena ascendente de ideales en $[x_1, \ldots, x_n]$. Entonces la condición de cadena ascendente para anillos artinianos implica que después de un número finito de iteraciones, la cadena se estabiliza, por lo que eventualmente debe ocurrir $in(G') = in(G)$. Por lo dicho en el párrafo anterior, esto implica que $G' = G$, por lo tanto, el algoritmo debe terminar después de un número finito de pasos. ■

Es necesario señalar que el Algoritmo 1.2 que presentamos en el Teorema 1.5.1 es una versión un tanto rudimentaria del algoritmo de Buchberger. Escogimos esta versión para entenderlo de una manera más clara, pero no es una manera muy práctica para implementarlo en lenguaje de programación. Obsérvese (como una primera optimización) que una vez que un residuo $\overline{\mathcal{S}(p,\, q)}^{G'} = 0$, este residuo permanece nulo inclusive si le añadimos más elementos al conjunto generador G'. Por lo que no hay necesidad de recalcular estos residuos en los pasos subsecuentes en el ciclo principal del algoritmo. De hecho, si agregamos nuestros nuevos generadores f_j de uno en uno, los únicos residuos que necesitan ser verificados son los $\overline{\mathcal{S}(f_i, f_j)}^{G'}$, para $i \leq j - 1$.

Es común que las bases de Gröbner calculadas a partir del Algoritmo 1.2 sean más grandes de lo necesario. Podemos eliminar algunos generadores no necesarios utilizando el siguiente hecho.

Lema 1.5.1. *Sea G una base de Gröbner para el ideal polinomial I. Sea $p \in G$ un polinomio tal que $\text{LT}(p) \in in(G - \{p\})$. Entonces $G - \{p\}$ es también una base de Gröbner para I.*

Demostración. Sabemos que $in(G) = in(I)$. Si $\text{LT}(p) \in in(G - \{p\})$, entonces $\text{LT}(G - \{p\}) = \text{LT}(G)$. De la definición, se sigue que $G - \{p\}$ es también una base de Gröbner para I. ■

Ajustando constantes para hacer todos los coeficientes 1 y quitando de G cualquier p tal que $\text{LT}(p) \in in(G - \{p\})$, llegamos a la siguiente definición.

Definición 1.5.1. Una *base de Gröbner mínima* para un ideal polinomial I, es una base de Gröbner G de I tal que:

(i) $\text{LC}(p) = 1$ para todo $p \in G$.

(ii) Para todo $p \in G$, se tiene $\text{LT}(p) \notin in(G - \{p\})$.

A continuación daremos una propiedad de las bases de Gröbner mínimas.

Proposición 1.5.1. *Sean G y $\widetilde{G}$ bases de Gröbner mínimas para un ideal monomial I, para un orden monomial fijo. Entonces $\text{LT}(G) = \text{LT}(\widetilde{G})$. Más aun, G y $\widetilde{G}$ tienen el mismo número de elementos.*

Demostración. Sean $G = \{g_1, \ldots, g_n\}$ y $\widetilde{G} = \{\widetilde{g}_1, \ldots, \widetilde{g}_m\}$ bases de Gröbner mínimas. Observemos que para toda i se tiene $\text{LT}(g_i) \in in(G) = \langle \text{LT}(G) \rangle = in(I) = \langle \text{LT}(\widetilde{G}) \rangle$. Por lo tanto, tenemos la siguiente expresión

$$\text{LT}(g_i) = \sum_{j=1}^{m} c_j \text{LT}(\widetilde{g}_j), \tag{1.11}$$

por la minimalidad de $\widetilde{G}$ tenemos que $\text{LT}(\widetilde{g}_j) \notin in(\widetilde{G} - \{\widetilde{g}_j\})$ para toda j, de aquí que $\text{LT}(\widetilde{g}_j) \neq \text{LT}(\widetilde{g}_k)$ para toda $k \neq j$. Al ser $\text{LT}(g_i)$ un monomio, entonces debemos tener que (1.11) realmente es así

$$\text{LT}(g_i) = c_j \text{LT}(\widetilde{g}_j) \quad \text{para alguna } j,$$

y como $\text{LC}(g_i) = 1 = \text{LC}(\widetilde{g}_j)$, entonces $c_j = 1$, por lo que $\text{LT}(g_i) = \text{LT}(\widetilde{g}_j)$, lo que da la biyección entre $\text{LT}(G)$ y $\text{LT}(\widetilde{G})$.

Falta ver que G y $\widetilde{G}$ tienen el mismo número de elementos. Para esto vamos a dar una correspondencia biyectiva. A cada $g_i \in G$ le hacemos corresponder $\widetilde{g}_j \in \widetilde{G}$ tal que $\text{LT}(g_i) = \text{LT}(\widetilde{g}_j)$. Es claro que esta correspondencia es suprayectiva, pues $\text{LT}(G) = \text{LT}(\widetilde{G})$. Ahora, si $\widetilde{g}_j$ y $\widetilde{g}_k$ son tales que $\text{LT}(\widetilde{g}_j) = \text{LT}(g_i) = \text{LT}(\widetilde{g}_j)$, entonces, al ser $\widetilde{G}$ una base de Gröbner mínima, entonces esto forza a que $\widetilde{g}_k = \widetilde{g}_j$ (esta igualdad es del polinomio $\widetilde{g}_j$ asignado a g_i, y no una igualdad entre polinomios), pues de lo contrario se tendría que $\text{LT}(\widetilde{g}_k) \in in(\widetilde{G} - \{\widetilde{g}_k\})$. Esto contradice la minimalidad de $\widetilde{G}$, por lo que la correspondencia es inyectiva, y por ende, también biyectiva.

■

Dado un ideal no nulo, podemos construir bases de Gröbner mínimas simplemente aplicando el Algoritmo 1.2, y luego usando el Lema 1.5.1 para eliminar todos los generadores innecesarios que fueran incluidos. Para ilustrar este proceso, volvemos al ideal I estudiado en el Ejemplo 1.5.1. Usando el orden $>_{grlex}$, habíamos encontrado una base de Gröbner

$$\begin{aligned} f_1 &= x^3 - 2xy, \\ f_2 &= x^2y - 2y^2 + x, \\ f_3 &= -x^2, \\ f_4 &= -2xy, \\ f_5 &= -2y^2 + x. \end{aligned}$$

Como algunos de los coeficientes iniciales son distintos a 1, el primer paso será multiplicar los generadores por constantes convenientes para hacerlos mónicos. Después observemos que $\text{LT}(f_1) = x^3 = -x \cdot \text{LT}(f_3)$. Por el Lema 1.5.1, podemos omitir a f_1 de la base de Gröbner para hacerla mínima. Análogamente, dado que $\text{LT}(f_2) = x^2y = -(1/2)x \cdot \text{LT}(f_4)$, también podemos eliminar f_2. Ya no hay más casos donde el término inicial de un generador divida al término inicial de otro generador. Entonces,

$$\widetilde{f}_3 = x^2, \qquad \widetilde{f}_4 = xy, \qquad \widetilde{f}_5 = y^2 - (1/2)x$$

es una base de Gröbner mínima para I.

Desafortunadamente, un ideal dado puede tener más de una base de Gröbner mínima. Por ejemplo, en el ideal I recién considerado, es fácil ver que

$$\widehat{f}_3 = x^2 + axy, \qquad \widehat{f}_4 = xy, \qquad \widehat{f}_5 = y^2 - (1/2)x \tag{1.12}$$

es también una base de Gröbner mínima, donde $a \in$ es cualquier constante. Entonces, podemos producir una infinidad de bases de Gröbner mínimas (suponiendo que es infinito). Afortunadamente, podemos distinguir una base de Gröbner mínima que será la mejor a comparación de las otras. La definición es la siguiente.

Definición 1.5.2. Una *base de Gröbner reducida* para un ideal polinomial I, es una base de Gröbner G para I, tal que:

(i) $\text{LC}(p) = 1$ para todo $p \in G$.

(ii) Para todo $p \in G$, ningún término de p está en $in(G - \{p\})$.

Obsérvese que para la base de Gröbner dada en (1.12), solamente cuando $a = 0$ nos queda una base reducida. En general, las bases de Gröbner reducidas tienen la siguiente propiedad.

Proposición 1.5.2. *Sea $I \neq \{0\}$ un ideal polinomial. Entonces, para un orden monomial dado, I tiene una única base de Gröbner reducida.*

Demostración. Sea G una base de Gröbner mínima para I. Decimos que $g \in G$ es *reducido para* G, significando que ningún monomio de g está en $in(G - \{g\})$. Nuestro objetivo es modificar G hasta que todos sus elementos sean reducidos.

Una primera observación un tanto obvia es que si g es reducido para G, entonces g es también reducido para cualquier otra base de Gröbner mínima de I que contenga a g y tenga el mismo conjunto de términos iniciales.

Luego, dado $g \in G$, sea $g' = \overline{g}^{G-\{g\}}$ y sea $G' = (G - \{g\}) \cup \{g'\}$. Afirmamos que G' es una base de Gröbner mínima para I. Para ver esto, primero note que $\text{LT}(g') = \text{LT}(g)$, puesto que cuando dividimos g entre $G - \{g\}$, justamente $\text{LT}(g)$ va al residuo, pues por la minimalidad de G se tiene que $\text{LT}(g)$ no es divisible por ningún elemento de $\text{LT}(G - \{g\})$. Esto muestra que $in(G') = in(G)$. Puesto que G' claramente está contenido en I, vemos que G' es una base de Gröbner mínima, y por la construcción, g' es reducido para G'.

Ahora, tómese los elementos de G y aplíquese el proceso anterior hasta que todos los elementos sean reducidos. La base de Gröbner debe cambiar cada vez que hacemos el proceso, pero nuestra observación previa muestra que una vez que un elemento es reducido, este permanece reducido puesto que nunca cambiamos el término inicial. Así es que terminamos con una base de Gröbner reducida.

Finalmente, para probar la unicidad, supóngase que G y $\widetilde{G}$ son bases de Gröbner reducidas para I. Entonces, en particular, G y $\widetilde{G}$ son bases de Gröbner mínimas, y gracias a la Proposición 1.5.1, tenemos que ambas tienen los mismos términos iniciales, es decir,

$$\text{LT}(G) = \text{LT}(\widetilde{G}).$$

Entonces, dado $g \in G$, existe $\widetilde{g} \in \widetilde{G}$ tal que $\text{LT}(g) = \text{LT}(\widetilde{g})$. Si podemos probar que $g = \widetilde{g}$, se seguirá que $G = \widetilde{G}$, y quedará probada la unicidad.

Para mostrar que $g = \widetilde{g}$, considérese $g - \widetilde{g}$. Esto está en I, y dado que G es una base de Gröbner, se sigue que $\overline{g - \widetilde{g}}^G = 0$. Pero también sabemos que $\text{LT}(g) = \text{LT}(\widetilde{g})$. Entonces estos términos se cancelan en $g - \widetilde{g}$, y los términos sobrevivientes no son divisibles entre ninguno de los $\text{LT}(G) = \text{LT}(\widetilde{G})$, puesto que G y $\widetilde{G}$ son reducidas. Esto muestra que $\overline{g - \widetilde{g}}^G = g - \widetilde{g}$, y entonces $g - \widetilde{g} = 0$. Esto completa la prueba. ■

Muchos sistemas de algebra computacional utilizan alguna versión del algoritmo de Buchberger para calcular bases de Gröbner. Estos sistemas siempre calculan bases de Gröbner cuyos elementos son múltiplos escalares de elementos de una base de Gröbner reducida. Esto significa que distintos sistemas darán esencialmente la misma respuesta para un problema dado.

Capítulo 2

Sizigias

Una resolución libre es un invariante asociado a un módulo graduado sobre un anillo graduado por los números naturales $\mathbb{N}$ o por $\mathbb{N}^n$. En este capítulo estudiaremos resoluciones libres mínimas de módulos graduados finitamente generados para el caso en que el anillo es el anillo de polinomios $S = \ [x_1, \ldots, x_n]$ sobre un campo $\ $, graduado por $\mathbb{N}$ con cada variable de grado 1. La información provista por las resoluciones libres es un refinamiento de la información que proveen los polinomios de Hilbert y las funciones de Hilbert. En este capítulo definiremos todos estos objetos y explicaremos las relaciones entre ellos.

2.1. Funciones y polinomios de Hilbert

En la segunda mitad del siglo diecinueve, la teoría de invariantes se colocó en el centro de estudio del álgebra. Se originó en un deseo por definir propiedades de una ecuación, o de una curva definida a su vez por una ecuación, que fuera invariante bajo algún conjunto de transformaciones geométricas definido y que pudiera ser expresado en términos de una función polinomial de los coeficientes de la ecuación. El ejemplo clásico es el discriminante de un polinomio en una variable. Es una función polinomial de los coeficientes, que no cambia bajo cambios de variable lineales, y que su anulación es la condición que determina cuando un polinomio tiene multiples raíces. Este ejemplo ha sido estudiado desde el trabajo de Leibniz: fue parte de su motivación para su invención de la notación matricial y de determinantes. El crecimiento de la geometría proyectiva compleja plana a principios del siglo diecinueve proveyó una gran cantidad nuevos ejemplos que se han vuelto importantes desde entonces.

El planteamiento general es fácil de explicar: Si un grupo G actúa por medio de transformaciones lineales en un espacio vectorial W de dimensión finita sobre un campo $\mathbb{K}$, la acción se extiende de manera única al anillo de polinomios S cuyas variables son una base de W. El problema fundamental en la teoría de invariantes era probar en casos bonitos - por ejemplo, cuando $\mathbb{K}$ es de característica cero y G es un grupo finito o un grupo especial

lineal- que el anillo de funciones invariantes S^G es finitamente generado como $\mathbb{K}-$álgebra, esto es, que cada función invariante puede ser expresada como un polinomio en un conjunto finito de generadores de funciones invariantes. Esto había sido probado, para cierto número de casos especiales, describiendo explícitamente los conjuntos finitos de generadores.

Un artículo típico del siglo diecinueve en invariantes estaba lleno de cálculos difíciles, y tenía como meta principal el calcular explícitamente un conjunto finito de invariantes que generaran todos los invariantes de una representación particular de un grupo particular. David Hilbert cambió para siempre este panorama con su trabajo, con el cual ganó por primera vez absoluto reconocimiento. Hilbert probó que el anillo de invariantes es finitamente generado para una clase amplia de grupos. Lo más sorprendente es que en su argumentación se mostraba sólo la existencia evitando los terribles cálculos. De hecho él nunca calculó ni siquiera un nuevo invariante; la idea principal de esto es lo que hoy se conoce como el *Teorema de la Base de Hilbert*, en el que se establece que submódulos de $S-$módulos finitamente generados, son a su vez finitamente generados.

Hilbert estudió las sizigias para mostrar que la función generadora de el número de invariantes de cada grado es una función racional. Él también mostró que si I es un ideal homogéneo del anillo de polinomios S, el "número de condiciones linealmente independientes para un polinomio homogéneo de grado d en S de pertenecer a I es una función polinomial en d", el ahora conocido como *polinomio de Hilbert*.

Definición 2.1.1. Sea $R = \bigoplus_{n\in\mathbb{N}} R_n$ un anillo graduado, decimos que M es un $R-$*módulo graduado*, si M es un $R-$módulo con una descomposición

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

con M_i subgrupos abelianos, y que satisfacen $R_i M_j \subset M_{i+j},\ \forall\ i, j$.

Cada elemento $x \in M$ es *homogéneo* si $x \in M_d$ para alguna d, y diremos que x es un elemento de *grado* d. Cada elemento $y \in M$ puede escribirse de manera única como suma finita $\sum_d y_d$, donde $y_d \in M_d$ para todo $d \geq 0$, y todas salvo un número finito de las y_d son 0.

Observación 2.1.1. *Recordemos que S es el anillo de polinomios $[x_1, \ldots, x_n]$, que es un anillo $\mathbb{N}^n-$graduado, sea $M = \bigoplus_{d\in\mathbb{Z}} M_d$ un $S-$módulo graduado, donde la $d-$ésima componente graduada es M_d. Si M es finitamente generado, entonces cada M_d es finitamente generado.*

Demostración. Supóngase que M es finitamente generado, pero M_s no es finitamente generado, entonces

$$\bigoplus_{s}^{\infty} M_i \subset M$$

es un submódulo que no es finitamente generado, y por tanto, M no puede ser finitamente generado. ■

La observación anterior nos motiva a la siguiente definición.

Definición 2.1.2. Sean $S = [x_1, \ldots, x_n]$, y M un $S-$módulo graduado finitamente generado. A la función

$$H_M(d) := \dim M_d$$

se le llama *función de Hilbert de* M.

Hilbert tenía el presentimiento de que toda la información encerrada en el infinito número de valores que podía tomar la función H_M, podía ser leída a partir de sólo un número finito de estos valores, y de una manera muy sencilla. La manera en cómo lo hizo Hilbert fue comparando M con módulos libres, usando resoluciones libres, que veremos más adelante. Por ahora, enunciaremos la idea de Hilbert.

Teorema 2.1.1 (Hilbert). *Sea* $S = [x_1, \ldots, x_n]$. *Si* M *es un* $S-$*módulo graduado finitamente generado, entonces* $H_M(d)$ *coincide, para* d *suficientemente grande, con un polinomio de grado* $\leq n-1$.

Definición 2.1.3. El polinomio del Teorema 2.1.1, denotado por $P_M(d)$, es llamado *polinomio de Hilbert para* M.

Antes de demostrar el teorema, necesitamos una notación para denotar cuando hemos alterado el módulo graduado M por haber "recorrido" su graduación a lugares.

Notación 1. *Para cualquier módulo graduado* M, *denotamos por* $M(a)$ *al módulo* M *trasladado por* a*:*

$$M(a)_d = M_{a+d}$$

Muchas aplicaciones entre módulos graduados mandan el grado de uno al grado del otro con una traslación en el grado, así que podemos pensar que dichas aplicaciones son de grado 0, pero de un módulo graduado en un módulo graduado trasladado. Por ejemplo, multiplicar por un elemento homogéneo de grado 1 en un módulo M, con nuestra notación, traslada el grado de M en 1; así podemos pensar esta multiplicación como una aplicación de grado 0 que va de $M(-1)$ a M.

Cabe hacer la distinción de que cuando se está hablando de $S-$módulos libres (donde $S = [x_1, \ldots, x_n]$) generados por un elemento de grado a, se usa la notación $S(-a)$.

Vamos a usar el siguiente resultado sobre funciones valuadas en los enteros para la demostración pendiente.

Lema 2.1.1. *Sea $\mathbb{Q}[n]$ el anillo de polinomios con coeficientes racionales que toman valores enteros. Sea $F(n)$ una función definida para enteros n suficientemente grandes, y $G(n) := F(n+1) - F(n)$. Entonces $F(n) \in \mathbb{Q}[n]$ si y sólo si $G(n) \in \mathbb{Q}[n]$, y si estas condiciones se satisfacen, entonces* $\deg F = 1 + \deg G$.

Demostración. Supongamos que $F(n) \in \mathbb{Q}[n]$, entonces claramente se tiene que $G(n) \in \mathbb{Q}[n]$, pues $\mathbb{Q}[n]$ es un anillo, y $G(n)$ no es más que una suma de dos elementos en ese anillo.

Observemos ahora que

$$F(n) = F(0) + \sum_{m=o}^{n-1} G(m),$$

así, si suponemos que $G(n) \in \mathbb{Q}[n]$, entonces el mismo argumento nos dice que $F(n) \in \mathbb{Q}[n]$, pues $\mathbb{Q}[n]$ es un anillo. Como $F(0)$ nos define una función de grado menor o igual que $G(0)$, entonces $\deg F(n)$ depende sólo de los términos de grado mayor en la suma $\sum_{m=o}^{n-1} G(m)$, por lo que $\deg F(n) \geq \deg G(n-1)$. De aquí que $\deg F = 1 + \deg G$. ■

Proposición 2.1.1. *Sea $H(s) \in \mathbb{Z}$ definida para todos los números naturales s. Si la "primera diferencia" $H'(s) = H(s) - H(s-1)$ coincide con un polinomio de grado $\leq n-1$ con coeficientes racionales para $s \geq s_0$, entonces $H(s)$ coincide con un polinomio de grado $\leq n$ con coeficientes racionales para toda $s \geq s_0$.*

Demostración. Supóngase que $Q(s)$ es un polinomio de grado $\leq n-1$ con coeficientes racionales tal que $H'(s) = Q(s)$ cuando $s \geq s_0$. Para cualquier entero s definamos

$$P(s) = H(s_0) + \sum_{t=s_0+1}^{s} Q(t),$$

donde la suma es tomada sobre todos los enteros entre $s_0 + 1$ y s, ya sea si $s \leq s_0 + 1$ o si $s_0 + 1 \leq s$. Para $s \geq s_0$ tenemos que $P(s) = H(s)$. Para toda s tenemos que $P(s) - P(s-1) = Q(s)$. Se sigue que $P(s)$ es un polinomio de grado $\leq n$ con coeficientes racionales, gracias al Lema 2.1.1. ■

Ahora estamos en condiciones de demostrar el Teorema 2.1.1.

Demostración del Teorema 2.1.1. Haremos inducción respecto al número de variables. Si $n = 0$, entonces M es simplemente un espacio vectorial de dimensión finita graduado. En este caso $H_M(s) = 0$ para todas las s grandes, y este es un polinomio de grado -1.

En el caso general, si $K \subset M$ es el kernel de la multiplicación por x_n, obtenemos una sucesión exacta de espacios vectoriales graduados, con aplicaciones de grado 0:

$$0 \longrightarrow K(-1) \longrightarrow M(-1) \xrightarrow{x_n} M \xrightarrow{\phi} M/x_nM \longrightarrow 0.$$

Tomando la componente de grado s en cada término en esta sucesión exacta, tenemos que son

$$K(-1)_s = K_{s-1}, \quad M(-1)_s = M_{s-1}, \quad M_s, \quad (M/x_nM)_s,$$

con estos términos, del álgebra lineal sabemos que se cumple

$$\dim\ M_s = \dim\ \mathrm{Im}(\phi) + \dim\ \mathrm{Ker}(\phi).$$

Por ser ϕ suprayectiva, y la sucesión exacta, tenemos

$$\dim\ M_s = \dim\ (M/x_nM)_s + \dim\ \mathrm{Im}(x_n),$$

observemos que

$$\dim\ M_{s-1} = \dim\ \mathrm{Im}(x_n) + \dim\ \mathrm{Ker}(x_n),$$

lo que implica que

$$\dim\ \mathrm{Im}(x_n) = \dim\ M_{s-1} - \dim\ K_{s-1},$$

y por tanto

$$\dim\ M_s = \dim\ (M/x_nM)_s + \dim\ M_{s-1} - \dim\ K_{s-1},$$

de lo que se sigue que

$$H_M(s) - H_M(s-1) = H_{M/x_nM}(s) - H_K(s-1).$$

Ahora, observemos que tanto K, como M/x_nM son módulos finitamente generados sobre $[x_1, \ldots, x_{n-1}]$. Por hipótesis de inducción, lo términos del lado derecho de la igualdad, para una s suficientemente grande, coinciden con un polinomio de grado menor o igual que $n-2$, y por la Proposición 2.1.1 se tiene el resultado. ■

Ahora haremos un breve análisis de las propiedades que hemos observado para $S = [x_1, \ldots, x_n]$ visto como un $-$módulo graduado, en particular, veremos una generalización de la función dim que consideramos anteriormente.

Definición 2.1.4. Sea $\mathcal{C}$ una clase de $R-$módulos (R no necesariamente graduado), y sea λ una función $\lambda : \mathcal{C} \to \mathbb{Z}$. Decimos que λ es aditiva si, para cada sucesión exacta corta

$$0 \rightarrowtail M' \longrightarrow M \longrightarrow M'' \twoheadrightarrow 0$$

en la que M, M', $M'' \in \mathcal{C}$, se tiene que $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

Proposición 2.1.2. *Sea* $0 \to M_0 \to M_1 \to \cdots \to M_r \to 0$ *una sucesión exacta de* $R-$*módulos, y sea* $K_i \subset M_i$ *el kernel de cada morfismo. Supóngase que para toda* $i \in \{0, 1, \ldots, r\}$ *se tiene que* M_i, $K_i \in \mathcal{C}$. *Entonces para cada función aditiva* λ *sobre* $\mathcal{C}$ *se tiene*

$$\sum_{i=0}^{r} (-1)^i \lambda(M_i) = 0.$$

Demostración. Para la sucesión exacta dada

$$0 \to M_0 \to M_1 \to \cdots \to M_r \to 0$$

Para cada i podemos considerar las siguientes sucesiones exactas cortas

$$0 \to N_i \hookrightarrow M_i \to N_{i+1} \to 0,$$

tomando $N_0 = N_{r+1} = 0$. Si consideramos una función aditiva λ, por definición se cumple $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$, y tomando las sumas alternadas de $\lambda(M_i)$ se obtiene el resultado. ■

Basados en esto podemos hacer la siguiente definición, pero cabe observar primero que si M es un $R-$módulo graduado, entonces cada M_i es un R_0-módulo, pues estamos pensando a R como un anillo $\mathbb{N}-$graduado.

Definición 2.1.5. Sea λ una función aditiva (con valores en $\mathbb{Z}$) en la clase de todos los R_0-módulos. Definimos la *serie de Hilbert* de M (con respecto a λ) como la serie de potencias

$$H(M,t) := \sum_{d=0}^{\infty} \lambda(M_d) t^d \quad \in \mathbb{Z}[[t]].$$

Proposición 2.1.3. *Un anillo $\mathbb{N}-$graduado $R = \bigoplus_{n\geq 0} R_n$ es de Noether si y sólo si R_0 es de Noether y R es finitamente generado como anillo sobre R_0.*

Demostración.

$\Rightarrow$: Sea $R_+ = \bigoplus_{n>0} R_n$, entonces $R_0 \cong R/R_+$, como R es de Noether, entonces este cociente, es decir, R_0 también lo es. R_+ es un ideal de R, al ser R de Noether, entonces R_+ es finitamente generado, por lo que podemos suponer que está generado por elementos homogéneos $x_1, \ldots, x_s$, de grados $k_1, \ldots, k_s$ respectivamente. Sea R' el subanillo de R generado por $x_1, \ldots, x_s$ sobre R_0. Probaremos por inducción sobre n que $R_n \subset R'$ para todo $n \geq 0$. Esto es evidentemente cierto para R_0. Sea $n > 0$, y sea $y \in R_n$. Puesto que $y \in R_+$, entonces y es una combinación lineal de las x_i, sea $y = \sum_{i=1}^{s} a_i x_i$, donde $a_i \in R_{n-k_i}$ (por convenio diremos $R_m = 0$ si $m < 0$). Puesto que cada $k_i > 0$, la hipótesis de inducción muestra que cada a_i es un polinomio en las x_i con coeficientes en R_0. Por tanto lo mismo es cierto para y, por lo que $y \in R'$. Por lo tanto $R_n \subset R'$ y por tanto $R = R'$.

$\Leftarrow$: Esto se cumple en virtud del Teorema 1.4.2 (Base de Hilbert).

■

Teorema 2.1.2 (Hilbert, Serre). *Sea R un anillo de Noether graduado, y M un $R-$módulo graduado finitamente generado. Entonces la serie de Hilbert $H(M,t)$ de la Definición*

2.1.5 es una función racional en t, y puede ser escrita de la forma

$$H(M,t) = \frac{f(t)}{\prod_{i=1}^{r}(1-t^{k_i})},$$

donde $f(t) \in \mathbb{Z}[t]$.

Demostración. Primero observemos que por la Proposición 2.1.3, se tiene que si R es un anillo de Noether graduado, entonces es finitamente generado.

La demostración la haremos por inducción sobre r, el número de generadores de R. Cuando $r = 0$, tenemos que $R = R_0$ que también es de Noether, por lo que para n suficientemente grande, $M_n = 0$, y la serie de potencias $H(M,t)$ resulta un polinomio. Cuando $r > 0$, la multiplicación por x_r nos define una aplicación R_0-lineal $M_n \to M_{n+k_r}$ para cada n; si denotamos por K_n y L_{n+k_r} al kernel y al cokernel, obtenemos una sucesión exacta

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{x_r} M_{n+k_r} \longrightarrow L_{n+k_r} \longrightarrow 0\ .$$

Sean $K = \bigoplus K_n$ y $L = \bigoplus L_n$. Entonces K es un submódulo de M, y $L = M/x_rM$, por lo que K y L son $R-$módulos finitos; más aún, $x_rK = x_rL = 0$, por lo que K y L pueden ser vistos como $(R/x_rR)-$módulos, y entonces podemos aplicar la hipótesis de inducción a $H(K,t)$ y $H(L,t)$. Ahora, tomando una función aditiva λ, junto con la sucesión exacta previa, obtenemos

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_r}) - \lambda(L_{n+k_r}) = 0.$$

Si multiplicamos esta última por t^{n+k_r} y sumamos sobre todas las n, obtenemos

$$t^{k_r}H(K,t) - t^{k_r}H(M,t) + H(M,t) - H(L,t) = g(t),$$

donde $g(t) \in \mathbb{Z}[t]$. Equivalentemente podemos escribir

$$(1-t^{k_r})H(M,t) = H(L,t) - t^{k_r}H(K,t) + g(t),$$

aplicando ahora la hipótesis de inducción obtenemos el resultado. ■

Recordemos que de la Definición 2.1.2, si $M = \bigoplus M_d$ es un $S-$módulo graduado, tenemos que la función de Hilbert $H_d(M) = \dim\ M_d < \infty$, entonces $\dim\ (-) : M_d \to \mathbb{Z}$ resulta ser una función positiva de $M\ \ \forall d$, esto nos motiva a las siguientes definiciones.

Definición 2.1.6. Sea $S = \ [x_1, \ldots, x_n]$, considerado como un anillo $\mathbb{N}^n-$graduado como en la Observación 1.1.1. Decimos que M es un *$S-$módulo $\mathbb{N}^n-$graduado*, si M es un $S-$módulo con una descomposición

$$M = \bigoplus_{\mathbf{b}\in\mathbb{N}^n} M_{\mathbf{b}},$$

donde $M_{\mathbf{b}}$ son subgrupos abelianos, y que satisfacen $\mathbf{x}^{\mathbf{a}}M_{\mathbf{b}} \subset M_{\mathbf{a}+\mathbf{b}}$ para todo $\mathbf{a}$, $\mathbf{b} \in \mathbb{N}^n$.

Definición 2.1.7. Sea M un $S-$módulo $\mathbb{N}^n-$graduado, la *serie de Hilbert* $\mathbb{N}^n-$*graduada* de M es la serie de potencias formal

$$H(M,\mathbf{x}) := \sum_{\mathbf{a}\in\mathbb{N}^n} H_{\mathbf{a}}(M)\cdot\mathbf{x}^{\mathbf{a}} = \sum_{\mathbf{a}\in\mathbb{N}^n} \dim\ (M_{\mathbf{a}})\cdot\mathbf{x}^{\mathbf{a}},$$

donde claramente $H(M,\mathbf{x}) \in \mathbb{Z}[[x_1,\ldots,x_n]]$.

Observemos que si consideramos las variables $x_i = t$ para toda i, entonces $H(M,\mathbf{x})$ coincide con la serie de Hilbert $H(M,t,\ldots,t)$ de la Definición 2.1.5.

Ejemplo 2.1.1. Nótese que en $\mathbb{Z}[[x_1,\ldots,x_n]]$, cada elemento de la forma $1-x_i$ es invertible, es decir, se cumple la igualdad

$$\frac{1}{1-x_i} = 1 + x_i + x_i^2 + \cdots + x_i^n + \cdots,$$

y puesto que para $S_{\mathbf{a}} = \{\mathbf{x}^{\mathbf{a}}\}$ se cumple dim $S_{\mathbf{a}} = 1$, entonces la serie de Hilbert para S misma es

$$H(S,\mathbf{x}) = \sum_{\mathbf{x}^{\mathbf{a}}\in S} \mathbf{x}^{\mathbf{a}} = \prod_{i=1}^{n} \frac{1}{1-x_i},$$

la cual es una función racional, como sabíamos por el Teorema 2.1.2.

♢

Este último ejemplo nos motiva a la siguiente observación.

Observación 2.1.2. *Recordemos que $S(-\mathbf{a})$ denota la traslación por $\mathbf{a}$ de S, o sea, al módulo libre generado por un elemento de grado $\mathbf{a}$, es decir, $S(-\mathbf{a}) \cong \langle\mathbf{x}^{\mathbf{a}}\rangle$ como módulos $\mathbb{N}^n-$graduados. La serie de Hilbert para una de dichas traslaciones de S es simplemente $\mathbf{x}^{\mathbf{a}}\cdot H(S,\mathbf{x})$, es decir,*

$$H(S(-\mathbf{a}),\mathbf{x}) = \frac{\mathbf{x}^{\mathbf{a}}}{\prod_{i=1}^{n}(1-x_i)}.$$

Así, si consideramos $I \subset$ como un ideal monomial, entonces la sere de Hilbert para el módulo S/I, no es más que la suma de todos los monomios que no están en I, es decir,

$$H(S/I,\mathbf{x}) = \sum_{\mathbf{x}^{\mathbf{a}}\notin I} \mathbf{x}^{\mathbf{a}}.$$

Si aplicamos el Teorema 2.1.2 a un módulo M de los que definimos en la Definición 2.1.6, entonces tenemos la siguiente definición.

Definición 2.1.8. Sea M un $S-$módulo $\mathbb{N}^n-$graduado. Si expresamos la serie de Hilbert para M como una función racional

$$H(M,\mathbf{x}) = \frac{\mathcal{K}(M,\mathbf{x})}{\prod_{i=1}^{n}(1-x_i)},$$

entonces al numerador $\mathcal{K}(M,\mathbf{x})$, lo llamaremos $K-$*polinomio* de M.

Con esta última definición, podemos observar que una manera de calcular la serie de Hilbert para un $S-$módulo $\mathbb{N}^n-$graduado M, puede ser mediante el cálculo del $K-$polinomio de M.

2.2. Resoluciones libres

La prueba que dimos para el Teorema 2.1.1 es muy diferente a la dada por Hilbert. En lugar de la inducción que nosotros utilizamos, él tuvo la idea de calcular $H_M(d)$ comparando M con módulos libres, y usando una resolución libre. Daremos a continuación las ideas de su prueba.

Definición 2.2.1. Sea R un anillo graduado, podemos entonces definir un $R-$*módulo libre graduado* M, como la suma directa de módulos de la forma $R(-d)$, es decir, $M = \bigoplus_{d\in\mathfrak{D}} R(-d)$

Cabe señalar que a diferencia de la definición hecha para $M(a)$ dada por la fórmula $M(a)_d = M_{a+d}$, nosotros no escribimos la misma notación para $R(-d)$, puesto que tiene una consecuencia un tanto molesta. Si escribimos $R(d)$, con el mismo significado que $M(d)$, entonces $R(d)_{-d} = R_0$, lo que implicaría que $R(d)$ tiene generadores de grado $-d$, en lugar de grado d. Es por eso que escribimos $R(-d)$ en lugar de $R(d)$.

Definición 2.2.2. Un *complejo de* $R-$*módulos* es una sucesión de módulos F_i, junto con aplicaciones $F_i \to F_{i-1}$ tales que la composición $F_{i+1} \to F_i \to F_{i-1}$ es siempre cero. La *homología* de este complejo en F_i es el módulo

$$\mathrm{Ker}(F_i \to F_{i-1})/\mathrm{Im}(F_{i+1} \to F_i).$$

Gracias a las definiciones anteriores, estamos listos para hacer una de las definiciones fundamentales de este trabajo.

Definición 2.2.3. Una *resolución libre* de un $R-$módulo M, es un complejo

$$\mathcal{F}: \ \cdots \to F_n \xrightarrow{\varphi_n} \cdots \to F_1 \xrightarrow{\varphi_1} F_0$$

de $R-$módulos libres tales que el $\mathrm{Coker}(\varphi_1) = F_0/\mathrm{Im}(\varphi_1) = M$, y $\mathcal{F}$ es exacta (a veces agregamos $\to 0$ al final de la sucesión, y decimos que $\mathcal{F}$ es exacta excepto en F_0).

Definición 2.2.4. Si para alguna $n < \infty$ se tiene que $F_{n+1} = 0$, pero $F_i \neq 0$ para toda $0 \leq i \leq n$, entonces decimos que $\mathcal{F}$ es una *resolución finita de longitud* n.

Definición 2.2.5. Diremos que una resolución $\mathcal{F}$ es una *resolución libre graduada* si R es un anillo graduado, los F_i son módulos libres graduados, y las aplicaciones φ_i son aplicaciones homogéneas de grado 0.

Por supuesto que solamente los módulos graduados pueden tener resoluciones libres graduadas.

Estamos ahora en posición para enunciar uno de los mejores resultados en algebra conmutativa en los artículos de Hilbert.

Teorema 2.2.1 (**Teorema de la sizigia de Hilbert**). *Si* $S = [x_1, \ldots, x_r]$, *entonces todo* $S-$*módulo graduado finitamente generado tiene una resolución libre graduada finita de longitud* $\leq r$, *de módulos libres finitamente generados.*

Demostración. Véase [6] Teorema 2.1, páginas 245 – 247. ■

Ahora aplicaremos este importante teorema para su propósito original.

Demostración de Hilbert del Teorema 2.1.1. Sea $S = [x_1, \ldots, x_r]$. Si $M = S(-d)$ para alguna d, entonces

$$H_{S(-d)}(a) = H_S(a+d) = \begin{pmatrix} a+d+r-1 \\ r-1 \end{pmatrix}.$$

Para ver esto, es suficiente mostrar que $H_S(d) = \binom{d+r-1}{r-1}$. Esta igualdad es probada fácilmente como sigue: Recordemos que $H_S(d) = \dim\ S_d$, por lo que hay que contar cuántos monomios mónicos de grado d hay en S, pues forman una base para S_d. Para esto, veamos que un monomio de grado d, digamos $m = x_1^{b_1} x_2^{b_2} \cdots x_r^{b_r}$, lo podemos indicar por una sucesión de los índices de sus factores, que ordenaremos de tal manera que tengamos una sucesión creciente de d enteros cada uno entre 1 y r. Para m, la sucesión estará dada como sigue

$$\underbrace{1, 1, \ldots, 1}_{b_1-\text{veces}}, \underbrace{2, 2, \ldots, 2}_{b_2-\text{veces}}, \ \ldots, \ \underbrace{r, r, \ldots, r}_{b_r-\text{veces}}.$$

Así, por ejemplo, el monomio $x_1^3 x_3^4$ lo podemos especificar conla sucesión $1, 1, 1, 3, 3, 3, 3$. Al sumar $i-1$ en el $i-$ésimo lugar de esta sucesión, obtenemos una representación única (como sucesión) del monomio m; que en nuestro ejemplo nos daría la sucesión $1, 2, 3, 6, 7, 8, 9$. Con esto, tenemos una representación para el polinomio m como un subconjunto de d elementos en el conjunto $\{1, 2, \ldots, r+d-1\}$, como hay $\binom{d+r-1}{d} = \binom{d+r-1}{r-1}$ de estos subconjuntos, entonces, ésta es la misma cantidad de monomios en S_d salvo múltiplos escalares. Por lo que $H_S(d) = \binom{d+r-1}{r-1}$.

Ya que tenemos la igualdad

$$H_{S(-d)}(a) = \binom{a+d+r-1}{r-1},$$

observemos que para $a \geq -(d+r-1)$, $H_{S(-d)}(a)$ coincide con el polinomio $Q(a)$ de grado $r-1$ dado por

$$\begin{aligned} Q(a) &= \frac{[a+(d+r-1)] \cdot [a+(d+r-2)] \cdot \cdots \cdot [a+d]}{(r-1)!} \\ &= \frac{a^{r-1}}{(r-1)!} + (\text{términos de orden inferior}). \end{aligned}$$

Si F es un módulo libre graduado finitamente generado, entonces F es una suma directa de varios $S(-d)$, así $H_F(a)$ es una suma finita de funciones de la forma $H_{R(-d)}(a)$.

El Teorema de la sizigia muestra que cualquier módulo graduado finitamente generado sobre $S = [x_1, \ldots, x_r]$ tiene una resolución libre graduada finita $\mathcal{F}$

$$\mathcal{F} : 0 \to F_r \to \cdots \to F_0 \to M \to 0.$$

Entonces

$$H_M(a) = \sum_i (-1)^i H_{F_i}(a)$$

es una combinación lineal de funciones que eventualmente son iguales a polinomios de grado $\leq r - 1$. ■

Obsérvese que esta prueba se basa en el cálculo del valor de $H_M(a)$ para todo a, no sólo para las a suficientemente grandes.

2.3. Sizigias de ideales monomiales

La palabra sizigia proviene del Griego $\sigma\upsilon\zeta\upsilon\gamma\iota\alpha$, que significa unión. El término sizigia ha sido usado como un término astronómico para la conjunción u oposición de planetas. Pero a mediados del Siglo XIX, y en particular desde el trabajo de Hilbert al final de ese siglo, el significado de la palabra tiene que ver con la solución de sistemas de ecuaciones lineales homogéneas sobre un anillo.

En esta sección analizaremos las sizigias para ideales monomiales y su relación con el algoritmo de Buchberger para mejorarlo.

La primer modificación que haremos será respecto al Teorema 1.4.3, el primer criterio de Buchberger, que dice que una base G de un ideal es una base de Gröbner cuando $\overline{\mathcal{S}(f,\, g)}^{G} = 0$ para todo $f,\, g \in G$. Como vimos en la Sección 1.5, dicho criterio es fundamental en el algoritmo de Buchberger. Entonces, una buena manera para optimizarlo es mostrando que necesitamos considerar menos $\mathcal{S}-$polinomios $\mathcal{S}(f,\, g)$.

Para identificar los $\mathcal{S}-$polinomios que podemos ignorar en el Teorema 1.4.3, necesitamos primero dar una visión más general de lo que significa tener residuo cero. La definición es la siguiente.

Definición 2.3.1. Con un orden monomial fijo, sea $G = \{g_1, \ldots, g_s\} \subset \ [x_1, \ldots, x_n]$. Dado $f \in \ [x_1, \ldots, x_n]$, decimos que f *se reduce a cero módulo* G, y escribimos

$$f \longrightarrow_G 0,$$

si f puede ser escrito en la forma

$$f = a_1 g_1 + \cdots + a_t g_t,$$

de tal manera que cada vez que $a_i g_i \neq 0$, entonces se tiene

$$\text{MGRAD}(f) \geq \text{MGRAD}(a_i g_i).$$

Para entender la relación entre la definición anterior, y el algoritmo de la división, tenemos el siguiente lema.

Lema 2.3.1. *Sea $G = (g_1, \ldots, g_s)$ un conjunto ordenado de elementos de $[x_1, \ldots, x_n]$ y fíjese $f \in \ [x_1, \ldots, x_n]$. Entonces $\overline{f}^{G} = 0$ implica $f \longrightarrow_G 0$, pero el inverso es falso en general.*

Demostración. Si $\overline{f}^{G} = 0$, entonces por el algoritmo de la división se tiene

$$f = a_1 g_1 + \cdots + a_t g_t + 0,$$

donde se cumple $\text{MGRAD}(a_i g_i) \leq \text{MGRAD}(f)$ cada que $a_i g_i \neq 0$. Esto muestra que $f \longrightarrow_G 0$. Para ver que el inverso falla, considere el ejemplo utilizado en la Observación 1.3.2, donde $f = xy^2 - x$ y $G = (xy + 1, y^2 - 1)$. El algoritmo de la división nos da

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y),$$

entonces $\overline{f}^G = -x - y \neq 0$, pero podemos escribir

$$xy^2 - x = 0 \cdot (xy + 1) + x \cdot (y^2 - 1),$$

y dado que

$$\text{MGRAD}(xy^2 - x) \geq \text{MGRAD}(x \cdot (y^2 - 1))$$

(de hecho son iguales), entonces $f \longrightarrow_G 0$. ■

Para ejemplificar cómo podemos utilizar la Definición 2.3.1, vamos a dar una versión más general del Teorema 1.4.3.

Teorema 2.3.1. *Una base $G = \{g_1, \ldots, g_s\}$ para un ideal I es una base de Gröbner si y sólo si $\mathcal{S}(g_i, g_j) \longrightarrow_G 0$ para toda $i \neq j$.*

Demostración. En el Teorema 1.4.3, dimos una demostración de este resultado, pero bajo la hipótesis de que $\overline{\mathcal{S}(g_i, g_j)}^G = 0$ para toda $i \neq j$. Pero si analizamos dicha prueba, veremos que todo lo que usamos fue que

$$\mathcal{S}(g_i, g_j) = \sum_{i=1}^{t} a_{ijk} g_i,$$

donde

$$\text{MGRAD}(a_{ijk} g_i) \leq \text{MGRAD}(\mathcal{S}(g_i, g_j))$$

(véase (1.7) y (1.8) en el Teorema 1.4.3). Esto justamente significa que $\mathcal{S}(g_i, g_j) \longrightarrow_G 0$, y de aquí el resultado.

■

Nótese que gracias al Lema 2.3.1, el Teorema 1.4.3 es un caso especial del Teorema 2.3.1, y ahora mostraremos que podemos garantizar que ciertos $\mathcal{S}-$polinomios se reducen a cero.

Proposición 2.3.1. *Dado un conjunto finito $G \subset [x_1, \ldots, x_n]$, supóngase que se tiene $f, g \in G$ tales que*

$$\text{MCM}(\text{LM}(f), \text{LM}(g)) = \text{LM}(f) \cdot \text{LM}(g),$$

es decir, que los monomios iniciales de f y g son primos relativos. Entonces $\mathcal{S}(f, g) \longrightarrow_G 0$.

Demostración. Para simplificar, supondremos que f y g han sido multiplicados por las constantes apropiadas para obtener $\text{LC}(f) = \text{LC}(g) = 1$. Escribamos $f = \text{LM}(f) + p$, $g = \text{LM}(g) + q$. Entonces, como $\text{MCM}(\text{LM}(f), \text{LM}(g)) = \text{LM}(f) \cdot \text{LM}(g)$, tenemos que

$$\begin{aligned} \mathcal{S}(f, g) &= \text{LM}(g) \cdot f - \text{LM}(f) \cdot g \\ &= (g - q) \cdot f - (f - p) \cdot g \\ &= g \cdot f - q \cdot f - g \cdot f + p \cdot g \\ &= p \cdot g - q \cdot f. \end{aligned} \tag{2.1}$$

Afirmamos que

$$\text{MGRAD}(\mathcal{S}(f, g)) = \text{máx}\{\text{MGRAD}(p \cdot g), \text{MGRAD}(q \cdot f)\}. \tag{2.2}$$

Para ver esto, observemos que en $pg - qf$, debe de suceder $\text{LM}(pg) \neq \text{LM}(qf)$, puesto que si $\text{LM}(pg) = \text{LM}(qf)$, entonces se tendría $\text{LM}(p) \cdot \text{LM}(g) = \text{LM}(q) \cdot \text{LM}(f)$, con lo que $\text{LM}(g) \mid \text{LM}(q) \cdot \text{LM}(f)$, como $\text{LM}(g)$ y $\text{LM}(f)$ son primos relativos, entonces debería tenerse $\text{LM}(g) \mid \text{LM}(q)$, pero esto es imposible pues $\text{LM}(g) > \text{LM}(q)$. Ahora, como $\text{LM}(pg) \neq \text{LM}(qf)$, entonces en $pg - qf$ no pueden cancelarse los términos iniciales, y por tanto la afirmación es cierta.

Observemos que (2.1) y (2.2) justamente muestran que $\mathcal{S}(f, g) \longrightarrow_G 0$. ■

Para ejemplificar el uso de esta proposición, sea $G = (yz + y,\ x^3 + y,\ z^4)$, y úsese $>_{grlex}$ en $[x, y, z]$. Entonces

$$\mathcal{S}(x^3 + y, z^4) \longrightarrow_G 0$$

por la Proposición 2.3.1. Sin embargo, aplicando el algoritmo de la división, es fácil verificar que

$$\mathcal{S}(x^3 + y, z^4) = yz^4 = (z^3 - z^2 + z - 1) \cdot (yz + y) + y,$$

de donde

$$\overline{\mathcal{S}(x^3 + y, z^4)}^G = y \neq 0.$$

Esto explica el por qué de la necesidad de la Definición 2.3.1: La proposición 2.3.1 es falsa si usamos la noción de residuo cero proveniente del algoritmo de la división, en lugar de la reducción a cero.

Observación 2.3.1. *La Proposición 2.3.1 nos da una versión más eficiente del Teorema 2.3.1: para probar que algo es base de Gröbner, sólo necesitamos tener* $\mathcal{S}(g_i, g_j) \longrightarrow_G 0$ *para aquellas* $i < j$*, donde* $\text{LM}(g_i)$ *y* $\text{LM}(g_j)$ *no sean primos relativos.*

Pero antes de implementar esta mejoría al algoritmo de Buchberger, vamos a explorar otra forma de mejorar el Teorema 2.3.1. La idea central será entender mejor el papel que juegan los $\mathcal{S}-$polinomios en la prueba del Teorema 1.4.3. Puesto que los $\mathcal{S}-$polinomios los construimos para cancelar términos iniciales, esto nos indica que debemos estudiar la cancelación con más generalidad. Daremos ahora la definición formal de sizigia.

Definición 2.3.2. En la Definición 2.2.3, a la imagen en F_i de el homomorfismo φ_i, le llamamos *el* $i-$*ésimo módulo de sizigias* de M.

Esta definición de sizigia puede no ser muy clara en cuanto a la manera de calcularlas. Para explicar un poco el uso, y de manera más clara también la definición de sizigia, hacemos la siguiente explicación.

En geometría algebraica sobre un campo , se estudia la geometría de las variedades a partir del estudio de las propiedades del anillo de polinomios $S = [x_1, \ldots, x_r]$, y sus

ideales. Para estudiar efectivamente los ideales es necesario también estudiar los módulos graduados, generalmente sobre S. La manera más sencilla de describir un módulo es por sus generadores y las relaciones que hay entre ellos.

Debemos pensar a un conjunto $A \subset M$ de generadores de un $S-$módulo M como una aplicación suprayectiva de un $S-$módulo libre $F = S^A$ sobre M, tal que al elemento base de F correspondiente al generador $m \in A$ lo manda al elemento $m \in M$. Sea M_1 el kernel de la aplicación $F \to M$; este conjunto es llamado *módulo de sizigias* de M correspondiente a la elección de los generadores, y una *sizigia* es un elemento de M_1, es decir, una relación lineal con coeficientes en S de los generadores escogidos. Cuando describimos a M por generadores y relaciones entre ellos, estamos escogiendo generadores para M y por tanto también generadores para el módulo de sizigias de M.

En el caso en que $r = 1$, es decir, cuando S es el anillo de polinomios en una variable, el módulo de sizigias resulta ser un módulo libre, puesto que para dominios de ideales principales, todo submódulo de un módulo libre es de nuevo libre. Pero cuando $r > 1$ debe suceder que cualquier conjunto de generadores de el módulo de sizigias tienen relaciones entre ellos. Para entender estas relaciones, seguimos el procedimiento anterior: escogemos un conjunto de generadores de las sizigias y los usamos para definir una aplicación que va de un nuevo módulo libre, digamos F_1, a M_1 sobreyectivamente; equivalentemente, tenemos una aplicación $\varphi_1 : F_1 \to F$ cuya imagen es M_1. Continuando de esta forma obtenemos una *resolución libre* de M, que como habíamos definido, es una sucesión de aplicaciones

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

donde cada F_i es un módulo libre, y cada aplicación es suprayectiva sobre el kernel de la siguiente aplicación. A la imagen M_i de φ_i es lo que definimos como el $i-$ésimo módulo de sizigias de M.

Vamos a introducir ahora la noción de una sizigia para los términos iniciales de un conjunto $F = \{f_1, \ldots, f_s\}$.

Definición 2.3.3. Sea $F = (f_1, \ldots, f_s)$. Una *sizigia* de los términos iniciales $\text{LT}(f_1), \ldots, \text{LT}(f_s)$ de F, es una $s-$ada de polinomios $\sigma = (h_1, \ldots, h_s) \in (\ [x_1, \ldots, x_n])^s = \bigoplus_{i=1}^s S\mathbf{e}_i$ (donde $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in (\ [x_1, \ldots, x_n])^s$, es la $s-$ada canónica con 1 en la $i-$ésima entrada, y 0 en las demás), tal que

$$\sum_{i=1}^{s} h_i \cdot \text{LT}(f_i) = 0.$$

Sea $\mathcal{S}(F)$ el subconjunto de $\bigoplus_{i=1}^s S\mathbf{e}_i$ que consiste de todas las sizigias de los términos iniciales de F, es decir,

$$\mathcal{S}(F) = \text{Ker}\{\bigoplus S\mathbf{e}_j \longrightarrow (\ [x_1, \ldots, x_n])^s / in(F)\}$$

es el módulo de sizigias.

Entonces una sizigia $\sigma \in \mathcal{S}(F)$ puede ser escrita como

$$\sigma = \sum_{i=1}^{s} h_i \mathbf{e}_i.$$

Para clarificar la notación de sizigia y $\mathcal{S}-$polinomios, considérese el par $\{f_i, f_j\} \subset F$ con $i < j$, y sea $\mathbf{x}^\gamma = \text{MCM}(\text{LT}(f_i), \text{LT}(f_j))$. Entonces

$$\sigma_{ij} = \frac{\mathbf{x}^\gamma}{\text{LT}(f_i)}\mathbf{e}_i - \frac{\mathbf{x}^\gamma}{\text{LT}(f_j)}\mathbf{e}_j \tag{2.3}$$

nos da una sizigia de los términos iniciales de F.

Definición 2.3.4. Un elemento $\sigma \in \mathcal{S}(F)$ es *homogéneo de multigrado* $\mathbf{a}$, con $\mathbf{a} \in \mathbb{N}^n$, si

$$\sigma = (c_1\mathbf{x}^{\mathbf{a}_1}, \ldots, c_s\mathbf{x}^{\mathbf{a}_s}),$$

donde $c_i \in$, y $\mathbf{a}_i + \text{MGRAD}(f_i) = \mathbf{a}$ cuando $c_i \neq 0$.

Es claro que la sizigia σ_{ij} definida en (2.3) es homogénea de multigrado γ. Podemos descomponer sizigias en sizigias homogéneas de la siguiente manera.

Lema 2.3.2. *Todo elemento de $\mathcal{S}(F)$ puede ser escrito de manera única como una suma de elementos homogéneos de $\mathcal{S}(F)$.*

Demostración. Sea $\sigma = (h_1, \ldots, h_s) \in \mathcal{S}(F)$. Considérese un exponente fijo $\mathbf{a} \in \mathbb{N}^n$, y sea $h_{i\mathbf{a}}$ el término de h_i (si es que hay, o cero en caso contrario) tal que $\text{MGRAD}(h_{i\mathbf{a}} \cdot f_i) = \mathbf{a}$. Entonces debemos tener

$$\sum_{i=1}^{s} h_{i\mathbf{a}}\text{LT}(f_i) = 0,$$

puesto que los $h_{i\mathbf{a}}\text{LT}(f_i)$ son los términos de multigrado $\mathbf{a}$ en la suma $\sum_{i=1}^{s} h_i\text{LT}(f_i) = 0$. Entonces

$$\sigma_{\mathbf{a}} := (h_{1\mathbf{a}}, \ldots, h_{s\mathbf{a}})$$

es un elemento homogéneo de $\mathcal{S}(F)$ de grado $\mathbf{a}$, y $\sigma = \sum_{\mathbf{a}} \sigma_{\mathbf{a}}$.

Para probar la unicidad, supongamos que $\sigma = \sum \sigma'_{\mathbf{a}}$. Consideremos i fija para cualquier grado $\mathbf{a} \in \mathbb{N}^n$, y observemos la $i-$ésima entrada de $\sigma'_{\mathbf{a}} = (h'_{1\mathbf{a}}, \ldots, h'_{s\mathbf{a}})$.

Dado que $h'_{i\mathbf{a}}$ tiene la propiedad de que $\text{MGRAD}(h'_{i\mathbf{a}} \cdot f_i) = \mathbf{a}$, y f_i es fijo, entonces

$$\text{MGRAD}(h'_{i\mathbf{a}}) = \begin{cases} \mathbf{a} - \text{MGRAD}(f_i), & \text{cuando } \text{MGRAD}(f_i) \leq \mathbf{a}; \\ 0, & \text{en otro caso.} \end{cases}$$

Tenemos entonces que

$$h_i = \sum_{\mathbf{a}} h_{i\mathbf{a}} = \sum_{\mathbf{a}} h'_{i\mathbf{a}}.$$

Como tanto $h_{i\mathbf{a}}$ como $h'_{i\mathbf{a}}$ son monomios mónicos del mismo grado, y la suma (conforme $\mathbf{a}$ corre sobre los grados) nos da un mismo polinomio h_i, entonces cada término de $\sum_{\mathbf{a}} h_{i\mathbf{a}}$ y $\sum_{\mathbf{a}} h'_{i\mathbf{a}}$ deben ser iguales, pues f_i es fija. Por lo tanto $h_{i\mathbf{a}} = h'_{i\mathbf{a}}$. Como esto es cierto para cada i, entonces $\sigma_{\mathbf{a}} = \sigma'_{\mathbf{a}}$ entrada a entrada. ■

Ahora podemos probar que las σ_{ij} forman una base para el módulo de sizigias de los términos iniciales.

Proposición 2.3.2. *Dado $F = (f_1, \ldots, f_s)$, cada sizigia $\sigma \in \mathcal{S}(F)$ puede ser escrita como*

$$\sigma = \sum_{i<j} u_{ij}\sigma_{ij},$$

con $u_{ij} \in [x_1, \ldots, x_n]$, y las sizigias σ_{ij} definidas como en (2.3).

Demostración. Gracias al Lema 2.3.2 podemos considerar a σ como homogénea de multigrado $\mathbf{a}$. Entonces σ debe tener al menos dos componentes distintas de cero, digamos $c_i\mathbf{x}^{\mathbf{a}_i}$, y $c_j\mathbf{x}^{\mathbf{a}_j}$, donde $i < j$. Entonces $\mathbf{a}_i + \text{MGRAD}(f_i) = \mathbf{a}_j + \text{MGRAD}(f_j) = \mathbf{a}$, lo que implica que $\mathbf{x}^\gamma = \text{MCM}(\text{LT}(f_i), \text{LT}(f_j))$ divide a $\mathbf{x}^{\mathbf{a}}$. Como

$$\sigma_{ij} = \frac{\mathbf{x}^\gamma}{\text{LT}(f_i)}\mathbf{e}_i - \frac{\mathbf{x}^\gamma}{\text{LT}(f_j)}\mathbf{e}_j,$$

entonces en la $i-$ésima componente de

$$\sigma - c_i \,\text{LC}(f_i)\, \mathbf{x}^{\mathbf{a}-\gamma} \cdot \sigma_{ij} \tag{2.4}$$

se tiene

$$c_i\, \mathbf{x}^{\mathbf{a}_i} - c_i\, \text{LC}(f_i)\mathbf{x}^{\mathbf{a}-\gamma}\left(\frac{\mathbf{x}^\gamma}{\text{LT}(f_i)}\right) = c_i\, \mathbf{x}^{\mathbf{a}_i} - \frac{c_i\, \mathbf{x}^{\mathbf{a}}}{\text{LM}(f_i)} = c_i\, \mathbf{x}^{\mathbf{a}_i} - c_i\, \mathbf{x}^{\mathbf{a}_i} = 0,$$

puesto que $\mathbf{x}^{\mathbf{a}}/\text{LM}(f_i) = \mathbf{x}^{\mathbf{a}_i}$, y $\mathbf{a}_i = \mathbf{a} - \text{MGRAD}(f_i)$.

Como en (2.4), la $i-$ésima componente es cero, y la otra componente que afectamos fue la $j-$ésima. Entonces, a partir de σ hemos producido una sizigia homogénea con menos componentes no cero. Continuando este proceso podemos escribir a σ como combinación lineal de las σ_{ij}, y hemos acabado. ■

Esta última proposición justifica la observación hecha antes de enunciar el Teorema 1.4.3, en la que dijimos que todas las cancelaciones pueden escribirse en términos de los $\mathcal{S}-$polinomios.

Una observación interesante es que no siempre necesitamos todas las σ_{ij} para generar el módulo de sizigias, es decir, el conjunto $\{\sigma_{ij}\}$ no siempre es un conjunto generador mínimo. Por ejemplo, sea $F = (x^2y^2 + z, xy^2 - y, x^2y + yz)$, y úsese $>_{lex}$ en $[x, y, z]$. Las tres sizigias correspondientes a los $\mathcal{S}-$polinomios son

$$\begin{aligned} \sigma_{12} &= (1, -x, 0), \\ \sigma_{13} &= (1, 0, -y), \\ \sigma_{23} &= (0, x, -y). \end{aligned}$$

Sin embargo, podemos ver que $\sigma_{23} = \sigma_{13} - \sigma_{12}$, por lo que σ_{23} es *redundante* en el sentido de que la podemos obtener a partir de una combinación lineal de σ_{12}, σ_{13}. En este caso $\{\sigma_{12}, \sigma_{13}\}$ forma una base para el módulo de sizigias. Más adelante en esta sección, daremos un método sistemático para crear bases más pequeñas de $\mathcal{S}(F)$.

Estamos listos ahora para enunciar una versión más refinada de nuestro criterio para saber cuándo un conjunto es una base de Gröbner.

Teorema 2.3.2. *Una base $G = (g_1, \ldots, g_s)$ de un ideal I es una base de Gröbner si y sólo si para cada elemento $\sigma = (h_1, \ldots, h_t)$ de una base homogénea para el módulo de sizigias $\mathcal{S}(G)$, tenemos*

$$\sigma \cdot G = \sum_{i=1}^{t} h_i g_i \longrightarrow_G 0.$$

Demostración. Vamos a usar la misma estrategia, y la misma notación, que en la demostración del Teorema 1.4.3. Vamos a empezar con $f = \sum_{i=1}^{t} h_i g_i$, donde $m(i) = \text{MGRAD}(h_i g_i)$, y $\mathbf{d} = \text{máx}\{m(i)\}$ la tomamos mínima de entre todas las maneras de escribir f en términos de $g_1, \ldots, g_s$. Como antes, necesitamos mostrar que $\text{MGRAD}(f) < \mathbf{d}$ nos lleva a una contradicción.

Sabemos que $\text{MGRAD}(f) < \mathbf{d}$ implica que $\sum_{m(i)=\mathbf{d}} \text{LT}(h_i) g_i$ tiene multigrado estrictamente menor, gracias a la ecuación (1.5) del Teorema 1.4.3. Esto significa que

$$\sum_{m(i)=\mathbf{d}} \text{LT}(h_i)\text{LT}(g_i) = 0,$$

por lo que

$$\sigma = \sum_{m(i)=\mathbf{d}} \text{LT}(h_i)\mathbf{e}_i$$

es una sizigia en $\mathcal{S}(G)$. Nótese que σ es homogénea de grado $\mathbf{d}$. Por hipótesis tenemos una base homogénea $\sigma_1, \ldots, \sigma_m$ de $\mathcal{S}(G)$ con la propiedad de que $\sigma_j \cdot G \longrightarrow_G 0$ para toda j. Podemos entonces escribir σ de la forma

$$\sigma = u_1\sigma_1 + \cdots + u_m\sigma_m. \tag{2.5}$$

Escribiendo las u_j's como sumas de términos y expandiendo, vemos que la igualdad (2.5) expresa a σ como una suma de sizigias homogéneas. Como σ es homogénea de multigrado $\mathbf{d}$, se sigue de la unicidad del Lema 2.3.2 que podemos descartar todas las sizigias que no son de multigrado $\mathbf{d}$. Entonces, en (2.5), podemos suponer que, para cada j, se tiene

$$u_j = 0, \quad \text{o bien,} \quad u_j\sigma_j \quad \text{es homogénea de multigrado } \mathbf{d}.$$

Supongamos que σ_j tiene multigrado γ_j. Si $u_j \neq 0$, entonces se sigue que u_j puede ser escrita de la forma $u_j = c_j\, \mathbf{x}^{\mathbf{d}-\gamma_j}$ para alguna $c_j \in$. Entonces, (2.5) puede reescribirse como

$$\sigma = \sum_j c_j\, \mathbf{x}^{\mathbf{d}-\gamma_j}\sigma_j,$$

donde la suma corre sobre aquellas j's en las que $u_j \neq 0$. Si tomamos el producto punto con G en cada lado de la igualdad, obtenemos

$$\sum_{m(i)=\mathbf{d}} \text{LT}(h_i)g_i \;=\; \sigma \cdot G \;=\; \sum_j c_j\, \mathbf{x}^{\mathbf{d}-\gamma_j}\sigma_j \cdot G. \tag{2.6}$$

Por hipótesis, $\sigma_j \cdot G \longrightarrow_G 0$, lo que significa que

$$\sigma_j \cdot G = \sum_{i=1}^{t} a_{ij} g_i, \tag{2.7}$$

donde

$$\text{MGRAD}(a_{ij}g_i) \leq \text{MGRAD}(\sigma_j \cdot G) \quad \forall\ i,\ j. \tag{2.8}$$

Obsérvese que (2.6), (2.7), y (2.8) son similares a las correspondientes (1.6), (1.7), y (1.8) del Teorema 1.4.3. De hecho, el resto de la prueba es idéntica a lo que hicimos en la prueba del Teorema 1.4.3. El único detalle que hay que checar es que $\mathbf{x}^{\mathbf{d}-\gamma_j}\sigma_j \cdot G$ tiene multigrado $< \mathbf{d}$.

Como para cada j, es cierto que σ_j es homogénea de multigrado γ_j, entonces

$$\sigma_j \cdot G = \sum_{i=1}^{t} a_{ij} g_i,$$

cumple con que $\text{MGRAD}(a_{ij}) + \text{MGRAD}(g_i) = \gamma_j$, pero también se tiene que

$$\sum_{i=1}^{t} a_{ij}\text{LT}(g_i) = 0,$$

por lo que $\text{MGRAD}(\sigma_j \cdot G) < \gamma_j$, pues se cancelan los términos de multigrado γ_j. Con esto, es claro que al multiplicar por $\mathbf{x}^{\mathbf{d}-\gamma_j}$ se tiene que

$$\text{MGRAD}(\mathbf{x}^{\mathbf{d}-\gamma_j}\sigma_j \cdot G) < \mathbf{d}.$$

Siguiendo la demostración del Teorema 1.4.3 completamos nuestra prueba.

■

Observemos que el Teorema 1.4.3 ya antes mencionado, es un caso particular de éste resultado. Ya que si usamos la base $\{\sigma_{ij}\}$ para las sizigias $\mathcal{S}(G)$, entonces los polinomios $\sigma_{ij} \cdot G$ a verificar son precisamente los $\mathcal{S}-$polinomios $\mathcal{S}(g_i,\, g_j)$.

Para explotar la potencia del Teorema 2.3.2, necesitamos aprender cómo construir bases más pequeñas para $\mathcal{S}(G)$. En seguida mostraremos que si empezamos con la base $\{\sigma_{ij} \mid i < j\}$, existe una manera sistemática de predecir cuando podemos suprimir elementos.

Teorema 2.3.3 (**Segundo criterio de Buchberger**). *Dado $G = (g_1, \ldots, g_s)$, supóngase que se tiene un subconjunto $\mathrm{S} \subset \{\sigma_{ij} \mid 1 \leq i < j \leq t\}$ que es una base de $\mathcal{S}(G)$. Además, supóngase que se tienen distintos elementos g_i, g_j, $g_k \in G$ tales que*

$$\textsc{lt}(g_k) \quad \textit{divide a} \quad \mathrm{MCM}(\textsc{lt}(g_i), \textsc{lt}(g_j)).$$

Si $\sigma_{ik}, \sigma_{jk} \in \mathrm{S}$, entonces $\mathrm{S} - \sigma_{ij}$ es también una base de $\mathcal{S}(G)$. (Nota: Si $i > j$, entonces tomamos $\sigma_{ij} = \sigma_{ji}$.)

Demostración. Por simplicidad, vamos a suponer que $i < j < k$. Sea

$$\mathbf{x}^{\gamma_{ij}} = \mathrm{MCM}(\textsc{lm}(g_i), \textsc{lm}(g_j)),$$

y sean $\mathbf{x}^{\gamma_{ik}}$, y $\mathbf{x}^{\gamma_{jk}}$ definidos de manera similar. Entonces nuestra hipótesis implica que tanto $\mathbf{x}^{\gamma_{ik}}$, como $\mathbf{x}^{\gamma_{jk}}$, ambos dividen a $\mathbf{x}^{\gamma_{ij}}$. Entonces se tiene

$$\begin{aligned}
\frac{\mathbf{x}^{\gamma_{ij}}}{\mathbf{x}^{\gamma_{ik}}}\,\sigma_{ik} - \frac{\mathbf{x}^{\gamma_{ij}}}{\mathbf{x}^{\gamma_{jk}}}\,\sigma_{jk} &= \frac{\mathbf{x}^{\gamma_{ij}}}{\mathbf{x}^{\gamma_{ik}}}\left(\frac{\mathbf{x}^{\gamma_{ik}}}{\mathrm{LT}(g_i)}\mathbf{e}_i - \frac{\mathbf{x}^{\gamma_{ik}}}{\mathrm{LT}(g_k)}\mathbf{e}_k\right) - \frac{\mathbf{x}^{\gamma_{ij}}}{\mathbf{x}^{\gamma_{jk}}}\left(\frac{\mathbf{x}^{\gamma_{jk}}}{\mathrm{LT}(g_j)}\mathbf{e}_j - \frac{\mathbf{x}^{\gamma_{jk}}}{\mathrm{LT}(g_k)}\mathbf{e}_k\right) \\
&= \frac{\mathbf{x}^{\gamma_{ij}}}{\mathrm{LT}(g_i)}\mathbf{e}_i - \frac{\mathbf{x}^{\gamma_{ij}}}{\mathrm{LT}(g_k)}\mathbf{e}_k - \frac{\mathbf{x}^{\gamma_{ij}}}{\mathrm{LT}(g_j)}\mathbf{e}_j + \frac{\mathbf{x}^{\gamma_{ij}}}{\mathrm{LT}(g_k)}\mathbf{e}_k \\
&= \frac{\mathbf{x}^{\gamma_{ij}}}{\mathrm{LT}(g_i)}\mathbf{e}_i - \frac{\mathbf{x}^{\gamma_{ij}}}{\mathrm{LT}(g_j)}\mathbf{e}_j \quad = \quad \sigma_{ij},
\end{aligned}$$

por lo que podemos escribir a σ_{ij} en términos de σ_{ik}, y σ_{jk}. Así, $\mathrm{S} - \sigma_{ij}$ es un conjunto generador. ■

Para incorporar el segundo criterio de Buchberger en un algoritmo para construir bases de Gröbner, vamos a usar los pares ordenados $(i,\, j)$ con $i < j$ para seguir el rastro de las sizigias que queremos conservar. Dado que algunas veces vamos a tener una $i \neq j$ donde no vamos a saber cuál de los dos índices es más grande, vamos a utilizar la siguiente notación: dada $i \neq j$, definimos

$$[i,\, j] = \begin{cases} (i,\, j) & \text{si } \; i < j \\ (j,\, i) & \text{si } \; i > j\,. \end{cases}$$

Podemos ahora establecer una versión mejorada del algoritmo de Buchberger que toma en cuenta los resultados probados hasta ahora.

Teorema 2.3.4. *Sea $I = \langle f_1, \ldots, f_s \rangle$ un ideal polinomial. Entonces una base de Gröbner para I puede ser construida en un número finito de pasos por el siguiente algoritmo:*

Algoritmo 2.1. Fíjese un ideal polinomial I generado por los polinomios $\{f_1, \ldots, f_s\}$ conservando el orden con que fueron listados.

Input: $F = (f_1, \ldots, f_s)$
Output: G, *una base de Gröbner para* $I = \langle f_1, \ldots, f_s \rangle$

{*iniciación*}
$B := \{(i,\, j) \;\mid\; 1 \le i < j \le s\}$
$G := F$
$t := s$
{*iteración*}
WHILE $B \neq \varnothing$ *DO*
Select $(i,\, j) \in B$
IF $\operatorname{MCM}(\operatorname{LT}(f_i),\, \operatorname{LT}(f_j)) \neq \operatorname{LT}(f_i) \cdot \operatorname{LT}(f_j)$ *AND*
Criterio$(f_i,\, f_j,\, B)$ *is false THEN*
$\mathcal{S} := \overline{\mathcal{S}(f_i, f_j)}^{G}$
IF $\mathcal{S} \neq 0$ *THEN*
$t := t + 1;\;\; f_t := \mathcal{S}$
$G := G \cup \{f_t\}$
$B := B \cup \{(i,\, t) \;\mid\; 1 \le i \le t - 1\}$
$B := B - \{(i,\, j)\}$.

Donde Criterio$(f_i,\, f_j,\, B)$ *es cierto si existe algún* $k \notin \{i,\, j\}$ *para el que las parejas* $[i, k]$ *y* $[j, k]$ ***no están*** *en* B, *y* $\operatorname{LT}(f_k)$ *divide a* $\operatorname{MCM}(\operatorname{LT}(f_i), \operatorname{LT}(f_j))$. *(Nótese que este criterio está basado en el Teorema 2.3.3.)*

Demostración. La idea básica del algoritmo es que B recoge sólo las parejas $(i,\, j)$ que van a ser consideradas. Más aún, el algoritmo sólo calcula el residuo de aquellos $\mathcal{S}-$polinomios $\mathcal{S}(g_i,\, g_j)$ para los cuales no se aplica ni la Proposición 2.3.1, ni el Teorema 2.3.3.

Para probar que el algoritmo funciona, primero observemos que en cada etapa del algoritmo, B tiene la propiedad de que si $1 \le i < j \le t$ y $(i,\, j) \notin B$, entonces

$$\mathcal{S}(f_i,\, f_j) \longrightarrow_G 0, \quad \text{o bien,} \quad \text{Criterio}(f_i,\, f_j,\, B) \;\; \text{es cierto.} \tag{2.9}$$

Inicialmente, esto es cierto puesto que B empieza siendo el conjunto de todos las posibles parejas. Debemos mostrar que si (2.9) es cierta para algún valor intermedio de B, entonces se mantiene cierta cuando B cambia, digamos a B'.

Para probar esto, supóngase que $(i,\, j) \notin B'$. Si $(i,\, j) \in B$, entonces una revisión del algoritmo muestra que $B' = B - \{(i, j)\}$. Ahora fijémonos en el paso antes de quitar $(i,\, j)$ de B. Si $\operatorname{MCM}(\operatorname{LT}(f_i), \operatorname{LT}(f_j)) = \operatorname{LT}(f_i) \cdot \operatorname{LT}(f_j)$, entonces $\mathcal{S}(f_i,\, f_j) \longrightarrow_G 0$ gracias a la Proposición 2.3.1, y así (2.9) es cierta. También, si Criterio$(f_i,\, f_j,\, B)$ es cierto, entonces claramente (2.9) es cierta. Ahora supóngase que cualquiera de estos dos fallan. En este caso, el algoritmo calcula el residuo $\mathcal{S} = \overline{\mathcal{S}(f_i,\, f_j)}^{G}$. Si $\mathcal{S} = 0$, entonces por el Lema2.3.1 se tiene $\mathcal{S}(f_i,\, f_j) \longrightarrow_G 0$. Finalmente, si $\mathcal{S} \neq 0$, entonces agradamos G como $G \cup \{\mathcal{S}\}$, y es claro entonces que $\mathcal{S}(f_i,\, f_j) \longrightarrow_{G'} 0$.

Nos resta analizar el caso en que $(i, j) \notin B$. Aquí, (2.9) se cumple para B, y por tanto para B'.

Ahora, necesitamos mostrar que G es una base de Gröbner cuando $B = \varnothing$. Para mostrar esto, sea t el número de elementos de G, y consideremos el conjunto $\mathcal{I}$ que consiste de todas las parejas (i, j) con $1 \leq i < j \leq t$ donde Criterio(f_i, f_j, B) es *falso* cuando (i, j) es escogido en el algoritmo. Afirmamos que $S = \{\sigma_{ij} \mid (i, j) \in \mathcal{I}\}$ es una base de $\mathcal{S}(G)$ con la propiedad de que $\sigma_{ij} \cdot G = \mathcal{S}(f_i, f_j) \longrightarrow_G 0$ para toda $\sigma_{ij} \in S$. Esta afirmación y el Teorema 2.3.2 prueban que G es una base de Gröbner.

Para probar la afirmación, obsérvese que $B = \varnothing$ implica que (2.9) es cierta para *todas* las parejas (i, j) con $1 \leq i < j \leq t$. Se sigue que $\mathcal{S}(f_i, f_j) \longrightarrow_G 0$ para toda $(i, j) \in \mathcal{I}$. Falta mostrar que S es una base de $\mathcal{S}(G)$. Para ver esto, primero nótese que podemos ordenar las parejas (i, j) de acuerdo a cuándo fueron removidas de B en el algoritmo. Ahora vayamos a través de las parejas en orden inverso, empezando con la última que se quitó, y borremos la pareja (i, j) para la cual Criterio(f_i, f_j, B) fuera cierto en el algoritmo. Después de ir a través de todas estas la parejas, sólo permanecen precisamente los elementos de $\mathcal{I}$. Vamos a mostrar que en cada paso de este proceso, las sizigias correspondientes a las parejas (i, j) sin borrar hasta el momento, forman una base de $\mathcal{S}(G)$. Esto en un principio es cierto, puesto que empezamos con todas las σ_{ij} que sabemos que son una base. Luego, si en algún punto borramos (i, j), entonces por la definición de Criterio(f_i, f_j, B) tenemos que existe una k tal que $\text{LT}(f_k)$ divide a $\text{MCM}(\text{LT}(f_i), \text{LT}(f_j))$, y $[i, k], [j, k] \notin B$. Entonces $[i, k]$ y $[j, k]$ fueron quitadas de B antes, y entonces σ_{ik} y σ_{jk} todavía están en el conjunto que estamos creando puesto que estamos yendo en orden inverso. Se sigue del Teorema 2.3.3 que seguimos teniendo una base, inclusive después de quitar σ_{ij}.

Por último, necesitamos ver que el algoritmo termina. Como en la prueba del Teorema 1.5.1, G siempre es una base de nuestro ideal, y cada vez que agrandamos G, el ideal monomial $in(G)$ se agranda estrictamente. Por la condición de cadena ascendente, se sigue que en algún punto, G debe de dejar de crecer, y entonces, eventualmente dejamos de agregar elementos a B. Dado que cada vez que pasamos por el ciclo WHILE ... DO quitamos un elemento de B, eventualmente debemos tener $B = \varnothing$, y el algoritmo termina. ■

Capítulo 3

Gráficas de Buchberger

En este capítulo utilizaremos técnicas de Geometría de cuerpos convexos, además de combinatoria y algebra, para expresar la información asociada a ideales monomiales arbitrarios. Vamos a empezar por ver los diagramas de escalera en el caso de dos y tres variables, para luego mostrar cómo las gráficas planas proveen resoluciones libres mínimas de ideales monomiales en tres variables. Para el resto de este capítulo vamos a considerar los ideales monomiales $I = \langle m_1, \ldots, m_r \rangle$ escrito de manera que ninguno de los m_i resulte redundante.

3.1. Ideales monomiales en dos variables

Cómo observamos en la primera sección del Capítulo 1 de este trabajo, del Lema 1.1.2 observamos que si $\mathbf{x^b} \in I = \langle \mathbf{x^a} \rangle_{\mathbf{a} \in A \subset \mathbb{N}^n}$, entonces se tiene $\mathbf{x^a} \mid \mathbf{x^b}$ para alguna $\mathbf{a} \in A$; esto significa que el conjunto

$$\mathbf{a} + \mathbb{N}^n = \{\mathbf{a} + \mathbf{c} \mid \mathbf{c} \in \mathbb{N}^n\}$$

consiste de los exponentes de todos los monomios divisibles por $\mathbf{x^a}$, y por tanto, el conjunto

$$A + \mathbb{N}^n = \{\mathbf{a} + \mathbf{c} \mid \mathbf{a} \in A, \mathbf{c} \in \mathbb{N}^n\}$$

consiste de los exponentes de todos los monomios en I. Vamos a estudiar la información que podemos obtener a partir de este conjunto. Primero lo haremos para el caso de ideales monomiales en dos variables.

Consideremos un monomio no nulo $m = x^a y^b \in [x, y]$. Entonces, el conjunto de exponentes de todos los múltiplos de m es

$$(a, b) + \mathbb{N}^2 = \{(a, b) + (c, d) \mid (c, d) \in \mathbb{N}^2\},$$

podemos graficar este conjunto como en la Figura 3.15.

Ahora consideremos un ideal monomial arbitrario I en el anillo de polinomios $[x, y]$. I puede ser escrito en términos de monomios generadores mínimos (en el sentido de que

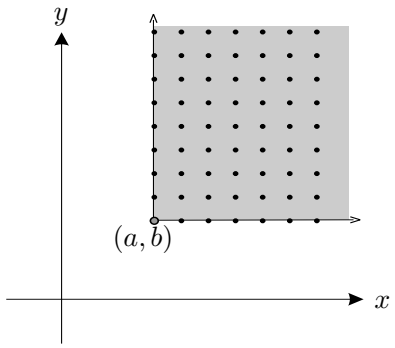

Figura 3.1: Exponentes de los múltiplos de m.

estamos considerando un conjunto mínimo de generadores de I), de la siguiente manera

$$I = \langle m_1, \ldots, m_r \rangle = \langle x^{a_1} y^{b_1}, x^{a_2} y^{b_2}, \ldots, x^{a_r} y^{b_r} \rangle,$$

con $a_1 > a_2 > \cdots > a_r \geq 0$ y $0 \leq b_1 < b_2 < \cdots < b_r$.

Esto nos permite representar al ideal I por medio de un *diagrama de escalera*, Figura 3.2, en el cual se muestra la interacción entre las regiones del plano que contienen (vectores de exponentes de) monomios que están en I, y aquellos que no caen dentro de I.

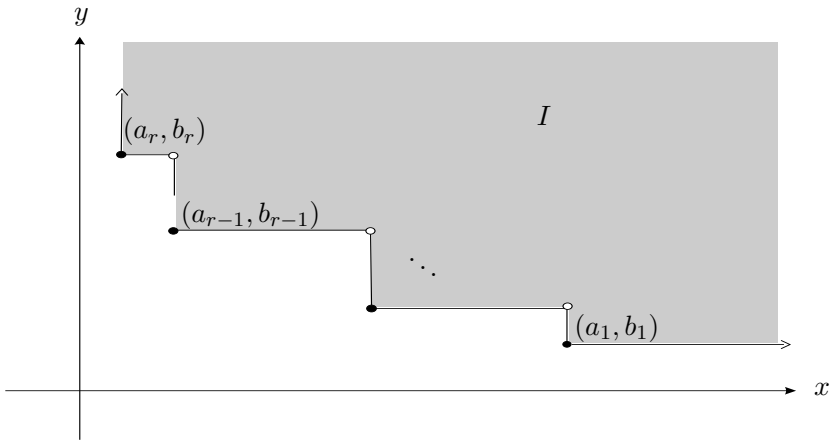

Figura 3.2: Diagrama de escalera para el ideal I.

Aclaremos que en esta figura, los puntos negros representan (los vectores exponentes de) los monomios que generan a I, mientras que los puntos blancos representan al mínimo común múltiplo de dos de estos monomios adyacentes.

Gracias a este diagrama de escalera podemos calcular, de una manera muy sencilla, el

$K-$polinomio de la Definición 2.1.8 para la serie de Hilbert $H(S/I;x,y)$ del $-$módulo S/I, como lo establece el siguiente resultado.

Proposición 3.1.1. *Sea $I = \langle m_1, \ldots, m_r\rangle$ un ideal monomial del anillo de polinomios $S = [x, y]$, si representamos el ideal I con el diagrama de escalera de la Figura 3.2, entonces el $K-$polinomio $\mathcal{K}(S/I;x,y) = 1 -$ puntos negros $+$ puntos blancos.*

Demostración. Gracias a la Observación 2.1.2, la serie de Hilbert para el $-$módulo S/I es la suma formal de todos los monomios que no están en I , y vista como función racional, tiene denominador $(1-x)(1-y)$. Para calcular el $K-$polinomio de S/I, primero vamos a calcular la serie de Hilbert, y luego multiplicarla por $(1-x)(1-y)$. Empecemos calculando $H(S/I;x,y)$, tomando la suma de todos los monomios en S,

$$\frac{1}{(1-x)(1-y)} = \sum_{\mathbf{x^a}\in S} \mathbf{x^a},$$

De esta suma debemos quitar todos los monomios que están en $I = \langle m_1, \ldots, m_r\rangle$, que son todos los monomios de los ideales principales $\langle m_i\rangle$, con lo que tenemos (haciendo abuso de la notación):

$$\sum_{\mathbf{x^a}\in S} \mathbf{x^a} - \sum_{i=1}^{r}\langle m_i\rangle = \frac{1}{(1-x)(1-y)} - \sum_{i=1}^{r}\langle m_i\rangle.$$

En esta suma están repetidos los términos que están en $\langle m_i\rangle \cap \langle m_j\rangle = \langle \text{MCM}(m_i, m_j)\rangle$. Por lo tanto, debemos sumar los ideales principales $\langle \text{MCM}(m_i,\, m_j)\rangle$, con lo que tenemos

$$\sum_{\mathbf{x^a}\in S} \mathbf{x^a} - \sum_{i=1}^{r}\langle m_i\rangle + \sum_{j<i}\langle \text{MCM}(m_i,\, m_j)\rangle =$$
$$= \frac{1}{(1-x)(1-y)} - \sum_{i=1}^{r}\langle m_i\rangle + \sum_{j<i}\langle \text{MCM}(m_i,\, m_j)\rangle,$$

Ahora notemos que en esta última expresión hay monomios que estamos agregando de más, esto quiere decir que en $\sum_{j<i}\langle \text{MCM}(m_i,\, m_j)$ estamos considerando ideales que no son necesarios, entonces es suficiente considerar los ideales de la forma $\langle \text{MCM}(m_i,\, m_{i+1})\rangle$. De esta manera tenemos

$$\begin{aligned} H(S/I;x,y) &= \sum_{\mathbf{x^a}\in S} \mathbf{x^a} - \sum_{i=1}^{r}\langle m_i\rangle + \sum_{j=1}^{r-1}\langle \text{MCM}(m_j,\, m_{j+1})\rangle \\ &= \frac{1}{(1-x)(1-y)} - \sum_{i=1}^{r}\langle m_i\rangle + \sum_{j=1}\langle \text{MCM}(m_j,\, m_{j+1})\rangle. \end{aligned}$$

Si escribimos $m_i = x^{a_i}y^{b_i}$ para $i = 1, \ldots, r$, entonces la expresión anterior podemos reescri-

birla de la siguiente manera

$$\begin{aligned} H(S/I;x,y) &= \sum_{x^{a_i}y^{b_i}\in S} x^{a_i}y^{b_i} - \sum_{i=1}^{r} x^{a_i+N}y^{b_i+M} + \sum_{j=1}^{r-1} x^{a_j+N}y^{b_{j+1}+M} \\ &= \frac{1}{(1-x)(1-y)} - \sum_{i=1}^{r} x^{a_i+N}y^{b_i+M} + \sum_{j=1}^{r-1} x^{a_j+N}y^{b_{j+1}+M}, \end{aligned}$$

con N y M corriendo sobre $\mathbb{N}$. Así, para calcular el $K-$polinomio de S/I, simplemente multiplicamos esta última expresión por $(1-x)(1-y)$, con lo que tenemos:

$$\begin{aligned} \mathcal{K}(S/I;x,y) &= (1-x)(1-y)H(S/I;x,y) \\ &= (1-x)(1-y)\sum_{x^iy^j\notin I} x^iy^j \\ &= 1 - \sum_{i=1}^{r} x^{a_i}y^{b_i} + \sum_{j=1}^{r-1} x^{a_j}y^{b_{j+1}} \\ &= 1 - \text{puntos negros} + \text{puntos blancos}. \end{aligned}$$

■

De esta última proposición podemos obtener una resolución libre mínima para S/I.

Proposición 3.1.2. *La resolución libre mínima de un ideal generado por r monomios en $S = [x,y]$ es de la forma*

$$0 \longleftarrow S \longleftarrow S^r \longleftarrow S^{r-1} \longleftarrow 0.$$

Las mínimas primeras sizigias son los vectores $y^{b_{i+1}-b_i}\mathbf{e}_i - x^{a_i-a_{i+1}}\mathbf{e}_{i+1}$ correspondientes a los pares adjacentes $\{x^{a_i}y^{b_i},\, x^{a_{i+1}}y^{b_{i+1}}\}$ de generadores mínimos para I.

Demostración. Sabemos por la Proposición 2.3.2 y por el Teorema 2.3.2 que el conjunto $\{\sigma_{ij} \mid i<j\}$, donde $\sigma_{ij} = y^{b_j-b_i}\mathbf{e}_i - x^{a_i-a_j}\mathbf{e}_j$, consituyen una base del primer módulo de sizigias. Por el segundo criterio de Buchberger (Teorema 2.3.3.), e inspeccionando el diagrama de escalera, tenemos que el subconjunto $\{\sigma_{ij} \mid j=i+1\}$ constituyen una base mínima de exactamente $r-1$ elementos.

■

La relación natural de adyacencia entre generadores mínimos de un ideal monomial en dos variables I también determina una descomposición *irredundante* de I en irreducibles. Por definición, dicha descomposición expresa a I como una intersección de ideales monomiales generados por potencias de las variables (*ideales monomiales irreducibles*), de tal manera que ningúno de los intersecandos pueden ser omitidos.

Proposición 3.1.3. *Sea $I \subset [x, y, z]$ un ideal monomial, la descomposición irredundante de I en irreducibles es*

$$I = \langle y^{b_1} \rangle \cap \langle x^{a_1}, y^{b_1} \rangle \cap \langle x^{a_2}, y^{b_3} \rangle \cap \cdots \cap \langle x^{a_{r-1}}, y^{b_r} \rangle \cap \langle x^{a_r} \rangle,$$

donde el primero o el último factor deben ser omitidos si $b_1 = 0$ o $a_1 = 0$.

Demostración. Después de remover factores comunes entre los generadores, podemos suponer que $b_1 = 0$ y $a_1 = 0$, así es que I es artiniano. Los ideales dados $\langle x^{a_i}, y^{b_{i+1}} \rangle$ son irreducibles y claramente contienen a I. Una inspección al diagrama de escalera nos muestra que cada monomio en la intersección debe estar también en I. ■

De las dos proposiciones previas correspondientes al anillo $[x, y]$, es natural preguntarse cómo puede ser generalizada la noción de monomios adyacentes en ideales monomiales en tres o más variables. Una respuesta a esto será dada en la Sección 3.3, pero antes daremos una introducción a la Teoría de Gráficas, que será un lenguaje necesario para el estudio de dicha sección.

3.2. Gráficas

En esta sección daremos algunos conceptos básicos junto con algunos resultados importantes de la Teoría de Gráficas, y muchas de las pruebas no las daremos aquí, pues sale del alcance de este trabajo, sin embargo, en todos los resultados cuyas pruebas omitamos daremos una referencia en dónde se pueda checar la prueba.

Este ápice de introducción a la basta Teoría de Gráficas es de gran importancia para familiarizarse con los términos, expresiones e ideas que aquí exponemos, pues estarán muy involucradas las gráficas en las secciones siguientes.

Definición 3.2.1. Una *gráfica* G consiste de un conjunto finito no vacío $V(G)$ de *vértices*, junto con un conjunto $E(G)$ de pares no ordenados de distintos vértices, llamados *aristas*. Si $x = \{u, v\} \in E(G)$, para $u, v \in V(G)$, decimos que u y v son vértices *adyacentes*. El *grado*, $d(v)$, de un vértice v es el número de aristas en las que v es incidente. El orden de la gráfica G es la cardinalidad de $V(G)$, es decir, $|V(G)|$.

Por conveniencia, escribiremos uv en lugar de $\{u, v\}$.

Definición 3.2.2. Una gráfica H es una *subgráfica* de una gráfica G si $V(H) \subseteq V(G)$ y $E(H) \subseteq E(G)$. Para cualquier $\varnothing \neq A \subseteq V(G)$, la *gráfica inducida* por A, denotada por $G[A]$, es la subgráfica de G en la que si $u, v \in A$, entonces $uv \in E(A)$ si y sólo si $uv \in E(G)$.

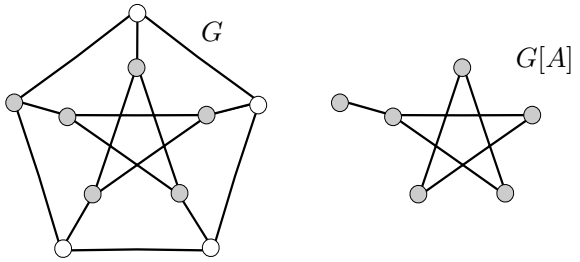

Figura 3.3: G y $G[A]$

Definición 3.2.3. Un *paseo* en una gráfica G es una sucesión alternante de vértices y aristas $v_0, x_1, v_1, \ldots, v_{n-1}, x_n, v_n$ (abreviado $v_0, v_1, \ldots, v_{n-1}, v_n$) que empieza y termina en vértices, en la que cada arista es incidente a los vértices precedente y siguiente a ella; n es la *longitud* del paseo. Si $v_0 = v_n$, decimos que el paseo es *cerrado*. Un paseo es un *camino* si todas las aristas son distintas, y es una *trayectoria* si todos los vértices son distintos. Un *ciclo* es una trayectoria cerrada.

Las trayectorias de longitud k serán denotadas por P^k, mientras que los ciclos de longitud k por C^k.

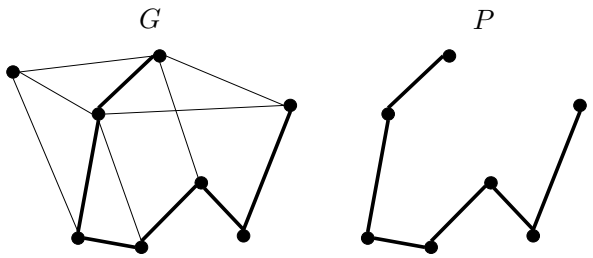

Figura 3.4: Una trayectoria $P = P^6$ en G.

Definición 3.2.4. Sea C un ciclo en una gráfica G. Una arista que une dos vértices de C pero que no está en C, se denomina *cuerda*. Así, un *ciclo inducido* en G es un ciclo que no contiene cuerdas (Figura 3.2).

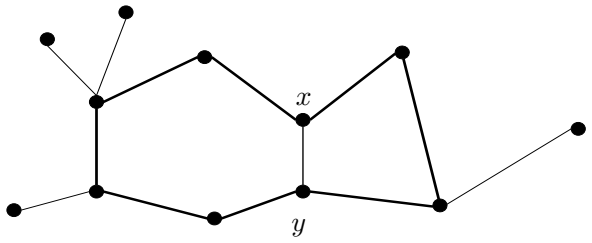

Figura 3.5: Un ciclo C^8 con cuerda xy, y ciclos inducidos C^6 y C^4.

Definición 3.2.5. Una gráfica G es *conexa* si cualesquiera dos vértices están conectados por una trayectoria en G. Una subgráfica conexa máxima de una gráfica G se llama *componente* de G.

Definición 3.2.6. Sea $G = (V, E)$ una gráfica. Si $X \subset V$ es tal que $G - X$ es disconexa, decimos entonces que X es un *separador*.

Definición 3.2.7. Una gráfica G es $k-$*conexa* (con $k \in \mathbb{N}$) si $|G| > k$ y $G - X$ es conexa para todo conjunto $X \subseteq V$ con $|V| < k$. En otras palabras, ningún par de vértices de G son separados por menos de k vértices distintos.

Así, las gráficas $1-$conexas son precisamente aquellas que habíamos definido como gráficas conexas.

Definición 3.2.8. Una gráfica $G = (V, E)$ es *bipartita* si V admite una partición en dos clases, en las que cada arista de G tiene sus extremos en clases diferentes. Vértices en la misma clase no son adyacentes. Si en una gráfica bipartita cada dos vértices de clases distintas son adyacentes, entonces decimos que es bipartita *completa*, y la denotamos por $K_{n,m}$.

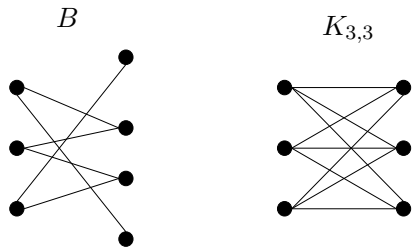

Figura 3.6: Gráfica B bipartita y gráfica bipartita completa $K_{3,3}$.

Enunciaremos ahora uno de los resultados más importantes en la teoría de gráficas.

Teorema 3.2.1 (de Menger (Versión Global))**.** *(i) Una gráfica es $k-$conexa si y sólo si contiene k trayectorias independientes entre cualesquiera dos vértices.*

(ii) Una gráfica es $k-$conexa por aristas si y sólo si contiene k trayectorias disjuntas por aristas entre cualesquiera dos vértices.

Daremos ahora las nociones básicas para trabajar con gráficas planas, para esto empezaremos con algunos pre-requisitos topológicos.

Un *segmento de línea* en $\mathbb{R}^2$ es un subconjunto de la forma $\{p + \lambda(q - p) \,|\, 0 \leq \lambda \leq 1\}$ para puntos distintos p, $q \in \mathbb{R}^2$. Un *polígono* es un subconjunto de $\mathbb{R}^2$ que es la unión de un número finito de segmentos de línea, y que es homeomorfo al círculo unitario $\mathbb{S}^1$. Un *arco poligonal* es un subconjunto de $\mathbb{R}^2$ que es la unión de un número finito de segmentos de línea y que es homeomorfo al intervalo unitario cerrado $[0, 1]$, y en ocasiones nos referiremos a este simplemente por arco. Si P es un arco entre x y y, entonces denotamos al conjunto de puntos $P \setminus \{x, y\}$, el *interior* de P, por $\overset{\circ}{P}$.

Sea $O \subseteq \mathbb{R}^2$ un conjunto abierto. Que dos puntos de O estén ligados por un arco define una relación de equivalencia en O. Las correspondientes clases de equivalencia son también abiertas; estas son las *regiones* de O. Un conjunto cerrado $X \subseteq \mathbb{R}^2$ se dice que separa a O si $O \setminus X$ tiene más de una región.

Teorema 3.2.2 (**de la curva de Jordan para polígonos**)**.** *Para todo polígono $P \subseteq \mathbb{R}^2$, el conjunto $\mathbb{R}^2 \setminus P$ tiene exactamente dos regiones, cada una de estas tiene a todo el polígono P como su frontera.*

Con la ayuda de el Teorema 3.2.2, no es difícil probar el siguiente lema.

Lema 3.2.1. *Sean x, y dos puntos, y P_1, P_2, P_3 tres arcos entre x y y que son disjuntos (salvo en x y y obviamente).*

(i) $\mathbb{R}^2 \setminus (P_1 \cup P_2 \cup P_3)$ *tiene exactamente tres regiones, con fronteras $P_1 \cup P_2$, $P_2 \cup P_3$ y $P_1 \cup P_3$.*

(ii) Si P es un arco entre un punto en $\overset{\circ}{P}_1$ y un punto en $\overset{\circ}{P}_3$ cuyo interior cae en la región de $\mathbb{R}^2 \setminus (P_1 \cup P_3)$ que contiene a P_2, entonces $\overset{\circ}{P} \cap \overset{\circ}{P}_2 \neq \varnothing$.

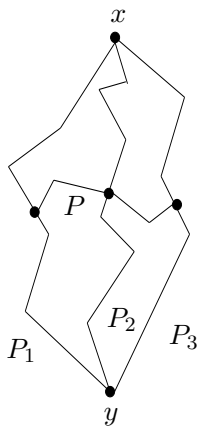

Figura 3.7: Los arcos del Lema 3.2.1(ii).

Ahora estamos en posición de definir una gráfica plana.

Definición 3.2.9. Una gráfica $G = (V, E)$ se dice que es *plana*, si G admite una inmersión en el plano tal que:

(i) $V \subset \mathbb{R}^2$;

(ii) toda arista de G es un arco entre dos vértices en la inmersión;

(iii) aristas diferentes tienen vértices extremos diferentes;

(iv) el interior de una arista en la inmersión no contiene ni vértices ni puntos de otros arcos.

Para toda gráfica plana G, el conjunto $\mathbb{R}^2 \setminus G$ es abierto, cuyas regiones llamaremos *caras* de G. Dado que G siempre es un conjunto acotado (en el sentido de estar contenido dentro de un disco suficientemente grande $\mathbb{D}$), exactamente una de sus caras es no acotada, la que contiene a $\mathbb{R}^2 \setminus \mathbb{D}$; llamamos a esta cara la *cara exterior* de G, y a las demás las *caras interiores*.

Tenemos el siguiente lema que establece algunas propiedades intuitivas de una gráfica plana.

Lema 3.2.2. *Sea G una gráfica plana y e una arista de G.*

(i) Si X es la frontera de una cara de G, entonces $e \subset X$, o bien $X \cap \overset{\circ}{e} = \varnothing$.

(ii) *Si e está en un ciclo $C \subseteq G$, entonces e está en la frontera de exactamente dos caras de G, y estas están contenidas en distintas caras de C.*

(iii) *Si e no está en un ciclo, entonces e está en la frontera de exactamente una cara de G.*

Demostración. Ver [7] página 87. ■

Proposición 3.2.1. *En una gráfica plana $2-$conexa, toda cara está acotada por un ciclo.*

Demostración. Ver [7] página 89. ■

En una gráfica $3-$conexa podemos identificar las fronteras de las caras de entre los otros ciclos en términos puramente combinatóricos.

Proposición 3.2.2. *Las fronteras de las caras en una gráfica plana $3-$conexa son precisamente sus ciclos inducidos y no separadores.*

Demostración. Sea G una gráfica plana $3-$conexa, y sea $C \subseteq G$. Si C es un ciclo inducido y no separador, entonces por el Teorema 3.2.2, sus dos caras no pueden contener ambas puntos de $G - C$. Entonces C acota una de las caras de G.

Inversamente, supóngase que C acota una cara f. Por la Proposición 3.2.1, C es un ciclo. Si C tiene una cuerda $e = xy$, entonces las componentes de $C - \{x, y\}$ están unidas por una $C-$trayectoria en G, puesto que G es $3-$conexa. Esta trayectoria y e van por la otra cara de C (no f) pero no la interseca, lo cual es una contradicción a la parte *(ii)* del Lema 3.2.1.

Solo resta probar que C no separa a cualesquiera dos vértices $x, y \in G - C$. Por el Teorema de Menger (3.2.1), x and y están unidos en G por tres trayectorias independientes. Claramente, f está dentro de una cara de la unión de estas trayectorias, y por el Lema 3.2.1 *(i)*, estas caras están acotadas por sólo dos de las trayectorias. La tercera entonces evita a f y a su frontera C. ■

Definición 3.2.10. Una gráfica plana G es *plana máxima*, o simplemente *máxima*, si al agregarle una nueva arista deja de ser plana.

Definición 3.2.11. Decimos que una gráfica plana G es una *triangulación* si cada cara de G (incluyendo la cara exterior) está acotada por un triángulo.

Proposición 3.2.3. *Una gráfica plana de orden al menos 3 es plana máxima si y sólo si es una triangulación plana.*

Demostración. Véase [7] página 90. ■

El siguiente resultado de Euler es un clásico de 1972, que marca uno de los orígenes en común entre la topología y la teoría de gráficas. El teorema relaciona el número de vértices, aristas y cars en una gráfica plana: tomados con signos correctos, estos números siempre suman 2. La forma general del teorema de Euler afirma los mismo pero para gráficas inmersas convenientemente en otras superficies también: la suma obtenida es siempre un número fijo que depende sólo de la superficie, no de la gráfica, y este número es diferente para distintas superficies (cerradas y orientables). Vamos a enunciar el Teorema de Euler en su forma más sencilla.

Teorema 3.2.3 (**Fórmula de Euler**). *Sea G una gráfica plana conexa con n vértices, m aristas, y l caras. Entonces*

$$n - m + l = 2.$$

Demostración. Véase [7] página 91. ■

Corolario 3.2.1. *Una gráfica plana con $n \geq 3$ vértices tiene a lo más $3n-6$ aristas. Toda triangulación plana con n vértices tiene exactamente $3n - 6$ aristas.*

Demostración. Por la Proposición 3.2.3, es suficiente probar la segunda afirmación. En una triangulación plana G, todas las fronteras de las caras tienen exactamente tres aristas, y cada arista es la frontera de exactamente dos caras, pues es arista de un ciclo. Denotemos con $F(G)$ al conjunto de caras de la gráfica G. La gráfica bipartita $E(G) \cup F(G)$ cuyo conjunto de aristas es $\{ef \mid e \subseteq G[f]\}$ tiene exactamente $2|E(G)| = 3|F(G)|$ aristas. De acuerdo con esta identidad, podemos reemplazar l por $2m/3$ en la fórmula de Euler, y obtener $m = 3n - 6$. ■

Daremos ahora un pequeño lema que nos será de utilidad.

Lema 3.2.3. *Una gráfica G plana máxima de orden $n \geq 4$ es $3-$conexa.*

Demostración. Véase [16] Lemma 2.3.3, página 31. ■

Como resultado del último lema, y de la Proposición 3.2.3 tenemos el siguiente corolario inmediato.

Corolario 3.2.2. *Una triangulación plana es una gráfica $3-$conexa.*

Daremos ahora una última definición antes de pasar al resultado que más queremos destacar de esta sección.

Definición 3.2.12. Si G es plana, la *longitud de una cara* de G es el número de aristas que tiene.

Ahora pasemos al siguiente resultado que nos servirá para trabajar ideales monomiales del anillo de polinomios en tres variables.

Lo que establece, es que para cierto tipo de triangulaciones, si se quitan a lo más los tres vértices de la cara exterior, lo que nos queda sigue siendo una gráfica conexa. Antes de enunciar el resultado, necesitamos aclarar al lector lo que para nosotros es un polígono convexo G, cuyos vértices están sobre tres líneas en posición general que se intersecan en tres vértices de G.

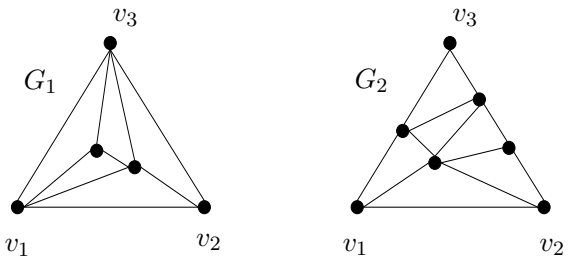

Figura 3.8: Triángulo triangulado G_1, y hexágono triangulado G_2

Queremos considerar gráficas que se vean como en la Figura 3.8, en las que globalmente podemos decir que es un triángulo triangulado, pero permitiendo tener puntos en los lados del triángulo. Así, en la siguiente proposición tengamos en mente este tipo de gráficas como las de la Figura 3.8, pero considerando como si se empezara con un polígono G, y se formara una triangulación H de G, en el sentido de que $V(G) \subseteq V(H)$, y H siendo una triangulación plana, que satisface con ser un polígono convexo; y que formaremos agregando puntos dentro del interior de G y añadiendo las aristas necesarias para que de como resultado una triangulación.

Proposición 3.2.4. *Sea G un polígono convexo, cuyos vértices están sobre tres líneas en posición general que se intersecan en v_1, v_2, $v_3 \in V(G)$. Si H es una triangulación de G y $|V(H)| \geq 4$ entonces $H[V(H) - \{v_1, v_2, v_3\}]$ es una gráfica conexa.*

Demostración. Haremos la demostración considerando dos casos, el primero será tomar gráficas que se ven como G_1 en la Figura 3.8, y el segundo caso será para gráficas como G_2 en la misma figura.

Caso 1: Supongamos que $V(G) = \{v_1, v_2, v_3\}$, como la gráfica G_1 en la Figura 3.8. Sea H una triangulación plana de G; entonces H es una gráfica plana cuyas caras son triángulos, gracias a la fórmula de Euler tenemos $c + n - e = 2$, donde c, n, e representan el número de caras, vértices y aristas respectivamente de la gráfica H. Supongamos que H no es una gráfica plana máxima, entonces existen dos vértices distintos v, w, tales que v y w son no adyacentes y que $H + vw$ sigue siendo una gráfica plana. Sea $\widetilde{H}$ una inmersión en el plano

de $H + vw$; entonces, si llamamos $H' = \widetilde{H} - vw$, tenemos que H' es plana y tiene una cara de longitud al menos 4. Además $H' \cong H$. Sea c' el número de caras de H', de la fórmula de Euler tenemos que $c = c'$. Sean l_i, y l'_i la longitud de la $i-$ésima cara de H y H' respectivamente. Como cada arista está en exactamente 2 caras, tenemos que $\sum_i l'_i = 2e$, $\sum_i l_i = 2e$, y también cada cara tiene 3 aristas, de lo que $\sum_i l_i = 3c$. de estas ecuaciones tenemos $\sum_i l'_i = 3c$, pero $3c = 3c'$, entonces $\sum_i l'_i = 3c'$. Por lo tanto todas las caras de H' tienen la misma longitud de las de H, es decir, todas son triángulos, lo cual es una contradicción puesto que en H' había una cara de longitud al menos 4.

Tenemos entonces que H es una gráfica plana máxima, y por el Lema 3.2.3 es $3-$conexa. Notemos que $\{v_1, v_2, v_3\}$ es una cara de H, y por la Proposición 3.2.2 tenemos que su frontera es un ciclo no separador, por lo que si lo removemos para formar $H[V(H) - \{v_1, v_2, v_3\}]$ permanece conexa.

Caso 2: Supongamos que $\{v_1, v_2, v_3\} \subsetneq V(G)$. Sean $\ell_1 = v_1v_2$, $\ell_2 = v_2v_3$, y $\ell_3 = v_3v_1$, los segmentos de líneas que unen los vértices $\{v_1, v_2, v_3\}$. Para cada ℓ_i que no es una arista de G, denótese con $u^i_1, \ldots, u^i_{k_i}$ a los vértices en ℓ_i, con $\{u^i_1, u^i_{k_i}\} = \ell_i \cap \{v_1, v_2, v_3\}$. Tracemos las aristas $u^i_1u^i_{k_i}$, $u^i_2u^i_{k_i}$, $\ldots$, $u^i_{k_i-2}u^i_{k_i}$ como en la Figura 3.9.

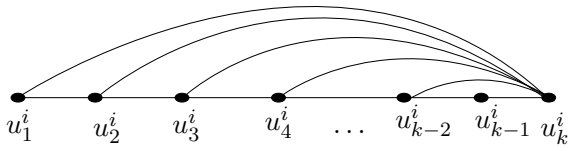

Figura 3.9: Trazo de aristas

Llamemos $\widehat{H}$ a la gráfica H más estas nuevas aristas, como toda gráfica plana tiene una representación en la que todas sus aristas son segmentos de línea, entonces $\widehat{H}$ satisface las condiciones del Caso 1. Por lo tanto $\widehat{H}[V(\widehat{H}) - \{v_1, v_2, v_3\}]$ es convexa. Como $\widehat{H}[V(\widehat{H}) - \{v_1, v_2, v_3\}] = H[V(H) - \{v_1, v_2, v_3\}]$ por construcción, se tiene el resultado. ■

Terminaremos esta sección con la siguientes definiciones.

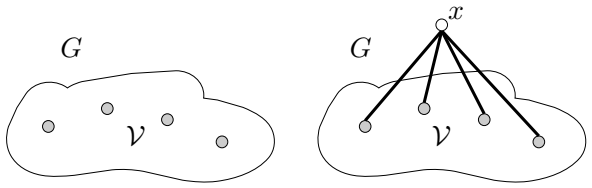

Figura 3.10: Gráfica G y su suspensión sobre $\mathcal{V}$

Definición 3.2.13. Dado un conjunto de vértices $\mathcal{V}$ en una gráfica G, definimos la *suspensión* de G sobre $\mathcal{V}$ simplemente añadiendo un nuevo vértice a G y añadiendo aristas que van desde este nuevo vértice a todos los vértices de $\mathcal{V}$.

En la Figura 3.10 damos un ejemplo de una gráfica G y su suspensión sobre un conjunto de vértices distinguidos $\mathcal{V}$.

Definición 3.2.14. Diremos que una gráfica G es *casi* $3-$*conexa* si tenemos un conjunto de 3 vértices distinguidos $\mathcal{V}$ tales que la suspensión de G sobre $\mathcal{V}$ resulta $3-$conexa.

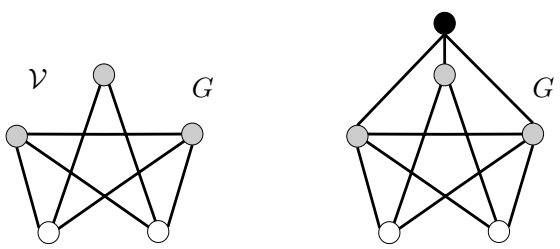

Figura 3.11: Gráfica casi $3-$conexa G y su suspensión sobre $\mathcal{V}$

En la Figura 3.11 tenemos un ejemplo de una gráfica G que satisface la condición de ser casi $3-$conexa. Notemos que en G, si quitamos los dos vértices blancos, es decir, los vértices que no están en $\mathcal{V}$, lo que nos queda es una gráfica disconexa, por lo que G no es $3-$conexa, pero su suspensión sobre $\mathcal{V}$ sí lo es.

3.3. La Gráfica de Buchberger

Encontrar conjuntos mínimos para las primeras sizigias de ideales monomiales tiene un gran impacto en la implementación de algoritmos para ideales arbitrarios. La conexión es a través de las bases de Gröbner.

Como vimos en la Sección 2.3, un conjunto $\{g_i\}_{i=1}^r$ de polinomios es una base de Gröbner bajo el orden de términos $<$ si cada $\mathcal{S}-$polinomio $\mathcal{S}(g_i, g_j)$ pude reducirse a cero módulo $\{g_1, \ldots, g_r\}$ usando el algoritmo de la división. Además, si llamamos $m_i = \text{LT}(g_i)$, entonces al $\mathcal{S}-$polinomio

$$\mathcal{S}(g_i, g_j) := \frac{\text{MCM}(m_i, m_j)}{m_i} g_i - \frac{\text{MCM}(m_i, m_j)}{m_j} g_j$$

le corresponde un elemento σ_{ij} del módulo libre S^r, de la forma

$$\sigma_{ij} := \frac{\text{MCM}(m_i, m_j)}{m_i} \mathbf{e}_i - \frac{\text{MCM}(m_i, m_j)}{m_j} \mathbf{e}_j.$$

Los $\binom{r}{2}$ elementos σ_{ij} generan al primer módulo de sizigias

$$syz(I) := \text{Ker}_S[m_1\, m_2 \cdots m_r]$$

del ideal monomial $I = \langle m_1, m_2, \ldots, m_r \rangle$, pero en general no lo generan de manera mínima, es decir, en general hay términos redundantes. Para poder hacer más eficiente el criterio de Buchberger (y por tanto también el algoritmo de Buchberger para calcular bases de Gröbner), es importante tomar ventaja de la estructura del módulo de sizigias $syz(I)$. El segundo criterio de Buchberger nos ayuda a encontrar bases más pequeñas a partir del conjunto $\{\sigma_{ij}\}$, simplemente considerando aquellas σ_{ij} tales que $i < j$, y que $\mathcal{S}(g_i, g_j) \longrightarrow_G 0$. Esto nos conduce a la siguiente definición.

Definición 3.3.1. La *gráfica de Buchberger* de un ideal monomial $I = \langle m_1, \ldots, m_r \rangle$, que denotamos con Buch$(I)$, tiene como vértices $\{1, \ldots, r\}$ y una arista (i, j) si alguna de las siguientes es cierta:

i) Si no hay un monomio m_k tal que m_k divida a MCM(m_i, m_j), o bien

ii) Si el grado de m_k es igual al de MCM(m_i, m_j) en alguna de las variables que coincida con MCM(m_i, m_j).

Observación 3.3.1. *Observemos en la definición anterior que, la condición para que una arista (i, j) no esté en la gráfica Buch(I) debe ser: Existe un m_k tal que m_k divide a* MCM(m_i, m_j) *y el grado de m_k es diferente al de* MCM(m_i, m_j) *en todas las variables en que coincidan.*

Para familiarizarnos con la última definición daremos en seguida unos ejemplos.

El primer ejemplo a considerar es el caso en el que I es un ideal monomial en dos variables, entonces Buch(I) consiste de los $r-1$ pares consecutivos de los generadores mínimos formando así una trayectoria.

Ejemplo 3.3.1. Considérese el ideal $J = \langle x^4, y^4, z^4, x^3y^2z, xy^3z^2, x^2yz^3\rangle \subset \ [x,y,z]$.

Nombremos $m_1 = x^4, \ldots, m_6 = x^2yz^3$ de acuerdo a como están listados. La siguiente tabla nos muestra todos los mínimos comunes múltiplos entre los generadores m_i.

MCM	x^4	y^4	z^4	x^3y^2z	xy^3z^2
x^2yz^3	x^4yz^3	$x^2y^4z^3$	x^2yz^4	$x^3y^2z^3$	$x^2y^3z^3$
xy^3z^2	$x^4y^3z^2$	xy^4z^2	xy^3z^4	$x^3y^3z^2$	
x^3y^2z	x^4y^2z	x^3y^4z	$x^3y^2z^4$		
z^4	x^4z^4	y^4z^4			
y^4	x^4y^4				

Notemos por ejemplo, que no hay ningún m_k ($k = 2, \ldots, 5$) que divida a MCM$(x^4, x^2yz^3) = x^4yz^3$, por lo que en Buch(I) hay una arista entre x^4 y x^2yz^3, sin embargo, para z^4 y x^3y^2z no es así, puesto que $m_6 = x^2yz^3$ divide a MCM$(z^4, x^3y^2z) = x^3y^2z^4$, y tienen distinta potencia en cada una de las variables. De esta forma, la tabla de incidencias para la gráfica es la que sigue

	x^4	y^4	z^4	x^3y^2z	xy^3z^2
x^2yz^3	1	0	1	1	1
xy^3z^2	0	1	1	1	
x^3y^2z	1	1	0		
z^4	1	1			
y^4	1				

Así tenemos como resultado final la gráfica de Buchberger, Buch(J), para el ideal J, que se muestra en la Figura 3.12.

Notemos que Buch(I) resultó ser una gráfica plana, y podemos obtener a partir de ella mucho más información, por ejemplo, en la Figura 3.12 tenemos tres aristas etiquetadas con los números *404*, *413* y *214*, que corresponden a los exponentes del mínimo común múltiplo entre los vértices de dichas aristas. Además tenemos una cara etiquetada con el número **414**, que corresponde al mínimo común múltiplo entre las aristas que delimitan esa cara. Entonces, por construcción, los vértices de Buch(J) corresponden a los generadores de J, las aristas corresponden a las primeras sizigias, y las caras a las segundas sizigias.

Así, la resolución libre mínima para S/I es de la forma

$$0 \leftarrow S \longleftarrow S^6 \longleftarrow S^{12} \longleftarrow S^7 \leftarrow 0.$$

Los sumandos corresponden a los 6 vértices, 12 aristas, y 7 caras del triángulo triangulado de la Figura 3.12.

También, las caras corresponden a las componentes irreducibles de J, es decir,

$$\begin{aligned} J &:= \langle x^4, y^4, z^4, x^3y^2z, xy^3z^2, x^2yz^3\rangle \\ &= \langle x^4, y^4, z\rangle \cap \langle x^4, y, z^4\rangle \cap \langle x, y^4, z^4\rangle \cap \langle x^4, y^2, z^3\rangle \cap \\ &\quad \langle x^3, y^4, z^2\rangle \cap \langle x^2, y^3, z^4\rangle \cap \langle x^3, y^3, z^3\rangle. \end{aligned}$$

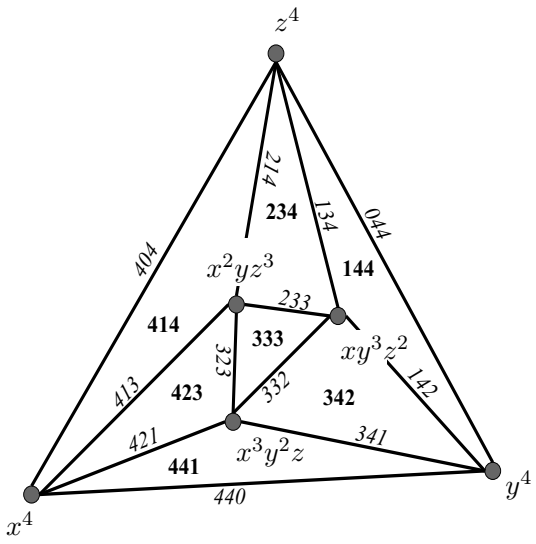

Figura 3.12: Buch(J)

Y por último, si escribimos una suma alternada de todas las etiquetas tenemos:

$$1 - x^4 - \ldots - x^2yz^3 + x^4y^4 + \ldots + xy^3z^4 - x^4y^4z - \ldots - x^3y^3z^3.$$

Este es el $K-$polinomio $\mathcal{K}(S/J;\, x, y, z)$. Notemos que si especializamos dicho polinomio obtenemos $\mathcal{K}(S/J;\, t, t, t) = 1 - 3t^4 - 3t^6 + 3t^7 + 9t^8 - 7t^9$, que es la notación usual para el $K-$polinomio.

$\diamondsuit$

Del ejemplo anterior es natural preguntarse si tanta información puede obtenerse siempre de la gráfica de Buchberger, antes de tratar de dar una respuesta a dicha pregunta analicemos un par de ejemplos más.

Ejemplo 3.3.2. Consideremos ahora el ideal $I = \langle xy^2z, xyz^3, x^2, y^3z^2\rangle \subset \quad [x, y, z]$. Este ideal tiene como gráfica de Buchberger la mostrada en la Figura 3.13, notemos que no está la arista que une 200 con 032 puesto que MCM$(x^2, y^3z^2) = x^2y^3z^2$ es dividido por xy^2z y tienen todas las potencias distintas, como señalamos en la Observación 3.3.1, sin embargo, sí está presente la arista que une 032 con 113 puesto que MCM$(y^3z^2, xyz^3) = xy^3z^3$ que es también dividido por xy^2z, pero en este caso ambos coinciden en el exponente de la variable x.

Ahora, pese a que Buch(I) es una gráfica plana, esta gráfica no nos representa la resolución libre mínima para S/I, puesto que la resolución libre mínima es:

$$0 \leftarrow S \longleftarrow S^4 \longleftarrow S^4 \longleftarrow S \leftarrow 0.$$

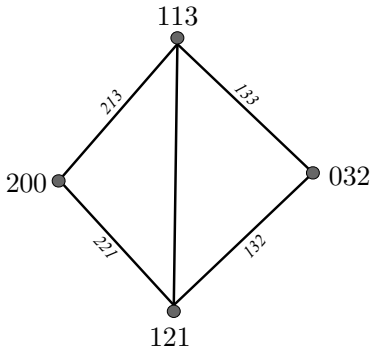

Figura 3.13: Buch(I)

Que aunque corresponde a 4 vértices, no corresponde ni a 5 aristas ni a 2 caras. Por lo que la planaridad de la gráfica Buch(I) no es suficiente para rescatar toda la información como en el Ejemplo 3.3.1.

♢

Por último analicemos el siguiente ejemplo que nos ayudará a familiarizarnos más con la gráfica de Buchberger, y que nos será de utilidad más adelante.

Ejemplo 3.3.3. Tomemos el ideal $I' = \langle x^2z, xyz, y^2z, x^5y^3, x^4y^4, x^3y^5\rangle \subset \quad [x, y, z]$. La gráfica de Buchberger está representada en la Figura 3.14. Observemos que en Buch(I') no está presente la arista que une 530 con 350, y esto es porque MCM$(x^5y^3, x^3y^5) = x^5y^5$ es dividido por x^4y^4, y las potencias de x y y son ambas distintas, por la Observación 3.3.1, sabemos que no debe estar presente dicha arista.

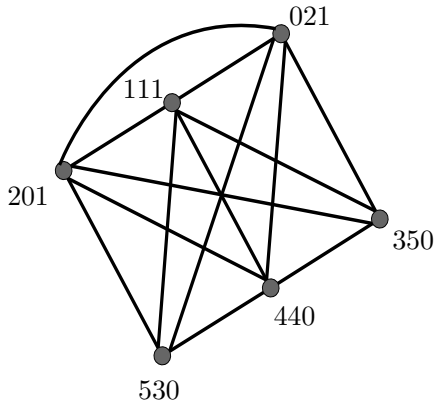

Figura 3.14: Buch(I') contiene a $K_{3,3}$

Claramente Buch(I') no es una gráfica plana puesto que contiene como subgráfica a $K_{3,3}$. La resolución libre mínima para I' es:

$$0 \leftarrow S \longleftarrow S^6 \longleftarrow S^7 \longleftarrow S^2 \leftarrow 0.$$

Claramente en este ejemplo la gráfica de Buchberger provee más aristas que primeras sizigias, y no están definidas las caras de Buch(I'), por lo que no está claro que se debe tomar de información para las segundas sizigias.

$\diamondsuit$

Tanto en el Ejemplo 3.3.2, como en el Ejemplo 3.3.3, se tiene más información de la debida en la gráfica de Buchberger, aunque los generadores de las primeras y segundas sizigias están contenidas en ellas, se tienen más aristas de las debidas. Esto es puesto que los ideales necesitan satisfacer una condición más fuerte, y que introduciremos más adelante, por lo pronto mostremos que en verdad la información acerca del módulo de sizigias realmente puede ser leído de la gráfica de Buchberger.

Proposición 3.3.1. *Dado un ideal monomial I, el módulo de sizigias $syz(I)$ está generado por las sizigias σ_{ij} correspondientes a las aristas (i,j) en Buch(I).*

Demostración. Observemos que

$$\frac{\text{MCM}(m_i,m_j,m_k)}{\text{MCM}(m_i,m_j)}\sigma_{ij} + \frac{\text{MCM}(m_i,m_j,m_k)}{\text{MCM}(m_j,m_k)}\sigma_{jk} + \frac{\text{MCM}(m_i,m_j,m_k)}{\text{MCM}(m_k,m_i)}\sigma_{ki} = 0, \qquad (3.1)$$

dado a cómo están definidas las σ_{ij}. Ahora, si (i,j) no es una arista de Buch(I), por la Observación 3.3.1, para alguna k, el coeficiente de σ_{ij} en (3.1) debe ser 1, mientras que los coeficientes de σ_{jk} y σ_{ki} son monomios no constantes, por lo que σ_{ij} cae dentro del $S-$módulo generado por otras sizigias de grado estrictamente menor, por lo que podemos quitar a σ_{ij} del conjunto de generadores de $syz(I)$ sin que caigamos en un ciclo. ■

Aunque la Proposición anterior nos muestra que realmente las sizigias representadas por aristas en Buch(I) forman un conjunto generador del primer módulo de sizigias, no forzosamente dicho conjunto resulta mínimo.

Antes de continuar con el estudio de la gráfica de Buchberger, rescatemos algo de la información que nos daba el diagrama de escalera para ideales monomiales en dos variables que estudiamos en la Sección 3.1.

Definición 3.3.2. La *superficie de escalera* de un ideal monomial $I \subset [x,y,z]$ es la frontera topológica del conjunto de vectores $(v_x,v_y,v_z) \in \mathbb{R}^3$ para los cuales hay un monomio $x^{u_x}y^{u_y}z^{u_z} \in I$ que satisface $u_i \leq v_i$ para toda $i \in \{x,y,z\}$.

En las Figuras 3.15, 3.16 y 3.17 se muestran las superficies de escalera de los Ejemplos 3.3.1, 3.3.2 y 3.3.3 respectivamente. En dichos diagramas se debe interpretar la superficie como la frontera entre lo que está en el ideal I, y lo que no está en I, con los puntos en el

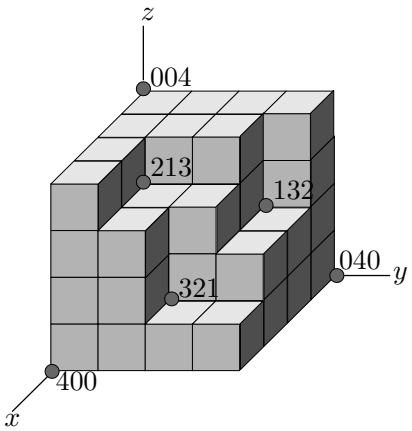

Figura 3.15: Superficie de escalera del ideal J del Ejemplo 3.3.1.

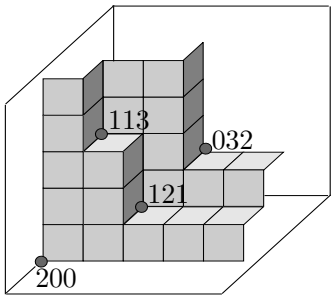

Figura 3.16: Superficie de escalera del ideal I del Ejemplo 3.3.2.

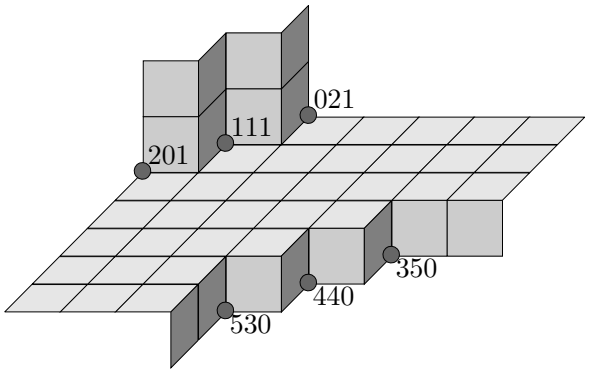

Figura 3.17: Superficie de escalera del ideal I' del Ejemplo 3.3.3.

enrejado estrictamente atrás de la superficie siendo aquellos que no pertenecen a I. Así, cualquier punto del enrejado que es visible en el diagrama de escalera es el vector de los

exponentes de un monomio en nuestro ideal I. Los puntos oscuros corresponden a los generadores mínimos de I; nótese cómo dichos puntos yacen en las esquinas "interiores".

La superficie de escalera es homeomorfa a $\mathbb{R}^2$ vía la proyección ortogonal con Kernel $(1,1,1)$. La gráfica de Buchberger puede ser inmersa en el diagrama de escalera de la siguiente forma: Para dibujar la arista de Buch(I) entre los monomios m_i y m_j, sólo hay que trazar los segmentos de línea que unen m_i con MCM(m_i, m_j) y el que une m_j con MCM(m_i, m_j). Para ilustrar este procedimiento, en la Figura 3.18 damos la inmersión de Buch(J) del Ejemplo 3.3.1 en su superficie de escalera.

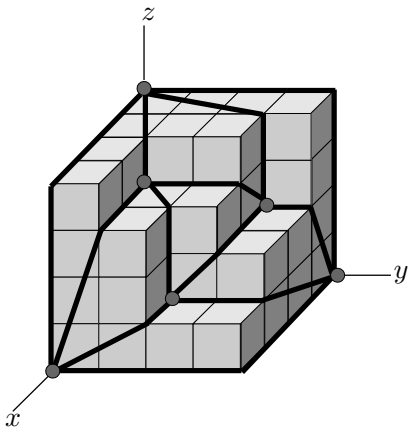

Figura 3.18: Buch(J) inmersa en la superficie de escalera.

3.4. Genericidad y deformaciones

En la sección anterior vimos que la gráfica de Buchberger puede proveer mucha información acerca del módulo de sizigias y de la resolución libre mínima para S/I, siendo I un ideal monomial, pero también vimos ejemplos de cuándo la gráfica de Buchberger no coincide con la resolución libre mínima para S/I. En esta sección mostraremos que la condición que se le debe pedir al ideal I es ser un ideal monomial "*fuertemente genérico*".

También veremos que dado un ideal monomial en general, podemos llevar a cabo un proceso de "deformación", en el que podamos rescatar la información mínima necesaria de la gráfica de Buchberger para poder describir la resolución libre mínima. Los dos resultados principales de esta sección, la planaridad en la Proposición 3.4.1 y la resolución libre en el Teorema 3.4.1, pueden ser probados utilizando solamente métodos de geometría en tres dimensiones; pero, como muchos resultados respectivos a gráficas planas, estos enunciados intuitivos requieren pruebas más técnicas de lo esperado.

Definición 3.4.1. Un ideal monomial I en $[x, y, z]$ es *fuertemente genérico* si cada par de generadores mínimos $x^i y^j z^k$ y $x^{i'} y^{j'} z^{k'}$ de I, satisfacen:

$$(i \neq i' \text{ o } i = i' = 0) \text{ y } (j \neq j' \text{ o } j = j' = 0) \text{ y } (k \neq k' \text{ o } k = k' = 0).$$

En otras palabras, dos generadores no coinciden en el exponente en ninguna de las variables que aparezcan al mismo tiempo en los dos.

Así, en el Ejemplo 3.3.1, el ideal $J = \langle x^4, y^4, z^4, x^3y^2z, xy^3z^2, x^2yz^3\rangle$ resulta ser fuertemente genérico, en cambio, en los Ejemplos 3.3.2 y 3.3.3, los ideales $I = \langle xy^2z, xyz^3, x^2, y^3z^2\rangle$, e $I' = \langle x^2z, xyz, y^2z, x^5y^3, x^4y^4, x^3y^5\rangle$ resultan no ser fuertemente genéricos, puesto que para I, los monomios xy^2z y xyz^3 coinciden en el exponente de la variable x; y análogamente, para el ideal I', los monomios x^2z, xyz, y^2z coinciden en el exponente de la variable z.

La condición para un ideal monomial I de ser fuertemente genérico realmente produce una gráfica plana, como la del ideal J del Ejemplo 3.3.1, y de la cuál se puede obtener la información para el cálculo de la resolución libre mínima, pero antes de dar la prueba de este hecho, vamos a dar una definición que nos será fundamental para el resto del capítulo.

Definición 3.4.2. Un ideal monomial I es *artiniano*, si dentro de su conjunto de generadores mínimos se incluyen las potencias puras de las variables, es decir, si $I = \langle m_1, \ldots, m_r\rangle$ es la descripción de I en generadores mínimos, entonces I es artiniano si $\{x^a, y^b, z^c\} \subset \{m_1, \ldots, m_r\}$.

En muchas de las pruebas de este capítulo es necesario considerar ideales artinianos, dado un ideal monomial I podemos encontrar un ideal monomial artiniano $\widehat{I}$ cuyo conjunto de generadores mínimos contenga los generadores mínimos de I.

Definición 3.4.3. Dado un ideal monomial $I = \langle m_1, \ldots, m_r \rangle$, podemos formar un ideal monomial artiniano $\widehat{I}$ agregando al conjunto de generadores de I, potencias puras de las variables suficientemente grandes, es decir, $\widehat{I} = \langle m'_1, \ldots, m'_s \rangle$, donde $\{m_1, \ldots, m_r, x^a, y^b, z^c\} = \{m'_1, \ldots, m'_s\}$, de tal manera que ningún monomio sea redundante. Así, a este proceso le llamamos una *artenianización* de I.

Para ejemplificar este proceso de artenianización, consideremos los ideales no artinianos de los Ejemplos 3.3.2 y 3.3.3. Para el ideal $I = \langle xy^2z, xyz^3, x^2, y^3z^2 \rangle$, una artenianización de I resulta ser $\widehat{I} = \langle xy^2z, xyz^3, x^2, y^3z^2, y^4, z^4 \rangle$. Para el ideal $I' = \langle x^2z,\ xyz,\ y^2z,\ x^5y^3,\ x^4y^4,\ x^3y^5 \rangle$ una artenianización sería $\widehat{I'} = \langle x^2z, xyz, y^2z, x^5y^3, x^4y^4, x^3y^5, x^7, y^7, z^2 \rangle$. Observemos que hay más de una manera de artinianizar un ideal, pero para nuestros fines es suficiente considerar una de ellas.

Ahora estamos en posición de enunciar la siguiente proposición.

Proposición 3.4.1. *Si I es un ideal monomial fuertemente genérico en $[x, y, z]$, entonces la gráfica de Buchberger Buch(I) es plana y conexa. Más aún, si I es artiniano, entonces Buch(I) consiste de las aristas en un triángulo triangulado.*

Demostración. Primero observemos que es suficiente considerar ideales monomiales artinianos. Si tomamos un ideal monomial artiniano y borramos todas las aristas y las regiones incidentes a uno o más de los $\{x^a, y^b, z^c\}$ en la gráfica de Buchberger, nos queda la gráfica de Buchberger del ideal sin el generador correspondiente, y dicha gráfica resultante es conexa gracias a la Proposición 3.2.4. Así, podemos considerar ideales artinianos, ya que si estamos trabajando con un ideal no artiniano, podemos "artenianizarlo", aplicar nuestra proposición y después "desartenianizarlo".

Ahora, en el ideal artiniano I, las caras acotadas en la superficie de escalera del ideal monomial I forman un disco topológico acotado por un triángulo con vértices x^a, y^b y z^c, los generadores de potencias puras de I. Como observamos antes, cada arista $\{m, m'\}$ de Buch(I) está representada en la superficie de escalera por la unión de dos segmentos de línea que van de m a MCM(m, m') y el otro que va de m' a MCM(m, m'). El hecho de que MCM(m, m') cae en la superficie de escalera es por cómo está definida esta. El hecho de que MCM(m, m') no tiene ninguna otra arista pasando por él, es una consecuencia de la genericidad.

Ahora, con la inmersión de Buch(I) en la superficie de escalera, lo que resta probar es que cada región de la subdivisión es un triángulo (es decir, acotada por exactamente 3 aristas de la gráfica de Buchberger). Esto será probando que las dos regiones que contienen una arista interior $\{m, m'\} \in$ Buch(I) es precisamente un triángulo. Este triángulo está producido encontrando al tercer generador m'' únicamente determinado, tal que el mínimo común múltiplo de $\{m, m', m''\}$ yace sobre la superficie de escalera; la región es entonces acotada por las aristas de Buchberger $\{m, m'\}$, $\{m, m''\}$, y $\{m', m''\}$. ■

Una gráfica plana G puede ser inmersa en el plano $\mathbb{R}^2$ normalmente en más de una forma, haciendo así la noción de "región de G "un tanto ambigua. Es usual hacer distinción entre

una gráfica plana y una inmersión particular de dicha gráfica.

Definición 3.4.4. Una *aplicación plana* es una gráfica G junto con una inmersión de G en una superficie homeomorfa al plano $\mathbb{R}^2$.

Habiendo hecho tal aclaración, nos referiremos a una aplicación plana simplemente con G si la inmersión está dada o es clara. Necesitamos que las superficies sean homeomorfas a $\mathbb{R}^2$ en vez de iguales, puesto que necesitamos dibujar aplicaciones planas en superficies de escalera. De hecho, el comentario previo a la prueba de la Proposición 3.4.1, y la prueba en sí, nos provee de una inmersión canónica de la gráfica de Buchberger de un ideal monomial fuertemente genérico en su superficie de escalera.

El siguiente teorema nos dice que las aplicaciones planas codifican las resoluciones libres mínimas en el sentido de que organizan con diagramas simples las sizigias y las relaciones entre ellas.

Teorema 3.4.1. *Dado un ideal monomial fuertemente genérico I en $[x, y, z]$, la aplicación plana Buch(I) provee una resolución libre mínima de I.*

Demostración. Empecemos por artinianizar I añadiendo potencias suficientemente grandes x^a, y^b y z^c. Lo que obtenemos es un ideal fuertemente genérico y artiniano, así, si obtenemos una resolución libre mínima para este ideal dada por una aplicación plana, entonces al borrar todas las aristas y regiones adyacentes a uno o más de los $\{x^a, y^b, z^c\}$ nos deja una resolución libre mínima para I. De hecho, el borrar aristas y regiones de la aplicación plana no tiene ningún efecto sobre las componentes $\mathbb{N}^3-$graduadas de grado menor o igual que $(a-1, b-1, c-1)$, e I no tiene sizigias de ningún otro grado, por lo tanto, asumimos que I es artiniano.

Cada triángulo en Buch(I) contiene una única "punta de montaña" en la superficie de escalera, localizada en la esquina exterior, y que corresponde al MCM(m, m', m''). Dicha punta está rodeada por MCM(m, m'), MCM(m, m''), y MCM(m', m''), cada una de las cuales representa una primer sizigia mínima de I. La punta de montaña representa una segunda sizigia relacionada a las tres dichas primeras sizigias por la igualdad en la prueba de la Proposición 3.3.1, y la relación que hay entre las primeras sizigias nos dice que todas las segundas sizigias mínimas son de esta forma. ■

Cabe mencionar que una resolución libre dada por una aplicación plana G con v vértices, e aristas y f caras, todas indexadas por monomios, tienen la forma

$$\mathcal{F}_G : \quad 0 \longleftarrow S \longleftarrow S^v \xleftarrow{\partial_E} S^e \xleftarrow{\partial_F} S^f \longleftarrow 0. \tag{3.2}$$

Si escribimos $m_{ij} = \text{MCM}(m_i, m_j)$ para cada $\{i, j\} \in E(G)$, y m_R denota al mínimo común múltiplo de los monomios que etiquetan las aristas de cada región R, entonces podemos describir de manera simple las aplicaciones ∂_E por

$$\partial_E(\mathbf{e}_{ij}) = \frac{m_{ij}}{m_j}\mathbf{e}_j - \frac{m_{ij}}{m_j}\mathbf{e}_j,$$

si además escogemos la orientación de la arista m_{ij}, como la que va del vértice m_i y llega al m_j, de esta forma tenemos que

$$\partial_F(\mathbf{e}_R) = \sum_{\substack{aristas \\ \{i,j\}\subset R}} \pm\frac{m_R}{m_{ij}} \cdot \mathbf{e}_{ij},$$

está descrita para cada región R, donde el signo es + precisamente cuando la orientación en $\{i, j\}$ coincide con una orientación en R en el sentido de las manecillas del reloj.

Así, el teorema anterior nos dice que dicha resolución libre resulta mínima cuando consideramos ideales monomiales fuertemente genéricos.

Enseguida mostraremos cómo aproximar ideales monomials arbitrarios mediante ideales fuertemente genéricos. La idea está basada en agregar números racionales pequeños a los exponentes en los generadores de I, de tal modo que no inviertan ninguna desigualdad estricta entre los grados en x, y, o z de cualesquiera dos generadores. Este proceso sucede dentro del anillo de polinomios $S_\epsilon = [x^\epsilon, y^\epsilon, z\epsilon]$, donde $\epsilon = 1/N$ para algún entero positivo N suficientemente grande, y que contiene a $S = [x, y, z]$ como subanillo. Las igualdades entre los grados de x, y y z pueden volverse desigualdades estrictas que potencialmente pueden ir en cualquier sentido.

Definición 3.4.5. Sean $I = \langle m_1, \ldots, m_r\rangle$ y $I_\epsilon = \langle m_{\epsilon,1}, \ldots, m_{\epsilon,r}\rangle$ ideales monomiales en S y S_ϵ respectivamente. Llamamos a I_ϵ una *deformación fuerte* de I, si el orden parcial en $\{1, 2, \ldots, r\}$ en el grado de la variable x de las $m_{\epsilon,i}$ refina el orden parcial del grado en x de los m_i, y lo mismo para y y z. También decimos que I es una *especialización* de I_ϵ.

Dado cualquier ideal monomial I, construir una deformación fuerte I_ϵ para I es fácil: simplemente hay que reemplazar cada generador m_i por un generador parecido $m_{\epsilon,i}$, de tal manera que $\lim_{\epsilon\to 0} m_{\epsilon,i} = m_i$. El ideal I_ϵ puede no ser fuertemente genérico, sin embargo, lo será si la deformación fuerte es escogida arbitrariamente, es decir, hay mucho más probabilidad de que I_ϵ resulte fuertemente genérico a que no sea así.

En general no nos serán de utilidad cualesquiera deformaciones fuertes, en la siguiente sección daremos la condición que necesitamos pedir a dichas deformaciones para que realicen el propósito que buscamos. Pero por ahora, para ejemplificar cómo son las deformaciones damos el siguiente ejemplo sencillo, y daremos ejemplos un poco más complicado más adelante.

Ejemplo 3.4.1. El ideal en S_ϵ dado por

$$\langle x^3, x^{2+\epsilon}y^{1+\epsilon}, x^2z^1, x^{1+2\epsilon}y^2, x^{1+\epsilon}y^1z^{1+\epsilon}, x^1z^{2+\epsilon}, y^3, y^{2-\epsilon}z^{1+2\epsilon}, y^{1+2\epsilon}z^2, z^3\rangle,$$

es una posible deformación fuertemente y genérica del ideal

$$\langle x, y, z\rangle^3 = \langle x^3, y^3, z^3, x^2y, x^2z, y^2z, xy^2, xz^2, yz^2, xyz\rangle,$$

del anillo S, y con ϵ cualquier número menor que 1. ♢

Antes de continuar, daremos una notación que nos ayudará a simplificar los enunciados.

Notación 2. *Para una resolución libre obtenida a partir de una aplicación plana, nos referiremos sólo con resolución plana.*

Proposición 3.4.2. *Supóngase que I es un ideal monomial en $[x, y, z]$ y I_ϵ es una deformación fuerte. Supóngase que se tiene la resolución plana dada por G_ϵ. Entonces, especializando los vértices (y por tanto también las aristas y las regiones) de G_ϵ nos resulta una resolución plana de I.*

Demostración. Considérese la resolución libre mínima $\mathcal{F}_{G_\epsilon}$ determinada por la triangulación G_ϵ. La especialización G de la aplicación plana G_ϵ, nos sigue dando un complejo $\mathcal{F}_G$ en los módulos libres sobre $[x, y, z]$, y lo que necesitamos probar es la exactitud. Considerando cualquier $\mathbb{N}^3-$grado fijo $\omega = (a, b, c)$, debemos mostrar la exactitud del complejo de espacios vectoriales sobre en la parte de grado ω en $\mathcal{F}_G$.

Definamos ω_ϵ como el vector de exponentes de

$$\text{MCM}(m_{\epsilon,i} \mid m_i \text{ divide } x^a y^b z^c).$$

Los sumandos que contribuyen para la parte de grado ω en $\mathcal{F}_G$ son precisamente aquellos sumandos de $\mathcal{F}_{G_\epsilon}$ que contribuyen a la parte de grado ω_ϵ, la cual sabemos que es exacta. ■

En la siguiente sección mostraremos como cualquier resolución plana puede ser transformada en una mínima removiendo sucesivamente aristas y uniendo regiones adyacentes. Por ahora, simplemente obtenemos una cota a partir de la Proposición 3.4.2 usando el Teorema de Euler (Teorema 3.2.3).

Corolario 3.4.1. *Un ideal I generado por $r \geq 3$ monomios en $[x, y, z]$ tiene a lo más $3r - 6$ primeras sizigias mínimas, y $2r - 5$ segundas sizigias mínimas. Dichas cotas se alcanzan si I es artiniano, fuertemente genérico, y si xyz divide a todos excepto a tres de los generadores mínimos (precisamente las potencias puras de las variables).*

Demostración. Escojamos una deformación fuerte I_ϵ de I de tal modo que I_ϵ resulte fuertemente genérico. La Proposición 3.4.2 implica que el número de sizigias mínimas de I están acotadas precisamente por el número de sizigias mínimas de I_ϵ, así, es suficiente probar la primera parte del corolario para el ideal I_ϵ. Del Teorema 3.4.1 inducimos que la resolución libre mínima de I_ϵ está dada por una aplicación plana. Así, del Teorema de Euler (Teorema 3.2.3) y del Corolario 3.2.1 obtenemos el resultado.

Para la segunda parte, considérese I como un ideal fuertemente genérico y artiniano. Sean x^a, y^b y z^c los tres generadores especiales de I. Cada uno de los otros generadores mínimos $x^i y^j z^k$ satisfacen $i \geq 1$, $j \geq 1$ y $z \geq 1$, por la condición de ser fuertemente genérico; así, $\{x^a, y^b\}$, $\{x^a, z^c\}$, y $\{y^b, z^c\}$ son aristas de Buch(I). Por la Proposición 3.4.1, Buch(I) es una triangulación de un triángulo, con r vértices tales que $r - 3$ vértices caen en el interior. Se sigue del Teorema 3.2.3 y del Corolario 3.2.1, que se deben tener $3r - 6$

aristas. Del Teorema de Euler, tenemos $v - e + (f + 1) = 2$, puesto que debemos considerar la cara externa de la triangulación como una de las caras de la gráfica. De aquí tenemos $r - (3r - 6) + f + 1 = 2$, y despejando f tenemos $f = 2r - 5$. El resultado ahora es inmediato de la minimalidad en el Teorema 3.4.1. ■

3.5. El algoritmo de Buchberger para resoluciones planas

En los ejemplos de la Sección 3.3 vimos que la no planaridad de la gráfica de Buchberger no nos proveía la información buscada para describir la resolución plana, nuestra meta para lo que resta del capítulo es mostrar que los obstáculos encontrados en dichos ejemplos pueden ser superados y así obtener una manera fácil y rápida de escribir una versión del algoritmo de Buchberger utilizando dichas gráficas.

Haremos uso ahora del par de definiciones con las que terminamos la Sección 3.2, en las que definimos la suspensión de una gráfica, y el significado de ser casi 3−conexa. En nuestro caso, el conjunto de vértices de nuestras gráficas serán los monomios que generan mínimamente cierto ideal I dentro de $[x, y, z]$. Notemos que cuando I es artiniano, este conjunto de vértices contiene un conjunto de tres vértices distinguidos $\mathcal{V}$: los generadores con potencias puras x^a, y^b, z^c, así nuestras gráficas de Buchberger serán triángulos triangulados como los mostrados en la Figura 3.8. Ahora enunciamos el resultado principal de este capítulo. Daremos una prueba a dicho teorema más adelante, ya que hayamos demostrado el Algoritmo 3.1, que utilizaremos para la prueba.

Teorema 3.5.1. *Todo ideal monomial I en $[x, y, z]$ tiene una resolución libre mínima dada por cierta aplicación plana. Además, si I es artiniano, entonces la gráfica G correspondiente a cualesquiera de dichas aplicaciones planas resulta casi 3−conexa.*

Los vértices, aristas y regiones acotadas de dicha aplicación plana están etiquetadas por los respectivos monomios o sus MCM, como en los ejemplos hasta ahora vistos. Esto nos determina una sucesión de módulos libres sobre $S = [x, y, z]$ como en (3.2). Empezaremos mostrando un algoritmo para encontrar una resolución plana como en el Teorema 3.5.1 para ideales artinianos.

Dada una deformación I_ϵ de un ideal monomial $I = \langle m_1, \ldots, m_r \rangle$, con $m_i = x^{a_i} y^{b_i} z^{c_i}$, escribamos al i−ésimo generador de la deformación como $m_{\epsilon,i} = x^{a_{\epsilon,i}} y^{b_{\epsilon,i}} z^{c_{\epsilon,i}}$. Dentro del Algoritmo 3.1 necesitaremos que las deformaciones fuertes satisfagan la condición

$$\begin{array}{lllllll} \text{si} & a_i = a_j & \text{y} & c_i < c_j & (\text{equivalentemente } b_i > b_j) & \Longrightarrow & a_{\epsilon,i} < a_{\epsilon,j} \\ \text{si} & b_i = b_j & \text{y} & a_i < a_j & (\text{equivalentemente } c_i > c_j) & \Longrightarrow & b_{\epsilon,i} < b_{\epsilon,j} \\ \text{si} & c_i = c_j & \text{y} & b_i < b_j & (\text{equivalentemente } a_i > a_j) & \Longrightarrow & c_{\epsilon,i} < c_{\epsilon,j}. \end{array} \tag{3.3}$$

Notemos que en la condición (3.3), por ejemplo, en el caso que $a_i = a_j$, la condición $c_i < c_j$ es equivalente a $b_i > b_j$, puesto que si pasa $c_i < c_j$ y $b_i < b_j$, entonces el monomio $x^{a_i} y^{b_i} z^{c_i}$ divide al monomio $x^{a_j} y^{b_j} z^{c_j}$, y lo mismo pasa equivalente en la coincidencia de las otras variables.

Definición 3.5.1. Sea I_ϵ una deformación fuerte de un ideal monomial I. Diremos que I_ϵ es una *deformación fuertemente genérica cíclicamente consistente*, si I_ϵ es un ideal fuertemente genérico, y satisface la condición (3.3).

Daremos ahora ejemplos de deformaciones fuertemente genéricas cíclicamente consistentes para los ejemplos estudiados en la Sección 3.3.

Ejemplo 3.5.1. Considérese el ideal $J = \langle x^4, y^4, z^4, x^3y^2z, xy^3z^2, x^2yz^3\rangle$ del Ejemplo 3.3.1. Una deformación fuertemente genérica cíclicamente consistente para J es $J_\epsilon = J$. Puesto que J misma satisface todas las condiciones, es decir, hacemos $\epsilon = 1$, o equivalentemente su denominador $N = 1$.

$\diamondsuit$

Ahora veremos un ejemplo un poco más interesante.

Ejemplo 3.5.2. Consideremos ahora el ideal $I = \langle xy^2z, xyz^3, x^2, y^3z^2\rangle$ del Ejemplo 3.3.2. Notemos que en nuestra situación, xy^2z y xyz^3 coinciden en el exponente de la variable x, como el exponente en z de xy^2z es 1, mientras que para xyz^3 es 3, por el criterio (3.3) debemos sumar ϵ al exponente en x de xyz^3. Así, una especialización fuertemente genérica para I sería

$$I_\epsilon = \langle xy^2z, x^{1+\epsilon}yz^3, x^2, y^3z^2\rangle.$$

Podemos tomar $N = 6$, o equivalentemente $\epsilon = 1/6$.

$\diamondsuit$

Ahora veamos qué sucede en el caso del Ejemplo 3.3.3. En dicho ejemplo daremos una descripción detallada del pensamiento algorítmico utilizado a la hora de encontrar deformaciones fuertes que utilizaremos dentro del Algoritmo 3.1.

Ejemplo 3.5.3. Tomemos el ideal $I' = \langle x^2z, xyz, y^2z, x^5y^3, x^4y^4, x^3y^5\rangle$. En este caso, primero vemos que xyz y y^2z coinciden en el exponente de la variable z. Como el exponente en y de xyz es 1, mientras que en y^2z es 2, por la condición (3.3) tenemos que debemos agregar ϵ al exponente en z de y^2z. Así, tenemos una especialización

$$\langle x^2z, xyz, y^2z^{1+\epsilon}, x^5y^3, x^4y^4, x^3y^5\rangle.$$

Pero dado que también el exponente en z de x^2z y xyz coincide, entonces, por el criterio (3.3) debemos sumar ϵ al exponente en z de xyz, y nos resultaría

$$\langle x^2z, xyz^{1+\epsilon}, y^2z^{1+\epsilon}, x^5y^3, x^4y^4, x^3y^5\rangle.$$

Aquí de nuevo tenemos una coincidencia en el exponente de la variable z para los monomios $xyz^{1+\epsilon}$ y $y^2z^{1+\epsilon}$, pero como lo hicimos anteriormente, el criterio (3.3) nos dice que debemos agregar ϵ al exponente en z de $y^2z^{1+\epsilon}$. De esta manera obtenemos el ideal

$$I'_\epsilon = \langle x^2z, xyz^{1+\epsilon}, y^2z^{1+2\epsilon}, x^5y^3, x^4y^4, x^3y^5\rangle.$$

Notemos que I'_ϵ satisface todas las condiciones para ser una deformación fuertemente genérica cíclicamente consistente de I si hacemos el denominador de ϵ un número más grande que 2, así, tómese por ejemplo $\epsilon = 1/11$. $\diamondsuit$

Aunque en los ejemplos anteriores escogimos ϵ de tal manera que I_ϵ resulte una especialización fuertemente genérica cíclicamente consistente, la ϵ propuesta no es única, aunque debemos considerar que queremos que

$$\lim_{\epsilon \to 0} m_{\epsilon,i} = m_i,$$

por lo que en nuestro caso, consideramos ϵ suficientemente chicas.

Damos ahora el algoritmo que nos ayudará a probar el Teorema 3.5.1, pero primero daremos una notación que nos servirá para simplificar nuestros enunciados a la hora de escribir el algoritmo.

Para un monomio $m_i = x^{a_i}y^{b_i}z^{c_i}$, tenemos su vector de grado $u_i = (a_i, b_i, c_i) \in \mathbb{N}^3$, el cuál vamos a representar por (a_i^v), con $v \in \mathbb{Z}/3\mathbb{Z}$, es decir, a^v representa a uno de los elementos de $\{a, b, c\}$, así $a^0 = a$, $a^1 = b$ y $a^2 = c$. Con esto podemos reescribir la condición de ser cíclicamente consistente por

$$a_i^v = a_j^v \quad \text{y} \quad a_i^{v+2} < a_j^{v+2} \implies a_{\epsilon,i}^v < a_{\epsilon,j}^v.$$

Con esta notación hecha, damos ahora el algoritmo.

Algoritmo 3.1. Input: un ideal monomial artiniano $I = \langle m_1, \ldots, m_n \rangle$ dentro de $[x, y, z]$, con $m_i = x^{a_i}y^{b_i}z^{c_i}$.

Output: una gráfica G que representa una resolución libre mínima para I.

A. Deformación de I: Hágase I_ϵ una deformación fuertemente genérica cíclicamente consistente de I, y sea $G = \text{Buch}(I_\epsilon)$.

B. Perturbación de la deformación: while $I_\epsilon \neq I$ do

   i) Encontrar una coordenada deformada mínima y un generador: $\hat{\imath}$ y $\hat{v}$ tal que $a_{\epsilon,\hat{\imath}}^{\hat{v}} = \text{mín}_j\{a_{\epsilon,j}^{\hat{v}} \mid a_{\epsilon,j}^{\hat{v}} \neq a_j^{\hat{v}}\}$, es decir, $a_{\epsilon,\hat{\imath}}^{\hat{v}}$ sea mínimo entre las coordenadas en $a^{\hat{v}}$ de la deformación y que satisfacen $a_{\epsilon,i}^{\hat{v}} \neq a_i^{\hat{v}}$.

   ii) Encontrar una región deformada mínima r de G correspondiente a la coordenada deformada mínima: una región en la que en su etiqueta (r^v) cumpla que $r^{\hat{v}} = a_{\epsilon,i}^{\hat{v}}$ y que $r^{\hat{v}+2}$ sea mínima entre dicho tipo de regiones. Nótese que la etiqueta de una región es el MCM de sus generadores, y que por región nos referimos a una región de G en la inmersión natural a la superficie de escalera. En otras palabras, una región es un ciclo de generadores[1] $C \subset \{m_1, \ldots, m_n\} \subset G$ para el cual ningún subconjunto es un ciclo y $\forall\ m_j \notin C$, $m_j \nmid \text{MCM}(C)$.

   iii) Encontrar un generador examinador de aristas: Encontrar al generador $m_{\epsilon,j}$ tal que $a_{\epsilon,j}^{\hat{v}} = \text{mín}_k\{a_{\epsilon,k}^{\hat{v}} \mid a_{\epsilon,k}^{\hat{v}+1} = r^{\hat{v}+1} \text{ y } a_{\epsilon,k}^{\hat{v}+2} < r^{\hat{v}+2}\}$.

[1]Nos referimos a una región como un ciclo mínimo en la gráfica G, que está formado por un triángulo y que está únicamente determinado por los tres generadores que la rodean

iv) Regresar la coordenada deformada mínima del generador deformado mínimo a su valor original: escríbase $a^{\hat{v}}_{\epsilon,\hat{\imath}} = a^{\hat{v}}_{\hat{\imath}}$, y reetiquétense las aristas y regiones de G concordantemente.

v) Uso del generador examinador de aristas: if $a^{\hat{v}}_{j} = a^{\hat{v}}_{\hat{\imath}}$, then bórrense de G la arista etiquetada con $\{a^{\hat{v}}_{\hat{\imath}}, r^{\hat{v}+1}, r^{\hat{v}+2}\}$, else déjese G sin cambios.

C. Salida: output la gráfica G etiquetada.

La ventaja de haber usado la notación introducida en el algoritmo, es que podemos trabajar y saber específicamente cómo tomar la deformación fuertemente genérica, sin importarnos cuál es la variable de coincidencia en los monomios. Para aclarar un poco la notación, trasladaremos un ejemplo a la notación anterior. Digamos que en el paso B.i) tenemos que la coordenada deformada mínima es la del generador $b_{\epsilon,\hat{\imath}}$ (el exponente de y en $m_{\epsilon,\hat{\imath}}$), es decir, $v = 1 \in \mathbb{Z}_3$ y así $b_{\epsilon,\hat{\imath}}$ es mínima y satisface $b_{\epsilon,\hat{\imath}} \neq b_{\hat{\imath}}$. Ahora, en el paso ii), supongamos que la región r encontrada tiene como etiqueta al monomio $x^{\alpha}y^{\beta}z^{\gamma}$, entonces, las condiciones que debemos verificar en este paso es que $\beta = b_{\epsilon,\hat{\imath}}$ y que α sea mínima. Para el paso iii), debemos encontrar un $m_{\epsilon,j}$ tal que el grado en z de $m_{\epsilon,j}$ sea γ, el grado en x sea menor que α, y que sea mínimo en el grado en y. En el paso iv), redefiniríamos I_ϵ al escribir $b_{\epsilon,\hat{\imath}} = b_{\hat{\imath}}$ y dejando igual los demás generadores. Para el paso v), en si algún $b_j = b_{\hat{\imath}}$, borraríamos la arista etiquetada por $x^{\alpha}y^{b_{\hat{\imath}}}z^{\gamma}$.

La razón del por qué escogimos deformaciones fuertes tan específicas como lo son las deformaciones fuertemente genéricas cíclicamente consistentes, es porque queremos tener control sobre las sizigias que estamos eliminando, en particular, a lo más una arista debe desaparecer en cada ocasión.

Demostración de validez del Algoritmo 3.1. Supóngase que I es un ideal fuertemente genérico, entonces no hay coincidencias en los exponentes, por lo que no es necesario hacer ninguna deformación, y el algoritmo termina inmediatamente, y correctamente gracias al Teorema 3.4.1, con la gráfica G como la resolución libre mínima. Así que para lo que resta

Supongamos ahora que I no es fuertemente genérico. Haremos la prueba por inducción en el número de pasos en el ciclo while - do. Primero supongamos que I_ϵ tiene una resolución libre mínima dada por G al principio del paso B. Mostraremos que la deformación I_ϵ levemente perturbada al final del ciclo, con una coordenada de un generador regresada a su valor original, es también resuelta mínimamente por la nueva gráfica G obtenida al final del ciclo.

Escojamos el generador deformado mínimo $m_{\epsilon,\hat{\imath}}$, y a la coordenada deformada mínima $\hat{v}$. Consideremos los puntos de la superficie de escalera cercanos a $m_{\epsilon,\hat{\imath}}$. Si un vector de grado $u = (a^v)$ tiene $a^{\hat{v}} = a^{\hat{v}}_{\hat{\imath}}$, entonces u cae en el plano correspondiente, el vector u cae en la superficie de escalera si además $\mathbf{x}^u \in I$ con $\mathbf{x}^w \notin I$ para $w = (b^v)$ tal que $b^{\hat{v}} < a^{\hat{v}}$, y $\mathbf{x}^w \in I$ para $b^{\hat{v}} > a^{\hat{v}}$.

Ahora, si u yace sobre la superficie de escalera, entonces $a^{\hat{v}+1} \geq a^{\hat{v}}_{\hat{\imath}}$. Supóngase que no, entonces $\mathbf{x}^u$ debe ser múltiplo de otro generador con la misma coordenada en $\hat{v}$, pero esto es

imposible puesto que las coordenadas deformadas son siempre únicas. Lo mismo se cumple para $\hat{v}+2$, así es que en $m_{\epsilon,\hat{\imath}}$, la superficie de escalera se ve localmente como la de un ideal principal, es decir, que existe un ideal monomial $J \subset \langle m_{\epsilon,\hat{\imath}} \rangle$ en que ningún elemento $j \in J$ coincida con $m_{\epsilon,\hat{\imath}}$ en ninguna coordenada, tal que la imagen de I_ϵ en $[x^\epsilon y^\epsilon z^\epsilon]/J$ es igual a la de $\langle m_{\epsilon,\hat{\imath}} \rangle$.

Dado que I_ϵ es artiniano (la superficie de escalera está acotada), para alguna r tenemos que $x^r_{\hat{v}+1} m_{\epsilon,\hat{\imath}}$ es el MCM de $m_{\epsilon,\hat{\imath}}$ y algún otro generador, es decir, alguna primera sizigia de I_ϵ debe tener esta forma; esta sizigia es única. Similarmente, dado que I_ϵ es artiniano, para alguna s tenemos que $x^s_{\hat{v}+2} x^r_{\hat{v}+1} m_{\epsilon,\hat{\imath}}$ es una segunda sizigia de I_ϵ; esta segunda sizigia está también únicamente determinada. Esta sizigia es el resultado de la rutina de encontrar una región deformada mínima del paso B.ii), y tenemos una manera de localizar esta región, que es más rápida que calcular y buscar sobre todas las regiones.

Enseguida encontramos el generador examinador de aristas; este generador hace que nuestra anterior búsqueda por la primera sizigia termine, es decir, este generador divide la etiqueta de la región deformada mínima y tiene a r como la coordenada $\hat{v}+1$. Por la minimalidad no puede suceder que tenga una coordenada $\hat{v}+2$ mayor o igual que la de $m_{\epsilon,\hat{\imath}}$, así es que debe tener una coordenada $\hat{v}+2$ estrictamente menor. Similarmente, debe tener también coordenada $\hat{v}$ estrictamente menor. Dado que la genericidad puede haber sido debilitada en esta etapa, es posible que más de un generador coincida con este criterio. Minimizando la coordenada $\hat{v}$ (o equivalentemente, maximizando la coordenada $\hat{v}+2$), podemos hacer esta elección única.

En el paso B.iv), redefinimos I_ϵ, y con ello también la superficie de escalera, al regresar la coordenada en $\hat{v}$ de $m_{\epsilon,\hat{\imath}}$ de vuelta a su valor original. Las arista de G permanecen igual, pero las etiquetas de un vértice y de sus aristas incidentes y regiones incidentes han sido cambiadas. Por la Proposición 3.4.2, G sigue siendo una resolución del nuevo ideal I_ϵ, sin embargo, la resolución puede no ser mínima.

La minimalidad de la resolución puede fallar si una etiqueta es compartida por más de una cara. Sólo la coordenada en $\hat{v}$ de un vértices ha cambiado, y ninguna etiqueta era compartida al principio del ciclo. Entonces cualquier etiqueta compartida debe involucrar un vértice reetiquetado, o una arista reetiquetada, o una región reetiquetada, incidente a $m_{\epsilon,\hat{\imath}}$, y un vértice, o arista, o región que no fue reetiquetada, y que tiene la misma coordenada en $\hat{v}$ que $a^{\hat{v}}_{\hat{\imath}}$ antes de la deformación. Ahora la condición de ser cíclicamente consistente entra en juego.

Para que una etiqueta sea compartida, las caras debe contener a un generador cuya coordenada en $\hat{v}$ sea $a^{\hat{v}}_{\hat{\imath}}$. Cualquier generador j con esta misma coordenada en $\hat{v}$ debe haber quedado sin deformar en el ciclo anterior, por tanto, por la minimalidad de $a^{\hat{v}}_{\hat{\imath}}$, debe tener tener una coordenada deformada en $\hat{v}$ menor que $m_{\hat{\imath}}$ en la deformación inicial. Entonces la coordenada en $\hat{v}+2$ no deformada de j debe ser a lo más igual que la de $m_{\hat{\imath}}$, o equivalentemente, la coordenada en $\hat{v}+1$ no deformada de j debe ser al menos la misma que la de $m_{\hat{\imath}}$, y entonces la deformación y la deformación perturbada refina los ordenes parciales en cada coordenada, y la actual coordenada en $\hat{v}+1$ de j debe ser al menos la de

$m_{\hat{\imath}}$. Esto implica que la coordenada $\hat{v}+1$ de j debe ser al menos r.

Todas las aristas y las regiones reetiquetadas tienen coordenada $\hat{v}+1$ a lo más r, por lo que las únicas aristas y regiones con r como coordenada $\hat{v}+1$ son las sizigias que encontramos anteriormente. La primera sizigia no podría convertirse en no mínima, pero la segunda sí podría haberse convertido en no mínima, y de ser así, en el paso B.v), borramos la (única posible) arista que evita esta minimalidad. ■

Antes de dar la prueba del Teorema 3.5.1, utilizaremos el Algoritmo 3.1 en los ejemplos de la Sección 3.3. En el caso del Ejemplo 3.3.1, como dijimos en el Ejemplo 3.5.1, el algoritmo inmediatamente termina, dejando Buch(J) como la gráfica de salida, puesto que J es ya fuertemente genérico y cíclicamente consistente.

Ejemplo 3.5.4. Ahora consideremos el ideal $I = \langle xy^2z, xyz^3, x^2, y^3z^2\rangle$. Primero necesitamos artenianizar I agregando, por ejemplo y^4 y z^4. Como vimos en el Ejemplo 3.5.2, una deformación fuertemente genérica cíclicamente consistente para I sería

$$I_\epsilon = \langle xy^2z, x^{1+\epsilon}yz^3, x^2, y^3z^2, y^4, z^4\rangle.$$

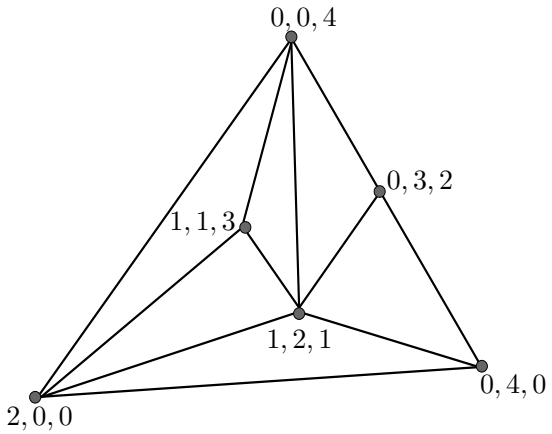

Figura 3.19: Buch(I_ϵ)

La gráfica de Buchberger para este ideal es la mostrada en la Figura 3.19. Ahora empezamos el ciclo del paso B en el algoritmo. Dado que $I_\epsilon \neq I$, empezamos la iteración del ciclo, y encontramos la coordenada deformada mínima, en este caso es la variable x del segundo generador, es decir, de $x^{1+\epsilon}yz^3$. Ahora necesitamos encontrar una región de G que tenga como etiqueta un monomio con dicha coordenada deformada en la variable x. Esta región es la correspondiente a los generadores xy^2z, $x^{1+\epsilon}yz^3$ y z^4, puesto que el MCM de estos monomios tiene como vector de grado $(1+\epsilon, 2, 4)$. Ahora, encontramos un generador para probar aristas, en este ejemplo sería el monomio xy^2z (porque en nuestro ejemplo $\hat{v} = 0$). Ahora, dejamos este generador a un lado, y regresamos la coordenada

deformada mínima a su valor original, y obtenemos en este caso $\langle xy^2z, xyz^3, x^2, y^3z^2, y^4, z^4\rangle$. Reetiquetamos G de acuerdo a esto y así obtenemos en este caso la misma gráfica que en la Figura 3.19, pero con las etiquetas siguientes:

La región triangular definida por xy^2z, xyz^3 y x^2, y que tiene etiqueta 2 2 3; la región triangular definida por xy^2z, xyz^3 y z^4, y que tiene etiqueta 1 2 4; la región triangular definida por xy^2z, x^2 y y^4, y que tiene etiqueta 2 4 1; la región triangular definida por xy^2z, x^2 y z^4, y que tiene por etiqueta 2 2 4; la región triangular definida por xy^2z, y^3z^2 y y^4, y que tiene por etiqueta 1 4 2; la región triangular definida por xy^2z, y^3z^2 y z^4, y que tiene por etiqueta 1 3 4; la región triangular definida por xyz^3, x^2 y z^4, y que tiene por etiqueta 2 1 4. Las aristas están dadas por la siguiente tabla:

Matriz de Adyacencia de la Gráfica de Buchberger Etiquetada

				1	2	1	1	1	3	2	0	0	0	3	2	0	4	0	0	0	4
1	2	1	:	0	0	0	1	2	3	2	2	1	1	3	2	1	4	1	1	2	4
1	1	3	:	1	2	3	0	0	0	2	1	3	0	0	0	0	0	0	1	1	4
2	0	0	:	2	2	1	2	1	3	0	0	0	0	0	0	2	4	0	2	0	4
0	3	2	:	1	3	2	0	0	0	0	0	0	0	0	0	0	4	2	0	3	4
0	4	0	:	1	4	1	0	0	0	2	4	0	0	4	2	0	0	0	0	0	0
0	0	4	:	1	2	4	1	1	4	2	0	4	0	3	4	0	0	0	0	0	0

Ahora usamos nuestro generador para probar aristas y ver si hay alguna arista que borrar. Como xy^2z y xyz^3 tienen la misma coordenada en x, debemos borrar una arista de G, utilizando el criterio del paso B.v). En este caso debemos borrar la arista que va de xy^2z a z^4 en la Figura 3.19.

Además, nuestro ideal originalmente no tenía a los últimos dos generadores, así es que quitando las aristas y uniendo las regiones correspondientes, obtenemos la gráfica de la Figura 3.20 como nuestra resolución libre mínima para I.

♢

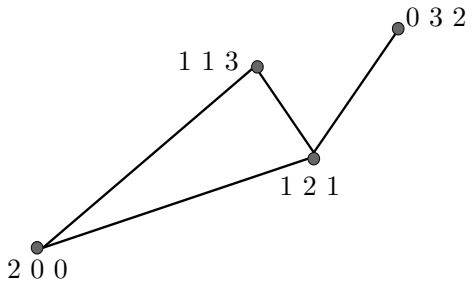

Figura 3.20: Resolución plana para I.

Ejemplo 3.5.5. Tomemos el ideal $I' = \langle x^2z, xyz, y^2z, x^5y^3, x^4y^4, x^3y^5\rangle$. Primero artenianizamos I' agregando x^6, y^6, z^6. Como vimos en el Ejemplo 3.5.3, una deformación fuertemente genérica cíclicamente consistente para I' sería

$$I'_\epsilon = \langle x^2z, xyz^{1+\epsilon}, y^2z^{1+2\epsilon}, x^5y^3, x^4y^4, x^3y^5, x^6, y^6, z^6\rangle.$$

La gráfica de Buchberger para este ideal es la mostrada en la Figura 3.21. Ahora, antes de estudiar el comportamiento del algoritmo en este ideal, vamos a convenir que los generadores están listados en orden, es decir, por ejemplo, para nosotros el séptimo generador será x^6, y así no resultará ambiguo, por ejemplo, el uso de m_3 para referirnos a $y^2z^{1+2\epsilon}$.

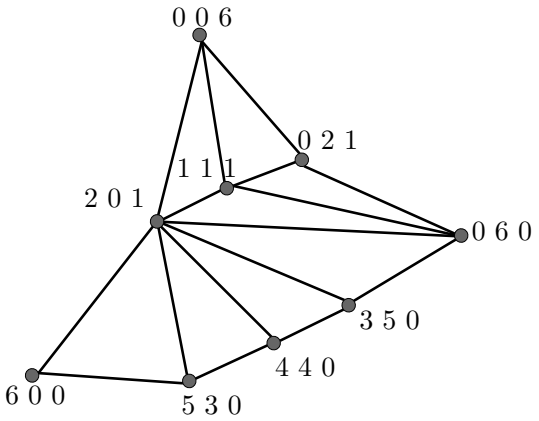

Figura 3.21: Buch(I'_ϵ).

Dado que $I' \neq I'_\epsilon$, empezamos la iteración del ciclo del paso B, y encontramos la coordenada deformada mínima, en este caso es la variable z del segundo monomio, es decir, $xyz^{1+\epsilon}$. Ahora encontramos una región en G cuya etiqueta tenga la variable deformada. Esta es la región correspondiente a los generadores m_1, m_2 y m_8 y tiene como etiqueta el vector $(2, 6, 1+\epsilon)$. Ahora encontramos el generador para probar aristas, en este ejemplo sería $m_1 = x^2z$, que tiene vector de grado $(2, 0, 1)$, ya que tiene la misma coordenada en x que $(2, 6, 1+\epsilon)$, la coordenada en y estrictamente menor. Ahora, dejamos este generador a un lado y regresamos la coordenada deformada mínima a su valor original, y obtenemos en este caso $\langle x^2z, xyz, y^2z^{1+2\epsilon}, x^5y^3, x^4y^4, x^3y^5, x^6, y^6, z^6\rangle$. Reetiquetamos G, y obtenemos en este caso la misma gráfica de la Figura 3.21. Ahora usamos nuestro generador para probar aristas y ver si hay alguna arista que borrar. Dado que m_1 y m_2 tienen la misma coordenada en z, que era la deformada, entonces hay que borrar una arista de G; como la arista que va de m_1 a m_8 tienen etiqueta $(2, 6, 1)$, entonces hay que borrar esta arista en el paso B.v).

Ahora como $I'_\epsilon = \langle x^2z, xyz, y^2z^{1+2\epsilon}, x^5y^3, x^4y^4, x^3y^5, x^6, y^6, z^6\rangle \neq I'$, entonces debemos seguir en la iteración del paso B. Encontramos la coordenada deformada mínima, en este

caso es en la variable z, del generador $m_3 = y^2z^{1+2\epsilon}$. Ahora encontramos la región de G que tenga como etiqueta un monomio con dicha coordenada deformada. Esta es la región definida por los generadores m_2, m_3 y m_8, y tiene como vector de grado $(1, 6, 1 + 2\epsilon)$. Encontramos al generador para probar aristas, ahora sería el monomio $m_2 = xyz$, lo ponemos a un lado y volvemos la coordenada deformada a su valor original, en este caso el resultado es de nuevo el ideal I'. Reetiquetamos la gráfica G, y usamos nuestro generador para probar aristas y ver si hay aristas por borrar. Ahora, dado que m_2 y m_3 coinciden en el exponente de la antes deformada variable z, entonces debemos borrar una arista de G. Esta arista debe tener como etiqueta al vector (1, 6, 1), y resulta ser la arista que une al monomio xyz con y^6. Así, nuestra gráfica de Buchberger final sería la de la Figura 3.22.

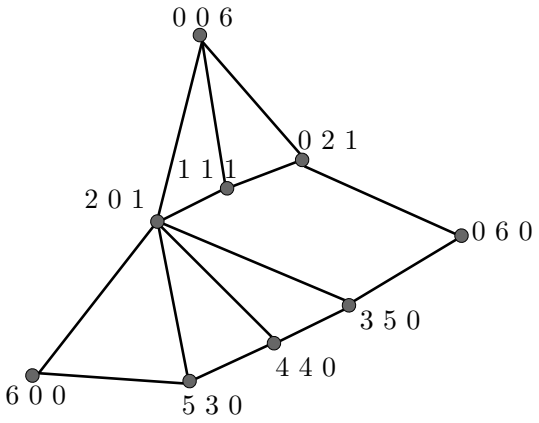

Figura 3.22: Buch(I'_ϵ) al final del algoritmo.

Como nuestro ideal I' originalmente no tenía las variables con potencias puras como generadores, quitando estos vértices de la gráfica en la Figura 3.22, con sus correspondientes aristas y regiones adyacentes, obtenemos la resolución libre mínima para I' dada por la gráfica de la Figura 3.23.

♢

Para terminar, ya que tenemos muy bien estudiado el Algoritmo 3.1, vamos a dar la prueba del Teorema 3.5.1.

Demostración del Teorema 3.5.1. El argumento que usamos al principio de la prueba al Teorema 3.4.1, también funciona aquí, así es que podemos reducir todo al caso artiniano. El Algoritmo 3.1 nos provee de una resolución libre mínima obtenida a partir de una aplicación plana. Lo que resta probar es que dicha gráfica G resulta casi 3−conexa.

Será suficiente producir tres trayectorias independientes (en el sentido de que las trayectorias sólo se intersecan en el vértice de salida y de llegada) a cada una de las potencias puras x^a, y^b, z^c, desde cada generador m_i de I. Es decir, aplicando el Teorema de Menger

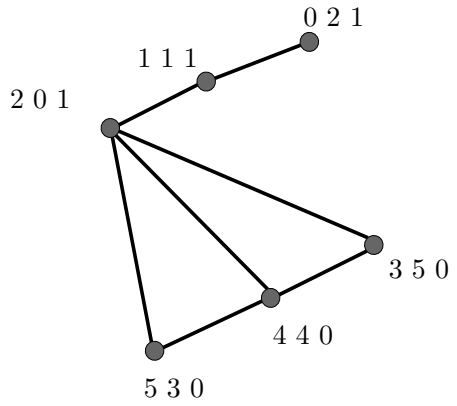

Figura 3.23: Resolución plana para el ideal I'.

(Teorema 3.2.1.) a la suspensión de G, debemos poder encontrar tres trayectorias independientes entre cualesquiera dos vértices. Consideremos la gráfica Buch(I) inmersa dentro de la superficie de escalera de I. Partiendo desde la esquina interior marcada por m_i, y viajando paralelamente al eje x, eventualmente topamos con un grado de una primera sizigia. Esta primera sizigia corresponde a una arista e de G. El otro punto donde termina e es un monomio m_j cuyas coordenadas en y y z son a lo más iguales a las de m_i. Continuando de esta forma, encontramos una sucesión de aristas en G, cuyos vértices tienen coordenada x estrictamente creciente, pero coordenadas en y y z decrecientes (no necesariamente de manera estricta). Repitiendo este proceso para las permutaciones cíclicas de x, y, z obtenemos las tres trayectorias deseadas. Estas se intersecan solamente en m_i puesto que son sucesiones monótonas. ■

Bibliografía

[1] K. Altmann and B. Sturmfels, *The graph of monomial ideals*, Journal of Pure and Applied Algebra **201** (2005), 250–263.

[2] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, New York, 1994.

[3] W. Bruns and J. Herzog, *Cohen-macaulay rings*, Cambridge University Press, Cambridge, 1993.

[4] B. Buchberger, *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal*, Ph.D. thesis, Univ. of Innsbruck, Math. Inst., 1965.

[5] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms : An introduction to computational algebraic geometry and commutative algebra*, 2a. ed., Springer-Verlag, New York, 1996.

[6] ———, *Using algebraic geometry*, Springer-Verlag, New York, 1998.

[7] R. Diestel, *Graph theory*, Springer Verlag, New York, 2005.

[8] G. Ewald, *Combinatorial convexity and algebraic geometry*, Springer-Verlag, New York, 1996.

[9] H. Li and F. Van Oystaeyen, *A primer of algebraic geometry: Constructive computational methods*, Marcel Dekker, New York, 2000.

[10] H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986.

[11] E. Miller, *Resolutions and duality for monomial ideals*, Ph.D. thesis, Univ. of California, Berkeley, 2000.

[12] ———, *Planar graphs as minimal resolutions of trivariate monomial ideals*, Documenta Mathematica (2002), no. 7, 43–90.

[13] E. Miller and B. Sturmfels, *Monomial ideals and planar graphs*, In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Honolulu) (M. Fossorier, H. Imai,

S. Lin, and A. Poli, eds.), Proceedings of AAECC, no. 13, Springer Lecture Notes in Computer Science 1719, Nov. 1999, pp. 19–28.

[14] ———, *Combinatorial commutative algebra*, Springer-Verlag, New York, 2005.

[15] E. Miller, B. Sturmfels, and K. Yanagawa, *Generic and cogeneric monomial ideals*, Journal of Symbolic Computation (2000), no. 29, 691–708.

[16] B. Mohar and C. Thomassen, *Graphs on surfaces*, Johns Hopkins University Press, Baltimore, 2001.

[17] J. Morton, *An implementation of the planar resolution algorithm*, preprint (2004), http://math.berkeley.edu/~mortonj/research.html.

[18] C. Musili, *Algebraic geometry for beginners*, Hindustan Book Agency, New Delhi, 2001.

[19] J. Rotman, *An introduction to homological algebra*, Springer-Verlag, New York, 2006.

[20] B. Sturmfels, *Grobner bases and convex polytopes*, American Mathematical Society, Univ. Lectures Series, no. 8, Providence, Rhode Island, 1996.

[21] W. V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, Springer-Verlag, Berlin, 2004.

[22] Charles A. Weibel, *An introduction to homological algebra*, Cambridge studies in advanced mathematics, no. 38, Cambridge University Press, Cambridge, 1994.

[23] A. T. White, *Graphs of groups on surfaces : Interactions and models*, Elsevier Science, Amsterdam, 2001.