Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

Unidad Iztapalapa

DIVISION DE CIENCIAS BASICAS E INGENIERÍA

"Bases SAGBI para anillos de coordenadas de Grassmannianas"

Tesis que presenta

Magdiel Delgado Castañeda

Matrícula: 2183802308

Para obtener el grado de

Maestro en Ciencias (Matemáticas)

Director

Dr. Felipe de Jesús Zaldívar Cruz

Departamento de Matemáticas

Jurados

Dr. Pedro Luis del Ángel Rodríguez

Dr. Enrique Javier Elizondo Huerta

Dr. Felipe de Jesús Zaldívar Cruz

Iztapalapa, Ciudad de México, Abril de 2021

Índice general

Agradecimientos

Quiero agradecer primeramente a Dios y a mi familia que siempre me han apoyado en todo momento. A mis papás y a mis hermanas. Gracias por siempre estar ahí.

Agradezco enormemente al Dr. Felipe Zaldívar Cruz, mi director de tesis, por todo su apoyo y enseñanzas durante los cursos de la maestría y durante la realización de este trabajo.

Así mismo agradezco a mis sinodales, Dr. Pedro Luis del Ángel y Dr. Javier Elizondo, por su disposición, tiempo y observaciones.

Finalmente, mi agradecimiento a CONACyT por el apoyo económico durante mis estudios de maestría.

Introducción

El concepto de *bases de Gröbner* fue introducido en el año 1965 por el matemático austríaco Bruno Buchberger. Una base de Gröbner es un conjunto generador de un ideal I del anillo de polinomios $K[x_1, \ldots, x_n]$ con ciertas propiedades especiales que permite simplificar de varias maneras el estudio del ideal dado. Una idea análoga puede considerarse si tomamos subálgebras del anillo de polinomios $K[x_1, \ldots, x_n]$ en lugar de ideales. Esto nos conduce al concepto de *bases* Sagbi, análogas de las bases de Gröbner de ideales.[1]

El objetivo de esta tesis es probar que el anillo de coordenadas de la variedad Grassmanniana tiene una base Sagbi. Este es un teorema original de *Bernd Sturmfels* dado en [9, Theorem 3.2.9] en 1993 y la demostración que damos sigue el texto [6] y las ideas del artículo [3], dando todos los preliminares y detalles requeridos para hacerlo autocontenido.

En el capítulo 1 introducimos las ideas generales de las *bases de Gröbner* junto con el algoritmo conocido como *algoritmo de Buchberger* que permite a partir de un sistema de generadores de un ideal dado, obtener una base de Gröbner en una cantidad finita de pasos. El capítulo 2 presenta distintas aplicaciones de las bases de Gröbner. En el capítulo 3 introducimos los ideales determinantales, que serán de suma importancia para el capítulo final. Así, en el capítulo 4 a través de la llamada *inmersión de Plücker* se prueba que la *Grassmanniana*, definida primeramente como el conjunto de ciertos subespacios de un espacio vectorial V, es una variedad proyectiva. Después mediante ciertas relaciones polinomiales, conocidas como *relaciones de Plücker* se caracterizan todos los puntos de dicha variedad. Finalmente, se prueba que existe una base Sagbi del anillo de coordenadas de la Grassmanniana.

[1]Sagbi es por sus siglas en inglés: *"Subalgebra analog to Gröbner bases for ideals"*.

1 Bases de Gröbner

Sean K un campo arbitrario y $S = K[x_1, \dots, x_n]$ el anillo de polinomios en n indeterminadas y con coeficientes en K considerado como anillo graduado en la forma usual (vea el Apéndice A para las propiedades genéricas de anillos conmutativos graduados y sus ideales).

En el anillo S los *monomios* juegan un papel importante, en primer lugar, considerando a S como un K-espacio vectorial; el conjunto de monomios forma una base de dicho espacio. Si se consideran dentro de S los ideales generados por monomios, las operaciones en estos ideales se verán traducidas a manipulaciones con los monomios generadores, lo que será conveniente en muchos casos.

1.1. Ideales monomiales

Definición 1.1 (Ideal monomial)**.** Un ideal monomial en $S = K[x_1, ..., x_n]$ es un ideal generado por monomios.

Ahora, queremos establecer cuándo un monomio u divide a otro monomio v. Decimos que $u = x_1^{a_1} \cdots x_n^{a_n}$ divide a $v = x_1^{b_1} \cdots x_n^{b_n}$ en $K[x_1, ..., x_n]$ si $a_i \leqslant b_i$ para toda i y lo denotamos por $u \mid b$.

Observación 1.2. Dado que $S = K[x_1, ..., x_n]$ es un DFU, existe (y es único salvo unidades) el máximo común divisor de u y v, así como el mínimo común múltiplo de u y v, éstos son respectivamente:

$$\mathrm{mcd}(u, v) = x_1^{\text{mín}\{a_1, b_1\}} \cdots x_n^{\text{mín}\{a_n, b_n\}}$$

$$\mathrm{mcm}(u, v) = x_1^{\text{máx}\{a_1, b_1\}} \cdots x_n^{\text{máx}\{a_n, b_n\}}.$$

Una característica importante de todo ideal monomial I es que un polinomio f pertenece a I si y sólo si los monomios que conforman f (que están en $\mathrm{sop}(f)$) están en I, situación que no ocurre en los ideales en general de S. Por ejemplo, sea $K[x_1, x_2]$ e $I = \langle x_1 + x_2, x_1^2 \rangle$.

El polinomio $f = 5(x_1 + x_2)$ es tal que $\operatorname{sop}(f) = \{x_1, x_2\} \nsubseteq I$. Así pues, a fin de caracterizar a los ideales monomiales, tenemos el siguiente resultado.

Teorema 1.3. *Sea* I *un ideal de* $K[x_1, ..., x_n]$. *Las siguientes condiciones son equivalentes:*

(1) I *es un ideal monomial*

(2) *Para todo* $f \in I$ *tenemos que* $\operatorname{sop}(f) \subseteq I$

Demostración. (1) $\Rightarrow$ (2): Sea $f \in I$, dado que I es monomial, entonces se tiene que existen $u_1, \ldots, u_m \in \mathfrak{M}$, donde $\mathfrak{M}$ es un conjunto de monomios generadores de I, y $f_1, \ldots, f_m \in S$ tal que $f = \sum_{i=1}^m f_i u_i$. De la igualdad anterior se sigue que $\operatorname{sop}(f) \subseteq \bigcup_{i=1}^m \operatorname{sop}(f_i u_i)$. Así, dado $u \in \operatorname{sop}(f)$ existe i tal que $u \in \operatorname{sop}(f_i u_i)$, así que u es de la forma $u = \nu u_i$ para algún monomio ν y por tanto $u \in I$, esto es, $\operatorname{sop}(f) \subseteq I$

(2) $\Rightarrow$ (1): Por otro lado, supongamos que para todo $f \in I$ tenemos que $\operatorname{sop}(f) \subseteq I$. Sea I ideal de S y tomemos cualquier conjunto generador de I, digamos $\{f_1, \ldots, f_n\}$. En general tenemos que $I \subseteq \langle \bigcup_{i=1}^n \operatorname{sop}(f_i) \rangle$, pues cualquier polinomio es combinación lineal de los elementos de su soporte, pero dado que por hipótesis tenemos que $\operatorname{sop}(f_i) \subseteq I$ para toda i entonces tenemos que $\bigcup_{i=1}^n \operatorname{sop}(f_i)$ está contenida en I y por tanto $I \subseteq \langle \bigcup_{i=1}^n \operatorname{sop}(f_i) \rangle \subseteq I$ por lo que I está generado por $\bigcup_{i=1}^n \operatorname{sop}(f_i)$, esto es, es un ideal monomial. □

El anillo $S = K[x_1, \ldots, x_n]$ es noetheriano por lo que sus ideales (en particular los ideales monomiales) son finitamente generados. Una situación deseable es que dado un ideal monomial I podamos tener un conjunto finito de *monomios* que generen a I. Esta situación es cierta y se sigue del siguiente resultado conocido como *lema de Dickson*:

Teorema 1.4 (Lema de Dickson)**.** *Sea* $\mathfrak{M}$ *un conjunto no vacío de monomios en* $K[x_1, ..., x_n]$, *entonces con respecto al orden parcial dado por la divisibilidad,* $\mathfrak{M}$ *tiene sólo un número finito de elementos mínimos.*

Demostración. Procederemos por inducción sobre el número de indeterminadas de S. Supongamos $n = 1$ y sea $\mathfrak{M}$ un conjunto de monomios de S, entonces $\mathfrak{M} = \{x_1^a : a \in A \subset \mathbb{N}\}$. Por el *principio del buen orden* en $\mathbb{N}$ existe $b \in A$ el menor elemento, luego x_1^b divide a x_1^a para todo $a \in A$, por lo que $\{x_1^b\}$ es el conjunto de elementos mínimos de $\mathfrak{M}$.

Supongamos ahora que $n > 1$ y sea $\mathfrak{N} = \{\mathbf{x^c} \in K[x_1, \ldots, x_{n-1}] : \mathbf{x^c} x_n^d \in \mathfrak{M}$, para algún $d \geqslant 0\}$. Aplicando la hipótesis de inducción al conjunto $\mathfrak{N}$ se tiene que el conjunto de elementos mínimos de $\mathfrak{N}$ es finito, digamos $\mathfrak{N}^{\text{mín}} = \{\mathbf{x^{c_1}}, \ldots, \mathbf{x^{c_r}}\}$. Por definición para cada $\mathbf{x^{c_j}}$ existe $a_j \geqslant 0$ tal que $\mathbf{x^{c_j}} x_n^{a_j} \in \mathfrak{M}$. Sea $a = \text{máx}\{a_1, \ldots, a_r\}$ y para cada b con $0 \leqslant b < \alpha$ sea $\mathfrak{N}_b = \{\mathbf{x^c} \in K[x_1, \ldots, x_{n-1}] : \mathbf{x^c} x_n^b \in \mathfrak{M}\}$. Nuevamente aplicando la hipótesis de inducción, tenemos que $\mathfrak{N}_b^{\text{mín}}$ es un conjunto finito. Denotamos el conjunto de los monomios $\mathbf{x^c} x_n^b$ como $\mathfrak{N}_b^{\text{mín}} x_n^b$ y por la forma en que está definido este conjunto tenemos que:

$$\mathfrak{M}^{\text{mín}} \subseteq \{\mathbf{x^{c_1}} x_n^{a_1}, \ldots, \mathbf{x^{c_r}} x_n^{a_r}\} \cup \bigcup_{b=0}^{a-1} \mathfrak{N}_b^{\text{mín}} x_n^b \tag{1.1}$$

Y dado que el lado derecho es un conjunto finito, tenemos que $\mathfrak{M}^{\text{mín}}$ es finito. □

Corolario 1.5. *Sea* I *un ideal monomial. Entonces cada conjunto de monomios que generan a* I *contiene un conjunto finito que genera a* I

Demostración. Sea $\mathfrak{M}$ un conjunto de monomios generadores de I, luego por el lema de Dickson el conjunto de elementos mínimos es finito, dicho conjunto es es un conjunto de monomios generadores de I. □

Si I es un ideal minimal, un conjunto de monomios generadores de I es llamado *mínimo* si cualesquiera de sus subconjuntos propios no generan a I. Un resultado que se desprende del corolario anterior es que existe un *único* conjunto mínimo generador de monomios de I. Denotamos dicho conjunto por $G(I)$.

1.1.1. Operaciones con ideales monomiales

Lema 1.6. *Sean* I *y* J *ideales monomiales. Entonces* $I+J$, IJ *e* $I \cap J$ *son ideales monomiales y además:*

(1) $G(I+J) \subseteq G(I) \cup G(J)$

(2) $G(IJ) \subseteq G(I)G(J)$

(3) *Si* $G(I) = \{u_1, ..., u_r\}$ *y* $G(J) = \{v_1, ..., v_s\}$. *Entonces:* $I \cap J = \langle\{\text{mcm}(u_i, v_j) : i = 1, ..., r;\ j = 1, ..., s\}\rangle$.

Demostración. Para el inciso (1) tenemos que dados dos conjuntos generadores de los ideales I y J, el ideal generado por la unión de éstos es un ideal que contiene tanto a I como a J y dado que $I + J$ es el ideal más pequeño que contiene a I y a J se sigue que la unión de los conjuntos generadores de I y J generan a $I + J$, luego el conjunto mínimo que genere a $I + J$ tendrá a lo más los elementos de $\subseteq G(I) \cup G(J)$.

Para (2) si consideramos I y J ideales, sabemos que el ideal IJ está generado por todos los productos de generadores de I con generadores de J, así un conjunto mínimo de generadores de IJ tendrá a lo más los elementos de $G(I)G(J)$ donde este último conjunto consta de todos los productos de elementos de $G(I)$ con elementos de $G(J)$

Para (3) tenemos que si $u \in I \cap J$ es un monomio, entonces existe $u_i \in G(I)$ y $v_j \in G(J)$ tal que $u_i|u$ y $v_j|u$. Por lo tanto $\text{mcm}(u_i, v_j)|u$ y así $u \in \langle\{\text{mcm}(u_i, v_j) : i = 1, ..., r;\ j = 1, ..., s\}\rangle$. Por otro lado, dado que $\text{mcm}(u_i, v_j)$ es múltiplo de u_i y de v_j, se sigue que $\text{mcm}(u_i, v_j) \in I \cap J$, lo que concluye la prueba. □

1.2. Órdenes monomiales

Consideremos el anillo de polinomios $S = K[x_1, ..., x_n]$. Buscamos definir un orden total en el conjunto de monomios de S, conjunto al que denotaremos por $\text{Mon}(S)$.

Definición 1.7 (Orden monomial)**.** Un orden monomial en S es un orden total $\leqslant$ en $\mathrm{Mon}(S)$ que satisface las siguientes propiedades:

(1) $1 \leqslant u$ para todo $u \in \mathrm{Mon}(S)$

(2) Si $u \leqslant v$ y $w \in \mathrm{Mon}(S)$ entonces: $uw \leqslant vw$

Antes de ver algunos ejemplos de órdenes monomiales, enunciamos una propiedad importante de éstos.

Proposición 1.8. *Sea $\leqslant$ un orden monomial en S. Entonces se tiene:*

(1) *Si $u, v \in \mathrm{Mon}(S)$ con $u \mid v$, entonces $u \leqslant v$*

(2) *Si $u_1, u_2, ...$ es una sucesión de monomios con $u_1 \geqslant u_2 \geqslant \cdots$, entonces existe un entero m tal que $u_i = u_m$, para todo $i \geqslant m$*

Demostración. El inciso (1) se sigue inmediatamente, pues si $u \mid v$ entonces existe $w \in \mathrm{Mon}(S)$ tal que $uw = v$. Además $1 \leqslant w$ por primera propiedad de orden monomial y por la segunda propiedad tenemos: $u \leqslant uw = v$, así $u \leqslant v$.

Para el inciso (2) sea $\mathcal{M} = \{u_1, \ldots, ...\}$. Por el lema de Dickson tenemos que este conjunto tiene un número finito de elementos mínimos (de acuerdo al orden dado por la divisibilidad), digamos $u_{i_1}, \ldots, u_{i_r}$ con $i_1 < i_2 < \cdots < i_r$. Sea j cualquier entero $\geqslant i_r$, entonces existe un entero $1 \leqslant k < r$ tal que $u_{i_k} | u_j$. Por (1) esto implica que $u_{i_k} \leqslant u_j$. Así, $u_{i_k} \geqslant u_{i_r} \geqslant u_j \geqslant u_{i_k}$, así que $u_{i_r} = u_j$. Por tanto, podemos escoger $m = i_r$ □

Ejemplos importantes de órdenes monomiales son los siguientes:

Ejemplo 1.8.1 (Orden lexicográfico puro). Sean $\mathbf{x}^{\mathbf{a}}$, $\mathbf{x}^{\mathbf{b}}$ dos monomios en S. Decimos que $\mathbf{x}^{\mathbf{a}} < \mathbf{x}^{\mathbf{b}}$ si la primera componente no nula de izquierda a derecha de $\mathbf{a} - \mathbf{b}$ es negativa. Por ejemplo: $x_1 x_2^2 < x_1^2 x_2$

Ejemplo 1.8.2 (Orden lexicográfico normal). Sean $\mathbf{x}^{\mathbf{a}}$, $\mathbf{x}^{\mathbf{b}}$ dos monomios en S. Decimos que $\mathbf{x}^{\mathbf{a}} < \mathbf{x}^{\mathbf{b}}$ si ya sea $\sum_{i=1}^{n} a_i < \sum_{i=1}^{n} b_i$ ó $\sum_{i=1}^{n} a_i < \sum_{i=1}^{n} b_i$ y la primera componente no nula de izquierda a derecha de $\mathbf{a} - \mathbf{b}$ es negativa. Por ejemplo, $x_1 x_2 < x_1^2 x_2$

Observe que con ambos ejemplos, podemos ordenar las indeterminadas de la siguiente manera: $x_1 > x_2 > \cdots > x_n$

1.2.1. Construcción de órdenes monomiales

Sea $<$ un orden monomial arbitrario con $x_n < x_{n-1} < \cdots < x_1$.

Podemos construír un nuevo orden monomial vía una permutación σ del conjunto $\{1, ..., n\}$. Sea $\sigma : \{1, ..., n\} \to \{1, ..., n\}$ una permutación. Definimos un nuevo orden monomial, denotado por $<_\sigma$, como sigue:

$$\mathbf{x}^{\mathbf{a}} <_\sigma \mathbf{x}^{\mathbf{b}} \iff \mathbf{x}^{\sigma(\mathbf{a})} < \mathbf{x}^{\sigma(\mathbf{b})}$$

donde $\sigma(\mathbf{e}) = (e_{\sigma(1)}, ..., e_{\sigma(n)})$ con $\mathbf{e} = (e_1, ..., e_n) \in \mathbb{N}^n$.

Es inmediato ver que en efecto $<_\sigma$ es un orden monomial y que satisface:

$$x_{\sigma(n)} <_\sigma x_{\sigma(n-1)} <_\sigma \cdots <_\sigma x_{\sigma(1)}$$

1.3. Ideales iniciales y bases de Gröbner

Sea $<$ un orden monomial en el anillo de polinomios $S = K[x_1, ..., x_n]$.

Obsérvese que si $f \neq 0$ es un polinomio en $S = K[x_1, ..., x_n]$, podemos identificar al mayor monomio u con respecto a $<$ y tal que $u \in \text{sop}(f)$. A dicho monomio lo llamamos *monomio inicial* y lo denotamos por $\text{in}_<(f)$. El coeficiente c de $\text{in}_<(f)$ lo llamamos *coeficiente principal* de f con respecto a $<$ y decimos que $c\text{in}_<(f)$ es el *término principal* de f. Por convención, definimos $\text{in}_<(0) = 0$, además $\text{in}_<(0) < \text{in}_<(f)$ para todo $f \neq 0$. El siguiente lema será útil para operar con polinomios y relacionarlos con sus monomios iniciales, específicamente para la suma y producto de ellos.

Lema 1.9. *Sea $<$ un orden monomial en $S = K[x_1, \ldots, x_n]$ y $f_1, \ldots, f_r$ polinomios no nulos en S. Entonces tenemos las siguientes reglas para los monomios iniciales de la suma y producto de éstos.*

(1) $\text{in}_<(f_1 \cdots f_r) = \text{in}_<(f_1) \cdots \text{in}_<(f_r)$

(2) $\text{in}_<(f_1 + \cdots + f_r) \leqslant \text{máx}\{\text{in}_<(f_1), \ldots, \text{in}_<(f_r)\}$ *y la igualdad se sostiene si y sólo si* $\sum_j a_j \neq 0$ *donde* a_j *es el coeficiente principal de* f_j *y la suma es sobre todos los* j *tales que tales que* $\text{in}_<(f_j) \geqslant \text{in}_<(f_i)$ *para todo* i.

Demostración. (1) Primeramente obsérvese que: $\text{in}_<(f_1) \cdots \text{in}_<(f_r) \geqslant u_1 \cdots u_r$ para todo $u_i \in \text{sop}(f_i)$, esto por definición de monomio inicial. La igualdad se da si y sólo si $u_i = \text{in}_<(f_i)$ para $i = 1, \ldots, r$. Así, dado que los monomios en $\text{sop}(f_1 \cdots f_r)$ son de la forma $u_1 \cdots u_r$ con $u_i \in \text{sop}(f_i)$ y como $\text{in}_<(f_1) \cdots \text{in}_<(f_r)$ pertenece a $\text{sop}(f_1 \cdots f_r)$ concluímos que $\text{in}_<(f_1 \cdots f_r) = \text{in}_<(f_1) \cdots \text{in}_<(f_r)$.

(2) Dado que $\text{sop}(f_1 + \cdots + f_r \subseteq \bigcup_{i=1}^r \text{sop}(f_i)$ tenemos que: $\text{in}_<(f_1 + \cdots + f_r) \leqslant \text{máx}\{v : v \in \bigcup_{i=1}^r \text{sop}(f_i)\} = \text{máx}\{\text{in}_<(f_1), \ldots, \text{in}_<(f_r\}$. Para la última parte sea v el máximo monomio inicial que aparece entre los f_i. Supongamos que $\sum_j a_j \neq 0$, donde la suma es sobre los j tales que $\text{in}_<(f_j) = v$, entonces $v \in \text{sop}(f_1 + \cdots + f_r)$. Por tanto, $\text{in}_<(f_1 + \cdots + f_r) \geqslant v = \text{máx}\{\text{in}_<(f_1), \ldots, \text{in}_<(f_r)\}$ y dado que ya hemos probado la otra desigualdad concluímos que $\text{in}_<(f_1 + \cdots + f_r) = \text{máx}\{\text{in}_<(f_1), \ldots, \text{in}_<(f_r)\}$. Recíprocamente si $\sum_{j=1}^k a_j = 0$, entonces $v \notin \text{sop}(f_1 + \cdots + f_r)$ y así tenemos que $\text{in}_<(f_1 + \cdots + f_r) \neq \text{máx}\{\text{in}_<(f_1), \ldots, \text{in}_<(f_r)\}$ lo que concluye la demostración. $\square$

A partir de los monomios iniciales podemos definir al ideal inicial de un ideal arbitrario I de S como sigue.

Definición 1.10 (Ideal inicial)**.** Sea I un ideal de S no nulo, el *ideal inicial* de I es el ideal monomial:

$$\mathrm{in}_<(\mathrm{I}) =< \mathrm{in}_<(f) : f \in \mathrm{I}, f \neq 0 >$$

Si $\mathrm{I} = \langle 0 \rangle$, definimos $\mathrm{in}_<(\mathrm{I}) = \langle 0 \rangle$.

Observación 1.11. En principio no podemos garantizar que $\mathrm{in}_<(\mathrm{I})$ sea generado por una cantidad finita de monomios iniciales. Sin embargo, dado que $\mathrm{in}_<(\mathrm{I})$ es un ideal monomial por el corolario 1.5 tenemos que existen $g_1, g_2, ..., g_m$ tales que:

$$\mathrm{in}_<(\mathrm{I}) = \langle \mathrm{in}_<(g_1), ..., \mathrm{in}_<(g_m) \rangle$$

Entonces dado un ideal inicial $\mathrm{in}_<(\mathrm{I})$ podemos garantizar la existencia de una cantidad finita de polinomios en I cuyos monomios iniciales generan a tal ideal inicial. La pregunta inmediata es *cómo* encontrar estos polinomios, situación que abordaremos en los siguientes resultados. Primeramente establecemos la siguiente definición.

Definición 1.12. Sea $\mathrm{I} \subseteq S$ un ideal y sea $<$ un orden monomial en S. Una colección de polinomios $g_1, g_2, ..., g_m$ en I tales que $\mathrm{in}_<(\mathrm{I}) = \langle \mathrm{in}_<(g_1), ..., \mathrm{in}_<(g_m)$, es llamada una *base de Gröbner* de I con respecto a $<$.

La observación 1.11 y la consecuente definición de una *base de Gröbner* de I con respecto a $<$ nos garantiza la existencia, pero no nos da una forma de calcular dicha base. Un caso particular es cuando el ideal I es principal; esto es: $\mathrm{I} = \langle g \rangle$ en cuyo caso es inmediato que g es una base de Gröbner de I.

De una manera más general discutiremos más adelante el algoritmo de Buchberger, el cual nos dará un método para calcular la base de Gröbner de un ideal. Antes de ello enunciaremos algunos resultados importantes previos.

Teorema 1.13 (Macaulay)**.** *Sea $<$ un orden monomial en S y sea I ideal propio de S. Entonces los monomios en S que no pertenecen a $\mathrm{in}_<(\mathrm{I})$ forman una K-base de S/I.*

Demostración. Primero veamos que los monomios que no pertenecen a $\mathrm{in}_<(\mathrm{I})$ son linealmente independientes módulo I. Supongamos lo contrario, entonces existe un polinomio no cero f en I tal que $\mathrm{sop}(f) \cap \mathrm{Mon}(\mathrm{in}_<(\mathrm{I})) = \emptyset$, pero esto contradice el hecho de que $\mathrm{in}_<(f) \in \mathrm{in}_<(\mathrm{I})$

Nos resta probar que las clases residuales de monomios en S que no pertenecen a $\mathrm{in}_<(\mathrm{I})$ generan a S/I como K-espacio vectorial. Para probar esto veamos que para todo $f \in S$ existe $g \in S$ tal que $f + \mathrm{I} = g + \mathrm{I}$ y $\mathrm{sop}(g) \cap \mathrm{Mon}(\mathrm{in}_<(\mathrm{I})) = \emptyset$. Supongamos lo contrario y sea $f \in S$ un polinomio con el monomio inicial más pequeño para el cual no podemos encontrar un polinomio g como hemos descrito. Sea c el coeficiente principal de f, entonces $f - c\,\mathrm{in}_<(f)$ tiene un monomio inicial más pequeño y así existe $g \in S$ con $\mathrm{sop}(g) \cap \mathrm{Mon}(\mathrm{in}_<(\mathrm{I})) = \emptyset$ y tal que $(f - c\,\mathrm{in}_<(f)) + \mathrm{I} = g + \mathrm{I}$. Así, $f + \mathrm{I} = (c\,\mathrm{in}_<(f) + g) + \mathrm{I}$. Si $\mathrm{in}_<(f) \notin \mathrm{in}_<(\mathrm{I})$, podemos reemplazar g por $c\,\mathrm{in}_<(f) + g$ contradiciendo así la elección de f. Si $\mathrm{in}_<(f) \in \mathrm{in}_<(\mathrm{I})$, entonces existe $h \in I$ con término principal 1 y $\mathrm{in}_<(h) = \mathrm{in}_<(f)$. Se sigue que $f - ch$ tiene un monomio inicial más pequeño que f. Así, encontramos un polinomio $g \in S$ con $\mathrm{sop}(g) \cap \mathrm{Mon}(\mathrm{in}_<(I) = \emptyset$ y $(f - ch) + I = g + I$. Dado que $f + I = (f - ch) + I$ tenemos una contradicción por la forma en que fue elegida f. $\square$

Un hecho que surge como consecuencia de este teorema es que todo ideal I en S tiene sólo una cantidad finita de ideales iniciales.

Hemos visto que un sistema de generadores de I no necesariamente es una base de Gröbner de I. Sin embargo, tenemos el siguiente resultado que garantiza que una vez hallada una base de Gröbner de un ideal tenemos un sistema de generadores de éste.

Teorema 1.14. *Sea I un ideal de S y sean $g_1, ..., g_n$ una base de Gröbner de I con respecto a un orden monomial $<$. Entonces $g_1, ..., g_n$ es un sistema de generadores de I*

Demostración. Si $f \in I$, entonces $\mathrm{in}_<(f)$
$ini_<(I) = \langle \mathrm{in}_<(g_1), ..., \mathrm{in}_<(g_n) \rangle$. Por lo tanto, existe un entero $1 \leqslant i \leqslant m$ y un monomio w tal que $\mathrm{in}_<(f) = w\,\mathrm{in}_<(g_i)$

Sea c el coeficiente de $\mathrm{in}_<(f)$ en f y d el coeficiente de $\mathrm{in}_<(g_i)$ en g_i y sea $h = f - cd^{-1}wg_i$. Entonces $h \in I$.

Si $h = 0$ entonces $f = cd^{-1}wg_i \in \langle g_1, ..., g_m \rangle$.

Ahora, asumamos $h \neq 0$. Dado que $\mathrm{in}_<(f) > \mathrm{in}_<(h)$ y dado que cada cadena estrictamente descendiente de monomios se estaciona, podemos aplicar un argumento de inducción y así asumir que h es una combinación lineal de los g_i con coeficientes en S. Dado que $f = h + cd^{-1}wg_i$, concluímos que $f \in (g_1, ..., g_m)$ $\square$

Dado que cada ideal tiene una base de Gröbner y cada base de Gröbner contiene una cantidad finita de elementos, tenemos así directamente el teorema de la Base de Hilbert.

Corolario 1.15 (Teorema de la base de Hilbert)**.** *Cada ideal en el anillo de polinomios S es finitamente generado.*

1.3.1. El algoritmo de la división

El siguiente resultado generaliza el algoritmo de la divisón para polinomios de una variable extendiéndolo a polinomios en varias variables y no sólo considerando un polinomio como divisor sino una cantidad finita de ellos. Precisamos esta idea a continuación.

Teorema 1.16 (Algoritmo de la división)**.** *Sean f y $g_1, ..., g_m$ polinomios en S con $g_i \neq 0$. Dado un orden monomial $<$, existen polinomios $q_1, ..., q_m$ y un polinomio $r \in S$ con*

$$f = q_1g_1 + q_2g_2 + \cdots + q_mg_m + r$$

tal que se cumplen las siguientes condiciones:

(1) *Ningún elemento de* $\mathrm{sop}(r)$ *está contenido en el ideal* $(\mathrm{in}_<(g_1, ..., \mathrm{in}_<(g_m))$

(2) $\mathrm{in}_<(f) \geqslant \mathrm{in}_<(q_i g_i)$ *para todo* i.

Una ecuación $f = q_1g_1 + q_2g_2 + \cdots + q_mg_m + r$ que satisface las dos condiciones del teorema es llamada una *expresión estándar* de f y r es llamado un *residuo* de f con respecto a $g_1, ..., g_m$. El polinomio f puede tener diferentes expresiones estándar y diferentes residuos con respecto a $g_1, ..., g_m$. Decimos que f se *reduce* a 0 con respecto a $g_1, ..., g_m$ si f tiene un residuo con respecto a $g_1, ..., g_m$ el cual es 0.

Proposición 1.17. *Dado un orden monomial* $<$ *en* S. *Asumimos que los polinomios* $g_1, ..., g_m$ *forman una base de Gröbner del ideal* $I = (g_1, ..., g_m)$. *Entonces cada polinomio* $f \in S$ *tiene un único residuo respecto a* $g_1, ..., g_m$.

Demostración. Sea $f \in S$ y sean $f = \sum_{i=1}^{m} q_i g_i + r$ y $f = \sum_{i=1}^{m} p_i g_i + r$ dos expresiones estándar de f. Entonces $h = r - s \in I$. Supongamos que $h \neq 0$.

Entonces $\mathrm{in}_<(h) \in \mathrm{in}_<(I) = (\mathrm{in}_<(g_1), ..., \mathrm{in}_<(g_m))$. Dado que $\mathrm{in}_<(h) \in \mathrm{sop}(r) \cup \mathrm{sop}(s)$ y r, s son residuos de f tenemos una contradicción. Por lo tanto $h = 0$, es decir $r = s$. □

De la proposición 1.17 se sigue el siguiente corolario que nos da una condición necesaria y suficiente para la pertenencia a un ideal dado I de un polinomio en S.

Corolario 1.18. *Sea* $I = \langle g_1, \ldots, g_m \rangle$ *un ideal y supongamos que* $g_1, \ldots, g_m$ *es una base de Gröbner de* I *respecto a algún orden monomial. Entonces* $f \in S$ *si y sólo si* f *se reduce a* 0 *respecto a* $g_1, \ldots, g_m$.

Demostración. Si $f \in I$, entonces considerando la expresión estándar de f tenemos $f = q_1g_1 + \cdots + q_mg_m + r$. Luego, $r = f - q_1g_1 + \cdots + q_mg_m$ por lo que $r \in I$. Supongamos $r \neq 0$, entonces $\mathrm{in}_<(r)\,\mathrm{in}_<(I) = \langle ini_<(g_1, \ldots, ini_<(g_m)) \rangle$ lo que contradice la definición de residuo en la expresión estándar de f, por lo que $r = 0$ y así f se reduce a 0 respecto a $g_1, \ldots, g_m$. Por otro lado, si f se reduce a 0 respecto a $g_1, \ldots, g_m$, entonces f es combinación lineal de dichos polinomios por lo que $f \in I$. □

Para finalizar esta sección realizamos un ejemplo del algoritmo de la división usando el software `Macaulay2`.

Ejemplo 1.18.1 (Ejemplo1). Sea $f = x^2 \in \mathbb{Z}[x, y]$. Buscamos calcular la expresión estándar de f respecto a los polinomios $q_1 = x - y^2$ y $q_2 = y$. Para lo cual calculamos en `Macaulay2` usando el algoritmo de la división.

```
i1 :  R=ZZ[x,y]

o1 = R

o1 : PolynomialRing

```

```
i2 :  f = x^2

       2
o2 = x

o2 : R

i3 : G={x-y^2,y}

           2
o3 = {- y  + x, y}

o3 : List

i4 : f// matrix{G}

o4 = {2} | x  |
     {1} | xy |

                2        1
o4 : Matrix R  <--- R
```

Observe que la salida o4 da los polinomios q_1 y q_2 que nos permite obtener la expresión estándar de f donde en este caso el residuo es 0. Así, podemos verificar fácilmente que la expresión estándar de f es:

$$f = x(x - y^2) + xy(y)$$

1.3.2. El criterio de Buchberger

Sea I un ideal de S. En esta parte discutiremos un algoritmo que permite, a partir de un sistema de generadores $\mathfrak{G}$ de I calcular una base de Gröbner.

Primeramente introducimos los llamados S-polinomios. Supóngase que se tenemos un ideal $I = \langle f, g\rangle$ generado por dos polinomios no cero. La cuestión es hallar una base de Gröbner de I. Sabemos que $\mathrm{in}_<(f)$, $\mathrm{in}_<(g)$ pertenecen a $\mathrm{in}_<(I)$. Observe que un candidato a polinomio $h \in I$ cuyo monomio inicial no esté en $\langle \mathrm{in}_<(f), \mathrm{in}_<(g)\rangle$ sería una combinación lineal de f y g tal que su término incial se cancele. En este sentido construímos tal polinomio llamado el S-polinomio de f y g definido de la siguiente manera:

$$S(f,g) = \frac{\mathrm{mcm}(\mathrm{in}_<(f), \mathrm{in}_<(g))}{c\,\mathrm{in}_<(f)} f - \frac{\mathrm{mcm}(\mathrm{in}_<(f), \mathrm{in}_<(g))}{d\,\mathrm{in}_<(g)} g$$

donde c y d son los coeficientes principales de f y g respectivamente.

Teorema 1.19. *Sea $<$ un orden monomial en S y sea $I = (g_1, ..., g_m)$ un ideal en S con $g_i \neq 0$ para todo i. Entonces las siguientes condiciones son equivalentes:*

(1) $g_1, ..., g_m$ *es una base de Gröbner de* I *con respecto a* $<$.

(2) $S(g_i, g_j)$ *se reduce a* 0 *con respecto a* $g_1, ..., g_m$ *para todo* $i < j$.

Demostración. (1) $\Rightarrow$ (2) Dado que $S(g_i, g_j) \in I$ y $g_1, ..., g_m$ es una base de Gröbner de I se sigue del corolario 1.18 que el residuo de $S(g_i, g_j)$ con respecto a $g_1, ..., g_m$ es 0.
(2) $\Rightarrow$ (1) Tenemos que mostrar que $\mathrm{in}_<(I) = (\mathrm{in}_<(g_1), ..., \mathrm{in}_<(g_m))$. En otras palabras, si $0 \neq f \in I$ tenemos que ver que el monomio $\mathrm{in}_<(f)$ pertenece a $(\mathrm{in}_<(g_1), ..., \mathrm{in}_<(g_m))$. Dado que $f \in I$, existen $h_1, ..., h_m \in S$ tal que $f = \sum_{i=1}^m h_i g_i$, se sigue del lema 1.9 que $\mathrm{in}_<(f) \leqslant \mathrm{máx}_i\{\mathrm{in}_<(h_i g_i)\}$. Si se da la igualdad, entonces

$$\mathrm{in}_<(f) = \mathrm{in}_<(h_i g_i) = \mathrm{in}_<(h_i)\,\mathrm{in}_<(g_i)$$

para algún i y por lo tanto $\mathrm{in}_<(f) \in (\mathrm{in}_<(g_1), ..., \mathrm{in}_<(g_m))$. De lo contrario tenemos que $\mathrm{in}_<(f) < \mathrm{máx}_i\{\mathrm{in}_<(h_i g_i)\}$. Afirmamos que en este caso existe una nueva presentación de $f = \sum_{i=1}^m h_i' g_i$ con la propiedad de que $\mathrm{máx}_i\{\mathrm{in}_<(h_i' g_i)\} < \mathrm{máx}_i\{\mathrm{in}_<(h_i g_i)\}$. Entonces, si es necesario podemos podemos modificar la presentación de f una y otra vez y después de un número finito de modificaciones obtener una presentación $f = \sum_{i=1}^m h_i'' g_i$ con $\mathrm{in}_<(f) = \mathrm{máx}_i\{\mathrm{in}_<(h_i'' g_i)\}$ y así habremos terminado. □

Con base en este teorema tenemos el llamado *algoritmo de Buchberger*. Dicho algoritmo nos permite calcular a partir de un sistema de generadores $\mathfrak{G}$ de un ideal I calcular una base de Gröbner y en un número finito de pasos. El algoritmo surge como consecuencia del *Criterio de Buchberger* descrito anteriormente y lo enunaciamos a continuación.

I Para cada par de elementos distintos de $\mathfrak{G}$, calculamos el S-polinomio y un residuo correspondiente.

II Si todos los S-polinomios se reducen a 0, entonces el algoritmo termina y $\mathfrak{G}$ es una base de Gröbner de I de acuerdo al teorema anterior. En otro caso, añadimos uno de los residuos no cero a nuestro sistema de generadores, llamamos a dicho sistema $\mathfrak{G}$ y volvemos al paso 1.

1.3.3. Bases de Gröbner reducidas

Sea $<$ un orden monomial en S e I un ideal de S. Dado que una base de Gröbner de I con respecto a $<$ no está claramente determinada de forma única estamos interesados en cierto tipo de unicidad para determinar una base de Gröbner de I, en ese sentido tenemos la siguiente definición.

Definición 1.20. Sea I en S un ideal. Entonces $\mathfrak{G} = g_1, ..., g_m$ es llamada una *base de Gröbner reducida* de I con respecto a $<$, si $\mathfrak{G}$ es una base de Gröbner con respecto a $<$ y satisfface las siguientes condiciones:

(1) El coeficiente principal de cada g_i es 1.

(2) Para todo $i \neq j$, ningún $u \in \mathrm{sop}(g_j)$ es divisible por $\mathrm{in}_<(g_i)$.

En efecto, tal base de Gröbner de I existe y podemos así de acuerdo al siguiente resultado asignar una base de Gröbner de forma única a un ideal I de S.

Teorema 1.21. *Cada ideal* I *tiene una única base de Gröbner reducida.*

Demostración. Sea $G(\mathrm{in}_<(I)) = \{u_1, ..., u_m\}$ y elijamos $g_1, ..., g_m \in I$ con $u_i = \mathrm{in}_<(g_i)$ para $i = 1, ..., m$.

Entonces $g_1, ..., g_m$ es una base de Gröbner de I, la cual, sin embargo, no es reducida. Sea

$$g_1 = \sum_{i=2}^{m} q_i g_i + h_1$$

una expresión estándar de g_1 con respecto a $g_2, ..., g_m$. Entonces ningún $u \in \mathrm{sop}(h_1)$ es divisible por $\mathrm{in}_<(g_i)$ para $i = 2, ..., m$ Tenemos que $\mathrm{in}_<(g_1) \geqslant \mathrm{in}_<(q_i g_i)$ para todo i. Si suponemos que $\mathrm{in}_<(g_1) = \mathrm{in}_<(q_i g_i)$ para algún i, entonces $u_1 = \mathrm{in}_<(q_i g_i) = \mathrm{in}_<(q_i)u_i$, lo cual es una contradicción dado que $u_1, ..., u_m$ es un sistema mínimo de generadores de $\mathrm{in}_<(I)$. Se sigue por tanto de la expresión de g_1 que $\mathrm{in}_<(h_1) = \mathrm{in}_<(g_1) = u_1$.

Supongamos que ya hemos encontrado $h_1, ..., h_i$ con la propiedad de que $\mathrm{in}_<(h_j) = u_j$ para $j = 1, ..., i$ y que para todo $j \leqslant i$ ningún $u \in \mathrm{sop}(h_j)$ es divisible por cualquier u_k con $k \neq j$. Si $i < m$, ponemos h_{i+1} como un residuo de g_{i+1} con respecto a $h_1, ..., h_i, g_{i+2}, ..., g_m$. Entonces con el mismo argumento para $i = 1$ tenemos $\mathrm{in}_<(h_{i+1}) = \mathrm{in}_<(g_{i+1}) = u_{i+1}$ y ningún $u \in \mathrm{sop}(h_{i+1})$ es divisible por cualquier u_k con $k \neq i + 1$.

Así, paso a paso podemos podemos reemplazar cada g_i por los h_i y finalmente obtener $h_1, ..., h_m$ la cual es de nuevo una base de Gröbner dado que $\mathrm{in}_<(h_i) = \mathrm{in}_<(g_i)$ para $i = 1, ..., m$. Por construcción esta nueva base de Gröbner satisface la segunda condición de la definición de base reducida.

Sea c_i el coeficiente principal de h_i y sea $g'_i = c_i^{-1} h_i$. Entonces obviamente $g'_1, ..., g'_m$ satisfacen las dos condiciones de la definición de base reducida de Gröbner de I. Veamos ahora la unicidad. Supongamos que $g_1, ..., g_r$ y $g'_1, ..., g'_s$ son ambas bases reducidas de Gröbner de I. Entonces $G(\mathrm{in}_<(I)) = \{\mathrm{in}_<(g_1), ..., \mathrm{in}_<(g_r))$ porque de otra forma la segunda condición de la definición base de Gröbner reducida no sería satisfecha. Lo mismo es cierto para $g'_1, ..., g'_s$. Se sigue que $r = s = m$ y podemos asumir que $\mathrm{in}_<(g_i) = \mathrm{in}_<(g'_i)$ para $i = 1, ..., r$. Asumimos que $g_j \neq g'_j$ para alguna j. Entonces $f = g_j - g'_j$, $f \neq 0$ y $\mathrm{in}_<(f) \in \mathrm{sop}(g_j - g'_j) \subset \mathrm{sop}(g_j) \cup \mathrm{sop}(g'_j)$. Digamos que $\mathrm{in}_<(f) \in \mathrm{sop}(g_j)$. Dado que $\mathrm{in}_<(f) \in \mathrm{in}_<(I)$, existe alguna i tal que $\mathrm{in}_<(g_i)$ divide a $\mathrm{in}_<(f)$. Por otro lado, dado que $\mathrm{in}_<(g_j) \notin \mathrm{sop}(g_j - g'_j)$, se sigue que $\mathrm{in}_<(f) < \mathrm{in}_<(g_j)$, esto implica que $i \neq j$ lo cual contradice la segunda condición de la definición de base de Gröbner reducida. □

2 Aplicaciones de bases de Gröbner

En este capítulo presentamos algunas aplicaciones importantes de las bases de Gröbner. El resultado principal de este capítulo es el teorema de eliminación de variables. También calculamos bases de Gröbner de la intersección de ideales, el ideal cociente y la saturación de un ideal. Otra aplicación importante será determinar cuando un elemento pertenece al radical de un ideal dado.

Comencemos esta sección con un ejemplo de un sistema de tres ecuaciones cuadráticas que nos ilustra la utilidad de tener la base de Gröbner de un ideal.

Ejemplo 2.0.1. Considere las ecuaciones:

$$x^2 + y^2 + z^2 = 1 \tag{2.1}$$
$$x^2 + z^2 = y \tag{2.2}$$
$$x = z \tag{2.3}$$

en $\mathbb{C}^3$. Estas ecuaciones determinan el ideal $I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z\rangle \subset \mathbb{C}[x, y, z]$. Queremos hallar todos los puntos de $\mathcal{V}(I)$ (el conjunto afín de ceros comunes de los polinomios del ideal I). Para ello podemos calcular una base de Gröbner respecto al orden lexicográfico; se puede considerar a I en $\mathbb{Q}[x, y, z]$ y usamos `Macaulay2` para obtener la base de Gröbner.

```
i1 : R=QQ[x,y,z, MonomialOrder => Lex];

i2 : I = ideal(x^2+y^2+z^2-1,x^2+z^2-y,x-z)

             2    2    2        2         2
o2 = ideal (x  + y  + z  - 1, x  - y + z , x - z)

o2 : Ideal of R

i3 : g=gb I

```

```
o3 = GroebnerBasis[status: done; S-pairs encountered up to degree 3]

o3 : GroebnerBasis

i4 : gens g

o4 = | 4z4+2z2-1 y-2z2 x-z |

             1        3
o4 : Matrix R  <--- R
```

Entonces, una base de Gröbner de I con respecto al orden lexicográfico, es:

$$g_1 = x - z \tag{2.4}$$
$$g_2 = -y + 2z^2 \tag{2.5}$$
$$g_3 = 4z^4 + 2z^2 - 1 \tag{2.6}$$

A fin de tener en g_3 un polinomio mónico, multiplicamos por $\frac{1}{4}$ sin que ello afecte la base calculada; por simplicidad de notación denotamos por g_3 a dicho múltiplo. Así, $g_3 = z^4 + \frac{1}{2}z^2 - \frac{1}{4}$ y por tanto g_1, g_2, g_3 forman una base de Gröbner de I. Así, obtenemos el sistema de ecuaciones $g_1(x, y, z) = 0, g_2(x, y, z) = 0, g_3(x, y, z) = 0$, el cual es un sistema equivalente a nuestro sistema original.

Dado que el polinomio g_3 sólo depende de z, podemos resolver para z^2 y obtenemos dos soluciones para z^2 a saber $\frac{-1}{4} - \frac{\sqrt{5}}{4}$ y $\frac{-1}{4} + \frac{\sqrt{5}}{4}$, luego tomando raíces cuadradas resolvemos para z y obtenemos:

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5} - 1}.$$

Sustituímos estos 4 valores en las ecuaciones $g_1 = 0$ y $g_2 = 0$ y resolvemos de forma única para x y y respectivamente. Así, hay 4 soluciones en total de $g_1 = g_2 = g_3 = 0$, dos reales y dos complejas.

Dado que $\mathcal{V}(I) = \mathcal{V}(g_1, g_2, g_3)$, hemos encontrado todas las soluciones del sistema de ecuaciones original.

Este ejemplo ilustra que al buscar resolver un sistema de ecuaciones formado por polinomios que generan cierto ideal I, el hecho de hallar una base de Gröbner de I hace que obtengamos un nuevo sistema equivalente (formado con los polinomios en dicha base) en el cual las ecuaciones a resolver se simplificaron de forma considerable. Lo anterior se pudo lograr considerando dos hechos importantes: Al hallar una base de Gröbner de I obtuvimos el polinomio g_3 en el cual *eliminamos* las variables x y y. Dicho de otra manera, $g_3 \in I \cap \mathbb{C}[z]$. Luego, una vez hallados los valores de z en $g_3 = 0$, pudimos extender estas soluciones a las soluciones del sistema original.

2.1. Eliminación de variables

Generalizando la idea del ejemplo 2.0.1, veremos que es importante, dados un ideal I del anillo $K[x_1, \ldots, x_n]$ y un entero t entre 1 y n, encontrar de manera efectiva un conjunto de generadores del ideal $I \cap K[x_{t+1}, \ldots, x_n]$ a partir de un sistema de generadores de I. Esto se puede lograr usando bases de Gröbner. Empezaremos definiendo el tipo de órdenes monomiales que son útiles para este fin.

Definición 2.1 (Orden de eliminación)**.** Sea $t \in \mathbb{Z}$, $1 \leqslant t \leqslant n$. Un *orden de eliminación* en S para $x_1, ..., x_t$ es un orden monomial $<$ que satisface la siguiente condición: para cualesquiera dos monomios $u, v \in S$ tal que $x_j \mid u$ para algún $1 \leqslant j \leqslant t$ y $x_j \nmid v$ para todo $1 \leqslant j \leqslant t$ se tiene que $u > v$.

Ejemplo 2.1.1. El orden lexicográfico puro 1.8.1 es un ejemplo de un orden de eliminación para $x_1, ..., x_t$ para cualesquiera $1 \leqslant t \leqslant n$. En efecto, sean t un entero entre 1 y n y $u = x_1^{a_1} \cdots x_n^{a_n}, v = x_1^{b_1} \cdots x_n^{b_n} \in S$ tal que $x_k \mid u$ para algún $1 \leqslant k \leqslant t$ y $x_j \nmid v$ para todo $1 \leqslant j \leqslant t$, entonces:

$$\begin{aligned} \mathbf{b} - \mathbf{a} &= (0, \ldots, 0, b_{t+1}, \ldots, b_n) - (a_1, a_2, \ldots, a_k, \ldots, a_t, \ldots, a_n) \\ &= (-a_1, -a_2, \ldots, -a_k, -a_{k+1}, \ldots, -a_t, b_{t+1} - a_{t+1}, \ldots, b_n - a_n) \end{aligned} \tag{2.7}$$

No se puede garantizar que $a_1, \ldots, a_{k-1}$ sean elementos mayores que cero, sin embargo, dado que $x_k \mid u$ entonces $a_k > 0$ y por tanto el primer elemento de izquierda a derecha en $\mathbf{b} - \mathbf{a}$ es negativo por lo que $u > v$ y así dicho orden es de eliminación.

Definición 2.2. Sea $I \subset S$ un ideal y $1 \leqslant t \leqslant n$ un entero. El ideal $I_t = I \cap K[x_{t+1}, ..., x_n]$ es llamado el t-*ideal de eliminación* de I

El siguiente teorema es el resultado principal de la eliminación de variables.

Teorema 2.3. *Sea $I \subset S$ un ideal y $1 \leqslant t \leqslant n$. Si G es una base de Gröbner de I con respecto a un orden de eliminación $<$ para $x_1, ..., x_t$, entonces $G_t = G \cap K[x_{t+1}, ..., x_n]$ es una base de Gröbner de I_t con respecto al orden inducido en el subanillo $K[x_{t+1}, ..., x_n]$.*

Demostración. Sea $G = \{g_1, \ldots, g_s\}$ una base de Gröbner de I y asumamos que $G_t = \{g_1, \ldots, g_r\}$, esto es, $g_1, \ldots, g_r \in K[x_{t+1}, \ldots, x_n]$ y $g_{r+1}, \ldots, g_s \notin K[x_{t+1}, \ldots, x_n]$. En particular, por elección del orden monomial tenemos que $\mathrm{in}_<(g_j) \notin K[x_{t+1}, \ldots, x_n]$ para todo $j > r$. Se mostrará que el conjunto $\{\mathrm{in}_<(g_1), \ldots, \mathrm{in}_<(g_r)\}$ genera a $\mathrm{in}_<(I_t)$. En efecto, sea $f \in I_t$ un polinomio no cero. Dado que $\mathrm{in}_<(f) \in \mathrm{in}_<(I)$ y $\mathrm{in}_<(f)$ es un monomio en las últimas $n - t$ variables, se tiene que $\mathrm{in}_<(g_j) | \mathrm{in}_<(f)$ para algún $j \leqslant r$ de donde $\mathrm{in}_<(f) \in \langle \mathrm{in}_<(g_1), \ldots, \mathrm{in}_<(g_r) \rangle$, por lo tanto se tiene que $\mathrm{in}_<(I_t) \subset \langle \mathrm{in}_<(g_1), \ldots, \mathrm{in}_<(g_r) \rangle$. □

Podemos reformular el teorema de eliminación en términos de ideales iniciales.

Corolario 2.4. *Sea* $I \subset S$ *un ideal y* $1 \leqslant t \leqslant n$ *un entero. Entonces:*

$$\mathrm{in}_{<}(I \cap K[x_{t+1}, ..., x_n]) = \mathrm{in}_{<}(I) \cap K[x_{t+1}, ..., x_n]$$

para cualquier orden de eliminación $<$ *para* $x_1, ..., x_t$.

Demostración. Se tiene que el t-ideal de eliminación de I es $I_t = I \cap K[x_{t+1}, ..., x_n]$ por definición. Por el teorema 2.3 se tiene que una base de Gröbner de dicho ideal son aquellos polinomios comunes a una base de Gröbner G de I y al anillo $K[x_{t+1}, ..., x_n]$. Por otro lado, $\mathrm{in}_{<}(I) \cap K[x_{t+1}, ..., x_n]$ tiene como base de Gröbner a los polinomios en G y que están en $K[x_{t+1}, ..., x_n]$, esto es, tanto el ideal del lado izquierdo como el del lado derecho tienen la misma base de Gröbner y por tanto la igualdad se sostiene. □

2.2. Geometría de la eliminación

Buscamos dar una interpretación geométrica del teorema de eliminación discutido en la sección anterior. La idea principal es que la eliminación corresponde a proyectar una variedad sobre un subespacio de menor dimensión. Por simplicidad de los argumentos trabajaremos en esta sección sobre el campo $K = \mathbb{C}$.

Primero definamos la proyección de una variedad afín. Supongamos que tenemos dados $V = \mathcal{V}(f_1, ..., f_s) \subset \mathbb{C}^n$. Para eliminar las primeras ℓ variables $x_1, ..., x_\ell$ consideraremos el morfismo de proyección:

$$\pi_\ell : \mathbb{C}^n \to \mathbb{C}^{n-\ell}$$

que manda $(a_1, ..., a_n)$ a $(a_{\ell+1}, ..., a_n)$. Si aplicamos π_ℓ a $V \in \mathbb{C}^n$ tenemos que $\pi_\ell(V) \subset \mathbb{C}^{n-\ell}$. Podemos relacionar $\pi_\ell(V)$ al ℓ-ésimo ideal de eliminación como sigue.

Lema 2.5. *Con la notación anterior, sea* $I_\ell = (f_1, ..., f_s) \cap \mathbb{C}[x_{\ell+1}, ..., x_n]$ *el* ℓ*-ésimo ideal de eliminación. Entonces en* $\mathbb{C}^{n-\ell}$ *tenemos:* $\pi_\ell(V) \subset \mathcal{V}(I_\ell)$.

Demostración. Fijamos un polinomio $f \in I_\ell$. Si $\langle a_1, ..., a_n \rangle \in V$, entonces f se anula en $\langle a_1, ..., a_n \rangle$ dado que $f \in \langle f_1, ..., f_s \rangle$. Pero f involucra solo a $x_{\ell+1}, ..., x_n$, entonces podemos escribir:

$$f(a_{\ell+1}, ..., a_n) = f(\pi_\ell(a_1, ..., a_n)) = 0$$

esto muestra que se anula en todos los puntos de $\pi_\ell(V)$. □

2.3. Aplicaciones a operaciones de ideales

El teorema de eliminación puede ser usado para obtener algoritmos para operaciones con ideales de polinomios.

2.3.1. Intersección de ideales

Buscamos obtener un procedimiento para calcular una base de Gröbner para la intersección de dos ideales de polinomios.

Para un ideal I de S y un polinomio $p(t)$ en una nueva variable t, denotamos por $p(t)I$ al ideal generado por $\{p(t)f : f \in I\} \subset S[t]$. Es fácil ver que si I es generado por $f_1, ..., f_r$ como un ideal de S, entonces $p(t)I$ está generado por $p(t)f_1, ..., p(t)f_r$ como un ideal en $S[t]$. La siguiente proposición nos permite expresar a $I \cap J$ considerando los ideales tI y $(1-t)J$, donde t es una nueva variable. Con ello, obtendremos un sistema de generadores de $I \cap J$.

Proposición 2.6. *Sean* $I, J \subset S$ *ideales. Entonces* $I \cap J = (tI + (1-t)J) \cap S$.

Demostración. La primera inclusión es simple. Sea $f \in I \cap J$. Entonces $f = tf + (1-t)f \in (tI + (1-t)J) \cap S$. Para la otra inclusión sea $g \in (tI + (1-t)J) \cap S$. Escribimos g como $g = h_1 + h_2$ donde $h_1 \in tI$ y $h_2 \in (1-t)J$. Así existen polinomios $h_1^{'} \in IS[t], h_2^{'} \in JS[t]$ tales que $h_1 = th_1^{'}$ y $h_2 = (1-t)h_2^{'}$. Se sigue que $g = th_1^{'} + (1-t)h_2^{'}$. Sustituyendo t por cero en esta igualdad tenemos $g = h_2^{'}(0, x_1, \ldots, x_n) \in J$. Y sustituyendo t por 1, tenemos que $g = h_1^{'}(1, x_1, \ldots, x_n) \in I$. Por lo tanto, tenemos que $g \in I \cap J$ □

Esta proposición nos provee de un procedimiento para calcular una base de Gröbner para $I \cap J$ si algunos sistemas de generadores para I y J están dados. En efecto, si I es generado por algunos polinomios $f_1, ..., f_r$ y J es generado por $g_1, ..., g_s$ entonces $tf_1, ..., tf_r, (1-t)g_1, ..., (1-t)g_s$ generan a $(tI + (1-t)J)$. Elegimos un orden de eliminación para la variable t en $S[t]$ y calculamos una base de Gröbner G de $(tI + (1-t)J)$. Por el teorema de eliminación se sigue que $G \cap S$ es una base de Gröbner de $I \cap J$.

Consideremos un ejemplo sencillo para ilustrar cómo podemos calcular un sistema de generadores de $I \cap J$ introduciendo una variable nueva t y haciendo los cálculos en $(tI + (1-t)J)$.

Ejemplo 2.6.1. Consideremos el anillo de polinomios $\mathbb{Q}[x, y]$ y los ideales $I = \langle x \rangle$, $J = \langle y \rangle$. Claramente, tenemos que $I \cap J = \langle xy \rangle$. Para llegar a esta conclusión usando eliminación, consideramos una nueva variable t y tomamos el ideal $(tI + (1-t)J)$ en $R = \mathbb{Q}[t, x, y]$, que resulta ser el ideal $L = \langle tx, y - ty \rangle$. Calculamos una base de Gröbner para el ideal L considerando un orden de eliminación para la primera variable, t. Por ejemplo, podemos considerar el orden lexicográfico como hemos hecho antes. Haciendo el cálculo en `Macaulay2`, obtenemos lo siguiente:

```
i1 : R=QQ[t,x,y, MonomialOrder => Lex];

i2 : I=ideal(x)

o2 = ideal x

o2 : Ideal of R
```

```
i3 : J=ideal(y)
o3 = ideal y
o3 : Ideal of R
i4 : L=ideal t*I+(1-t)*J
o4 = ideal (t*x, - t*y + y)
o4 : Ideal of R
i5 : g=gb L
o5 = GroebnerBasis[status: done; S-pairs encountered up to degree 3]
o5 : GroebnerBasis
i6 : gens g
o6 = | xy ty-y tx |
             1       3
o6 : Matrix R  <--- R
i7 : eliminate(L,t)
o7 = ideal(x*y)
o7 : Ideal of R
```

Así, calculando una base de Gröbner de $(tI + (1-t)J)$ y luego eliminando la variable t, obtenemos el resultado esperado, a saber $I \cap J = \langle xy \rangle$.

2.3.2. Ideal cociente o ideal trasladado

Sean $I, J \subset S$ ideales de polinomios con $J = \langle g_1, ..., g_s \rangle$. A fin de determinar una base de Gröbner de $(I : J)$ usamos la igualdad $(I : J) = \bigcap_{i=1}^{s} (I : \langle g_i \rangle)$. Por tanto, podemos reducir el problema al caso cuando J es un ideal principal.

Proposición 2.7. *Sea* $I \subset S$ *un ideal y* $g \in S$ *un polinomio, si* $\{q_1, ..., q_r\}$ *es un conjunto de generadores para* $I \cap \langle g \rangle$*, entonces* $\{q_1/g, ..., q_r/g\}$ *es un conjunto de generadores para* $(I : g)$*.*

Demostración. Sea $\mathfrak{H} = \{q_1/g, ..., q_r/g\}$. Es claro que $\langle g \rangle \mathfrak{H} \subset \langle q_1, ..., q_r \rangle \subset I$, así se tiene que $\mathfrak{H} \subset (I : \langle g \rangle)$. Recíprocamente, sea $f \in (I : \langle g \rangle)$. Se sigue que $fg \in I \cap \langle g \rangle$, así $fg \in \langle q_1, ..., q_r \rangle$. Luego, como todos los polinomios $q_1, ..., q_r$ son divisibles por g, se sigue que $f \in \mathfrak{H}$. $\square$

2.3.3. Saturación y pertenencia al radical

Para un ideal homogéneo I de S hemos definido la saturación de I, es decir, $I^{\text{sat}} = (I : \mathfrak{m}^\infty) = \bigcup_{i=1}^{\infty}(I : \mathfrak{m}^i)$.

Podemos calcular una base de Gröbner de I^{sat} con los procedimientos ya descritos aplicados a $I : \mathfrak{m}^i$ y obtener sucesivamente bases reducidas de Gröbner de $(I : \mathfrak{m}^i)$ para $i \geqslant 1$. Una vez que la secuencia de ideales se estabiliza obtenemos una base de Gröbner de la saturación.

Describimos ahora otra forma de calcular la saturación. Para un ideal I de S y un polinomio $f \in S$, consideramos:

$$(I : f^\infty) = \{g \in S : \text{existe } i > 0, f^i g \in I\}$$

Se verifica fácilmente que $(I : f^\infty)$ es un ideal de S y que es homogéneo si I y f son homogéneos y además:

$$(I : f^\infty) = \bigcup_{i=1}^{\infty}(I : f^i)$$

Llamamos a este ideal la *saturación de* I *con respecto a f*.

Se puede verificar que $I^{\text{sat}} = \bigcap_{i=1}^{n}(I : x_i^\infty)$. Así, es suficiente dar un procedimiento para calcular una base de Gröbner de la saturación de un ideal con respecto a un polinomio f.

Proposición 2.8. *Sea* $I \subset S$ *un ideal y* $f \in S$ *un polinomio. Consideremos* t *una nueva variable y* $\bar{I}$ *el ideal generado en* $S[t]$ *por el ideal* I *y el polinomio* $1-ft$. *Entonces* $(I : f^\infty) = \bar{I} \cap S$.

Demostración. Para la primera inclusión sea $g \in (I : f^\infty)$. Entonces existe $i \geqslant 1$ tal que $u = gf^i \in I$. Entonces $g = gf^i t^i + (1 - f^i t^i)g = ut^i + (1 - ft)(1 + ft + \cdots + f^{i-1}t^{i-1})g \in \langle I, 1-ft\rangle$. Esto muestra que $(I : f^\infty) \subset \bar{I} \cap S$. Para la otra inclusión sea $g \in \bar{I} \cap S$. Escribimos $g = u + v(1 - tf)$, donde $u \in IS[t]$ y $v \in S[t]$. Si I es generado por $f_1, \ldots, f_s$, entonces $u = a_1 f_1 + \cdots + a_s f_s$ para algunos polinomios $a_1, \ldots, a_s \in S[t]$. Así:

$$g = a_1 f_1 + \cdots + a_s f_s + v(1 - tf)$$

Sustituyendo t por $1/f$ en la expresión anterior tenemos que:

$$g = a_1(1/f, x_1, \ldots, x_n) f_1 + \cdots + a_s(1/f, x_1, \ldots, x_s) f_s$$

Eliminando los denominadores en esta expresión encontramos un i suficientemente grande tal que $f^i g \in I$ puede ser expresado como combinación de $f_1, \ldots, f_s$ con coeficientes en S, lo cual implica que $f^i g \in I$, esto es, $g \in (I : f^\infty)$, lo que conluye la demostración. □

Por lo tanto, para encontrar una base de Gröbner de $(I : f^\infty)$, necesitamos eliminar la variable t de la base de Gröbner del ideal $\langle I, 1 - ft\rangle \subset S[t]$, así necesitamos considerar un orden de eliminación para t. Esta proposición puede ser usada como una prueba de *pertenencia al radical*. En efecto, $f \in \sqrt{I}$ si y sólo si $(I : f^{\infty}) = S$, esto es, si la base reducida de Gröbner de $I^{\sim}$ es $\{1\}$.

Ejemplo 2.8.1. Considérese el anillo de polinomios $\mathbb{Q}[x, y]$ y sea $J = \langle xy^2+2y^2, x^4-2x^2+1\rangle$. Dado un polinomio $f = y - x^2 + 1$ deseamos saber si $f \in \sqrt{I}$ para lo cual usamos la proposición 2.8 y las observaciones consecuentes introduciendo una nueva variable z y calculando una base de Gröbner del ideal $I = \langle J, 1 - fz\rangle \subset R = \mathbb{Q}[x, y, z]$ con respecto a un orden de eliminación. Usando el orden lexicográfico, podemos hacer el cálculo con `Macaulay2` y se tiene lo siguiente:

```
i1 : R=QQ[x,y,z, MonomialOrder => Lex];

i2 : I=ideal(x*y^2+2*y^2,x^4-2*x^2+1,1-z*y+z*x^2-z)

                 2      2    4      2        2
o2 = ideal (x*y   + 2y  , x   - 2x   + 1, x z - y*z - z + 1)

o2 : Ideal of R

i3 : g=gb I

o3 = GroebnerBasis[status: done; S-pairs encountered up to degree 13]

o3 : GroebnerBasis

i4 : gens g

o4 = | 1 |

               1       1
o4 : Matrix R  <--- R
```

Así, por la salida o4 obtenemos que $\{1\}$ es base de Gröbner de I, donde $I = \langle J, 1 - ft\rangle \subset \mathbb{Q}[x, y, z]$, por tanto $f \in \sqrt{J}$.

2.4. Morfismos de K-álgebras

Consideremos $S = K[x_1, ..., x_n]$ y $S' = K[y_1, ..., y_m]$ dos álgebras de polinomios y tomemos $f_1, ..., f_n$ polinomios en S' y un ideal $I' \subset S'$. Por teorema A.3 tenemos un morfismo $\psi : S \to S'/I'$ con $\psi(x_i) = f_i + I'$ para todo $1 \leqslant i \leqslant n$. Entonces, para cualquier ideal $I \subset \ker(\psi)$ existe un morfismo $\varphi : S/I \to S'/I'$ con la propiedad de que $\varphi(x_i + I) = \psi(x_i) = f_i + I'$.

La siguiente proposición y su corolario nos permiten un conjunto de generadores para $\ker(\varphi)$ usando eliminación de variables.

Proposición 2.9. *Sea* $\varphi : S/I \to S'/I'$ *un homomorfismo de* K*-álgebras con* $\varphi(x_i +$

I) $= f_i + I'$ *para* $1 \leqslant i \leqslant n$*, donde* $f_1, ..., f_n \in S'$*. Sea* $R = K[x_1, ..., x_n, y_1, ..., y_m]$, $J = I'R + (x_1 - f_1, ..., x_n - f_n)$ *y* $L = J \cap S$*. Entonces* $\ker(\varphi)$ *es la imagen del ideal* L *en* S/I*, esto es* $\ker(\varphi) = (I + L)/I$.

Demostración. Sea $g + I \in \ker(\varphi)$. Se sigue que $g(f_1, \ldots, f_n) + I' = 0$, así $g(f_1, \ldots, f_n) \in I'$. Si $g = \sum c_a \mathbf{x}^{\mathbf{a}}$, entonces podemos escribir:

$$g = \sum g' + g = \sum c_a \mathbf{f}^{\mathbf{a}} = g' + g(f_1, \ldots, f_n)$$

con $g' \in (x_1 - f_1, \ldots, x_n - f_n)$, por lo tanto $g \in J \cap S = L$ y $g + I \in (I + L)/I$ Recíprocamente, sea $g \in L = J \cap S$ y $\{h_1, \ldots, h_r\} \subset S'$ un conjunto de generadores de I'. Entonces existen algunos polinomios $a_1, \ldots, a_r, b_1, \ldots, b_n \in R$ tal que:

$$g = a_1 h_1 + \cdots + a_r h_r + b_1(x_1 - f_1) + \cdots + b_n(x_n - f_n)$$

Sustituyendo x_i por f_i en la igualdad anterior, para $1 \leqslant i \leqslant n$, tenemos que:

$$g(f_1, \ldots, f_n) \in (h_1, \ldots, h_r) = I'$$

Por lo tanto, $\varphi(g + I) = g(f_1, \ldots, f_n) + I' = 0$ y así $g + I \in \ker(\varphi)$ □

Corolario 2.10. *Sean* $f_1, ..., f_n \in S'$ *polinomios y* $\varphi : S \to S'$ *el homomorfismo de* K-*álgebras definido por* $x_i \mapsto f_i$ *para* $1 \leqslant i \leqslant n$*. Sea* $J = (x_1 - f_1, ..., x_n - f_n) \subset R = K[x_1, ..., x_n, y_1, ..., y_m]$*. Entonces* $\ker(\varphi) = J \cap S$.

Demostración. Basta tomar $I = I' = (0)$ en la proposición anterior. □

Este corolario nos permite resolver el siguiente problema. Dada una familia de ecuaciones paramétricas $x_1 = f_1, ..., x_n = f_n$ con $f_1, ..., f_n \in S'$ podemos encontrar las relaciones implícitas entre los polinomios $f_1, ..., f_n$.

Ejemplo 2.10.1 (El anillo de Rees). Sea $I \in S$ un ideal homogéneo generado por los polinomios homogéneos $f_1, ..., f_q$ y t una nueva indeterminada sobre K. El anillo de Rees denotado por $\mathcal{R}(I)$ es el subanillo de $S[t]$ dado por:

$$\mathcal{R}(I) = \bigoplus_{j \geqslant 0} I^j t^j = S[f_1 t, ..., f_q t$$

Considere la presentación de $\mathcal{R}(I)$,

$$\varphi : R = S[u_1, ..., u_q] \to \mathcal{R}(I),$$

definido por $x_i \mapsto x_i$ para $1 \leqslant i \leqslant n$ y $u_j \mapsto f_j t$ para $1 \leqslant j \leqslant q$

$J = \ker(\varphi)$ es un ideal de $S[u_1, ..., u_q]$ el cual es llamado el *ideal de presentación* de $\mathcal{R}(I)$. Por el corolario 2.10 tenemos:

$$J = (u_1 - f_1 t, ..., u_q - f_q t) \cap R.$$

Sea $\mathfrak{G}$ una base de Gröbner de $(u_1 - f_1 t, ..., u_q - f_q t)$ con respecto a un orden de eliminación para t en el anillo de polinomios $K[t, x_1, ..., x_n, u_1, ..., u_q]$. Entonces $\mathfrak{G} \cap R$ es una base de Gröbner del ideal de presentación J.

Podemos definir el ejemplo anterior sin suponer que el ideal I es homogéneo.Primero definimos la *filtración de un anillo.*

Definición 2.11 (*Filtración de un anillo*)**.** Sean A un anillo, $\mathcal{I} = \{I_n\}_{n=0}^{\infty}$ una sucesión de ideales de A. $\mathcal{I}$ es llamada una filtración de A si:

(i) $I_0 = A$.

(ii) $I_n \supseteq I_{n+1}$.

(iii) $I_n I_m \subseteq I_{n+m}$ para todo n, m.

Ejemplo 2.11.1. $\{I^n\}$, donde I es un ideal de A, es una filtración de A.

Definición 2.12 (*Álgebra de Rees*)**.** Sean A un anillo (no necesariamente graduado), I un ideal de A y consideremos la filtración $\mathcal{I} = \{I^n\}_{n=0}^{\infty}$ de A. Definimos el *álgebra de Rees* del ideal I por:

$$\mathrm{Rees}_A(I) = R^*(I) := \bigoplus_{n \geqslant 0} I^n = A \oplus I \oplus I^2 \oplus ...$$

Vale la pena hacer algunos comentarios respecto a esta definición. Primeramente, se puede observar el paralelismo que existe con el anillo de polinomios $K[x]$ si escribimos el anillo de polinomios como:

$$K[x] = \bigoplus_{n \in \mathbb{N}} K \tag{2.8}$$

Así, si consideramos el polinomio $p(x) = (a_0, a_1, ..., a_n, 0, 0, ...)$ usando la notación usual para polinomios tenemos:

$$(a_o, a_1, ..., a_n, 0, 0, ...) = a_0 x^0 + a_1 x + \cdots + a_n x^n \tag{2.9}$$

Obsérvese que en el lado derecho de (2.9) la introducción de la indeterminada x permite identificar la posición de cada uno de los coeficientes de $p(x)$ en el lado izquierdo de dicha ecuación; así a pesar de que todos los coeficientes están en K e incluso cuando éstos pueden ser iguales entre sí, podemos diferenciarlos por su posición, la cual queda determinada de forma explícita por la indeterminada x. Por lo anterior, podemos escribir:

$$K[x] = \bigoplus_{n \in \mathbb{N}} K = \bigoplus_{n \in \mathbb{N}} Kx^n = \underbrace{Kx^0}_{\mathrm{gr}\,0} \oplus \underbrace{Kx}_{\mathrm{gr}\,1} \oplus \underbrace{Kx^2}_{\mathrm{gr}\,2} \oplus \underbrace{Kx^3}_{\mathrm{gr}\,3} \oplus \cdots \tag{2.10}$$

En el caso de la definición 2.12 tenemos una situación bastante similar, pues $I^n \subset A$ para todo $n \geqslant 0$, por lo que puede haber ambigüedad en la notación, así, la introducción de una *indeterminada* t resulta bastante útil para identificar la posición de cada componente en un elemento dado de $\mathrm{Rees}_A(I)$.

Así, podemos escribir:

$$\begin{aligned} \mathrm{Rees}_A(I) := \bigoplus_{n \geqslant 0} I^n &= A \oplus I \oplus I^2 \oplus ... = I^0 \oplus IA \oplus I^2A \oplus \cdots \\ &= I^0 \oplus It \oplus I^2t^2 \oplus \cdots \end{aligned} \tag{2.11}$$

Definición 2.13 (Homogenización)**.** Sea $f \in S$ un polinomio de grado d y $f = \sum_{i=0}^{d} f_i$ su descomposición en componentes homogéneos. Entonces

$$f^h = \sum_{i=0}^{d} t^{d-i} f_i$$

es un polinomio homogéneo de grado d en el anillo $S[t]$. El polinomio f^h es llamada la *homogenización de* f. Si $g \in S[t]$ es un polinomio homogéneo, denotamos por $\bar{g}$ su *deshomogenización*, esto es, el polinomio de S que es obtenido de g por la sustitución $t \mapsto 1$.

Definición 2.14. Sea $I \in S$ un ideal. La *homogenización* de I es el ideal I^h generado por $\{f^h : f \in I\}$

Un orden monomial $<$ en S es llamado graduado si para cualesquiera monomios $u, v \in S$ tenemos que $\mathrm{gr}(u) < \mathrm{gr}(v)$ implica que $u < v$. Ejemplos de este tipo de órdenes son el orden lexicográfico y el orden lexicográfico inverso.

2.5. Ideales de formas iniciales

Dado un orden monomial $<$ en S, $\mathrm{in}_<(I)$ es el ideal monomial generado por los monomios principales de los polinomios de I con respecto al orden dado. En caso de que el orden monomial sea graduado, entonces el monomio principal de cualquier polinomio f es de grado máximo entre todos los monomios del soporte de f. Sin embargo, para un ideal $I \in S$ es también interesante estudiar los llamados *ideales de formas iniciales*.

Sea $f = f_0 + f_1 + \cdots f_d \in S$ un polinomio no cero expresado en su descomposición homogénea y sea $j = \min\{i : f_i \neq 0\}$. f_j es llamada la *forma inicial* de f y es denotada por $\mathrm{In}(f)$.

Definición 2.15. Sea $I \in S$ un ideal. El ideal de formas iniciales de I es $\mathrm{In}(I) = \langle \mathrm{in}(f) : f \in I \rangle$.

Lo más interesante de estudiar ideales de formas iniciales se desprende del hecho de que éstos están fuertemente relacionados a *conos tangentes* de variedades. Si $\mathcal{V} = \mathcal{V}(\mathrm{I}) \subset \mathsf{K}^n$ es una variedad algebraica afín que contiene al origen, entonces el *cono tangente* de $\mathcal{V}$ en 0 es:

$$C_0(\mathcal{V}) = \mathcal{V}(\mathrm{in}(f) : f \in \mathcal{I}(\mathcal{V})).$$

Proposición 2.16. *Sea* $\mathrm{I} \in S$ *un ideal,* $\mathrm{I}^h \subset S[t]$ *y* $\mathbb{G}$ *una base de Gröbner de* I^h *con respecto a* $<$*. Entonces* $\mathrm{In}(\mathrm{I}) = \langle \mathrm{In}(\bar{g}) : g \in \mathbb{G} \rangle$*, donde* $\bar{g}$ *es la deshomogenización de* g*.*

Demostración. Sea $f \in \mathrm{I}$. Asumimos que para todos los polinomios $h \in \mathrm{I}$ con la propiedad que $\mathrm{in}_<(\mathrm{In}(h)) < \mathrm{in}_<(\mathrm{In}(f))$, tenemos $\mathrm{In}(h) \in \langle \mathrm{In}(\bar{g}), g \in \mathbb{G} \rangle$ y mostraremos que $\mathrm{In}(f) \in (\mathrm{In}(\bar{g}), g \in \mathbb{G})$. Sea $f = f_i + \cdots f_{d-1} + f_d$ donde $f_i = \mathrm{In}(f)$. Entonces $f^h = t^{d-i} f_i + \cdots t f_{d-1} + f_d$. Claramente, tenemos que $\mathrm{in}_<(f^h) = t^{d-i}\,\mathrm{in}_<(\mathrm{In}(f))$. Dado que $\mathbb{G}$ es una base de Gröbner de I^h, existe $g \in \mathbb{G}$ tal que $\mathrm{in}_<(g) \mid \mathrm{in}_<(f^h)$. Por otro lado, tenemos que $\mathrm{in}_g = t^e\,\mathrm{in}_<(\mathrm{In}(\bar{g}))$ para algún $e \geqslant 0$. Por lo tanto, tenemos que $t^e\,\mathrm{in}_<(\mathrm{In}(\bar{g})) \mid t^{d-i}\,\mathrm{in}_<(\mathrm{In}(f))$. Como $\mathrm{in}_<(\mathrm{In}(\bar{g}))$ y $\mathrm{in}_<(\mathrm{In}(f))$ son monomios en S, se sigue que $\mathrm{in}_<(\mathrm{In}(\bar{g})) \mid \mathrm{in}_<(\mathrm{In}(f))$. Así, podemos encontrar $c \in \mathsf{K}$, $c \neq 0$ y un monomio $\mathbf{x^a} \in S$ tal que el término principal de $\mathrm{In}(f)$ es igual a $c\mathbf{x^a}\,\mathrm{in}_<(\mathrm{In}(\bar{g}))$. Si $\mathrm{In}(f) = c\mathbf{x^a}\,\mathrm{in}_<(\mathrm{In}(\bar{g}))$ entonces habremos terminado. De otro modo, sea $h = f - c\mathbf{x^a}\bar{g}$. Entonces, $\mathrm{In}(h) = \mathrm{In}(f) - c\mathbf{x^a}\,\mathrm{In}(\bar{g})$ tiene la propiedad que $\mathrm{in}_<(\mathrm{In}(h)) < \mathrm{in}_<(\mathrm{In}(f))$; así por inducción, $\mathrm{In}(h) \in (\mathrm{In}(\bar{g}) : g \in \mathbb{G}$. Por lo tanto, $\mathrm{In}(f) \in (\mathrm{In}(\bar{g}) : g \in \mathbb{G})$. $\square$

Observe que el conjunto $\{\mathrm{In}(\bar{g}) : g \in \mathbb{G}\}$ no es necesariamente una base de Gröbner de $\mathrm{In}(\mathrm{I})$ con respecto al orden inducido en S por $<$.

3 Ideales determinantales

Los anillos de semigrupos y sus ideales tóricos son ampliamente estudiados tanto desde un enfoque algebraico como desde un punto de vista combinatorio. Esta clase de anillos incluyen al anillo de polinomios S, el cual es asociado con el semigrupo $\mathbb{N}^n$. Además de su importancia propia, los ideales tóricos son parte de la clase de ideales definidos por condiciones determinantales. Estos ideales determinantales son el objeto de este capítulo. Veremos que la teoría de bases de Gröbner juega un papel importantes en el estudio de las propiedades de estos ideales. En este capítulo veremos propiedades de este tipo de anillos y su relación con el estudio de las bases de Gröbner.

3.1. Anillos de semigrupos e ideales tóricos

En esta sección daremos las definiciones básicas de anillos de semigrupos y sus ideales tóricos. Veremos además que éstos últimos se caracterizan por ser ideales primos y generados por binomios.

Sea $\mathbb{Z}$ el conjunto de los enteros y $\{\mathbf{h}_1, \ldots, \mathbf{h}_q\}$ un subconjunto de $\mathbb{Z}^n$, donde n es un entero positivo. Sea H el submonoide del grupo aditivo de $\mathbb{Z}^n$ generado por $\mathbf{h}_1, \ldots, \mathbf{h}_q$, esto es:

$$H = \mathbb{N}\mathbf{h}_1 + \cdots + \mathbb{N}\mathbf{h}_q = \{a_1\mathbf{h}_1 + \cdots + a_q\mathbf{h}_q : a_i \in \mathbb{N}, 1 \leqslant i \leqslant q\} \subseteq \mathbb{Z}^n.$$

H es llamado un *semigrupo afín* (un cono reticular en $\mathbb{Z}^n$).

Sea $K[x_1, x_1^{-1}, ..., x_n, x_n^{-1}]$ el anillo de polinomios de Laurent y $K[H]$ el subanillo de $K[x_1, x_1^{-1}, ..., x_n, x_n^{-1}]$ generado sobre K por los monomios $f_i = \mathbf{x}^{\mathbf{h}_i}$ para $i = 1, \ldots, q$, donde $\mathbf{x}^{\mathbf{c}} = x_1^{c_1} \cdots x_n^{c_n}$ si $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{Z}^n$.

Obviamente, $\mathbf{x}^{\mathbf{g}} \in K[H]$ si y sólo si $\mathbf{g} \in H$. Los elementos de $K[H]$ son expresiones polinomiales en $f_1, ..., f_q$ con coeficientes en K. La K-álgebra $K[H]$ es llamada el *anillo de semigrupo* asociado con el semigrupo afín H.

Por ejemplo, si $H = \mathbb{Z}^n$, entonces $K[\mathbb{Z}^n] = K[x_1, x_1^{-1}, ..., x_n, x_n^{-1}]$ y si $H = \mathbb{N}^n$, entonces $K[\mathbb{N}^n] = K[x_1, ..., x_n]$.

En lo siguiente consideraremos semigrupos afines que son generados por un número finito de vectores $\mathbf{h}_1, ..., \mathbf{h}_q \in \mathbb{N}^n$. En este caso, $K[H]$ es una K-subálgebra del anillo de polinomios S.

Sea $R = K[t_1, ..., t_q]$ el anillo de polinomios en indeterminadas $t_1, ..., t_q$ y $\varphi : R \to K[H]$ el morfismo de K-álgebras definido por $t_i \mapsto f_i = \mathbf{x}^{\mathbf{h}_i}$ para $i = 1, ..., q$.

Se pueden considerar diferentes graduaciones en $K[H]$. Por ejemplo, $K[H]$ es $\mathbb{Z}$-graduado con la $\mathbb{Z}$-graduación inducida de S, esto es, $K[H]_d = K[H] \cap S_d$, donde S_d es la componente homogénea de S de grado d.

En este caso, $\varphi : R \to K[H]$ es un homomorfismo graduado si ponemos $\mathrm{gr}(t_i) = \mathrm{gr}(f_i)$ para $i = 1, ..., q$. Cuando todos los generadores de $K[H]$ tienen el mismo grado, digamos d, entonces $K[H]$ puede ser incluso vista como una álgebra graduada estándar si consideramos $K[H]_i = K[H] \cap S_{di}$ para $i \geqslant 0$. Claramente, en este caso $\varphi : R \to K[H]$ es un homomorfismo graduado de K-álgebras graduadas estándar.

Por otro lado, podemos considerar la $\mathbb{Z}^n$-graduación natural en S y la graduación inducida en $K[H]$, esto es; $K[H]_a = K[H] \cap S_{\mathbf{a}}$ para todo $a \in \mathbb{Z}^n$. Con respecto a esta graduación de $K[H]$, $\varphi : R \to K[H]$ es nuevamente graduado si asignamos a cada t_i el $\mathbb{Z}^n$-grado de f_i.

φ es claramente suprayectiva. Su núcleo, denotado por P_H es un ideal graduado de R. Además, dado que $K[H] \simeq R/P_H$ y $K[H] \subset S$ es un dominio, se sigue que P_H es un ideal primo. P_H es llamado el *ideal tórico* de H.

Para un polinomio $h \in R$, tenemos que $\varphi(h) = h(f_1, \ldots, f_q)$. En particular para un monomio $\mathbf{t}^{\mathbf{u}} = t_1^{u_1} \cdots t_q^{u_q} \in R$ tenemos que $\psi(\mathbf{t}^{\mathbf{u}}) = f_1^{u_1} \cdots f_q^{u_q} = \mathbf{x}^{\sum_{i=1}^{q} u_i \mathbf{h}_i}$.

Sea $\pi : \mathbb{N}^q \to H$ el homomorfismo de grupos definido por $\pi(\mathbf{u}) = \sum_{i=1}^{q} u_i \mathbf{h}_i$ para $\mathbf{u} = (u_1, \ldots, u_q) \in \mathbb{N}^q$. Entonces $\varphi(\mathbf{t}^{\mathbf{u}}) = \mathbf{x}^{\pi(\mathbf{u})}$ para todo $\mathbf{t}^{\mathbf{u}} \in R$.

Observe que si A es la matriz de tamaño $n \times q$ cuyas columnas son los elementos $\mathbf{h}_1, ..., \mathbf{h}_q \in \mathbb{N}^n$, entonces podemos expresar a φ en términos de dicha matriz A, esto es:

$$\varphi(\mathbf{t}^{\mathbf{u}}) = \mathbf{x}^{\pi(\mathbf{u})} = \mathbf{x}^{A\mathbf{u}}.$$

Obsérvese que dicha matriz A determina el morfismo de K-álgebras φ y por tanto el ideal tórico asociado al semigrupo afín H.

De acuerdo al capítulo anterior, usando eliminación de variables tenemos la siguiente situación: Si $J = \langle t_1 - f_1, \ldots, t_q - f_q \rangle \subset K[t_1, \ldots, t_q, x_1, \ldots, x_n]$, el ideal tórico asociado a H es $P_H = J \cap K[t_1, \ldots, t_q]$. Por ello, calcular una base de Gröbner de P_H se reduce a considerar un orden de eliminación para $x_1, \ldots, x_n$ y si G es una base de Gröbner de J, entonces $G \cap K[t_1, \ldots, t_q]$ será una base de Gröbner de P_H.

Ejemplo 3.0.1. Sea $H \subset \mathbb{N}^2$ el semigrupo afín generado por $\mathbf{h}_1 = (2, 0), \mathbf{h}_2 = (1, 1), \mathbf{h}_3 = (0, 2)$. Entonces, el anillo de semigrupo asociado a H es $K[H] = K[x_1^2, x_1x_2, x_2^2] \subset K[x_1, x_2]$.

Queremos calcular una base de Gröbner de $P_H \in K[t_1, t_2, t_3]$ y usamos el orden lexicográfico, el cual es un orden de eliminación.

En este caso, la matriz asociada al ideal tórico es:

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

Usamos `Macaulay2` y a partir de la matriz A obtenemos el siguiente código:

```
i1 : needsPackage "FourTiTwo"

o1 = FourTiTwo

o1 : Package

i2 : needsPackage "Depth"

o2 = Depth

o2 : Package

i3 : needsPackage "Polyhedra"

o3 = Polyhedra

o3 : Package

i4 : needsPackage "Quasidegrees"

o4 = Quasidegrees

o4 : Package

i5 : A=matrix"2,1,0;0,1,2"

o5 = | 2 1 0 |
     | 0 1 2 |

                2         3
o5 : Matrix ZZ  <--- ZZ

i6 : R=QQ[x,y,z, MonomialOrder=>Lex];

i7 : toricGroebner(A,R)

                      2
o7 = ideal(- x*z + y )

o7 : Ideal of R
```

Obsérvese que para fines del cálculo en `Macaulay2` consideramos el ideal P_H en $K[x, y, z]$, haciendo así la identificación: $t_1 \mapsto x$, $t_2 \mapsto y$ y $t_3 \mapsto z$.

Luego, en o_7 obtuvimos el ideal tórico $\langle -xz + y^2 \rangle = \langle xz - y^2 \rangle$ generado por una base de Gröbner.

Por tanto, una base de Gröbner de P_H es $\{t_1t_3 - t_2^2\}$.

Un *binomio* es un polinomio el cual es una diferencia de dos monomios. Un ideal polinomial es un *ideal binomial* si es generado por un conjunto de binomios. Note que un ideal binomial no contiene ningún monomio.

El siguiente lema muestra que cualquier ideal tórico puede ser generado por binomios.

Lema 3.1. *Sea* P_H *el ideal tórico de un anillo de semigrupo* H*. Entonces el conjunto de binomios* $\{\boldsymbol{t}^{\boldsymbol{u}} - \boldsymbol{t}^{\boldsymbol{v}} : \boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}^q, \pi(\boldsymbol{u}) = \pi(\boldsymbol{v})\}$ *genera a* P_H *como un* K*-espacio vectorial. En particular,* P_H *es un ideal binomial.*

Demostración. Claramente por la definición de φ y π tenemos que $\mathbf{t}^{\mathbf{u}} - \mathbf{t}^{\mathbf{v}} \in P_H$ para todo $\mathbf{u}, \mathbf{v} \in \mathbb{N}^q$ tal que $\pi(\mathbf{u}) = \pi(\mathbf{v})$. Por otro lado, dado que P_H es $\mathbb{Z}^n$ graduado, es suficiente centrarnos en los polinomios homogéneos de P_H con respecto a la $\mathbb{Z}^n$ graduación. Sea $f = c_1\mathbf{t}^{\mathbf{u}_1} + \cdots + c_s\mathbf{t}^{\mathbf{u}_s}$ un polinomio homogéneo en P_H donde $c_1, \ldots, c_s \in K - 0$. Por la suposición de f se sigue que todos los monomios $\mathbf{t}^{\mathbf{u}_i}$ son mapeados al mismo monomio $\mathbf{x}^{\mathbf{h}}$ bajo φ, donde $h = \pi(\mathbf{u}_1) = \cdots = \pi(\mathbf{u}_s)$. Entonces, obtenemos $0 = \varphi(f) = (\sum_{i=1}^{s} c_i)\mathbf{x}^{\mathbf{h}} = 0$, de donde $\sum_{i=1}^{s} c_i = 0$. Obtenemos así que $c_1 = -c_2 - \cdots - c_s$. Por tanto, podemos escribir $f = c_2(\mathbf{t}^{\mathbf{u}_2} - \mathbf{t}^{\mathbf{u}_1} + \cdots + c_s(\mathbf{t}^{\mathbf{u}_s} - \mathbf{t}^{\mathbf{u}_1})$ lo cual concluye la prueba. $\square$

Para un vector $\mathbf{v} \in \mathbb{Z}^q$ denotamos por $\mathbf{v}^+$ y $\mathbf{v}^-$ a los vectores con componentes no negativas definidas como sigue:

$$v_i^+ = \begin{cases} v_i & \text{si } v_i \geqslant 0, \\ 0 & \text{en otro caso} \end{cases} \qquad \text{y} \qquad v_i = \begin{cases} 0 & \text{si } v_i > 0, \\ -v_i & \text{si } v_i \leqslant 0. \end{cases}$$

Claramente tenemos que $v = \mathbf{v}^+ - \mathbf{v}^-$ y esta descomposición de $\mathbf{v}$ en vectores con coeficientes no negativos es única.

En particular cada binomio en R cuyos monomios tengan soportes disjuntos pueden ser escritos como $f_{\mathbf{v}} = \mathbf{t}^{\mathbf{v}^+} - \mathbf{t}^{\mathbf{v}^-}$ donde $\mathbf{v}$ es un vector en $\mathbb{Z}^q$.

Se puede verificar que para cualesquiera $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^q$ tenemos:

$$f_{\mathbf{v}}f_{\mathbf{w}} = uf_{\mathbf{v}+\mathbf{w}} - \mathbf{t}^{\mathbf{v}^-}f_{\mathbf{w}} - \mathbf{t}^{\mathbf{w}^-}f_{\mathbf{v}}$$

Una *retícula* es un submódulo de un $\mathbb{Z}$-módulo libre de rango finito. A cada retícula podemos asociarle un ideal binomial.

Definición 3.2. Sea $L \subset \mathbb{Z}^q$ una retícula. El *ideal reticular* asociado a L es el ideal binomial $I_L = \langle \mathbf{t}^{\mathbf{v}^+} - \mathbf{t}^{\mathbf{v}^-} : \mathbf{v} \in L \rangle$.

Proposición 3.3. *Sea* $I \subset R$ *un ideal binomial primo, entonces* I *es un ideal reticular.*

Demostración. Dado que I es un ideal primo podemos asumir que sus generadores son de la forma $f_{\mathbf{v}}$ con $\mathbf{v} \in \mathbb{Z}^q$. Se sigue que si $f_{\mathbf{v}} = \mathbf{t}^{\mathbf{v}^+} - \mathbf{t}^{\mathbf{v}^-} \in I$ entonces $f_{-\mathbf{v}} = -f_{\mathbf{v}} \in I$. Por lo tanto es suficiente mostrar que si $f_{\mathbf{v}}, f_{\mathbf{w}} \in I$, entonces $f_{\mathbf{v}+\mathbf{w}} \in I$. Usando la identidad (*), tenemos que existe un monomio $u \in R$ tal que $uf_{\mathbf{v}+\mathbf{w}} \in I$. Pero, claramente $u \notin I$, así que $f_{\mathbf{v}+\mathbf{w}} \in I$ dado que I es un ideal primo. □

Con lo anterior tenemos el siguiente resultado de gran importancia.

Teorema 3.4. *Sea* $I \subset R$ *un ideal binomial primo. Entonces* I *es un ideal tórico.*

Demostración. Por proposición anterior, $I = I_L$ donde $L \subset \mathbb{Z}^q$ es la retícula generada por los vectores $\nu \in \mathbb{Z}^q$ con la propiedad de que los binomios asociados f_ν generan a I.

Primero mostramos que el módulo $\mathbb{Z}^q/L$ es libre de torsión y por lo tanto libre. En otras palabras, mostraremos que si $\nu \in \mathbb{Z}^q$ y $m > 1$ es un entero tal que $m\nu \in L$, equivalentemente $f_{m\nu} \in I$, entonces $\nu \in L$, esto es, $f_\nu \in I$.

Sea $f_{m\nu} = t^{m\nu^+} - t^{m\nu^-} \in L$. Si $car(K) = 0$, entonces descomponemos $f_{m\nu} = f_\nu g$, donde $g = t^{(m-1)\nu^+} + t^{(m-2)\nu^+}t^{\nu^-} + \cdots + t^{\nu^+}t^{(m-2)\nu^-} + t^{(m-1)\nu^-} \in R$.

Usando las sustituciones $t_i \mapsto 1$ para $i = 1, ..., q$, vemos que $g \notin I$ dado que todos los binomios se anulan en esta sustitución. Por lo tanto, $f_\nu \in I$ dado que I es un ideal primo.

Si $car(K) = p > 0$, entonces escribimos $m = p^e m'$ donde $e \geqslant 0$, $m' \geqslant 1$ son enteros tales que p no divide a m'. En este caso, descomponemos a $f_{m\nu}$ como $f_\nu^{p^e} g'$, donde $g' = (t^{p^e\nu^+})^{m'-1} + \cdots t^{p^e\nu^-})^{m'-1} \in R$. Usando de nuevo las sustituciones $t_i \mapsto 1$ para $i = 1, ..., q$, tenemos que $g' \notin I$. Dado que I es un ideal primo, se sigue que $f_\nu^{p^e} \in I$, de donde $f_\nu \in I$.

Sea n el rango del módulo libre $\mathbb{Z}^q/L$ y $\bar{h}_1, ..., \bar{h}_q$, los generadores de $\mathbb{Z}^q/L$ vistos como vectores con n componentes. Sea $K[H] \subset K[x_1^{\pm 1}, ..., x_n^{\pm 1}]$ el anillo semigrupo generado por $x^{\bar{h}_1}, ..., x^{\bar{h}_q}$ y $\phi : R \to K[H]$ el morfismo de K-álgebras dado por $t_i \mapsto x^{\bar{h}_i}$ para $i = 1, ..., q$. Entonces, se puede ver que el núcleo de ϕ es precisamente I, con lo cual I es ideal tórico. □

3.2. Bases de Gröbner de ideales tóricos

En esta sección nuestro interés es dar las principales propiedades de las bases de Gröbner de ideales tóricos.

Proposición 3.5. *Sea* H *un semigrupo afín y* P_H *su ideal tórico. Sea* $<$ *un orden monomial en* R *y* $\mathcal{G}$ *la base reducida de Gröbner de* P_H *con respecto a* $<$. *Entonces, todo elemento de* $\mathcal{G}$ *es un binomio de la forma* $\boldsymbol{t^u} - \boldsymbol{t^v}$ *con* $\pi(\boldsymbol{u}) = \pi(\boldsymbol{v})$.

Demostración. Sea G un conjunto de generadores de P_H. Por el lema 3.1 podemos elegir esos generadores de la forma $\mathbf{t^u} - \mathbf{t^v}$ con $\pi(\mathbf{u}) = \pi(\mathbf{v})$. Aplicando el *Algoritmo de Buchberger*, en cada paso cuando obtenemos un residuo no cero, éste es nuevamente un binomio $\mathbf{t}^{\mathbf{w}}-\mathbf{t}^{\mathbf{w'}}$ con $\pi(\mathbf{w}) = \pi(\mathbf{w'})$. Por lo tanto, P_H tiene una base de Gröbner con respecto al orden dado formado con binomios de la forma $\mathbf{t}^{\mathbf{u}} - \mathbf{t}^{\mathbf{v}}$ con $\pi(\mathbf{u}) = \pi(\mathbf{v})$. Aplicando las reducciones necesarias para obtener una base reducida de Gröbner, obtenemos nuevamente binomios de este tipo, por lo cual la prueba es completada. $\square$

Esta proposición muestra que cualquier base reducida de Gröbner de P_H consiste de monomios $\mathbf{t}^{\mathbf{u}} - \mathbf{t}^{\mathbf{v}}$ con $\pi(\mathbf{u}) = \pi(\mathbf{v})$.

Definición 3.6. Un binomio $\mathbf{t}^{\mathbf{u}} - \mathbf{t}^{\mathbf{v}} \in P_H$ es llamado *primitivo* si no hay otro binomio $\mathbf{t}^{\mathbf{r}} - \mathbf{t}^{\mathbf{s}} \in P_H$ tal que $\mathbf{t}^{\mathbf{r}} \mid \mathbf{t}^{\mathbf{u}}$ y $\mathbf{t}^{\mathbf{s}} \mid \mathbf{t}^{\mathbf{v}}$.

Proposición 3.7. *Sea P_H el ideal tórico de un semigrupo afín H y $\mathcal{G}$ la base reducida de Gröbner de P_H con respecto a un orden monomial. Entonces cualquier binomio de $\mathcal{G}$ es primitivo.*

Demostración. Sea $g = \mathbf{t}^{\mathbf{u}} - \mathbf{t}^{\mathbf{v}}$ un monomio de $\mathcal{G}$ con $\mathrm{in}(g) = \mathbf{t}^{\mathbf{u}}$. Dado que $\mathcal{G}$ es reducida, se sigue que $\mathbf{t}^{\mathbf{v}} \notin \mathrm{in}_<(P_H)$. Asumamos que existe $h = \mathbf{t}^{\mathbf{r}} - \mathbf{t}^{\mathbf{s}} \in P_H$ con $h \neq g$ tal que $\mathbf{t}^{\mathbf{r}} \mid \mathbf{t}^{\mathbf{u}}$ y $\mathbf{t}^{\mathbf{s}} \mid \mathbf{t}^{\mathbf{v}}$. Si $\mathrm{in}_<(h) = \mathbf{t}^{\mathbf{r}}$, entonces debemos de tener que $\mathbf{t}^{\mathbf{r}} = \mathbf{t}^{\mathbf{u}}$. Se sigue que $h' = \mathbf{t}^{\mathbf{v}} - \mathbf{t}^{\mathbf{s}}$ pertenece a P_H y $\mathrm{in}_<(h') = \mathbf{t}^{\mathbf{v}}$ dado que $\mathbf{t}^{\mathbf{s}} \mid \mathbf{t}^{\mathbf{v}}$, lo cual es una contradicción. Por lo tanto, $\mathrm{in}_<(h) = \mathbf{t}^{\mathbf{s}}$ lo cual lleva a una contradicción nuevamente pues $\mathbf{t}^{\mathbf{s}} \mid \mathbf{t}^{\mathbf{v}}$. $\square$

3.3. Ideales determinantales

El objetivo de esta sección es estudiar ideales determinantales por medio de bases de Gröbner.

Consideremos un campo K y una matriz de indeterminadas $X = (x_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$. Denotamos por $K[X]$ al anillo de polinomios con coeficientes en K e indeterminadas $x_{i,j}$. Los generadores de la K-álgebra $K[X]$ son los elementos $x_{i,j}$, los cuales son menores de tamaño 1 de la matriz X, luego los productos de dichos menores (monomios) forman una K-base del espacio vectorial $K[X]$.

En este sentido, ahora estamos interesados en tomar no únicamente los menores de tamaño 1 sino todos los menores de la matriz X como generadores de la K-álgebra $K[X]$, por lo que ahora los productos de menores aparecen como *"monomios"*, que a diferencia de los monomios usuales, estos son productos no de 1-menores sino de menores de todos los tamaños acotados por el $\min\{m, n\}$. El objetivo primeramente es obtener un subconjunto adecuado de dichos productos de menores de tal forma que sea linealmente independiente y por tanto sea una K-base de $K[X]$. Así pues, definiremos en esta sección un tipo especial de productos de menores, que llamaremos *monomios estándar* y probaremos que forman una K-base de $K[X]$. Éstos serán útiles para poder calcular bases de Gröbner de ideales determinantales.

Sean K un campo y una matriz de indeterminadas $X = (x_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$ como hemos considerado antes. Sea $1 \leqslant t \leqslant \min\{m, n\}$ un entero. Fijamos dos sucesiones de enteros:

$$1 \leqslant a_1 < a_2 < \cdots < a_t \leqslant m$$

$$1 \leqslant b_1 < b_2 < \cdots < b_t \leqslant n$$

y consideramos el determinante

$$[a_1 \cdots a_t \mid b_1 \cdots b_t] := \det \begin{pmatrix} x_{a_1 b_1} & x_{a_1 b_2} & \cdots & x_{a_1 b_t} \\ x_{a_2 b_1} & x_{a_2 b_2} & \cdots & x_{a_2 b_t} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_{a_t b_1} & x_{a_t b_2} & \cdots & x_{a_t b_t} \end{pmatrix}$$

Cualquiera de estos determinantes es llamado *t-menor* de X. El conjunto de t-menores de X se denota por M_t. El ideal generado por todos los t-menores será denotado por $I_t(X)$.

Existe un orden parcial natural definido en el conjunto $M(X)$ de todos los menores de X, definido como sigue:

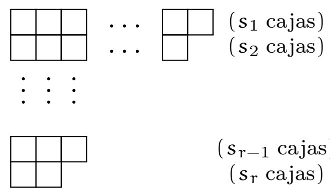
$$[a_1 \cdots a_t \mid b_1 \cdots b_t] \preceq [c_1 \cdots c_s \mid d_1 \cdots d_s]$$

si y sólo si $t \geqslant s, a_i \leqslant c_i, b_i \leqslant d_i$ para $i = 1, ..., s$.

Llamamos a una matriz incompleta A de enteros positivos $(a_{i,j})$ con $1 \leqslant i \leqslant r$ y $1 \leqslant j \leqslant s_i$ tal que $s_1 \geqslant s_2 \geqslant \cdots \geqslant s_r$ con filas estrictamente crecientes y columnas débilmente crecientes un *tablero de Young estándar* y diagramáticamente se representa como:

$$\begin{array}{|c|c|c|cc|c|c|l} \hline a_{11} & a_{12} & & \cdots & \multicolumn{1}{|c|}{} & a_{1s_1} & \multicolumn{1}{c}{} & (s_1 \text{ cajas}) \\ \hline a_{21} & a_{22} & & \cdots & \multicolumn{1}{|c|}{a_{2s_2}} & \multicolumn{1}{c}{} & & (s_2 \text{ cajas}) \\ \hline \multicolumn{1}{c}{\vdots} & \multicolumn{1}{c}{\vdots} & \multicolumn{1}{c}{\vdots} & & & & & \\ \hline & & & & & & & (s_{r-1} \text{ cajas}) \\ \hline a_{r1} & a_{rs_r} & \multicolumn{1}{c}{} & & & & & (s_r \text{ cajas}) \\ \cline{1-2} \end{array}$$

La *forma* del tablero es la sucesión $(s_1, ..., s_r)$ y $s_1 + \cdots s_r$ es llamado el *grado* del tablero A y se denota $\operatorname{gr} A$. Diagramáticamente se ve como el tablero anterior sin los enteros que rellenan las cajas, por ejemplo como:



Un *bitablero* es un par ordenado $T = (A, B)$ de tableros de la misma forma y definimos que $\operatorname{gr} T = \operatorname{gr} A = \operatorname{gr} B$. Usualmente los representaremos como dos tableros uno a continuación de otro:

Definición 3.8 (Monomio estándar)**.** Un producto de menores $\delta = \delta_1 \cdots \delta_s$ tal que $\delta_1 \preceq \delta_2 \preceq \cdots \preceq \delta_s$ decimos que es un monomio estándar.

Un monomio estándar puede ser identificado naturalmente con un *bitablero*. Por ejemplo, si $\delta = \delta_1\delta_2\delta_3$ con $\delta_1 = [124 \mid 123]$, $\delta_2 = [13 \mid 23]$ y $\delta_3 = [24 \mid 25]$, entonces el bitablero asociado está dado en la siguiente figura.

1	2	4		1	2	3
1	3			2	3	
2	4			2	5	

Para el cálculo de bases de Gröbner de $I_t(X)$ necesitamos la correspondencia de Knuth-Robinson-Schensted. A fin de ilustrar dicho proceso describimos el algoritmo de empujones de Schensted a continuación.

3.3.1. Correspondencia de Knuth-Robinson-Schensted

Recuérdese primeramente que se ha visto que podemos identificar monomios estándar con bitableros estándar de Young. En esta subsección buscamos establecer una correspondencia biunívoca entre el conjunto de monomios estándar y el conjunto de monomios en $K[X]$. Esto se hará a partir de la llamada *correspondencia de Knuth-Robinson-Schensted*, que denotaremos algunas veces por simplicidad como *KRS*. Esta biyección puede ser construída usando el *algoritmo de empujones de Schensted* iniciando con un tablero vacío y sucesivamente insertando los valores $\sigma_1, ..., \sigma_n$ de la permutación σ en los números $1, ..., n$; estos forman la segunda línea cuando σ está dado en notación de dos líneas.

El algoritmo de empujones de Schensted lo podemos describir de la siguiente manera:

Dado un tablero de Young (semiestándar), digamos T y $x \in \mathbb{N}$ arbitrario, podemos construír un nuevo tablero denotado por $T \longleftarrow x$, el cual tiene una caja más en el que se coloca x. Procedemos de la siguiente manera:

(1) Si x es $\geqslant$ que todas las entradas en el primer renglón de T, añadimos una caja con x al final del primer renglón de T.

(2) En caso contrario, buscamos en el primer renglón de T la entrada x más a la izquierda y que es $>$ que x, insertamos x en dicha caja empujamos afuera a la entrada x.

(3) Si T consta de un solo renglón, añadimos a T un nuevo renglón con una única caja en el extremo izquierdo donde se coloca a x.

(4) Si T tiene más de un renglón, repetimos los pasos (1) y (2) pero con el segundo renglón de T y el número x que se empujó del renglón previo en el paso (2).

(5) Terminamos cuando la última entrada removida se pueda colocar al final del renglón siguiente acorde a (1), o añadimos un nuevo renglón con una única caja donde ponemos la última entrada removida acorde a (3).

A fin de establecer primeramente la correspondencia de monomios estándar (o bitableros estándar) con monomios en $K[X]$ introducimos el *algoritmo de eliminación*. Para ello, considérese un tablero estándar de Young A, con forma $(s_1, \dots, s_r)$ y un índice $q \leqslant r$ tal que $s_k > s_{k+1}$. A partir de ello construímos un tablero de Young estándar B y un elemento x de A determinados de la siguiente manera:

- Definimos la sucesión $k_q, k_{q-1}, \dots, k_1$, poniendo el primer elemento $k_q = s_q$ y eligiendo los últimos $q-1$ elementos de esta sucesión como el elemento más grande $\leqslant s_i$ tal que $a_{ik_i} \leqslant a_{i+1,k_{i+1}}$.
- Definimos B como el tablero estándar que se obtiene removiendo el elemento a_{qs_q} de la q-ésima fila del tablero A y sustituyendo la entrada a_{ik_i} de la i-ésima fila por $a_{i+1k_{i+1}}$ con $i = 1, \dots, q-1$.
- Fijamos $x = a_{1k_1}$.

Observe que con este algoritmo en efecto generamos un tablero estándar B cuya forma es $(s_1, \dots, s_q - 1, \dots, s_r)$. Ilustramos este hecho con un ejemplo.

Ejemplo 3.8.1. Sea $A = (a_{ij})$ un tablero con forma $(s_1, s_2, s_3) = (3, 2, 1)$ como se indica en la siguiente figura:

1	2	4
3	5	
4		

Elegimos $q = 3$, por lo que para determinar la sucesión k_3, k_2, k_1 tenemos: $k_1 = s_3 = 1$, luego para determinar k_2 observamos que el mayor entero $\leqslant s_2$ es 2, sin embargo, $5 = a_{22} \nleq a_{31} = 4$, por lo que el mayor entero menor a s_2 que cumple la condición dada es 1, pues en efecto: $3 = a_{21} \nleq a_{31} = 4$, por lo que $k_2 = 1$. De la misma manera, elegimos k_1 observando que $4 = a_{13} \nleq a_{21} = 3$, pero $2 = a_{12} \nleq a_{21} = 3$, por lo que $k_1 = 2$.

De acuerdo al algoritmo, definimos el tablero B con las sustituciones:

$$a_{12} \leftrightarrow a_{21}$$

$$a_{21} \leftrightarrow a_{31}$$

Por último, el elemento x es igual a_{12}, esto es $x = 2$. El tablero B queda determinado por la figura:

1	3	4
4	5	

En efecto, la forma de B es $(3, 2)$.

El algoritmo de eliminación tiene un proceso inverso que describimos a continuación, conocido como *algoritmo de inserción*. Al igual que con el algoritmo de eliminación, partimos de un tablero estándar $A = (a_{ij})$ de forma $(s_1, \ldots, s_r)$ y un entero x y construímos un tablero B y un índice q determinados de la siguiente manera:

- Fijamos $i = 1$ y $B = A$
- Si $s_i = 0$ o $x > a_{is_i}$, entonces añadimos x al final de la i-ésima fila de B, ponemos $q = i$ y finalizamos el algoritmo.
- De otra manera, sea k_i el elemento más pequeño j tal que $x \leqslant a_{js_i}$, reemplazamos $b_{k_i s_i}$ con x, ponemos $x = a_{k_i s_i}$, $i = i + 1$ y regresamos al paso anterior.

El tablero B resultante es tal que su forma es $(s_1, \ldots, s_q + 1, \ldots, s_r)$. Esta operación es inversa del proceso de eliminación descrito anteriormente. Ilustraremos un ejemplo, partiendo ahora del tablero estándar obtenido en el ejemplo 3.8.1, que después de aplicar el algoritmo de inserción genera el tablero estándar A con el que inició dicho ejemplo.

Ejemplo 3.8.2. Considérese el entero $x = 2$ y el tablero estándar $A = (a_{ij})$ cuya forma es $(s_1, s_2) = (3, 2)$ determinado por el siguiente diagrama:

1	3	4
4	5	

Observe que a lo más en 3 pasos habremos terminado pues $s_3 = 0$ y el algoritmo termina cuando $s_i = 0$ ó $x > a_{is_i}$. Luego de aplicar el algoritmo, obtenemos el tablero A dado por el digrama siguiente:

1	2	4
3	5	
4		

Además del entero $q = 3$.

Los ejemplos 3.8.1 y 3.8.2 ilustran el hecho de que si aplicamos el algoritmo de eliminación a un tablero estándar A y un entero q obtenemos un tablero estándar B y un entero x; luego el algoritmo de inserción aplicado al tablero B y al entero x nos da como resultado el tablero A y el número q, esto es, los algoritmos mencionados son inversos uno del otro.

En el siguiente resultado definiremos la llamada *correspondencia KRS* usando los algoritmos descritos anteriormente.

Teorema 3.9 (Correspondencia KRS)**.** *Existe una biyección entre el conjunto de monomios estándar o bitableros estándar y los monomios en* $K[X]$.

Demostración. En principio veremos que la correspondencia KRS es una biyección entre el conjunto de bitableros estándar y el conjunto de matrices de dos renglones de cierto tipo. Supongamos que partimos de un bitablero estándar $T = (A \mid B) = (a_{ij} \mid b_{ij})$. Construímos un bitablero T' y un par de enteros ℓ, r como sigue:

(i) Elegimos la entrada más grande u en el tablero izquierdo, A. Supongamos que $\{(i_1, j_1, \ldots, (i_u, j_u)\}$, con $i_1 < \ldots < i_u$, es el conjunto de índices (i,j) tal que $\ell = a_{ij}$. Sea $p = i_u$ y $q = j_u$. Llamamos a (p,q) la posición pivote.

(ii) Sea A' el tablero estándar que se obtiene de A al quitar el elemento a_{pq}.

(iii) Aplicamos el algoritmo de eliminación a la pareja (B, p) y obtenemos un bitablero estándar B' y un entero r.

(iv) Definimos $T' = (A' \mid B')$.

Este proceso lo llamamos el *algoritmo KRS*. Considerando así, el bitablero T de forma $(s_1, \ldots, s_p)$, definimos $k = s_1 + \cdots + s_p$ y la matriz de dos renglones como sigue:

$$\mathsf{KRS}(T) = \begin{pmatrix} \ell_1 & \ell_2 & \cdots & \ell_{k-1} & \ell_k \\ r_1 & r_2 & \cdots & r_{k-1} & r_k \end{pmatrix}$$

Comenzamos de $T_k = T$, luego el *algoritmo KRS* aplicado a T_i para $i = k, k-1, \ldots, 1$ produce el bitablero T_{i-1} y la pareja (ℓ_i, r_i).

Inversamente, aplicamos el *algoritmo de inserción* a la línea inferior de la matriz para construír el tablero derecho B: En el paso i insertamos r_i en el tablero obtenido después del $i-1$-ésimo paso. De forma simultánea se genera el tablero de la izquierda A poniendo el elemento ℓ_i en la posición que se agrega al tablero de la derecha por la i-ésima inserción.

Sólo resta ver, que dicho arreglo o matriz de dos renglones se puede identificar con un monomio en $K[X]$, esto se logra muy fácil asignando a la matriz:

$$\begin{pmatrix} \ell_1 & \ell_2 & \cdots & \ell_{k-1} & \ell_k \\ r_1 & r_2 & \cdots & r_{k-1} & r_k \end{pmatrix}$$

el monomio:

$$x_{\ell_1 r_1} x_{\ell_2 r_2} \cdots x_{\ell_k r_k}.$$

De esta manera, mediante esta construcción identificamos de forma biunívoca a cada bitablero estándar o monomio estándar con un monomio en $K[X]$ y viceversa. $\square$

3.3.2. Bases monomiales de ideales determinantales

El primer resultado que necesitamos son las *relaciones de Plücker* que satisfacen los menores de rango máximo[1] en X. Denotemos por $S(\ell_1, \ldots, \ell_u)$ al grupo simétrico con u elementos ℓ_i. Considere el grupo simétrico $S = S(i_t, \ldots, i_m, j_1, \ldots, j_t)$ y el producto directo $S' = S(i_t, \ldots, i_m) \times S(j_1, \ldots, j_t)$, subgrupo de S.

Lema 3.10 (Relaciones de Plücker)**.** *Los menores de rango máximo m de X satisfacen*

$$\sum_{\bar{\sigma} \in S/S'} \operatorname{sgn} \sigma [i_1 \cdots i_{t-1} \sigma(i_t) \cdots \sigma(i_m)][\sigma(j_1) \cdots \sigma(j_t) j_{t+1} \cdots j_m] = 0 \tag{3.1}$$

Demostración. Observe primeramente que si $\sigma \in S$ es tal que su restricción está en $S(i_t, \ldots, i_m)$ entonces, claramente la restricción de σ también estará en $S(j_1, \ldots, j_t)$. Esto es, si $\sigma \in S$ permuta los elementos $\{i_t, \ldots, i_m\}$ entre ellos, entonces se sigue que σ permuta los elementos $\{j_1, \ldots, j_t\}$ entre ellos. Así, las permutaciones que se consideran en la suma son sólo aquellas que intercambian un subconjunto no vacío de $\{i_t, \ldots, i_m\}$ con un subconjunto de $\{j_1, \ldots, j_t\}$.

Considérese la matriz $m \times n$ de indeterminadas x_{ij}:

$$X = (v_1, \ldots, v_n) = \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix} \text{ donde } v_i \text{ es la columna i-ésima de } X.$$

Observe que en la suma 3.1, los sumandos que la conforman son productos de dos m-menores determinados por la elección de m-columnas, pero cada uno de ellos es una coordenada de Plucker para un subespacio W de dimensión m. Por lo ya mencionado, la suma 3.1 depende únicamente de las permutaciones σ que intercambian subconjuntos de elementos $\{i_t, \ldots, i_m\}$ con subconjuntos de elementos $\{j_1, \ldots, j_t\}$ y por tanto sólo se consideran esas columnas. Denotamos dichas columnas por $v_{i_t}, \ldots, v_{i_m}, v_{j_1}, \ldots, v_{j_t}$ que son $m+1$ vectores, por tanto, la suma 3.1 es un elemento en $\wedge^{m+1}(K^m) = 0$, por lo que dicha suma se anula. $\square$

Sea $M_m(X) \subseteq M(X)$ el subconjunto de menores de tamaño m y denote por $K[X_m]$ la subálgebra de $K[X]$ generada por $M_m(X)$.

[1] Vea la subsección 4.2, en especial el teorema 4.14 donde se muestra que estos polinomios cuadráticos son los generadores del ideal de anulación de la variedad de Grassmann.

Lema 3.11. *Los monomios estándar de tamaño* m *generan la subálgebra* $K[X_m]$ *como espacio vectorial.*

Demostración. Consideremos dos menores en $M_m(X)$, digamos $[i_1 \cdots i_m]$, $[j_1 \cdots j_m]$, entonces $1 \leqslant i_k \leqslant n$ y $1 \leqslant j_k \leqslant n$ y además $i_1 < \cdots < i_m$ y $j_1 < \cdots < j_m$. Supongamos que dichos menores son tales que: $i_k \leqslant j_k$ para todo k tal que $1 \leqslant k \leqslant s-1$, pero $i_s > j_s$

Entonces por 3.10 tenemos que:

$$\sum_{\sigma \in S/S'} \operatorname{sgn} \sigma [i_1 \cdots i_{s-1} \sigma(i_s) \cdots \sigma(i_m)][\sigma(j_1) \cdots \sigma(j_s) j_{s+1} \cdots j_m] = 0 \tag{3.2}$$

donde $S = S(i_s, \ldots, i_m, j_1, \ldots, j_s)$ y $S' = S(i_s, \ldots, i_m) \times S(j_1, \ldots, j_s)$.

Observe que $[i_1 \cdots i_m][j_1 \cdots j_m]$ no es un monomio estándar pues $i_s > j_s$ y corresponde al sumando donde $\sigma = \mathrm{id}$, luego podemos despejarlo de 3.2 y podemos entonces expresarlo como una combinación lineal de productos de menores de la forma $[k_1 \cdots k_m][\ell_1 \cdots \ell_m]$ con $\sigma \neq \mathrm{id}$, en los que ordenamos de manera ascendente sus columnas. Recuérdese que en $[k_1 \cdots k_m]$ tenemos que $k_r = i_r$ para $r = 1, \ldots, s-1$ y $k_s = \sigma(i_s) = j_\mu$ donde $\mu \in \{1, \ldots, s\}$ y $j_1 < \cdots < j_s$ y dado que $i_s > j_s$ tenemos que $\sigma(i_s) = k_s < i_s$. Similarmente, $k_{s+1} = \sigma(i_{s+1}) = j_{\mu'}$, donde $\mu' \in \{1, \ldots, s\} \setminus \{\mu\}$, y como $i_{s+1} > i_s$ se sigue que $\sigma(i_{s+1}) = k_{s+1} < s+1$. De esta misma manera, se sigue que $k_{s+2} < i_{s+2} \ldots k_m < i_m$, por tanto:

$$[k_1 \cdots k_m] \preceq [i_1 \cdots i_m] \tag{3.3}$$

Por otro lado, afirmamos que:

$$[k_1 \cdots k_s] \preceq [\ell_1 \cdots \ell_s] \tag{3.4}$$

En efecto, para los primeros $s-1$ elementos se sigue fácilmente, pues $k_1 = i_1 \leqslant \sigma(j_1) = \ell_1$, donde la desigualdad anterior se da pues $\sigma(j_1) \in \{i_s, \ldots, i_m\}$ y además $i_m \geqslant \cdots \geqslant i_s \geqslant i_1$. Por tanto, $k_r \leqslant \ell_r$ para $r = 1, \ldots, s-1$. Además, $k_s = \sigma(i_s) \leqslant \ell_s$ pues de lo anterior $\ell_1, \ldots, \ell_{s-1}$ ya han sido definidos. Y por último, si $[k_1 \cdots k_m] \not\preceq [\ell_1 \cdots \ell_m]$, entonces existe $s' > s$ tal que $k_{s'} > \ell_{s'}$, por lo que estamos en las condiciones con las que comenzamos al considerar los menores $[i_1 \cdots i_m]$, $[j_1 \cdots j_m]$, entonces aplicando el mismo procedimiento a $[k_1 \cdots k_m][\ell_1 \cdots \ell_m]$ usando 3.10 podemos expresarlo como una combinación lineal de productos de menores de la forma $[k'_1 \cdots k'_m][\ell'_1 \cdots \ell'_m]$ que cumplirán relaciones análogas a 3.3 y 3.4 y nuevamente aplicamos el mismo procedimiento. Así, este proceso inductivo muestra que en un número finito de pasos a partir de los menores con los que comenzamos: $[i_1 \cdots i_m]$y$[j_1 \cdots j_m]$ podemos expresar a $[i_1 \cdots i_m][j_1 \cdots j_m]$ como una combinación lineal de productos de menores de la forma $[k_1 \cdots k_m][\ell_1 \cdots \ell_m]$, tales que:

$$[k_1 \cdots k_m] \preceq [i_1 \cdots i_m] \tag{3.5}$$

y

$$[k_1 \cdots k_m] \preceq [\ell_1 \cdots \ell_m] \tag{3.6}$$

Esto es, cada producto $[k_1 \cdots k_m][\ell_1 \cdots \ell_m]$ es un monomio estándar, por lo que tenemos que $[i_1 \cdots i_m][j_1 \cdots j_m]$ es una combinación lineal de monomios estándar. Note que $[k_1 \cdots k_m]$ y $[\ell_1 \cdots \ell_m]$ se obtienen de $[i_1 \cdots i_m][j_1 \cdots j_m]$ por intercambio de algunos índices, de acuerdo a 3.2.

Ahora queremos probar que un producto finito de longitud mayor a 2 de m-menores se puede expresar como una combinación lineal de monomios estándar. Sea $\delta = \delta_1 \cdots \delta_\mu$ un producto de m-menores con $\mu > 2$, si δ es un monomio estándar no hay nada que hacer. Supongamos que δ no es un monomio estándar, entonces existe un índice k tal que $\delta_k \not\preceq \delta_{k+1}$. Por lo que ya hemos hecho anteriormente, podemos expresar a $\delta_k\delta_{k+1}$ como una combinación lineal de monomios estándar. Sustituímos esta expresión de $\delta_k\delta_{k+1}$ en el producto original δ y afirmamos que obtenemos una expresión de δ como combinación lineal de monomios estándar. □

La consecuencia importante es el siguiente teorema.

Teorema 3.12. *Los monomios estándar forman una K-base de $K[X]$, esto es:*
(1) *Los monomios estándar generan a $K[X]$.*
(2) *Los monomios estándar son linealmente independientes en $K[X]$. Además:*
(3) *Si un producto de menores $\delta\gamma$ no es un monomio estándar, entonces tiene la siguiente representación dada por monomios estándar:*

$$\delta\gamma = \sum \alpha_i \eta_i \rho_i$$

donde $\alpha_i \in K$, $\alpha_i \neq 0$ y $\eta_i\rho_i$ es un monomio estándar tal que $\eta_i \prec \delta, \gamma \prec \rho_i$.

Demostración. (1) Extendemos el resultado del lema 3.11 en X_m al conjunto de menores $M(X)$ de X extendiendo la matriz X de tamaño $m\times n$ a una matriz X' de tamaño $m\times(n+m)$, esto es, añadiendo n columnas a X.

$$X' = \begin{pmatrix} x_{11} & \cdots & x_{1n} & x_{1,n+1} & \cdots x_{1,n+m} \\ \vdots & & \vdots & \vdots & \vdots \\ x_{m1} & \cdots & x_{mn} & x_{m,n+1} & \cdots x_{m,n+m} \end{pmatrix}$$

Luego, podemos considerar el morfismo de K-álgebras de $\varphi : K[X'] \to K[X]$ sustituyendo cada entrada de X por la correspondiente entrada de la siguiente matriz:

$$\begin{pmatrix} x_{11} & \cdots & x_{1n} & 0 & \cdots & \cdots & 0 & 1 \\ & & & \vdots & & \iddots & \iddots & 0 \\ \vdots & & \vdots & \vdots & \iddots & \iddots & \iddots & \vdots \\ & & & 0 & \iddots & \iddots & & \vdots \\ x_{m1} & \cdots & x_{mn} & 1 & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

notando que claramente φ es suprayectivo. Restringiendo el dominio del morfismo φ a $K[M(X')]$ tenemos el morfismo de K-álgebras:

$$\varphi' : K[M(X')] \to K[X].$$

Luego,

$$\varphi'([j_1 \cdots j_m]) = \pm[i_1 \cdots i_t \mid j_1 \cdots j_t]$$

donde $t = \text{máx}\{\ell : j_\ell \leqslant n\}$ y los $i_1, \ldots, i_t$ han sido elegidos de tal forma que:

$$\{i_1, \ldots, i_t, n + m + 1 - j_m, \ldots, n + m + 1 - j_{t+1}\} = \{1, \ldots, m\}$$

por lo que φ' es claro que es suprayectiva, además dado que φ' se definió en términos de la matriz $(X \mid T)$, donde T es la matriz anti-identidad (con 1's en la antidiagonal) cuyo determinante es -1, se sigue que φ' establece una correspondencia biyectiva entre $M_m(X'_m)$ y $M(X) \cup \{\pm 1\}$.

A fin de tener una representación un elemento arbitrario de $K[X]$ como combinación lineal de bitableros estándar vemos dicho elemento en $K[M_m(X')]$ a través de su preimagen bajo φ', así la imagen es *rectificada* y aplicando φ' tenemos el elemento en $K[X]$ con la expresión deseada.

(2) Considerando $K[X]$ como álgebra graduada, sea $K[X]_d$ la componente homogénea de grado d de $K[X]$, esto es, el subespacio vectorial de los polinomios homogéneos de $K[X]$ de grado d junto con el polinomio cero. $K[X]_d$ está generado como espacio vectorial por todos los monomios de grado d.

Sabemos que $K[X]$ está generado por monomios estándar de acuerdo a (1), entonces $K[X]_d$ también está generada por monomios estándar, además éstos son polinomios homogéneos, pues todo menor de X es un polinomio homogéneo, entonces, $K[X]_d$ está generada por monomios estándar de grado d en $K[X]$. Queremos ver que los monomios estándar en cada componente homogénea $K[X]_d$ son linealmente independientes y por tanto forman una base.

De acuerdo a la *correspondencia de Knuth-Robinson–Schensted* 3.9 tenemos que existe una biyección entre el conjunto de monomios estándar en $M(X)$ y los monomios de $K[X]$. Dicha correspondencia nos dice que para cada grado d, hay tantos monomios estándar como monomios en $K[X]_d$ y dado que los monomios forman una K-base de $K[X]_d$ y sabemos que los monomios estándar generan a $K[X]_d$ entonces, estos últimos deben ser linealmente independientes.

(3) De acuerdo al lema 3.10 las relaciones de Plücker son polinomios homogéneos cuadráticos, por lo que si δ y γ son menores de tamaño m en $K[X]$ tenemos que en cada término del lado derecho de $\delta\gamma = \sum \alpha_i \eta_i \rho_i$ hay exactamente dos factores η_i y ρ_i. Como la rectificación en $K[X]$ corresponde, por medio de φ', a la rectificación en $K[M(X')]$, al rectificar el lado derecho de $\delta\gamma$, cada término no puede subir de grado, esto es, hay a lo más dos factores en cada sumando. Queremos ver que $\eta_i \prec \delta$. Observe que por la última

parte del lema 3.11, en específico la ecuación 3.5, tenemos que en la expresión de $\delta\gamma$ como combinación lineal de monomios estándar se tiene que $\eta_i \preceq \delta$. Para ver que $\eta_i \preceq \gamma$ simplemente consideramos ahora $\gamma\delta$ para aplicar el mismo procedimiento de rectificación, dado que $\delta\gamma = \gamma\delta$ y los monomios estándar son linealmente independientes. Usando la independencia lineal de los monomios estándar podemos probar que δ, $\gamma \preceq \rho_i$. En efecto, dado que la rectificación en $K[X]$ corresponde, por medio de φ', a la rectificación en $K[M(X')]$, basta con probar esta relación en $K[M(X')]$. Recuérdese que en el conjunto de menores $M(X')$ tenemos el orden parcial $\preceq$. Consideramos el orden parcial inverso $\preceq'$ que surge de reordenar las columnas de la matriz X' en el orden $m+n, m+n-1, \ldots, 1$. Salvo un signo, respecto a este orden $\preceq'$, tenemos los mismos monomios estándar que con el orden $\preceq$. Por tanto, rectificando con respecto al orden parcial inverso $\preceq'$ tal y como se hizo con $\preceq$ tenemos que δ, $\gamma \preceq \rho_i$, lo que concluye la prueba. $\square$

Definición 3.13. Sea $(M, \leqslant)$ un conjunto parcialmente ordenado. Decimos que un subconjunto P de M es un ideal si para cada $y \in M$, P contiene a todo x tal que $x \leqslant y$.

Observación 3.14. Sea N un ideal en $(M(X), \preceq)$ y consideremos el ideal $I \subseteq K[X]$ generado por N, es decir, $I = NK[X]$. Todo elemento de I es una combinación lineal de elementos δp con $\delta \in N$ y $p \in K[X]$. Por el teorema 3.12 tenemos que podemos expresar a δp como combinación lineal de monomios estándar $\gamma = \gamma_1 \cdots \gamma_s$ tal que $\gamma_1 \npreceq \delta$. Luego, como N es ideal se sigue que $\gamma_1 \in N$. Así, los monomios estándar $\gamma = \gamma_1 \cdots \gamma_s$ con $\gamma_1 \in N$ forman una base de $I = NK[X]$ en $K[X]$.

A partir de este resultado, probamos el siguiente teorema.

Teorema 3.15. *Sea t un entero con $1 \leqslant t \leqslant \min\{m, n\}$. Entonces los monomios estándar $\delta = \delta_1\delta_2 \cdots \delta_r$ con $\operatorname{gr}\delta_1 \geqslant t$ forman una K-base de $I_t(X)$.*

Demostración. Sea $N = \{\delta : \delta \in M(X), \operatorname{gr}\delta \geqslant t\}$. Obsérvese que N es un ideal de $M(X)$ por la forma en que está definido el orden $\preceq$ en el conjunto de menores $M(X)$. En efecto, si $\gamma \in N$, entonces dado $\delta \in M(X)$ con $\delta \preceq \gamma$ es tal que $\operatorname{gr}\delta \geqslant \operatorname{gr}\gamma \geqslant t$ y por tanto $\delta \in N$. Por la observación 3.14 tenemos que los monomios estándar $\delta = \delta_1\delta_2 \cdots \delta_r$ con $\operatorname{gr}\delta_1 \geqslant t$ forman una K-base de $NK[X]$. Obsérvese que los elementos en $NK[X]$ son combinaciones lineales de menores de tamaño mayor o igual que t con coeficientes en $K[X]$. Luego, dado que para cada $s \geqslant 1$, podemos expresar un $t+s$-menor en términos de t-menores, tenemos que $NK[X] = I_t(X)$, lo que completa la demostración. $\square$

Nos interesa calcular una base de Gröbner de $I_t(X)$. Para ello, fijamos un *orden diagonal monomial*, esto es, un orden monomial que seleciona la diagonal de un menor como su término inicial. En otras palabras, si $\delta = [a_1 \cdots a_t \mid b_1 \cdots b_t]$ entonces:

$$\operatorname{in}_<(\delta) = x_{a_1 b_1} x_{a_2 b_2} \cdots x_{a_t b_t}$$

Antes de enunciar el siguiente resultado de gran importancia, consideremos un módulo S-módulo graduado $M = \bigoplus_{i\in\mathbb{Z}} M_i$, finitamente generado y la siguiente función numérica, llamada la *función de Hilbert* de M.

$$H(M,-) : \mathbb{Z} \to \mathbb{Z}_+$$

dada por $H(M,i) = \dim_K(M_i)$. La serie de potencias formal de Laurent:

$$\mathrm{Hilb}_M(t) = \sum_i H(M,i)t^i$$

y la llamamos la *serie de Hilbert* del módulo M. Necesitaremos el resultado siguiente:

Lema 3.16. *Si* K *es un campo, para el anillo de polinomios* S*, un ideal graduado* $I \subset S$*, un orden monomial* $<$ *y un ideal monomial* $J \subset \mathrm{in}_<(I)$*, las siguientes condiciones son equivalentes:*

(i) $J = \mathrm{in}_<(I)$

(ii) $\mathrm{Hilb}_{S/I}(t) = \mathrm{Hilb}_{S/J}(t)$.

Demostración. En efecto, consideremos las componentes homogéneas de $S/\mathrm{in}_<(I)$ y de S/J que son respectivamente, $S_i/\mathrm{in}_<(I)\cap S_i$ y $S_i/J\cap S_i$, para toda i. Dado que $J \subset \mathrm{in}_<(I)$, por hipótesis, se sigue que $S_i/\mathrm{in}_<(I)\cap S_i$ es subespacio vectorial de $S_i/J\cap S_i$ para toda i y por lo tanto $\dim_K S_i/\mathrm{in}_<(I)\cap S_i \leqslant \dim_K S_i/J\cap S_i$, para toda i. Luego:

$$\mathrm{Hilb}_{S/\mathrm{in}_<(I)}(t) = \sum_i \dim_K S_i/\mathrm{in}_<(I)\cap S_i \leqslant \sum_i \dim_K S_i/J\cap S_i = \mathrm{Hilb}_{S/J}(t)$$

Así, $\mathrm{Hilb}_{S/\mathrm{in}_<(I)}(t) \leqslant \mathtt{Hilb}_{S/J}(t)$ y la igualdad se sostiene si y sólo si $J = \mathrm{in}_<(I)$.

De lo anterior, sólo resta ver que $\mathrm{Hilb}_{S/\mathrm{in}_<(I)}(t) = \mathrm{Hilb}_{S/I}(t)$. Por definición de la función de Hilbert, basta mostrar que:

$$\dim_K S_i/\mathrm{in}_<(I)\cap S_i = \dim_K S_i/I\cap S_i$$

Dado que I es un ideal graduado consideremos la i-ésima componente graduada, I_i que es un ideal de S_i y tomemos los monomios en S_i que no están en $\mathrm{in}_<(I_i)$. Por 1.13 dichos monomios (módulo I_i) son una base de $S_i/I_i = S_i/I\cap S_i$ y dado que dicho espacio es de dimensión finita tenemos que el conjunto de los monomios en S_i que no están en $\mathrm{in}_<(I_i)$ es finito, digamos $\{f_1,\dots,f_j\}$ y $\{\bar{f_1},\dots,\bar{f_j}\}$ es una base de $S_i/I_i = S_i/I\cap S_i$.

Dado que $f_i \notin \mathrm{in}_<(I_i)$, se sigue que f_i módulo $\mathrm{in}_<(I_i)$ es no nulo en $S_i/\mathrm{in}_<(I_i)$ y afirmamos que forman una base de $S_i/\mathrm{in}_<(I_i)$, además $\mathrm{in}_<(I_i) = \mathrm{in}_<(I)\cap S_i$ con lo que habremos terminado la prueba. □

Consideremos un ejemplo haciendo el cálculo en `Macaulay2` para la serie de Hilbert de un ideal dado.

Ejemplo 3.16.1. Sea $\mathbb{Q}[x_1, x_2, x_3, x_4]$ el anillo de polinomios en 4 variables sobre $\mathbb{Q}$ y sea $I = \langle x_1^2 - x_2x_3, x_3^2x_4, x_1x_2x_3, x_4^3\rangle$. A fin de simplificar notación en el código, usamos las variables x, y, z, w para x_1, x_2, x_3, x_4 respectivamente. Entonces, haciendo el cálculo de la serie de Hilbert de I tenemos:

```
i1 : QQ[x,y,z,w]

o1 = QQ[x, y, z, w]

o1 : PolynomialRing

i2 : I=ideal(x^2-y*z,w*z^2,x*y*z,w^3)

             2         2           3
o2 = ideal (x  - y*z, z w, x*y*z, w )

o2 : Ideal of QQ[x, y, z, w]

i3 : hilbertSeries(I)

          2     3     5    6     7    8
     1 - T  - 3T  + 6T  - T  - 3T  + T
o3 = ----------------------------------
                         4
                  (1 - T)

o3 : Expression of class Divide

i4 : reduceHilbert(o3)

                2     3    5
     1 + 3T + 5T  + 4T  - T
o4 = -----------------------
             (1 - T)

o4 : Expression of class Divide
```

Por lo tanto, de acuerdo a o_4, $\mathrm{Hilb}_I(t) = \frac{1+3t+5t^2+4t^3-t^5}{1-t}$

Observación 3.17. Otra presentación de la función de Hilbert está dada por:

$$\mathrm{Hilb}_M(t) = \frac{P_M(t)}{(1-t)^d}$$

donde d en esta presentación es la dimensión de Krull de M y $P_M(t)$ es un polinomio tal que $P_M(1) \neq 0$.

Corolario 3.18. *Sean* K *un campo,* $S = K[x_1, \ldots, x_n]$, I *un ideal graduado de* S *y* $<$ *un orden monomial en* S. *Entonces* $\dim S/I = \dim S/\operatorname{in}_<(I)$

Demostración. Por el lema 3.16 los anillos graduados S/I y $S/\operatorname{in}_<(I)$ tienen la misma función de Hilbert, luego por la observación 3.17, la función de Hilbert determina la dimensión de Krull, por lo que concluímos que $\dim S/I = \dim S/\operatorname{in}_<(I)$. □

Usaremos el lema 3.16 en el siguiente teorema que permite obtener una base de Gröbner para $I_t(X)$ si consideramos un orden monomial diagonal.

Teorema 3.19. *Para cualquier orden monomial diagonal el conjunto de todos los t-menores de X es una base de Gröbner de $I_t(X)$.*

Demostración. Por el teorema 3.15 los monomios estándar $\delta = \delta_1\delta_2\cdots\delta_r$ con $\operatorname{gr}(\delta_1) \geqslant t$ forman una K-base de $I_t(X)$. Denotemos este conjunto de monomios estándar como D_t. Por el teorema 3.9, para cada $\delta \in D_t$, el monomio $\mathsf{KRS}(\delta)$ contiene como factor la diagonal principal de un t-menor de X. Por lo tanto, para $\delta \in D_t$ existe un t-menor σ tal que $\operatorname{in}_<(\sigma) \mid \mathsf{KRS}(\delta)$. Así, si J denota el ideal generado por los monomios iniciales de los t-menores de X, vemos que $\mathsf{KRS}(D_t) \subset J \subset \operatorname{in}_<(I_t(X))$.

Para un subconjunto $\mathcal{S} \subset K(X)$ que consiste de polinomios homogéneos, denotamos por $K\mathcal{S}$ el K-espacio vectorial generado por los elementos de $\mathcal{S}$. Entonces $K\mathcal{S}$ es un K-espacio vectorial graduado, cuya componente graduada i-ésima la denotamos por $(K\mathcal{S})_i$. Dado que $(KD_t)_i = I_t(X)_i$ tenemos que para todo i

$$\dim_K I_t(X)_i = \dim_K(K(\mathsf{KRS}(D_t))_i) \leqslant \dim_K J_i \leqslant \dim_K \operatorname{in}_<(I_t(X))_i = \dim_K I_t(X)_i.$$

Consecuentemente, $\operatorname{Hilb}_{S/J}(t) = \operatorname{Hilb}_{S/\operatorname{in}_<(I_t(X))}(t)$ y se sigue el resultado deseado. □

3.3.3. El complejo inicial de un ideal determinantal

Hemos visto que para cualquier orden diagonal monomial $<$, el conjunto de todos los t-menores de X es una base de Gröbner de $I_t(X)$. Así que para tal orden monomial tenemos:

$$\operatorname{in}_<(I_t(X)) = (\{x_{a_1b_1}x_{a_2b_2}\cdots x_{a_tb_t}\}1 \leqslant a_1 < a_2 < \cdots a_t \leqslant m, 1 \leqslant b_1 < b_2 < \cdots b_t \leqslant n)$$

Obsérvese que tenemos que $\operatorname{in}_<(I_t(X))$ es un ideal inicial libre de cuadrados. Así, identificando la variable x_{ij} con el punto $(i,j) \in [m]x[n]$, podemos ver al ideal $\operatorname{in}_<(I_t(X))$ como el ideal Stanley-Reisner de un complejo simplicial en el conjunto de vértices $[m]x[n]$. Denotamos este complejo simplicial por Δ_t y lo llamamos el *complejo inicial* del ideal determinantal $I_t(X)$

Teorema 3.20. *El anillo determinantal $K[X]/I_t(X)$ es un dominio entero con:*

$$\dim_K K[X]/I_t(X) = (m+n-t+1)(t-1).$$

Demostración. Por el corolario 3.18 tenemos:

$$\dim K[X]/I_t(X) = \dim K[X]/\operatorname{in}_<(I_t(X)) = \dim \Delta_t + 1 = \max\{|F| : F \in \Delta_t\}.$$

Dado que cualquier camino de P_r a Q_r tiene cardinalidad $m+n-(2r-1)$ se sigue que todas las *caras* de Δ_t tienen cardinalidad:

$$\sum_{r=1}^{t-1}(m+n-(2r-1)) = (t-1)(m+n-t+1)$$

Esto produce la fórmula de dimensión deseada.

A fin de ver que $K[X]/I_t(X)$ es un dominio, procedemos por inducción sobre t. La afirmación para $t=1$ es inmediata. Ahora, sea $t>1$; entonces x_{1n} no pertenece a ninguna diagonal de X. Sea $<$ un orden monomial. Entonces x_{1n} no divide a ningún generador de $\mathrm{in}_<(I_t(X))$. Por lo tanto, x_{1n} no es un divisor de cero en $K[X]/\mathrm{in}_<(I_t(X))$. Así, el lema subsiguiente implica que x_{1n} no es un divisor de cero en $K[X]/I_t(X)$ tampoco. Se sigue que el mapeo natural:

$$K[X]/I_t(X) \to (K[X]/I_t(X))_{x_{1n}}$$

es inyectivo. Lo anterior implica que $K[X]/I_t(X)$ es un dominio, una vez probado que $(K[X]/I_t(X))_{x_{1n}}$. Para ver esto último, observe que se sigue por inducción, pues:

$$(K[X]/I_t(X))_{x_{1n}} \cong (K[Y]/I_{t-1}(Y))[x_{11},...,x_{1n},x_{2n},...,x_{mn}][x_{1n}^{-1}]$$

donde $Y=(y_{ij})_{i=2,...,m;j=1,...,n-1}$ es una matriz de indeterminadas. Este isomorfismo es inducido por el isomorfismo de K-álgebras

$$K[X] \to K[Y][x_{11},...,x_{1n},x_{2n},...,x_{mn}][x_{1n}^{-1}]$$

dado por las sustituciones:

$$x_{ij} \mapsto y_{ij} + x_{1j}x_{in}x_{1n}^{-1}$$

para $i=2,...,m$, $j=1,...,n-1$

$$x_{ij} \mapsto x_{ij}$$

para $i=1$ ó $j=n$. De hecho, esta sustitución, mapea X a la matriz Z, de la cual se obtiene la matriz X' con entradas $x'_{1n}=x_{1n}$,$x'_{ij}=0$ para $i=1$ ó $j=n$ y $x'_{ij}=y_{ij}$ para $i\geqslant 2$y $j\leqslant n-1$ limpiando la última columna y el primer renglón de Z con x_{1n} como un elemento pivote. De esto se deduce que para $I_t(Z)$, que es imagen de $I_t(X)$ bajo esta sustitución, tenemos que $I_t(Z)=x_{1n}I_{t-1}(X')=x_{1n}I_{t-1}(Y)=I_{t-1}(Y)$. □

4 Bases Sagbi

En este capítulo introducimos las *bases* Sagbi[1] con el fin de estudiar subálgebras de anillos de polinomios usando la misma idea que con las bases de Gröbner. En el caso de bases de Gröbner de un ideal se consideraba un orden monomial en $S = K[x_1, \ldots, x_n]$ y un ideal I de S, luego a partir de los generadores del ideal inicial de I, $\text{in}_<(I)$, se obtenía una base de Gröbner de I. Usando la misma idea se puede considerar ahora una subálgebra dada A del anillo de polinomios S y definir el *álgebra inicial* de A. De esta forma se obtendrá un álgebra $\text{in}_<(A)$ generada sobre K por monomios de S. Así, los elementos cuyos monomios iniciales generen dicha álgebra nos conducirá al concepto de *bases* Sagbi.

Definición 4.1. Sea K un campo y A una subálgebra del anillo de polinomios S. Dado un orden monomial en S, denotamos $\text{in}_<(A)$ a la K-subálgebra de S generada sobre K por todos los monomios $\text{in}_<(f)$ con $f \in A$. El álgebra $\text{in}_<(A)$ es llamada el *álgebra inicial* de A con respecto al orden monomial $<$. Un conjunto $\mathcal{S} \subset A$ es llamado una *base de* Sagbi de A con respecto a $<$ si los elementos $\text{in}(f)$ con $f \in \mathcal{S}$ generan la K-álgebra $\text{in}_<(A)$.

Proposición 4.2. *Sea $A \subset K[x, y]$ una subálgebra monomial de $K[x, y]$, es decir, generada por monomios, tal que contiene al conjunto de monomios $P = \{xy^i : i \geqslant 0\}$, pero no potencias puras de y. Entonces P es parte de cualquier conjunto mínimo de generadores de A.*

Demostración. Sea G un conjunto mínimo de generadores de A. Procederemos por inducción sobre las potencias i de xy^i para mostrar que $P \subset G$.

Si $i = 0$, claramente $xy^i = x \in G$, pues $x \in A$ y por tanto todo conjunto generador de A debe contener a x, en particular $x \in G$.

Similarmente, si $i = 1$, dado que $xy^i = xy \in A$ y como $y \notin A$, se sigue que xy debe ser un elemento en cualquier conjunto generador de A, en particular en G.

Para el paso inductivo, asumamos que $xy^i \in G$ para $i = 0, \ldots, k$ con $k > 1$. Queremos

[1]Usamos el término Sagbi por las iniciales en inglés de *"Subalgebra analog to Gröbner bases for ideals"*.

ver que $xy^{k+1} \in G$. Supongamos lo contrario, luego considerando el elemento xy^{k+1} en A, tenemos que $xy^{k+1} = xy^k y$, dado que el conjunto mínimo de generadores G contiene a $x, xy, \ldots, xy^k$ y $xy^{k+1} \notin G$, se sigue que $y \in G$, lo cual es una contradicción. Por tanto, $xy^i \in G$ para todo $i \geqslant 0$. En particular, observe que A no es finitamente generada. $\square$

En lo siguiente, asumiremos que A es una K-álgebra finitamente generada. Observe que esto no implica que $\text{in}_<(A)$ es finitamente generada. Para construír un ejemplo de esto, usaremos la proposición 4.2.

Ejemplo 4.2.1. Sean $g_1 = x + y$, $g_2 = xy$ y $g_3 = xy^2$ polinomios en $K[x, y]$ y sea $A = K[g_1, g_2, g_3]$. Considérese un orden monomial $<$ tal que $x > y$. Afirmamos que $\text{in}_<(A)$ no es finitamente generada y para ver esto usando la proposición 4.2 basta ver que los monomios xy^i para todo $i \geqslant 0$ están en $\text{in}_<(A)$. Procederemos por inducción sobre i. De acuerdo al orden monomial $<$, tenemos que $\text{in}_<(g_1) = x$, $\text{in}_<(g_2) = xy$, $\text{in}_<(g_3) = xy^2$. Por tanto, se sigue directamente que para $i = 0, 1, 2$, $xy^i \in \text{in}_<(A)$. Sea ahora $j > 2$y supongamos que $xy^{j-1} \in \text{in}_<(A)$. Luego, $xy^j = g_1(xy^{j-1}) - g_2(xy^{j-2}) \in \text{in}_<(A)$. Por tanto, $xy^i \in \text{in}_<(A)$ para todo $i \geqslant 0$. Así, $\text{in}_<(A)$ no es finitamente generada.

Por otro lado, si $\text{in}_<(A)$ es finitamente generada se sigue que A lo es. Esto es consecuencia del siguiente resultado.

Proposición 4.3. *Si* $\text{in}_<(A) = K[\text{in}_<(f_1), ..., \text{in}_<(f_m)]$ *entonces* $A = K[f_1, ..., f_m]$.

Demostración. Sea $B = K[f_1, ..., f_m]$ y asumamos que $B \neq A$. Sea $f \in A \setminus B$ con el monomio inicial más pequeño. Dado que $\text{in}_<(f) \in \text{in}_<(A)$ existen enteros $a_i \geqslant 0$ y $c \in K$, con $c \neq 0$, tal que $\text{in}_<(f) = c\,\text{in}_<(f_1)^{a_1} \cdots \text{in}_<(f_m)^{a_m}$. Se sigue que $g = f - cf_1^{a_1} \cdots f_m^{a_m} \in A$ con $\text{in}_<(g) < \text{in}_<(f)$. Así concluímos que $g \in B$, pero entonces $f \in B$ también, lo cual es una contradicción. Por lo tanto $A = B$. $\square$

En el caso de que A sea generado por polinomios homogéneos, entonces A hereda una graduación natural de S, donde cada componente homogénea está dada por $A_i = A \cap S_i$ para toda i. En esta situación tenemos el siguiente resultado.

Proposición 4.4. *Sea* $A = K[\text{in}_<(f_1), ..., \text{in}_<(f_m)]$ *una* K*-subálgebra de* S *con la propiedad de que cada* $f_i \in S$ *es un polinomio homogéneo. Entonces:*

$$\text{Hilb}_A(t) = \text{Hilb}_{\text{in}_<(A)}(t).$$

Demostración. Dado un entero i y polinomios homogéneos $g_1, ..., g_r$ con coeficiente principal 1 tal que $\text{in}_<(g_1), ..., \text{in}_<(g_r)$ es una K-base de $\text{in}_<(A)_i$, entonces existe una $c \in K$ tal que ya sea $g - cg_j = 0$ o bien $\text{in}_<(g - cg_j) < \text{in}_<(g)$. En el primer caso habremos terminado; en el segundo caso asumimos por un argumento de inducción que $g - cg_j \in \sum_{k=1}^{r} Kg_k$ por lo que concluímos que $\text{Hilb}_A(t) = \text{Hilb}_{\text{in}_<}(A)(t)$. $\square$

Sean $<$ un orden monomial en S, $f_1, ..., f_m$ polinomios en S con coeficiente principal 1 y $\text{in}_<(f_1), ..., \text{in}_<(f_m)$ sus respectivos monomios iniciales; donde $\text{in}_<(f_j) = \mathbf{x}^{\mathbf{a}_j}$ para cada j. Sea $H = \{\mathbf{h}_1, ..., \mathbf{h}_m\} \subset \mathbb{N}^n$ donde $\mathbf{h}_j = \mathbf{a}_j$, es decir, H es el conjunto de los exponentes de cada monomio inicial $\text{in}_<(f_j)$, $j = 1, ..., m$. H es un semigrupo afín al que le asociamos su anillo de semigrupo que es $K[H] = K[\text{in}_<(f_1), ..., \text{in}_<(f_m)]$.

Por tanto, considerando el anillo de polinomios $R = K[y_1, ..., y_m]$ podemos considerar el morfismo $\psi : R = K[y_1, ..., y_m] \to K[\text{in}_<(f_1), ..., \text{in}_<(f_m)]$ y el núcleo de dicho morfismo que por definición es un ideal tórico, esto es, $J_0 = \ker(\psi)$. Dicho ideal tórico por el lema 3.1 es generado por un conjunto de binomios.

El resultado siguiente nos da una condición necesaria y suficiente para garantizar que $f_1, ..., f_m$ es una base Sagbi de $K[f_1, \ldots, f_m]$ si tenemos ciertas condiciones en los binomios generadores.

Teorema 4.5. *Sean $<$ un orden monomial en S, $f_1, ..., f_m$ polinomios en S con coeficiente principal 1 y $A = K[f_1, ..., f_m]$ la K-subálgebra de S generada por $f_1, ..., f_m$. Sea $\varphi : R = K[y_1, ..., y_m] \to A$ una presentación*[2] *de A con $\varphi(y_i) = f_i$ para $i = 1, ..., m$, $J = \ker(\varphi)$ el ideal de presentación de A. Además, sea $B = K[\text{in}_<(f_1), ..., \text{in}_<(f_m)]$ y $J_0 = \ker(\psi)$ donde $\psi : R = K[y_1, ..., y_m] \to B$ es el morfismo de K-álgebras con $\psi(y_i) = \text{in}_<(f_i)$ para $i = 1, ..., m$.*

Sea $\boldsymbol{y}^{a_1} - \boldsymbol{y}^{b_1}, ..., \boldsymbol{y}^{a_r} - \boldsymbol{y}^{b_r}$ un sistema de binomios generadores del ideal tórico J_0. Entonces $f_1, ..., f_m$ es una base de Sagbi de A si y sólo si las relaciones $\boldsymbol{y}^{a_1} - \boldsymbol{y}^{b_1}, ..., \boldsymbol{y}^{a_r} - \boldsymbol{y}^{b_r}$ pueden levantarse a relaciones de A; esto es para cada j existen elementos $c_a^{(j)} \in K$ tales que:

$$\boldsymbol{f}^{\boldsymbol{a}_j} - \boldsymbol{f}^{\boldsymbol{b}_j} = \sum_{\boldsymbol{a}} c_a^{(j)} \boldsymbol{f}^{\boldsymbol{a}}$$

con $\text{in}_<(\boldsymbol{f}^{\boldsymbol{a}}) < \text{in}_<(\boldsymbol{f}^{\boldsymbol{a}_j})$ para toda $\boldsymbol{a}$, donde $\boldsymbol{f}^{\boldsymbol{a}} = f_1^{a_1} \cdots f_m^{a_m}$, para $\boldsymbol{a} = (a_1, ..., a_m)$. Si las condiciones equivalentes se cumplen, entonces los polinomios:

$$G_j(y_1, ..., y_m) = \boldsymbol{y}^{a_j} - \boldsymbol{y}^{b_j} - \sum_{a} c_a^{(j)} \boldsymbol{y}^{a}, \qquad j = 1, ..., r$$

generan J.

Demostración. Supongamos que el conjunto dado de monomios generadores de J_0 puede ser levantado. Mostramos primero que cualquier otro binomio $\mathbf{y}^{\mathbf{c}} - \mathbf{y}^{\mathbf{d}}$ en J_0 puede ser levantado. Con este fin, le damos a R una estructura de anillo $\mathbb{Z}^n$-graduado poniendo $\text{gr}(y_j) = c_j$ donde $\text{in}_<(f_j) = \mathbf{x}^{c_j}$. Con esta graduación de R, el ideal J_0 es $\mathbb{Z}^n$-graduado. Así, $\mathbf{y}^{\mathbf{c}} - \mathbf{y}^{\mathbf{d}}$ es una K-combinación lineal de binomios de la forma $\mathbf{y}^{\mathbf{g}}(\mathbf{y}^{\mathbf{a}_j} - \mathbf{y}^{\mathbf{b}_j})$ con $\text{gr}\, \mathbf{y}^{\mathbf{c}} = \text{gr}\, \mathbf{y}^{\mathbf{g}} \mathbf{y}^{\mathbf{a}_j}$. Esto implica que $\text{in}_<(\mathbf{f}^{\mathbf{c}}) = \text{in}_<(\mathbf{f}^{\mathbf{g}}) in_<(\mathbf{f}^{\mathbf{a}_j})$. Dado que $\mathbf{y}^{\mathbf{a}_j} - \mathbf{y}^{\mathbf{b}_j}$ puede ser levantado, tenemos:

$$\mathbf{f}^{\mathbf{a}_j} - \mathbf{f}^{\mathbf{b}_j} = \sum_{\mathbf{a}} c_{\mathbf{a}}^{(j)} \mathbf{f}^{\mathbf{a}}$$

[2] Es decir, un epimorfismo de un anillo de polinomios con coeficientes en K sobre A.

con $\mathrm{in}_<(\mathbf{f}^{\mathbf{a}}) < \mathrm{in}_<(\mathbf{f}^{\mathbf{a}_j})$ para toda $\mathbf{a}$.

Se sigue que $\mathbf{y}^{\mathbf{g}}(\mathbf{y}^{\mathbf{a}_j} - \mathbf{y}^{\mathbf{b}_j})$ se puede levantar, ya que:

$$\mathbf{f}^{\mathbf{g}}(\mathbf{f}^{\mathbf{a}_j} - \mathbf{f}^{\mathbf{b}_j}) = \sum_{\mathbf{a}} c_a^{(j)} \mathbf{f}^{\mathbf{g}} \mathbf{f}^{\mathbf{a}}.$$

Ahora, dado que $\mathbf{f}^{\mathbf{c}} - \mathbf{f}^{\mathbf{d}}$ es una K-combinación lineal de elementos de la forma $\mathbf{f}^{\mathbf{g}}(\mathbf{f}^{\mathbf{a}_j} - \mathbf{f}^{\mathbf{b}_j})$ y dado que cada uno de ellos es una combinación lineal de monomios en f_i cuyos monomios iniciales son menores que $in_<(f^c)$ se sigue que $\mathbf{f}^{\mathbf{c}} - \mathbf{f}^{\mathbf{d}}$ pueden ser expresados de la misma forma, en otras palabras $\mathbf{y}^{\mathbf{c}} - \mathbf{y}^{\mathbf{d}}$ se puede levantar.

Ahora, vamos a mostrar que $B = in_<(A)$. Para este fin sea $h \in A$ y no cero. Tenemos que mostrar que $in_<(h) \in B$. Dado que $h \in A$ tenemos que $h = \sum_a d_a \mathbf{f}^{\mathbf{a}}$ con $d_{\mathbf{a}} \in K$. Si $in_<(\mathbf{f}^{\mathbf{a}}) = in_<(h)$ habremos terminado. En otro caso:

$$\max\{\mathrm{in}_<(\mathbf{f}^{\mathbf{a}}) : d_{\mathbf{a}} \neq 0\} > \mathrm{in}_<(h).$$

Sean $\mathbf{a}_1, ..., \mathbf{a}_s$ los exponentes para los cuales $in_<(\mathbf{f}^{\mathbf{a}})$ es máximo. Entonces tenemos $\sum_{i=1}^{s} d_{a_i} = 0$ y así:

$$\sum_{i=1}^{s} d_{a_i} \mathbf{f}^{\mathbf{a}_i} = \sum_{i=2}^{s} d_{a_i} (\mathbf{f}^{\mathbf{a}_i} - \mathbf{f}^{\mathbf{a}_1})$$

Dado que $\mathrm{in}_<(\mathbf{f}^{\mathbf{a}_1}) = \mathrm{in}_<(\mathbf{f}^{\mathbf{a}_i})$, vemos que $\mathbf{y}^{\mathbf{a}_1} - \mathbf{y}^{\mathbf{a}_i} \in J_0$ y dado que todos los binomios en J_0 pueden ser levantados, se sigue que $\sum_{i=1}^{s} d_{a_i} \mathbf{f}^{\mathbf{a}_i}$ puede ser reescrita como una K-combinación lineal L de monomios $\mathbf{f}^{\mathbf{b}}$ en los f_j con:

$$\mathrm{in}_<(\mathbf{f}^{\mathbf{b}}) < \max\{\mathrm{in}_<(\mathbf{f}^{\mathbf{a}}) : d_a \neq 0\}$$

Así, si sustituímos la suma $\sum_{i=1}^{s} d_{a_i} \mathbf{f}^{\mathbf{a}_i}$, la cual es parte de la suma $\sum_a d_a \mathbf{f}^{\mathbf{a}}$ por la combinación lineal L, obtenemos una nueva presentación de $h = \sum_a d'_a \mathbf{f}^{\mathbf{a}}$ con:

$$\max\{\mathrm{in}_<(\mathbf{f}^{\mathbf{a}}) : d'_{\mathbf{a}} \neq 0\} > \mathrm{in}_<(h)\} < \max\{\mathrm{in}_<(\mathbf{f}^{\mathbf{a}}) : d_{\mathbf{a}} \neq 0\} > \mathrm{in}_<(h)\}.$$

Únicamente aplicamos un argumento de inducción para concluír la prueba.

Inversamente, asumimos que $B = \mathrm{in}_<(A)$ y sean $\mathbf{y}^{\mathbf{c}} - \mathbf{y}^{\mathbf{d}} \in J_0$. Dado que $in_<(\mathbf{f}^{\mathbf{c}}) = in_<(\mathbf{f}^{\mathbf{d}})$ se sigue que $\mathrm{in}_<(\mathbf{f}^{\mathbf{c}} - \mathbf{f}^{\mathbf{d}}) < in_<(\mathbf{f}^{\mathbf{c}})$ y con un argumento de inducción como en el anterior caso tenemos que $\mathbf{y}^{\mathbf{c}} - \mathbf{y}^{\mathbf{d}}$ tienen levantamiento.

Finalmente, mostramos que las relaciones $G_j(y_1, ..., y_m)$ generan a J. Para ver esto, sea $H(y_1, ..., y_m) \in J$ con $H(y_1, ..., y_m) = \sum_{\mathbf{a}} c_{\mathbf{a}} y^{\mathbf{a}}$ un elemento arbitrario. Usando el hecho de que $H(f_1, ..., f_m) = 0$ el argumento anteriormente presentado el cual muestra que $B = \mathrm{in}_<(A)$ si el conjunto de generadores dado puede ser levantado, también muestra que módulo las relaciones $G_j(y_1, ..., y_m)$ la suma $\sum_{\mathbf{a}} c_{\mathbf{a}} y^{\mathbf{a}}$ puede ser reescrita como $\sum_{\mathbf{a}} c'_{\mathbf{a}} y^{\mathbf{a}}$ tal que:

$$\max\{\mathrm{in}_<(\mathbf{f}^{\mathbf{a}}) : c'_{\mathbf{a}} \neq 0\} > \mathrm{in}_<(h)\} < \max\{in_<(\mathbf{f}^{\mathbf{a}}) : c_{\mathbf{a}} \neq 0\} > \mathrm{in}_<(h)\}$$

Así, por inducción se sigue la conclusión deseada. $\square$

4.1. Anillos de Hibi

Recordemos que una relación $\leqslant$ sobre un conjunto P es un orden parcial si es *reflexiva*, *antisimétrica* y *transitiva* . Decimos así que la pareja $(\mathsf{P}, \leqslant)$ es un conjunto parcialmente ordenado o *copo*.

Sea $(\mathsf{P}, \leqslant)$ un conjunto parcialmente ordenado y sea $\mathsf{H} \subseteq \mathsf{P}$, entonces a es una cota superior de H si $h \leqslant a$ para todo $h \in \mathsf{H}$. Una cota superior a de H es el *supremo* de H si es la mínima cota superior de H, esto es, para cualquier cota superior b de H se tiene que $a \leqslant b$. Denotamos al supremo de H por $\sup \mathsf{H}$ o $\vee \mathsf{H}$. De manera análoga definimos cota inferior e *ínfimo* , es decir, la máxima cota inferior, la cual denotamos por $\text{ínf}\, \mathsf{H}$ o bien $\wedge \mathsf{H}$. Tanto la notación de *supremo* como de *ínfimo* están justificadas por la unicidad de estos elementos que se verifica fácilmente.

Un conjunto parcialmente ordenado $(\mathsf{L}, \leqslant)$ es una *retícula* si $\sup\{a, b\}$ y $\text{ínf}\{a, b\}$ existen para cualesquiera $a, b \in \mathsf{L}$. Usaremos la siguiente notación para sup e ínf:

$$a \vee b = \sup\{a, b\}$$

$$a \wedge b = \text{ínf}\{a, b\}$$

y diremos que $\wedge$ y $\vee$ son el *ínfimo* y el *supremo* respectivamente.

Usando un argumento de inducción y las propiedades del orden parcial se verifica fácilmente que un conjunto parcialmente ordenado $(\mathsf{L}, \leqslant)$ es una retícula si $\sup \mathsf{H}$ y $\text{ínf}\, \mathsf{H}$ existen para cualquier conjunto finito H no vacío en L.

Definición 4.6 (Retícula distributiva)**.** Una retícula $(\mathsf{L}, \vee, \wedge)$ es una retícula distributiva si se cumple la siguiente igualdad para cualesquiera $a, b, c \in \mathsf{L}$: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Ejemplo 4.6.1. Sea $\mathsf{P} = \{p_1, \ldots, p_n\}$ un *copo* finito. Un *ideal copo* I de P es un subconjunto de P que satisface que para todo $p \in I$, si $q \in \mathsf{P}$ y $q \leqslant p$ entonces $q \in I$. Consideremos el conjunto de todos los ideales copo de P al que denotaremos por $\mathcal{I}(\mathsf{P})$. Se verifica fácilmente que $\mathcal{I}(\mathsf{P})$ es una subretícula del conjunto potencia de P, por lo que es una retícula distributiva, considerando las operaciones $\vee$ y $\wedge$ como la unión e intersección respectivamente y dado que éstas operaciones son distributivas en el conjunto potencia de P se sigue que $\mathcal{I}(\mathsf{P})$ es una retícula distributiva.

Ejemplo 4.6.2. Dado $n \in \mathbb{N}$ y el conjunto $\mathsf{P} = [n] = \{1, \ldots, n\}$ con el orden usual. Luego, $\mathcal{I}(\mathsf{P})$ está formado por $\emptyset$, $[n]$ y $[k]$ para $k = 1, \ldots, n-1$. por lo que tendríamos $n+1$ ideales en $\mathcal{I}(\mathsf{P})$. Dado que para cualesquiera par de ideales $I = [k]$, $J = [\ell]$ en $\mathcal{I}(\mathsf{P})$ tenemos que $I \subset J$ o bien $J \subset I$ se sigue que: $I \wedge J = [\text{mín}\{k, \ell\}]$ e $I \vee J = [\text{máx}\{k, \ell\}]$. $\mathcal{I}([n])$ nos ilustra el ejemplo típico de una retícula distributiva.

Un elemento δ en una retícula distributiva es llamado *unión irreducible* si es diferente del único elemento más pequeño en la retícula y no puede ser escrito como unión de dos elementos de la retícula propiamente más pequeños que δ, es decir, siempre que $\delta = a \vee b$ se tiene que $\delta = a$ o $\delta = b$. Un *isomorfismo* de retículas L y L' es una función biyectiva $\varphi : \mathsf{L} \to \mathsf{L}'$ que preserva el orden.

Teorema 4.7 (Teorema de representación de Birkhoff)**.** *Sea* L *una retícula distributiva finita y* P *el conjunto de elementos unión irreducibles de* L*, entonces* P *es un conjunto parcialmente ordenado y* L *es isomorfa a* $\mathcal{I}(\mathsf{P})$*.*

Demostración. Si $x \in \mathsf{L}$, sea $I_x = \{a \in \mathsf{P} : a \leqslant x\}$. Claramente I_x es un ideal de P, es decir, $I_x \in \mathcal{I}(\mathsf{P})$. También, si $x \leqslant x'$ en L, entonces $I_x \subseteq I_{x'}$ en $\mathcal{I}(\mathsf{P})$ y así la función $\varphi : \mathsf{L} \to \mathcal{I}(\mathsf{P})$ dada por $\varphi(x) = I_x$ preserva el orden. Para ver que φ es biyectiva, sea $\psi : \mathcal{I}(\mathsf{P}) \to \mathsf{L}$ la función que a cada ideal $I = \{x_1, \ldots, x_k\} \in \mathcal{I}(\mathsf{P})$ le asocia el elemento $x = x_1 \vee \cdots \vee x_k \in \mathsf{L}$. La función ψ preserva el orden porque si $I \subseteq J$ en $\mathcal{I}(\mathsf{P})$ e $I = \{x_1, \ldots, x_k\}$ y $J = \{x_1, \ldots, x_k, \ldots, x_\ell\}$, entonces $x_1 \vee \cdots \vee x_k \leqslant x_1 \vee \cdots \vee x_k \vee \cdots \vee x_\ell$. Ahora, si $x \in \mathsf{L}$, $\varphi(x) = I_x = \{x_1, \ldots, x_k\}$ y $z = \psi(I_x) = x_1 \vee \cdots \vee x_k$, como $x_i \leqslant x$ entonces $z = x_1 \vee \cdots \vee x_k \leqslant x$. Para la otra desigualdad, suponga primero que x es unión-irreducible; entonces, $x \in I_x$ y por lo tanto $x \leqslant z$. Suponga ahora que x no es unión-irreducible; entonces se puede escribir como $x = y_1 \vee \cdots \vee y_t$ con los y_i unión irreducibles. Así, $y_i \leqslant x$ por lo que $y_i \in I_x$ y por lo tanto $y_i \leqslant z$, de donde se sigue que $x = y_1 \vee \cdots \vee y_t \leqslant z$. Se tienen así las desigualdades $x \leqslant z$ y $z \leqslant x$ y por lo tanto la composición $\psi \circ \varphi = \mathrm{id}$ y como L y $\mathcal{I}(\mathsf{P})$ son finitos, se sigue que φ y ψ son biyectivas. □

Sea L una retícula distributiva finita y K campo. Definimos el *álgebra libre generada por* L de la siguiente manera: Sea $a \in \mathsf{L}$ y considerando una copia $\mathsf{K}a$ del campo K definimos el *álgebra libre generada por* L como:

$$[\mathsf{L}] = \bigoplus_{a \in \mathsf{L}} \mathsf{K}a$$

Obsérvese que $\mathsf{L} \hookrightarrow [\mathsf{L}]$ pues podemos definir una función $\varphi : \mathsf{L} \to [\mathsf{L}]$ dada por $\varphi(a) = 1a$. Consideremos el conjunto $\mathsf{G} = \{ab - (a \vee b)(a \wedge b) : a, b \in \mathsf{L}\}$ de $[\mathsf{L}]$ y tomemos I como el ideal generado por G, entonces definimos el *anillo de Hibi*, denotado por $\mathsf{K}[\mathsf{L}]$ como:

$$\mathsf{K}[\mathsf{L}] = [\mathsf{L}] \big/ I.$$

Otra manera de ver lo anterior es considerar una indeterminada x_a para cada $a \in \mathsf{L}$ y el anillo de polinomios $\mathsf{K}[x_a : a \in \mathsf{L}]$. Entonces, el ideal $I \subseteq \mathsf{K}[x_a : a \in \mathsf{L}]$ generado por los binomios $x_a x_b - x_{a \vee b} x_{a \wedge b}$ (relaciones de Hibi). Entonces, el anillo de Hibi es el cociente:

$$\mathsf{K}[x_a : a \in \mathsf{L}] / \langle x_a x_b - x_{a \vee b} x_{a \wedge b} \rangle. \tag{4.1}$$

Ejemplo 4.7.1. En el ejemplo 4.6.2, para la retícula distributiva $\mathsf{L} = \mathcal{I}([n])$ con $n + 1$ elementos. Queremos construír el anillo de Hibi de dicha retícula. Obsérvese que en $[\mathcal{I}([n])]$ tenemos $n + 1$ elementos generadores, los cuales podemos enumerar de la siguiente manera:

$$\emptyset \mapsto 1$$

$$[1] \mapsto x_1$$

$$[2] \mapsto x_2$$
$$\vdots$$
$$[n] \mapsto x_n$$

Sean J_1, J_2 ideales de L, como ya se ha observado se tiene que $J_1 \subset J_2$ o $J_2 \subset J_1$, entonces $J_1 J_2 - (J_1 \vee J_2)(J_1 \wedge J_2) = 0$ por lo que el ideal I generado por las relaciones $J_1 J_2 - (J_1 \vee J_2)(J_1 \wedge J_2)$ para J_1, J_2 ideales de L es el ideal 0. Así, el anillo de Hibi $K[\mathcal{J}[n]] = [\mathcal{J}([n])]/I = [\mathcal{J}([n])]$ que hemos visto que tiene por generadores a los elementos $1, x_1, x_2, \ldots, x_n$, es $\mathcal{J}([n]) = K[x_1, \ldots, x_n]$.

En general, sea $P = \{p_1, \ldots, p_n\}$ un *copo* finito. Consideremos $\mathcal{J}(P)$ la retícula de ideales. Para cada ideal I en $\mathcal{J}(P)$ consideramos una variable x_I y el anillo de polinomios sobre K en dichas variables, esto es: $T = K[x_I : I \in \mathcal{J}(P)]$. Obsérvese que se tiene así un anillo de polinomios en un número finito de variables, dado que hay un número finito de variables. Para cada $p_i \in P$ elegimos una variable x_{p_i}, a fin de simplificar la notación sea $x_i := x_{p_i}$ e introducimos una nueva variable s para así poder considerar el anillo de polinomios $S = K[x_1, \ldots, x_n, s]$.

Sea $I \in \mathcal{J}(P)$. Para cada $p_i \in I$ tenemos una variable x_I, luego sea $x_I = \prod_{p_i \in I} x_i$, así podemos considerar el siguiente conjunto de monomios $\{s x_I : I \in \mathcal{J}(P)\}$. Dicho conjunto es un conjunto generador de un submonoide $M \subseteq S$ con el producto usual en S y cuyos exponentes (que son $(n+1)$-adas de enteros no negativos) a los que denotamos por $\mathbf{h}$ generan un cono en una retícula Γ en $\mathbb{Z}^{n+1}$. Note hay tantos vectores $\mathbf{h}$ como ideales $I \in \mathcal{J}(P)$. Como en la sección 3.1 considere el anillo de semigrupo $K[M]$ y el morfismo suprayectivo $\varphi : T \to K[M]$ dado por $x_I \mapsto s x_I$. Por la sección 3.1, $\ker(\varphi)$ es un ideal tórico al que denotamos por P_M. Por otra parte, en $K[M]$ sea I el ideal generado por las relaciones de Hibi y considere el cociente $K[M]/I$ que es el anillo de Hibi $K[\mathcal{J}(P)]$. Entonces, la composición $T \to K[M] \to K[M]/I = K[\mathcal{J}(P)]$ es suprayectiva con el mismo núcleo P_M por lo que $K[\mathcal{J}(P)] \simeq T/P_M$. Al ser $K[\mathcal{J}(P)]$ un anillo de polinomios módulo un ideal tórico, se dice que $K[\mathcal{J}(P)]$ es un anillo tórico.

4.2. El anillo de coordenadas de la variedad Grassmanniana

Consideremos un K-espacio vectorial de dimensión finita V, digamos n. Podemos generalizar las ideas con las que construímos el espacio proyectivo $\mathbb{P}^n$ y ver el espacio proyectivo $\mathbb{P}(V)$ como el conjunto de todas las *rectas* en V que pasan por el origen, esto es, los subespacios vectoriales de dimensión 1. Si en lugar de tomar únicamente los subespacios de dimensión 1 consideramos los subespacios de dimensión, digamos $m \leqslant n$, podemos tomar el siguiente conjunto:

$$G(m, V) = \{W \subseteq V : W \text{ es subespacio de dimensión } m \text{ de } V\}.$$

Recuerde ahora que la *potencia tensorial* m-ésima de V es el espacio vectorial:

$$T^m V = V \otimes_K \cdots \otimes_K V$$

con m factores. Consideremos ahora, el subespacio $M \subseteq T^m V$ generado por los tensores de la forma $u_1 \otimes \cdots \otimes u_m \in T^m V$ con $u_i = u_j$ para algún par $i \neq j$. Podemos así, formar el K- espacio vectorial cociente $T^m V \diagup M$ al que denotamos por $\wedge^m V$ y llamamos m-*ésima potencia exterior*. Si $v_1 \otimes \cdots \otimes v_m \in T^m V$ usaremos la siguiente notación:

$$v_1 \wedge \cdots \wedge v_m = v_1 \otimes \cdots \otimes v_m + M \in \wedge^m V$$

Todo elemento de $\wedge^m V$ es una combinación lineal finita de elementos $v_1 \wedge \cdots \wedge v_m$ a los que llamamos *tensores alternantes*.

Lema 4.8. *Usando la notación previa tenemos que:*

(1) *Si en* $v = v_1 \wedge \cdots \wedge v_m$ *hay dos factores repetidos tenemos que* $v = 0$

(2) $v_1 \wedge \cdots \wedge v_m = 0$ *si y sólo si* $v_1, \ldots, v_m$ *son linealmente dependientes.*

(3) *Si* $\sigma \in S_m$*, el grupo simétrico en* m *letras, entonces*

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(m)} = \operatorname{sgn}(\sigma) v_1 \wedge \cdots \wedge v_m.$$

(4) $\dim(\wedge^m V) = \binom{n}{m}$ *con base dada por los elementos de la forma* $e_{i_1} \wedge \cdots \wedge e_{i_m}$ *para* $1 \leqslant i_1 < i_2 < \cdots i_m \leqslant n$*, donde* $e_1, \ldots, e_n$ *es una base del espacio vectorial* V.

Demostración. (1) Es inmediato de la definición de producto $\wedge$, pues si hay factores repetidos en $v_1 \wedge \cdots \wedge v_m$, tenemos que $v_1 \otimes \cdots \otimes v_m \in M$ y por tanto $v = 0$.

(2) Supongamos que $v_1, \ldots, v_m$ son linealmente dependientes, entonces podemos expresar algún v_i como combinación lineal de los demás elementos. Sin perder generalidad, supongamos que: $v_m = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{m-1} v_{m-1}$. Luego, sustituyendo v_m y desarrollando el producto $\wedge$, tenemos:

$$v_1 \wedge \cdots \wedge v_{m-1} \wedge v_m = \alpha_1 (v_1 \wedge \cdots \wedge v_{m-1} \wedge v_1) + \cdots + \alpha_{m-1} (v_1 \wedge \cdots \wedge v_{m-1} \wedge v_{m-1}).$$

Dado que en cada uno de los $m-1$ términos del lado derecho hay elementos v_j repetidos, tenemos por (1) que $v_1 \wedge \cdots \wedge v_m = 0$.

Para la otra implicación, por contrapositiva supongamos que $v_1, \ldots, v_m$ son linealmente independientes, queremos ver que $v_1 \wedge \cdots \wedge v_m \neq 0$. Procedamos por contradicción y supongamos que $v_1 \wedge \cdots \wedge v_m = 0$, entonces por definición $v_1 \otimes \cdots \otimes v_m \in M$ y por tanto para algún par i, j, $i \neq j$ en $\{1, \ldots, d\}$ se tiene que $v_i = v_j$, lo que contradice el hecho de que $v_1, \ldots, v_m$ son linealmente independientes.

(3) Procederemos por inducción sobre el número de transposiciones en que se descompone σ. Observe que si $m = 2$ se tiene:

$$0 = (v_1 + v_2) \wedge (v_1 + v_2) = v_1 \wedge v_1 + v_1 \wedge v_2 + v_2 \wedge v_1 + v_2 \wedge v_2$$

por lo que $v_2 \wedge v_1 = -v_1 \wedge v_2$. De este hecho se sigue que si σ es una transposición se cumple la condición.

Para el paso inductivo sea σ permutación (que no es una transposición), tenemos entonces que podemos expresar a σ como producto de transposiciones. Supongamos que la propiedad se cumple para cualquier permutación que se expresa como producto de k transposiciones, donde k es menor que el número de transposiciones en que se descompone σ.

Sean $v_1, \ldots, v_m \in \wedge^m V$ y sea $\sigma \in S_m$, luego podemos expresar a σ como $\sigma = \mu\tau$ donde μ es una transposición y τ es un producto de transposiciones (menos que el número de transposiciones en los que se descompone σ), luego:

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(m)} = v_{\mu\tau(1)} \wedge \cdots \wedge v_{\mu\tau(m)} = -v_{\tau(1)} \wedge \cdots \wedge v_{\tau(m)},$$

donde esta última igualdad se cumple dado que μ es una transposición y genera un cambio de signo en el producto.

Luego, usando la base de inducción se tiene:

$$-v_{\tau(1)} \wedge \cdots \wedge v_{\tau(m)} = -\operatorname{sgn}(\tau) v_1 \wedge \cdots \wedge v_m$$

y como $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\mu)\operatorname{sgn}(\tau) = -\operatorname{sgn}(\tau)$, concluímos que:

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(m)} = \operatorname{sgn}(\sigma) v_1 \wedge \cdots \wedge v_m.$$

(4) Sea $\{e_1, \ldots, e_n\}$ una base de V. Primeramente tenemos que cualquier tensor $v \in \wedge^m V$ es combinación lineal finita de expresiones de la forma $v_1 \wedge \cdots \wedge v_m$ y dado que cada vector $v_1, \ldots, v_d$ puede expresarse en términos de la base $\{e_1, \ldots, e_n\}$, usando las propiedades básicas del producto $\wedge$ podemos expresar a v como combinación lineal de elementos $e_{i_1} \wedge \cdots \wedge e_{i_m}$ para $1 \leqslant i_1 < i_2 < \cdots i_m \leqslant n$, una vez que éstos son ordenados. Observe por otro lado que el conjunto:

$$\{e_{i_1} \wedge \cdots \wedge e_{i_m} : 1 \leqslant i_1 < i_2 < \cdots i_m \leqslant n\}$$

tiene $\binom{n}{m}$ y por la parte (1) y (2) del lema es linealmente independiente. Así, se tiene que $\{e_{i_1} \wedge \cdots \wedge e_{i_m} : 1 \leqslant i_1 < i_2 < \cdots i_m \leqslant n\}$ es una base de $\wedge^m V$ y por tanto $\dim(\wedge^m V) = \binom{n}{m}$. $\square$

La inmersión de Plücker

Consideremos ahora la siguiente función:

$$\varphi : \mathsf{G}(m, V) \to \mathbb{P}(\wedge^m V)$$

que está dada de la siguiente manera: consideremos un subespacio vectorial W de dimensión m con $\mathcal{B} = \{w_1, \dots, w_m\}$ una base y tomemos el elemento $0 \neq w_1 \wedge \cdots \wedge w_m \in \wedge^m V$. Queremos ver que el punto $[w_1 \wedge \cdots \wedge w_m] \in \mathbb{P}(\wedge^d V)$ no depende de la base elegida sino solo del subespacio W. Para ver esto, tomemos otra base $\mathcal{B}' = \{w'_1, \dots, w'_m\}$ y veamos que los elementos $w_1 \wedge \cdots \wedge w_m$ y $w'_1 \wedge \cdots \wedge w'_m$ sólo difieren por el determinante δ de la matriz de cambio de base de W, esto es, por un escalar no cero $\delta \in K^*$. Entonces, el punto $[W] \in \mathbb{P}(\wedge^m V)$ que corresponde al punto $w_1 \wedge \cdots \wedge w_m$ está unívocamente determinado por el subespacio W y no depende de la elección de la base de W. Así, tenemos la función definida por $\varphi(W) = [W]$.

Proposición 4.9. $\varphi : \mathsf{G}(m, V) \to \mathbb{P}(\wedge^m V)$ *es inyectiva.*

Demostración. Para ver que φ es inyectiva veamos que tiene inversa por la izquierda. Sea $\rho : \mathbb{P}(\wedge^m V) \to \mathsf{G}(m, V)$ dada por $\rho([\omega]) = \{v \in V : v \wedge \omega = 0 \in \wedge^{m+1} V\}$. Queremos ver que $\rho \circ \varphi = \mathrm{id}$.

Sea $W \in \mathsf{G}(m, V)$ con base $\mathcal{B} = \{w_1, \dots, w_m\}$, de modo que $[w_1 \wedge \cdots \wedge w_m] = \varphi(W)$. Dado que para cualquier $w \in W$ el conjunto $\{w, w_1, \dots, w_m\}$ es linealmente dependiente, por el lema 4.8 se tiene que $w \wedge w_1 \wedge \cdots \wedge w_m = 0$, así $W \subseteq \rho \circ \varphi(W)$.

Por otro lado, si $v \in \rho \circ \varphi(W)$ entonces $v \wedge w_1 \wedge \cdots \wedge w_m = 0$. Luego, extendemos el conjunto linealmente independiente $\{w_1, \dots, w_m\}$ a una base $\mathcal{B} = \{w_1, \dots, w_m, w_{m+1}, \dots, w_n\}$ de V y así, podemos escribir a v como

$$v = \sum_{i=1}^{n} a_i w_i$$

Por lo tanto, tenemos:

$$\left(\sum_{i=1}^{n} a_i w_i \right) \wedge w_1 \wedge \cdots \wedge w_m = 0$$

con $a_i \in K$. Distribuímos usando las propiedades del producto $\wedge$. Luego, $a_i = 0$ para todo $i > m$; entonces: $v = a_1 w_1 + \cdots + a_d w_m$, es decir, $v \in W$. Así, $\rho \circ \varphi(W) \subset W$. De todo lo anterior tenemos que $\rho \circ \varphi(W) = W$, esto es, $\rho \circ \varphi = \mathrm{id}$. Por lo tanto, φ es inyectiva. $\square$

La función φ de la proposición anterior es conocida como *la inmersión de Plucker* y nos permite ver a la Grassmanniana $\mathsf{G}(m, V)$ como un subconjunto del espacio proyectivo $\mathbb{P}(\wedge^m V)$.

Lema 4.10. *Sea* $w \in \wedge^m V$ *y considere la función lineal* $\varphi_w : V \to \wedge^{m+1} V$ *dada por* $\varphi_w(v) = w \wedge v$. *Entonces:* $0 \neq w \in \wedge^m V$ *es descomponible si y sólo si* $\dim_K(\ker \varphi_w) \geqslant m$.

Demostración. Supongamos que $0 \neq w \in \wedge^m V$ es descomponible. Entonces tenemos que $w = w_1 \wedge \cdots \wedge w_m$ con $w_i \in V$. Por el lema 4.8 tenemos que $w_1, \ldots, w_m$ son linealmente independientes. Además, $0 = w \wedge w = w \wedge w_1 \wedge \cdots \wedge w_m$, por lo que tenemos que $w_1, \ldots, w_m$ forman parte de una base del núcleo de φ_w, entonces $\dim_K(\ker \varphi_w) \geqslant m$.

Por otro lado, supongamos que $\dim_K(\ker \varphi_w) \geqslant m$. Sea $\{v_1, \ldots, v_s\}$ una base de $\ker \varphi_w$ y completémosla a una base de V, digamos $\{v_1, \ldots, v_s, v_{s+1}, \ldots, v_n\}$, asumiendo que $\dim V = n$. Luego, al tener ya una base de V se sigue que podemos escribir a w en términos de una base de $\wedge^m V$:

$$w = \sum_{1 \leqslant i_1 < \cdots < i_m \leqslant m} a_{i_1 \cdots i_m} v_{i_1} \wedge \cdots \wedge v_{i_m}.$$

Dado que:

$$\varphi_w(v_i) = \left(\sum_{1 \leqslant i_1 < \cdots < i_m \leqslant m} a_{i_1 \cdots i_m} v_{i_1} \wedge \cdots \wedge v_{i_m} \right) \wedge v_i = 0$$

para $i \in \{1, \ldots, s\}$, pues $v_1, \ldots, v_s \in \ker(\varphi_w)$, se sigue que $\{1, \ldots, s\} \subseteq \{i_1, \ldots, i_m\}$ cuando $a_{i_1 \cdots i_m} \neq 0$, por lo que $s \leqslant m$, pero dada la suposición de que $\dim_K(\ker \varphi_w) \geqslant m$, tenemos que $s = m$. Por tanto, podemos escribir a w como $w = \alpha v_1 \wedge \cdots \wedge v_m$ con $\alpha \in K$. Por tanto, w es descomponible. $\square$

Observación 4.11. Por el teorema de la dimensión y de acuerdo al lema 4.10 tenemos que $0 \neq w \in \wedge^m V$ es descomponible si y sólo si $\operatorname{rang}(\varphi_w) \leqslant n - m$.

Hemos visto que bajo la inmersión de Plucker podemos ver a la Grasmaniana dentro del espacio proyectivo, veremos que de hecho, su imagen es una variedad proyectiva.

Teorema 4.12. $\varphi(G(m, V)) \subseteq \mathbb{P}(\wedge^m V)$ *es una variedad proyectiva.*

Demostración. Probaremos que $\varphi(G(m, V))$ es cerrada en $\mathbb{P}(\wedge^m V)$. Para ver esto consideremos la función $\Phi : \wedge^m V \to \operatorname{Hom}_K(V, \wedge^{m+1} V)$ dada por $\Phi(w) = \varphi_w$ que claramente es lineal. Por tanto, las entradas de la matriz asociada $[\varphi_w]$ son coordenadas homogéneas en $\mathbb{P}(\wedge^m V)$ y $\varphi(G(m, V))$ es la subvariedad de $\mathbb{P}(\wedge^m V)$ definida por la anulación de los menores de tamaño $> n - m$ de dicha matriz. Por lo tanto, la imagen de la inmersión de Plucker es cerrada en $\mathbb{P}(\wedge^m V)$. $\square$

4.2.1. Las relaciones de Plücker

Otra manera de ver la inmersión de Plücker es la siguiente: escojamos una base $e_1, \ldots e_n$ de V. Entonces, los vectores de la forma $e_{i_1} \wedge \cdots \wedge e_{i_m}$ con $1 \leqslant i_1 < \cdots < i_m \leqslant n$ forman una base de $\wedge^m V$ y así, todo $0 \neq w \in \wedge^m V$ se puede escribir de forma única de la siguiente manera:

$$w = \sum_{i_1 < \cdots < i_m} p_{i_1 \cdots i_m} e_{i_1} \wedge \cdots \wedge e_{i_m}$$

donde los coeficientes $p_{i_1\cdots i_m}$ no son todos cero, pues $w \neq 0$. Se dice que éstas son las *coordenadas de Plucker* del punto $[w] \in \mathbb{P}(\wedge^m V)$.

Podemos ahora describir la inmersión de Plucker $\varphi : G(m, V) \to \mathbb{P}(\wedge^m V)$ escogiendo una base $w_1, \ldots, w_m$ de $W \in G(d, V)$ y escribimos cada w_i en términos de la base y $e_1, \ldots, e_n$ de V:

$$\begin{aligned} w_1 &= x_{11}e_1 + \cdots + x_{1n}e_n \\ w_2 &= x_{21}e_1 + \cdots + x_{2n}e_n \\ &\vdots \\ w_m &= x_{m1}e_1 + \cdots + x_{mn}e_n \end{aligned} \tag{4.2}$$

Entonces tenemos $\varphi(W) = [w_1 \wedge \cdots \wedge w_m] = [(x_{11}e_1 + \cdots + x_{1n}e_n) \wedge \cdots \wedge (x_{m1}e_1 + \cdots + x_{mn}e_n)]$. Al desarrollar en el lado derecho, tenemos que sólo quedan los términos de la forma $e_{i_1} \wedge \cdots \wedge e_{i_m}$ con índices diferentes, donde cada e_{i_j} se puede elegir en cualquiera de las m expresiones entre los paréntesis del lado derecho. Consideremos el grupo simétrico S_m y una permutación $\sigma \in S_m$ de los m índices. Podemos suponer que $i_1 < \cdots < i_m$ mediante dicha permutación, afectando al sumando con $e_{i_1} \wedge \cdots \wedge e_{i_m}$ por el factor $\operatorname{sgn}(\sigma)$. En cada sumando $e_{i_1} \wedge \cdots \wedge e_{i_m}$ se pueden escoger los coeficientes de e_{i_1} en cada uno de los paréntesis del lado derecho para la expresión de $\varphi(W)$ como $x_{1i_1}, \ldots, x_{mi_1}$. Similarmente para e_{i_2} sus coeficientes pueden ser $x_{1i_2}, \ldots, x_{mi_2}$ y lo mismo para los otros vectores e_{i_j}. Tomando en cuenta el reordenamiento $i_1 < \cdots < i_m$ mediante la permutación σ, cada una de las elecciones de los factores de $e_{i_1} \wedge \cdots \wedge e_{i_m}$ aporta el coeficiente $x_{\sigma(i_1)i_1} \cdots x_{\sigma(i_m)i_m}$ y al final se suma sobre todas las elecciones $\sigma \in S_m$. Denote por $I_m[n]$ al conjunto de $(i_1, \ldots, i_m)$ con $1 \leqslant i_j \leqslant n$ y diferentes dos a dos. Luego, se sigue que:

$$\varphi(W) = \sum_{\substack{\underline{i}=(i_1,\ldots,i_m)\in I_d[n] \\ \sigma\in S_d}} \left(\operatorname{sgn}(\sigma)(x_{\sigma(i_1)i_1} \cdots x_{\sigma(i_m)i_m})\right) e_{i_1} \wedge \cdots \wedge e_{i_m} \tag{4.3}$$

donde las sumas internas, que son las coordenadas de Plucker, son determinantes de submatrices cuadradas de de la matriz $X = (x_{ij})$ de tamaño $m \times n$ formada por los coeficientes (4.2) que expresan los w_i en términos de los e_j:

$$X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & & & \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix} \tag{4.4}$$

y estas submatrices de tamaño $m \times m$ denotadas $X_{\underline{i}}$ escogen m columnas de X usando la m-ada ordenada $\underline{i} = (i_1, \ldots, i_m)$. Las coordenadas de Plucker de W son los menores

$$p_{\underline{i}} = p_{i_1,\ldots,i_m} = \det X_{\underline{i}} \tag{4.5}$$

Observe que un cambio de base sólo cambia estas coordenadas por un factor no cero, que sería el determinante de la matriz de cambio de base. La inmersión de Plucker es el morfismo dado para $W \in \mathsf{G}(m, V)$ mediante:

$$\varphi(W) = [\ldots, p_{\underline{i}}, \ldots] \in \mathbb{P}(\wedge^m V)$$

variando $\underline{i} = (i_1, \ldots, i_m) \in I_m[n]$, donde $I_m[n] = \{\underline{i} = (i_1, \ldots, i_m) : 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n\}$ es un conjunto de índices para los básicos de $\wedge^m V$. El resultado principal determina los puntos de $\mathbb{P}(\wedge^m V)$ que pertenecen a la variedad de Grassmann $\mathsf{G}(m, V)$. A fin de probar este resultado considérese primeramente la siguiente observación:

Observación 4.13. Podemos considerar un caso particular del lema 3.10 para $t = 1$, esto es, intercambiando sólo un elemento arbitrario del menor $[j_1 \cdots j_m]$, digamos j_h, con el elemento i_m del menor $[i_1 \cdots i_m]$. Para ello, primeramente consideramos la permutación σ que cambia elemento j_h con j_{h-1} y así sucesivamente hasta tener j_h en la primera posición, por lo que $\operatorname{sgn}(\sigma) = (-1)^h$ y así las relaciones de Plucker son de la siguiente manera:

$$\sum_{h=1}^{m} (-1)^h [i_1 \cdots i_{m-1} j_h][j_1 \cdots j_{h-1} i_m j_{h+1} \cdots j_m] = 0 \tag{4.6}$$

O bien, podemos escribirlas como:

$$\sum_{h=1}^{m+1} (-1)^h [i_1 \cdots i_{m-1} j_h][j_1 \cdots \hat{j_h} \cdots j_m j_{m+1}] = 0 \tag{4.7}$$

donde $i_1, \ldots, i_{m-1}, j_1, \ldots, j_{m+1}$ están en $\{1, \ldots, n\}$ y la acción de quitar el elemento j_h del menor $[j_1 \cdots j_h \cdots j_m j_{m+1}]$ lo denotamos por $\hat{j_h}$.

Teorema 4.14 (Relaciones de Plücker)**.** *Sean* V *un espacio vectorial de dimensión* n *y* $1 \leqslant m \leqslant n$ *un entero. Un punto* $[W] \in \mathsf{G}(m, V)$ *si y sólo si satisface las relaciones de Plücker del lema* 3.10*:*

$$\sum_{\overline{\sigma} \in S/S'} \operatorname{sgn}(\sigma)[i_1, \ldots, i_{s-1}, \sigma(i_s), \ldots, \sigma(i_m)][\sigma(j_1), \ldots, \sigma(j_s), j_{s+1}, \ldots, j_m] = 0.$$

Demostración. Primeramente, sea $[W] \in \mathsf{G}(m, V)$. Hemos señalado anteriormente que $[W]$ es visto en $\mathbb{P}(\wedge^m V)$ como un vector coordenado en $\binom{n}{m}$ coordenadas de Plucker, esto es, se tiene que $\varphi(W) = [W] = [\ldots, p_{\underline{i}}, \ldots]$, donde $p_{\underline{i}}$ son menores de tamaño m variando $\underline{i} = (i_1, \ldots, i_m) \in I_m[n]$. De acuerdo al lema 3.10 tenemos que los menores de rango máximo m satisfacen dichas relaciones, por lo que las coordenadas de $[W]$ las satisfacen.

Inversamente, queremos ver que todo punto que satisface las *relaciones de Plucker* proviene de un elemento de $\mathsf{G}(m, V)$.

Sea $q = [\ldots, q_{\underline{i}}, \ldots]$ en $\mathbb{P}(\wedge^m V)$ que satisface las *relaciones de Plucker*, entonces $q_{\underline{s}} \neq 0$ para algún $\underline{s}$ en $I_m[n]$. Dado que estamos considerando coordenadas homogéneas, podemos asumir que $q_{\underline{s}} = 1$. Definimos la matriz A de $m \times n$ como $A = (a_{ik}) = q_{s_1,\ldots,s_{k-1},i,s_k,\ldots s_m}$, observe que la matriz que resulta de elegir las $s_1, \ldots, s_m$ columnas de A, denotada por $A_{\underline{s}}$, resulta ser la matriz identidad de $m \times m$, pues por definición si $i = k$, tenemos $a_{ik} = 1$ y cero en otro caso. Así, A tiene rango m y representa un subespacio U en $G(m, V)$. Queremos ver que $\varphi(U) = q$, o bien, en términos de coordenadas: $\varphi_{\underline{j}}(A) = q_{\underline{j}}$ para todo $\underline{j} \in I_m[n]$, donde $\varphi_{\underline{j}}(A)$ es la $\underline{j}$-ésima coordenada de Plucker. Probaremos esto en base a la cardinalidad de $\underline{j} \cap \underline{s}$ y de forma descendente. Por tanto, comenzamos en el supuesto de que $\underline{j} = \underline{s}$, entonces $\varphi_{\underline{j}}(A) = \det(A_{\underline{s}}) = 1 = q_{\underline{s}}$. Si $\underline{j} = (s_1, \ldots, s_{k-1}, i, s_{k+1}, \ldots, s_m)$, entonces por la definición de A tenemos que $\varphi_{\underline{j}}(A) = a_{ik} = q_{\underline{j}}$, por lo que el resultado se sigue si $\#\{\underline{j} \cap \underline{s}\} \geqslant m - 1$. Ahora, tomemos $\underline{j} \in I_m[n]$ y observe que por la forma en que escribimos las relaciones de Plucker en la observación 4.13, tomando $(s_1, \ldots, s_{m-1})$ y $(s_m, j_1, \ldots, j_d)$ y recordando que el punto q satisface dichas relaciones por hipótesis, tenemos:

$$q_{\underline{s}} q_{\underline{j}} \pm \sum q_{\underline{s'}} q_{\underline{j'}} = 0.$$

donde $\#\{\underline{s} \cap \underline{j'}\} > \#\{\underline{s} \cap \underline{j}\}$, pues alguna entrada en $(j_1, \ldots, j_m)$ que no está en $\underline{s}$ ha sido reemplazada por s_m en $\underline{j'}$. Así, por hipótesis de inducción se sigue que $q_{\underline{j'}} = \varphi_{\underline{j'}}(A)$. Observe que dado que $\underline{s}$ y $\underline{s'}$ difieren por sólo una entrada, tenemos que $q_{\underline{s'}} = \varphi_{\underline{s'}}(A)$. Hemos probado que A satisface las relaciones de Plucker, por lo que:

$$\varphi_{\underline{s}}(A) \varphi_{\underline{j}}(A) \pm \sum \varphi_{\underline{s'}}(A) \varphi_{\underline{j'}}(A) = 0.$$

Concluímos, entonces que:

$$\varphi_{\underline{s}}(A) \varphi_{\underline{j}}(A) = q_{\underline{s}} q_{\underline{j}},$$

y dado que $\varphi_{\underline{s}}(A) = 1 = q_{\underline{s}}$, tenemos que $\varphi_{\underline{j}}(A) = q_{\underline{j}}$. Así, dado que A es la matriz que representa a $U \in G(m, V)$, tenemos que todo punto q que satisface las *relaciones de Plucker* proviene de un subespacio U en la Grassmanniana $G(m, V)$, lo que concluye la prueba. $\square$

Para la matriz de indeterminadas $X = (x_{ij})$ de tamaño $m \times n$ considere el anillo de polinomios en mn indeterminadas con coeficientes en K:

$$K[X] = K[x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}, \ldots, x_{m1}, \ldots, x_{mn}]$$

Por el teorema 4.14 el *anillo de coordenadas* de la variedad de Grassmann $G(m, V)$ es:

$$K[G(m, V)] = K[X] \diagup I(G(m, V)).$$

que es generada como álgebra por los menores de rango máximo m de X que satisfacen las relaciones de Plücker.

Observación 4.15. Si en el teorema 3.10 consideramos $\underline{i} = (i_1, \dots, i_m)$, $\underline{j} = (j_1, \dots, j_m)$ en $I_m[n]$ entonces para cualquier entero $1 \leqslant s \leqslant m$ y tomando el grupo de permutaciones $S = S(i_1, \dots, i_m, j_1, \dots, j_m)$, podemos escribir las relaciones de Plucker como:

$$\sum_{\sigma \in S} p_{\sigma(\underline{i})} p_{\sigma(\underline{j})} = 0.$$

Y para cada s tal que $1 \leqslant s \leqslant m$ y cada par $\underline{i}$, $\underline{j}$ hay a lo más m relaciones de Plucker.

Ejemplo 4.15.1. Consideremos el caso particular de la Grassmanniana $G(2,4) \subseteq \mathbb{P}(\wedge^2 V) = \mathbb{P}^5$. A fin de caracterizar a $G(2,4)$, queremos obtener las relaciones de Plucker. Debemos considerar entonces de acuerdo al lema 4.14 y la observación 4.15 dos sucesiones $\underline{i}$, $\underline{j}$ en $I_2[4]$. Por la condición de orden que tenemos en las sucesiones de enteros tenemos que hay 6 posibilidades, que son $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$. Elegimos un m tal que $1 \leqslant m \leqslant 2$ y un par $\underline{i}$, $\underline{j}$. Para $m = 1$ y el par $\underline{i} = (1,2)$, $\underline{j} = (3,4)$ tenemos el grupo de permutaciones $S = S(1,3,4)$ que consta de $3! = 6$ permutaciones. La identidad nos genera el elemento $p_{1,2}p_{3,4}$ y ahora consideramos las permutaciones que intercambian subconjuntos no vacíos de $\{1\}$ con subconjuntos no vacíos de $\{3,4\}$, por lo que tenemos dos de ellas (transposiciones) que surgirían de intercambiar al elemento 3 con 1 y 4 con 1, esto es:

$$\sigma_1 = (13) = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 1 & 4 \end{pmatrix}$$

$$\sigma_2 = (14) = \begin{pmatrix} 1 & 3 & 4 \\ 4 & 3 & 1 \end{pmatrix}$$

Aplicando ambas a los pares $\underline{i}$, $\underline{j}$, tenemos:

$$\sigma_1(\underline{i}) = (3,2)$$

$$\sigma_1(\underline{j}) = (1,4)$$

$$\sigma_2(\underline{i}) = (4,2)$$

$$\sigma_2(\underline{j}) = (3,1)$$

Dado que ambas permutaciones son impares, tendremos que corresponden a elementos con signo $-$, que son respectivamente: $-p_{1,4}p_{2,3}$ y $-p_{1,3}p_{2,4}$. Procedemos ahora con $s = 2$ y el mismo par $\underline{i} = (1,2)$, $\underline{j} = (3,4)$. Ahora tenemos el grupo de permutaciones $S = S(1,2,4)$. Nuevamente tenemos 6 permutaciones y además de la identidad, consideramos las que intercambian subconjuntos no vacíos de $\{1,2\}$ con $\{4\}$. Así, tenemos las siguientes dos transposiciones:

$$\sigma_1 = (14) = \begin{pmatrix} 1 & 2 & 4 \\ 4 & 2 & 1 \end{pmatrix}$$

$$\sigma_2 = (24) = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 4 & 2 \end{pmatrix}$$

Aplicando ambas a los pares $\underline{i}$, $\underline{j}$, tenemos:

$$\sigma_1(\underline{i}) = (4, 2)$$

$$\sigma_1(\underline{j}) = (3, 1)$$

$$\sigma_2(\underline{i}) = (1, 4)$$

$$\sigma_2(\underline{j}) = (3, 2)$$

Nuevamente dado que ambas permutaciones son impares, tendremos que corresponden a elementos con signo $-$, que son respectivamente: $-p_{1,3}p_{2,4}$ y $-p_{1,3}p_{2,4}$. Hemos obtenido los mismos elementos del caso $s = 1$. Entonces la única relación no trivial de Plucker es:

$$p_{1,2}p_{3,4} - p_{1,3}p_{2,4} + p_{1,4}p_{2,3} = 0.$$

Así, $G(2, 4)$ es el conjunto de ceros de un polinomio cuadrático en $\mathbb{P}^5$. Esta hipersuperficie cuádrica se conoce como la *cuádrica de Klein*.

4.2.2. Una base Sagbi para el anillo de coordenadas de la Grasssmanniana

Consideremos un campo K y $X = (x_{ij})_{i=1,\ldots,m;j=1,\ldots,n}$ una matriz de indeterminadas. Denotamos por $K[X]$ al anillo de polinomios sobre K con indeterminadas x_{ij} y a A la K-subálgebra de $K[X]$ generada por todos los menores máximos de X, es decir, A es el *anillo de coordenadas* de la variedad Grassmanniana de los K-subespacios vectoriales de dimensión m de K^n. Queremos estudiar al anillo A mediante su álgebra inicial con respecto al orden lexicográfico inducido por el orden de las variables:

$$x_{11} > x_{12} > \cdots > x_{1n} > x_{21} > x_{22} > \cdots > x_{m1} > x_{m2} > \cdots > x_{mn}$$

Por convención denotamos el menor máximo de X con columnas $1 \leqslant a_1 < a_2 < \cdots \leqslant n$ por $[a_1, \ldots, a_m]$. Entonces:

$$\mathrm{in}_<[a_1, \ldots, a_m] = x_{1a_1}x_{2a_2}\cdots x_{ma_m}.$$

En el conjunto $\mathfrak{L}$ de todos los menores máximos definimos un orden parcial:

$$[a_1, \ldots, a_m] \leqslant [b_1, \ldots, b_m]$$

si y sólo si $a_i \leqslant b_i$ para todo i. Este conjunto parcialmente ordenado admite ínfimos y supremos; de hecho tenemos que:

$$[a_1, \ldots, a_m] \vee [b_1, \ldots, b_m] = [\text{máx}\{a_1, b_1\}, \ldots, \text{máx}\{a_m b_m\}]$$

$$[a_1, \ldots, a_m] \wedge [b_1, \ldots, b_m] = [\text{mín}\{a_1, b_1\}, \ldots, \text{máx}\{a_m b_m\}].$$

Es claro que $\mathfrak{L}$ es una retícula distributiva con ínfimo y supremo como hemos descrito. En lo siguiente de la sección fijaremos un orden monomial diagonal $<$. Sea B la K-álgebra generada sobre K por los monomios iniciales de los menores máximos de X. Nuestro objetivo es encontrar una base SAGBI de A, es decir, probar que $B \simeq \mathrm{in}_<(A)$. Primeramente introducimos las *relaciones de Hibi.*

Sea T el anillo de polinomios sobre K en las variables t_δ con $\delta \in \mathcal{L}$ y sea $\psi : T \to B$ el homomorfismo de K-álgebras tal que $\psi(t_\delta) = \mathrm{in}_<(\delta)$. Observe que las relaciones de Hibi definidas como sigue:

$$t_{\delta_1}t_{\delta_2} - t_{\delta_1 \vee \delta_2}t_{\delta_1 \wedge \delta_2}$$

donde $\delta_1, \delta_2 \in \mathcal{L}$ pertenecen a $J = \ker \psi$.

Usando el teorema 4.5 tenemos el resultado que nos permite obtener una base SAGBI de A:

Teorema 4.16. *Los menores máximos de* X *forman una base* SAGBI *de* A*. En otras palabras,* $B = \mathrm{in}_<(A)$.

Demostración. Aplicamos el teorema 4.5 para mostrar que las relaciones de Hibi pueden ser levantadas. Para ver esto usamos el hecho de que cualquier producto de dos menores incomparables puede ser *rectificado*. Esto quiere decir lo siguiente: Sean $\delta_1 = [a_1, a_2, \ldots, a_m]$ y $\delta_2 = [b_1, b_2, \ldots, b_m]$ dos menores incomparables (con respecto al orden parcial dado en $\mathcal{L}$). Entonces δ_1, δ_2 pueden ser escritos como una combinación lineal ℓ de productos de menores $[c_1, c_2, \ldots, c_m][d_1, d_2, \ldots, d_m]$ satisfaciendo la siguiente condición:

$$[c_1, c_2, \ldots, c_m] \leqslant [d_1, d_2, \ldots, d_m]$$

$$[c_1, c_2, \ldots, c_m] \leqslant [\mathrm{mín}\{a_1, b_1\}, \ldots, \mathrm{mín}\{a_m, b_m\}]$$

La sucesión $(c_1, c_2, \ldots, c_m, d_1, d_2, \ldots, d_m)$ se obtiene de la sucesión $(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_m)$ por medio de una permutación.

Entre los sumandos potenciales en ℓ tenemos también $(\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2)$. El hecho crucial a observar es que cualquier producto de menores máximos $\sigma\tau$ satisfaciendo la condición anterior el cual es diferente de $(\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2)$ tiene la propiedad de que $\mathrm{in}_<(\sigma\tau) < \mathrm{in}_<(\delta_1\delta_2) = \mathrm{in}_<((\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2))$

En efecto, sea k un entero tal que: $c_i = \mathrm{mín}\{a_i, b_i\}$ y $d_i = \mathrm{máx}\{a_i, b_i\}$. Nótese primeramente que debido a la segunda condición descrita anteriormente y la elección de k, la secuencia $(c_k, \ldots, c_m, d_k, \ldots, d_m)$ y la secuencia $\mathcal{S} = (a_k, \ldots, a_m, b_k, \ldots, b_m)$ coinciden vía una permutación de sus elementos. Si $c_k \neq \mathrm{mín}\{a_k, bk\}$, entonces la primera condición implica que $c_k < \mathrm{mín}\{a_k, bk\}$, lo cual es imposible pues $c_k \in \mathcal{S}$. Asumiendo sin perder generalidad que $a_k < b_k$ tenemos entonces que $c_k = a_k$ y $d_k \neq \mathrm{máx}\{a_k, bk\}$. Suponemos que $d_k < \mathrm{máx}\{a_k, bk\}$. Si $d_k = a_k$ llegamos a una contradicción dado que c_k y d_k son elementos diferentes de la secuencia $\mathcal{S}$ mientras que a_k es el único elemento más pequeño en $\mathcal{S}$, Por otro lado, si $d_k < \mathrm{máx}\{a_k, b_k\}$ y $d_k \neq a_k$, entonces existe $j > k$ con $a_j < b_k$ tal que $d_k = a_j$. Se sigue que $a_{k+1} \leqslant a_j < b_k < b_{k+1}$, así que $\text{mín}\{a_{k+1}, b_{k+1}\} = a_{k+1}$. Esto implica que:

$$a_k = c_k < c_{k+1} \leqslant \text{mín}\{a_{k+1}, b_{k+1}\} = a_{k+1}.$$

Se sigue que $c_{k+1} = a_{k+1}$ dado que entre a_k y a_{k+1} no hay otro elemento de la secuencia $\mathcal{S}$ y c_{k+1} pertenece a esta secuencia. Procediendo de la misma manera obtenemos que:

$$a_{j-1} = c_{j-1} < c_j \leqslant \text{mín}\{a_j, bj\} = a_j$$

Así, se deduce como antes que $c_j = a_j$. Dado que también tenemos que $d_k = a_j$ se sigue que a_j aparece dos veces en la secuencia $c_k, \ldots, c_m, d_k, \ldots, d_m$ la cual es una permutación de la secuencia $\mathcal{S}$. Sin embargo, a_j aparece exactamente una vez en la secuencia $(a_k, \ldots, a_m)$ y no puede aparecer en $(b_k, \ldots, b_m)$ dado que $a_j < b_k < \ldots < b_m$.

Se concluye que $d_k > \text{máx}\{a_k, b_k\}$. Ahora, se tiene que:

$$\text{in}_<((\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2)) = x_{1,a_1} x_{1,b_1} \cdots x_{k-1,a_{k-1}} x_{k-1,b_{k-1}} x_{k,a_k} x_{k,b_k} \cdots$$

y

$$\text{in}_<(\sigma\tau) = x_{1,a_1} x_{1,b_1} \cdots x_{k-1,a_{k-1}} x_{k-1,b_{k-1}} x_{k,a_k} x_{k,d_k} \cdots$$

con $d_k > b_k$. Esto muestra que en efecto $\text{in}_<(\sigma\tau) < \text{in}_<(\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2)$. Dado que $\delta_1\delta_2 - \mathfrak{l} = 0$, el monomio inicial de $\delta_1\delta_2$ debe cancelarse con el monomio inicial de un sumando en $\mathfrak{l}$. Sin embargo, por lo que se ha visto este sumando tiene que ser $(\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2)$. Así $(\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2)$ de hecho aparece en ℓ con coeficiente 1. Se sigue que:

$$\delta_1\delta_2 - (\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2) = \ell'$$

donde $\ell' = \mathfrak{l} - (\delta_1 \wedge \delta_2)(\delta_1 \vee \delta_2)$ es una combinación lineal de productos de menores máximos $\sigma\tau$ con $\text{in}_<(\sigma\tau) < \text{in}_<(\delta_1\delta_2)$ como se quería. $\square$

4.3. Perspectivas

Consideremos V un K-espacio vectorial de dimensión n. Supongamos que V tiene asociada una forma bilineal no degenerada y alternante, digamos $b : V \times V \to K$. Se dice que V es un espacio vectorial simpléctico y la forma bilineal asociada es una forma simpléctica.

Dado que b es alternante, $b(x, x) = 0$ para todo $x \in V$ se sigue que b es antisimétrica. En efecto: Sea $x, y \in V$, entonces $0 = b(x + y, x + y) = b(x, x) + b(x, y) + b(y, x) + b(y, y)$ de donde $b(x, y) = -b(y, x)$. Dado que el espacio vectorial V tiene dicha forma bilineal alternante y no degenerada b se sigue que $\dim(V) = 2n$ para n un número natural.

Tomemos un caso particular, supongamos que V es de dimensión 1 y que $\text{car}(K) \neq 2$ y sea $\{x\}$ una base de V, luego como b es antisimétrica tenemos que $b(x, x) = -b(x, x)$ por lo que $b(x, x) = 0$ luego para cualquier elemento $v \in V$ tenemos que $v = \lambda x$ con $\lambda \in K$ entonces

$b(v,x) = b(\lambda x, x) = \lambda b(x,x) = 0$ pero $x \neq 0$ pues $\{x\}$ es base de V, lo que contradice el hecho de que b es no degenerada.

En general, si $\operatorname{car}(K) \neq 2$ y dado que b es alternante la matriz de la forma bilineal, digamos A es antisimétrica, esto es $A = -A^t$. Digamos que $\dim V = m$, entonces:

$$\det(A) = \det(A^t) = (-1)^m \det(A^t) = (-1)^m \det(A). \tag{4.8}$$

Dado que b es no degenerada, la matriz A es invertible y por tanto $\det(A) \neq 0$, entonces $(-1)^m = 1$ y por tanto m debe ser par.

Queremos considerar Grassmannianas que estén relacionadas con la forma bilineal b. Consideremos subespacios W de V de dimensión $d < 2n$ que cumplan la siguiente condición:

Si $w, w' \in W \subseteq V$ entonces $b(w, w') = 0$. Es decir, la forma bilineal b restringida a W es 0. Dichos subespacios W que satisfacen esta condición los llamamos *isotrópicos*.

En principio estos subespacios tienen dimensión a lo más $2n$, sin embargo, se prueba que podemos acotar de forma más precisa la dimensión de todos los espacios isotrópicos de V que será a lo más n.

En efecto, sea W un subespacio isotrópico de V. Entonces $W \subset W^{\perp}$. Dado que $\dim V = \dim W + \dim W^{\perp} \geqslant 2\dim W$, esto último pues $W \subset W^{\perp}$, así se sigue que $\dim W \leqslant n$ donde $\dim V = 2n$.

Estamos interesados en los subespacios isotrópicos de dimensión máxima, es decir, aquellos de dimensión n. Llamamos a estos subespacios *subespacios Lagrangianos*.

Consideremos ahora la Grassmanniana $G(n, 2n)$, es decir, el conjunto de los subespacios vectoriales de dimensión n de V, donde la dimensión de V es $2n$ y consideremos el conjunto $L(n, 2n)$ de todos subespacios Lagrangianos de V:

$$L(n,2n) = \{W \in G(n,2n) : \text{W es isotrópico} \subseteq G(n,2n)\}. \tag{4.9}$$

Queremos ver que también es una variedad algebraica, la llamada variedad *Lagrangiana-Grassmanniana*. Por otro lado, tal y como se ha visto en el último capítulo, podemos obtener otra descripción de la Grassmanniana partiendo de una base de W, digamos $\mathcal{B} = \{w_1, \ldots, w_n\}$ y enviando dicha base mediante la inmersión de Plucker al punto $[w_1 \wedge \cdots \wedge w_n] \in \mathbb{P}(\wedge^n V)$, por lo que:

$$G(n,2n) = \{w_1 \wedge \cdots \wedge w_n \in \mathbb{P}(\wedge^n V) : w_1, \ldots, w_n \text{ son linealmente independientes}\}. \tag{4.10}$$

De la misma manera, podemos obtener una descripción de la Lagrangiana-Grassmanniana considerando que los subespacios W de $L(n, 2n)$ son isotrópicos, es decir la forma bilineal b restringida a W es 0. Esto basta con garantizarlo en una base de W, por lo que:

$$L(n,2n) = \{w_1 \wedge \cdots \wedge w_n \in G(n,2n) : b(w_i, w_j) = 0, \forall i,j\}. \tag{4.11}$$

Tomando el espacio simpléctico V, considérese la potencia exterior $\wedge^n V$ y el mapeo lineal $f : \wedge^n V \to \wedge^{n-2} V$ (una contracción) dado por:

$$w_1 \wedge \cdots \wedge w_n \mapsto \sum_{1 \leqslant r < s \leqslant n} \pm b(w_r, w_s) w_1 \wedge \cdots \wedge \hat{w}_r \wedge \cdots \wedge \hat{w}_s \wedge \cdots \wedge w_n = 0. \tag{4.12}$$

donde $\hat{w}$ denota que dicho término es omitido. f es lineal y podemos considerar su núcleo, digamos E. Sea $\mathbb{P}(E)$ la proyectivización de E, entonces bajo la inmersión de Plucker $\mathbb{P}(E)$ es un subespacio cerrado e irreducible de $\mathbb{P}(\bigwedge^n V)$ y está definido por polinomios lineales homogéneos, esto es $\mathbb{P}(E) = Z(g_1, \ldots, g_N)$, el conjunto de ceros de polinomios lineales homogéneos $g_1, \ldots, g_N$ sobre el campo K. La Lagrangiana-Grassmanniana resulta ser los puntos en común de $\mathbb{P}(E)$ con la variedad Grassmaniana, teniendo así que es una variedad algebraica.

Lema 4.17. $L(n, 2n) = G(n, 2n) \cap \mathbb{P}(E)$.

Demostración. Por la definición de $L(n, 2n)$ se sigue claramente la primera contención. Para la otra contención tomemos $w \in G(n, 2n) \cap \mathbb{P}(E)$, así w es la clase de equivalencia de $v_1 \wedge \cdots \wedge v_n$ donde $v_1, \ldots, v_n$ son linealmente independientes y $f(w) = 0$, esto es,

$$f(w) = \sum_{1 \leqslant i < j \leqslant n} b(v_i, v_j) v_1 \wedge \cdots \wedge \hat{v_i} \wedge \cdots \wedge \hat{v_j} \wedge \cdots \wedge v_n = 0$$

por lo que $b(v_i, v_j) = 0$ para todos $1 \leqslant i < j \leqslant n$ y por tanto $w \in L(2, n)$. □

Observación 4.18. Dado que $\mathbb{P}(E) = Z(g_1, \ldots, g_N)$ y la Grassmanniana está generada por los polinomios cuadráticos de Plucker, digamos $G(n, 2n) = Z(f_1, \ldots, f_M)$, entonces:

$$L(n, 2n) = Z(f_1, \ldots, f_M, g_1, \ldots, g_N). \tag{4.13}$$

Asumiendo K algebraicamente cerrado tenemos que existe un hiperplano $H \subseteq \mathbb{P}(E)$ tal que $L(n, 2n) \subseteq H$. Para este hiperplano H existe un polinomio lineal homogéneo h tal que $H = Z\langle g_1, \ldots, g_N, h\rangle$ con $\{g_1, \ldots, g_N, h\}$ un conjunto mínimo de generadores. Por tanto, los ideales asociados satisfacen: $I(Z\langle g_1, \ldots, g_N, h\rangle) \subseteq I(Z\langle f_1, \ldots, f_M, g_1, \ldots, g_N\rangle) = \sqrt{\langle f_1, \ldots, f_M, g_1, \ldots, g_N\rangle} = \langle f_1, \ldots, f_M, g_1, \ldots, g_N\rangle$. Esta última igualdad se satisface porque $L(n, 2n)$ es irreducible. Por tanto:

$$h \in I(Z\langle g_1, \ldots, g_N, h\rangle) \subseteq \langle f_1, \ldots, f_M, g_1, \ldots, g_N\rangle \tag{4.14}$$

y dado que h es lineal, se sigue que $h \in \langle g_1, \ldots, g_N\rangle$, lo cual es una contradicción.

Esto es, es un ideal radical y por tanto es el ideal de anulación de la variedad Lagrangiana-Grassmanniana.

Así, una idea para un trabajo posterior puede ser buscar una Base Sagbi del anillo de coordenadas de la variedad Lagrangiana-Grassmanniana.

A Anillos conmutativos graduados

Notación y terminología

En el desarrollo de este trabajo consideraremos sólo anillos conmutativos y con uno, a menos que se especifique lo contrario. Usaremos K y $K[x_1, ..., x_n]$ para denotar a un campo arbitrario y al anillo de polinomios en n indeterminadas, respectivamente.

A.1. Anillos de polinomios

En esta sección introducimos algunos conceptos y propiedades importantes del anillo $K[x_1, ..., x_n]$, así como también de sus ideales. Asumiremos la teoría básica de anillos en general. Considerando la estructura de campo de K y las operaciones usuales en el anillo $K[x_1, ..., x_n]$: suma y multiplicación por escalar, es fácil verificar que $K[x_1, ..., x_n]$ es un K espacio vectorial. Los elementos básicos son de la forma:

$$x_1^{a_1} \cdots x_n^{a_n}$$

Con $a_i \in \mathbb{N}$. Dichas expresiones las llamamos **monomios** . Así, un elemento arbitrario en $K[x_1, ..., x_n]$ es una combinación lineal finita de monomios y es llamada **polinomio**. Por tanto, el anillo $K[x_1, ..., x_n]$ será referido como el *anillo de polinomios en n indeterminadas*.

Por convención, en un monomio omitimos los factores con exponente cero y denotamos por 1 al monomio en el cual toda a_i es igual a 0.

A fin de simplificar notación, en ocasiones escribiremos $\mathbf{x}^{\mathbf{a}}$ para denotar al monomio $x_1^{a_1} \cdots x_n^{a_n}$, donde $\mathbf{a} = (a_1, ..., a_n) \in \mathbb{N}^n$.

Así, podemos escribir un polinomio $f \in K[x_1, ..., x_n]$ como:

$$f = \sum_{\mathbf{a} \in \mathbb{N}^n} = c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}$$

donde $c_{\mathbf{a}} \in K$ y $c_{\mathbf{a}} = 0$ para *casi toda* $\mathbf{a}$, es decir, salvo un número finito de ellas.

Sea $\operatorname{sop}(f) = \{\mathbf{x}^{\mathbf{a}} : c_{\mathbf{a}} \neq 0\}$. Por lo dicho anteriormente este conjunto de monomios es finito y lo llamamos el **soporte** de f.

Obsérvese que $\operatorname{sop}(f) = \emptyset$ si y sólo si $f = 0$. Por último, es preciso recordar la definición formal de las operaciones suma y producto de polinomios que dan estructura de anillo a $K[x_1, ..., x_n]$.

Sean:

$$f = \sum_{\mathbf{a}\in\mathbb{N}^n} = c_{\mathbf{a}}\mathbf{x}^{\mathbf{a}}$$

$$g = \sum_{\mathbf{a}\in\mathbb{N}^n} = d_{\mathbf{a}}\mathbf{x}^{\mathbf{a}}$$

Entonces, definimos la suma y producto respectivamente:

$$f + g = \sum_{\mathbf{a}\in\mathbb{N}^n} = (c_{\mathbf{a}} + d_{\mathbf{a}})\mathbf{x}^{\mathbf{a}}$$

Para la multiplicación, primero recuérdese que la multiplicación de dos *términos* está dada por: $c\mathbf{x}^{\mathbf{a}} \cdot d\mathbf{x}^{\mathbf{b}} = cd\mathbf{x}^{\mathbf{a}+\mathbf{b}}$

Dado que un polinomio es una suma finita de estos términos, podemos generalizar de lo anterior el producto de dos polinomios dados:

$$fg = \sum_{g\in\mathbb{N}^n} \sum_{\mathbf{a}+\mathbf{b}=\mathbf{g}} (c_{\mathbf{a}}d_{\mathbf{b}})\mathbf{x}^{\mathbf{g}}$$

Definición A.1 (K-álgebra)**.** Sea K un campo. Una K-álgebra es un anillo en el cual podemos considerar a K como un subanillo de éste.

En el caso del anillo $K[x_1, ..., x_n]$, podemos identificar a K con los polinomios constantes y por tanto $K[x_1, ..., x_n]$ es una K-álgebra.

Definición A.2. Sean A y B K-álgebras. Se dice que un morfismo de anillos $\varphi : A \to B$ es un morfismo de álgebras si $\varphi(a) = a$ para todo $a \in K$, es decir, si φ restringido a K es la identidad.

Teorema A.3. *Sea R una K-álgebra y sean $\alpha_1, ..., \alpha_n$ elementos arbitrarios en R. Entonces existe un único morfismo de K-álgebras*

$$\varphi : K[x_1, ..., x_n] \to R$$

tal que: $\varphi(x_i) = \alpha_i$ para todo $i = 1, ..., n$

Demostración. Supongamos que tal morfismo de K-álgebras, φ existe. Sea $f = \sum_{\mathbf{a}\in\mathbb{N}^n} c_{\mathbf{a}}\mathbf{x}^{\mathbf{a}}$ un polinomio arbitrario en $K[x_1, ..., x_n]$. Luego, dado que φ es morfismo de K-álgebras se tiene:

$$\varphi(f) = \sum_{\mathbf{a}\in\mathbb{N}^n} \varphi(c_{\mathbf{a}})\varphi(\mathbf{x}^{\mathbf{a}}) = \sum_{\mathbf{a}\in\mathbb{N}^n} c_{\mathbf{a}}\alpha^{\mathbf{a}} \tag{A.1}$$

Donde $\alpha = \alpha_1 \cdots \alpha_n$. Por tanto, si tal morfismo φ existe, éste está unívocamente determinado por los elementos $\alpha_1, \ldots, \alpha_n$ de R por lo que debe ser definido como en A.1. Observe que φ está definido por la sustitución de las variables x_i por los elementos α_i de R, por ello se φ se conoce como el *morfismo de sustitución*. $\square$

A.2. Anillos graduados e ideales homogéneos

En esta sección introducimos los Anillos graduados y los ideales homogéneos

Definición A.4 (Anillo graduado)**.** Sea A un anillo, decimos que A es un anillo *graduado* si existe una familia de subgrupos $\{A_n\}_{n\in\mathbb{N}}$ de A tal que:

(1) $A = \bigoplus_n A_n$ (Como grupos abelianos)

(2) $A_n \cdot A_m \subseteq A_{n+m}$ para todo n, m

A la descomposición de A como suma directa de los subgrupos A_n le llamamos *graduación* en A.

Ejemplos

(1) Considerando $A_0 = A$ y $A_n = 0$ para todo $n > 0$, tenemos la *graduación trivial* en A.

(2) Consideremos el anillo de polinomios $\mathbb{R}[x]$. Observe que $\mathbb{R}[x] = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \cdots$ Al tomar cualquier polinomio $P \in \mathbb{R}[x]$ cada monomio de P tiene asociado un *grado*, por ello, para hacer esta distinción podemos escribir:

$$\mathbb{R}[x] = \underbrace{\mathbb{R}}_{\text{gr}\,0} \oplus \underbrace{\mathbb{R}x}_{\text{gr}\,1} \oplus \underbrace{\mathbb{R}x^2}_{\text{gr}\,2} \oplus \underbrace{\mathbb{R}x^3}_{\text{gr}\,3} \oplus \cdots$$

Esta descomposición de $\mathbb{R}[x]$ permite distinguir de forma precisa cada monomio de cualquier polinomio P

Por ejemplo, en el polinomio $P = (-1, 6, 0, 3, 3, 0, 0, ...) = -1+6x+3x^3+3x^4$ podemos distinguir el elemento 3 de grado 3 del elemento 3 de grado 4.

Además, $\mathbb{R}\mathbb{R} = \mathbb{R}$.

Entonces, considerando $A_n = \mathbb{R}$ para todo $n > 0$, tenemos una graduación $\{A_n\}_{n\in\mathbb{N}}$ de $R[x]$

Lo anterior se puede generalizar al anillo de polinomios con coeficientes en un campo K e indeterminadas $x_0, x_1, ..., x_n$ como ilustramos en el siguiente ejemplo.

(3) Sea $A = K[x_0, x_1, ..., x_n]$, el anillo de polinomios sobre un campo K.

Sea A_d el conjunto de los polinomios homogéneos de grado d en $K[x_0, x_1, ..., x_n]$

Puede probarse que cada A_d es un subgrupo aditivo de A y que para todos $d, e \geqslant 0$, $A_d A_e \subseteq A_{d+e}$, además que todo polinomio $P \in A$ se puede escribir de forma única como suma de polinomios homogéneos. Así, tenemos una graduación en A:

$$A = \bigoplus_{d \geqslant 0} A_d$$

Definición A.5 (Componentes y elementos homogéneos)**.** Sea $A = \bigoplus_{n \geqslant 0} A_n$ un anillo graduado. El grupo A_n es llamado el *componente homogéneo* de A de grado n y los elementos de A_n son llamados *elementos homogéneos* de grado n. Así, 0 es un elemento homogéneo de todos los grados.

Todo elemento de A tiene una única representación como suma de elementos homogéneos. Es decir, dado $a \in A$ tenemos $a = \sum_{n \geqslant 0} a_n$, con $a_n \in A_n$ para todo n y $a_n = 0$ para casi todo n.

Esta última expresión la llamamos la *descomposición homogénea* de a y a_n es llamado el *componente homogéneo* de a de grado n.

Teorema A.6. *Sea A un anillo graduado y definamos $A_+ = \bigoplus_{n \geqslant 1} A_n$, entonces:*

(1) A_0 es un subanillo de A y cada A_n es un A_0-submódulo de A

(2) A_+ es un ideal de A y se tiene el isomorfismo $A_0 \simeq A/A_+$.

Demostración. (1) Para ver que A_0 es un subanillo de A tenemos que ver que es cerrado bajo multiplicación y que contiene al 1 de A. Lo primero es claro pues al ser A graduado tenemos $A_0 A_0 \subseteq A_0$. Luego, escribimos $1 = \sum_{n \geqslant 0} e_n$ (suma finita) con $e_n \in A_n$. Entonces:

$$e_i = 1 e_i = \sum_{n \geqslant 0} e_n e_i$$

Dado que la representación de cada e_i es única; comparando elementos homogéneos, se tiene: $e_i = e_0 e_i$ para toda i.

En particular, $e_0 = e_0 1 = \sum_{n \geqslant 0} e_0 e_n = \sum_{n \geqslant 0} e_n = 1$ y así $1 \in A_0$. Por lo anterior, concluímos que A_0 es un subanillo de A. Por otro lado dado que cada A_n es un subgrupo de A para ver que A_n es un A_0-submódulo de A tenemos que ver que para todo $x \in A_0$ y para todo $a \in A_n$ se tiene que $xa \in A_n$. En efecto, sea $x \in A_0$, $a \in A_n$, luego por ser A graduado tenemos que $A_0 A_n \subseteq A_{0+n} = A_n$, entonces $xa \in A_n$ y por lo tanto cada A_n es un A_0-submódulo de A.

(2) Definamos $\varphi : A \to A_0$ por $\varphi(a) = \varphi(\sum_{n\geqslant 0} a_n) = a_0$, claramente φ es un morfismo de anillos bien definido pues la descomposición homogénea de cada elemento de A es única, además es claro que φ es sobreyectivo. Por último, veamos que $a = \sum_{n\geqslant 0} a_n \in \ker(\varphi) \Leftrightarrow \varphi(a) = a_0 = 0$, es decir, un elemento $a \in \ker(\varphi)$ si y sólo si su componente homogénea de grado cero es cero. Por lo tanto $\ker(\varphi) = A_+$ y así, aplicando el *Primer Teorema de Isomorfismo* para anillos tenemos que:

$$A_0 \simeq A\diagup A_+$$

Es decir, el siguiente diagrama conmuta.

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\pi"'] & A_0 \\ A\diagup A_+ \arrow[ur, dashed, "f"'] & \end{tikzcd}$$

□

Lema A.7. *Para un ideal* I *de un anillo graduado* A*, las siguientes condiciones son equivalentes:*

(1) *Para todo* $a \in I$ *todos los componentes homogéneos de* a *están en* I.

(2) $I = \bigoplus_{n\geqslant 0}(I \cap A_n)$

(3) I *es generado (como ideal) por elementos homogéneos.*

Demostración. (1) (1)⇒(2) Sea $a \in I$, entonces a tiene una única expresión de la forma $a = \sum_n a_n$ (suma finita) con $a_n \in A_n$, para todo n; luego por (1) $a_n \in I$, para todo n por tanto $a = \sum_n a_n$ (suma finita) con $a_n \in (I \cap A_n)$ para toda n y esta expresión es única. (2)⇒(3) Sea $a \in I$, entonces $a = \sum_n a_n$ (suma finita), con $a_n \in (I\cap A_n)$, entonces I es generado por $\bigcup_{n\geqslant 0}(I\cap A_n)$, el cual es un conjunto de elementos homogéneos. (3)⇒(1) Supongamos que I es generado por un conjunto S de elementos homogéneos. Sea $a \in I$ y $n \geqslant 0$; consideremos la componente homogénea a_n de a de grado n. Queremos ver que $a_n \in I$ Dado que I es generado por S, tenemos que existen $s_1, ..., s_r \in S$ y $b_1, ..., b_r \in A$ tal que:

$$a = \sum_{i=1}^{r} b_i s_i \tag{A.2}$$

Sea $b_i = \sum_j b_{i,j}$ la descomposición homogénea de b_i con $b_{i,j} \in A_j$, para todo i, j. Luego, sea $d_i = \mathrm{gr}(s_i)$ Entonces, comparando los elementos homogéneos de grado n en A.2 tenemos:

$$a_n = b_{1,n-d_1}s_1 + \cdots + b_{r,n-d_r}s_r \in I$$

□

Definición A.8 (Ideal homogéneo)**.** Un ideal I de A que satisface alguna de las condiciones equivalentes del teorema anterior es llamado un *Ideal homogéneo.*

La introducción de este tipo de ideales nos permite dotar a un anillo cociente de una graduación.

Si I es un ideal homogéneo de A, entonces el anillo cociente A/I adquiere una graduación dada por $(A/I)_n = A_n/I_n$ llamada la *graduación cociente*. Más aun, si A/I es un anillo graduado entonces I es un ideal homogéneo.

Lema A.9. *Sea* $A = \bigoplus_{n\geqslant 0} A_n$ *un anillo graduado, entonces* A/I *es un anillo graduado si y sólo si* I *es un ideal homogéneo de* A.

Demostración. $\Rightarrow$) Primero supongamos que I es un ideal homogéneo.

Por hipótesis A es un anillo graduado, esto es, $A = \bigoplus_{n\geqslant 0} A_n$ y el ideal I es homogéneo, entonces $I = \bigoplus_{n\geqslant 0}(I \cap A_n)$.

Queremos ver que $A/I = \bigoplus_{n\geqslant 0} A_n/(I\cap A_n) := \bigoplus_{n\geqslant 0} B_n$ es una graduación.

Para demostrar lo anterior, veamos que en efecto, la descomposición anterior es una graduación, lo cual equivale a probar lo siguiente.

(1) Cada $A_n/(I \cap A_n)$ es un subgrupo de A/I

Sea n un número natural fijo y sea $i{:}A_n \to A$ la inclusión de A_n en A. Consideremos también las proyecciones canónicas $\pi : A \to A/I$ y $\pi_n : A_n \to A_n/(I \cap A_n)$ y la restricción de π a A_n a la que denotaremos por f.

Observe que $\ker(f) = I \cap A_n$ pues, $x \in \ker(f) \Leftrightarrow f(x) = [x] = [0] \Leftrightarrow x \in I$.

Así, por el *Primer Teorema de isomorfismos* (para grupos) tenemos que, existe un morfismo de grupos $\overline{f}$ inyectivo tal que el siguiente diagrama conmuta. Esto es, el morfismo $\overline{f}$ está dado por $\overline{f}([x]) = f(x)$ para $x \in A_n$.

Por lo tanto, $A_n/I \cap A_n$ es subgrupo de A/I para toda $n \in \mathbb{N}$.

(2) $A/I = \bigoplus_{n\geqslant 0} A_n/(I \cap A_n) := \bigoplus_{n\geqslant 0} B_n$

Primeramente veamos que $A/I = \sum_{n\geqslant 0} A_n/(I \cap A_n)$

$\subset$) Sea $[x] \in A/I$, luego $x \in A$ y dado que A es anillo graduado, se tiene que $x = \sum_{i\geqslant 0} a_i$, donde $a_i \in A_i$.

Luego, $[x] = [\sum_{i\geqslant 0} a_i] = \sum_{i\geqslant 0}[a_i]$ donde $[a_i] \in A/(I \cap A_n)$

Por lo tanto, $A/I \subset \sum_{n\geqslant 0} A_n/(I \cap A_n)$

$\supset$) Es inmediato, pues $A_n/(I\cap A_n)$ es subgrupo de A/I para toda $n \geqslant 0$, por tanto $\sum_{n\geqslant 0} A_n/(I\cap A_n)$ es subgrupo de A/I; en particular $\sum_{n\geqslant 0} A_n/(I\cap A_n) \subset A/I$.

Ahora veamos que $A_i \diagup (I \cap A_i) \cap \sum_{\substack{j \geqslant 0 \\ j \neq i}} A_j \diagup (I \cap A_j) = \{0\}$

Sea $x \in A_i \diagup (I \cap A_i) \cap \sum_{\substack{j \geqslant 0 \\ j \neq i}} A_j \diagup (I \cap A_j)$; entonces:

$$[x] \in \overline{f}(A_i \diagup (I \cap A_i))$$

y

$$[x] \in \sum_{\substack{j \geqslant 0 \\ j \neq i}} \overline{f}(A_j \diagup (I \cap A_j))$$

Por lo tanto, existen $y_i \in A_i$ y $y_j \in A_j$, para $j \geqslant 0$ y $j \neq i$ tal que:

$$[x] = \overline{f}([y_i]) = \sum_{\substack{j \geqslant 0 \\ j \neq i}} \overline{f}([y_j])$$

Entonces

$$\overline{f}([y_i]) - \sum_{\substack{j \geqslant 0 \\ j \neq i}} \overline{f}([y_j]) = [0]$$

Por tanto

$$\alpha = y_i - \sum_{\substack{j \geqslant 0 \\ j \neq i}} y_j \in I \tag{A.3}$$

Luego, como I es ideal homogéneo y A.3 es una descomposición homogénea de α, cada elemento homogéneo de α está en I, es decir, $y_i, -y_j \in I$, para $j \neq i$. Luego, $y_i \in I$ para todo $i \in \mathbb{N}$.

Así, $y_i \in I \cap A_i$

Entonces,

$$\pi(y_i) = [0] = \overline{f}(\pi_n(y_i)) = \overline{f}([0]) = [0] = [x]$$

Por lo tanto, $[x] = [0]$ y así $A_i \diagup (I \cap A_i) \cap \sum_{\substack{j \geqslant 0 \\ j \neq i}} A_j \diagup (I \cap A_j) = \{0\}$.

(3) $B_m B_n \subset B_{m+n}$

Sean $[a_n] \in B_n$, $[a_m] \in B_m$; donde $a_n \in A_n$ y $a_m \in A_m$.

Luego, como A es anillo graduado, se tiene que $a_n a_m \in A_{n+m}$, entonces $[a_n a_m] \in B_{n+m}$

Por lo tanto, A/I es un anillo graduado.

$\Leftarrow$) Supongamos ahora que A/I es un anillo graduado, esto es, tenemos la siguiente graduación $A/I = \bigoplus_{n\geqslant 0} B_n$, donde B_i es subgrupo de A/I para $n \geqslant 0$.

Queremos ver que I es un ideal homogéneo.

Sea $x \in I$, entonces $[x] = [0] \in A/I$ y además, por ser A anillo graduado, se tiene:

$$x = x_1 + \cdots + x_n$$

donde $x_i \in A_i$.

Luego,

$$[x] = [0] = [x_1] + [x_2] + \cdots + [x_n] = [0] + [0] + \cdots + [0]$$

pues [0] se expresa de forma única como suma de elementos en A/I dado que A/I es un anillo graduado. Entonces $[x_i] = [0]$ para toda $i \in \{0, ..., n\}$ y por tanto $x_i \in I$.

Esto es, para todo $x \in I$ sus componentes homogéneas están en I, por lo tanto, I es ideal homogéneo. □

A.2.1. Ideales

Con el fin de introducir los ideales monomiales y propiedades importantes de éstos, recordemos algunas propiedades importantes de los ideales.

Sean I y J ideales de un anillo A, definimos su suma $I + J$ como el conjunto de todos los elementos $a + b$ donde $a \in I, b \in J$. Éste es el menor ideal que contiene a I y a J.

Así mismo, definimos el producto de dichos ideales como el ideal generado por todos los productos ab donde $a \in I, b \in J$. Dicho ideal es el conjunto de todas las sumas finitas $\sum_i a_i bi$ con $a_i \in I$, $b_i \in J$.

Tanto $I + J$ como IJ son ideales. Así mismo son ideales $I \cap J$ y el llamado *ideal cociente o ideal trasladado*: $(I : J =)\{f \in A \mid fJ \subseteq I\}$.

Además, si I,J,K son ideales, tenemos:

(1) $IJ = JI,\ I + J = J + I$

(2) $I(JK) = (IJ)K,\ \ I + (J + K) = (I + J) + K$

(3) $I(J + K) = IJ + IK$

(4) $IJ \subseteq I \cap J$

(5) $I \cap J + I \cap K \subseteq I \cap (J + K)$

(6) $I : JK = (I : J) : K$

(7) $I:(J+K)=(I:J)\cap(I:K)$

(8) $I:K\ +J:K\subseteq(I+J):K$

Proposición A.10. *Si* K *un campo algebraicamente cerrado el anillo* $K[x_1,...,x_n]$ *tiene un solo ideal maximal graduado, a saber* $\langle x_1,...,x_n\rangle$.

Demostración. Primeramente, $\langle x_1,\dots,x_n\rangle$ es un ideal graduado pues está generado por elementos homogéneos, además $K[x_1,\dots,x_n]/\langle x_1,\dots,x_n\rangle\simeq K$ por lo que $\langle x_1,\dots,x_n\rangle$ es un ideal máximo. Para probar la unicidad, supóngase que existe otro ideal $\mathfrak{m}'$ en $K[x_1,\dots,x_n]$ que es graduado y máximo. Dado que, en particular $\mathfrak{m}'$ es máximo en $K[x_1,\dots,x_n]$ por el teorema de los ceros de Hilbert $\mathfrak{m}'$ es de la forma $\langle x_1-a_1,\dots,x_n-a_n\rangle$ con $a_1,\dots,a_n\in K$, pero dado que es homogéneo se tiene que $a_1=\ldots=a_n=0$ por lo que $\mathfrak{m}'=\langle x_1,\dots,x_n\rangle$ □

Introducimos ahora la *saturación* de un ideal.

Definición A.11. Sea $I\subset S=K[x_1,...,x_n]$ un ideal graduado y $\mathfrak{m}=<x_1,...,x_n>$ el ideal graduado máximo de S. Decimos que I es saturado si $(I:\mathfrak{m})=I$. Observe que directamente de la definición tenemos que $I\subset(I:\mathfrak{m})$.

Llamamos la *saturación* de I al ideal $I^{sat}=(I:\mathfrak{m}^\infty)=\bigcup_{i=1}^\infty(I:\mathfrak{m}^i)$. Dicho nombre está justificado pues en efecto I^{sat} es un ideal saturado de acuerdo a la siguiente proposición.

Proposición A.12. *Sean* $I,J\subset S$ *ideales graduados. Entonces se tiene que:*

I I^{sat} *es saturado*

II *Si* $I\subset J$ *entonces* $I^{sat}\subset J^{sat}$

III *Si* I,J *son saturados entonces* $I\cap J$ *es saturado.*

Demostración. I Queremos ver que $(I^{sat}:\mathfrak{m})=I^{sat}$. Basta ver que $(I^{sat}:\mathfrak{m})\subset I^{sat}$ pues la otra contención siempre se cumple. Para ver esto, supongamos que $f\in I^{sat}:\mathfrak{m}$ entonces para todo $g\in\mathfrak{m}$ se tiene que $fg\in I^{sat}$, luego $fg\in I^{sat}:\mathfrak{m}^k$ para algún $k\geqslant 1$. De lo anterior se sigue que $f\in(I:\mathfrak{m}):\mathfrak{m}=I:\mathfrak{m}^{k+1}\subseteq I:\mathfrak{m}^\infty=I^{sat}$, por lo tanto se satisface la igualdad.

II Sea $f\in I^{sat}$ entonces $f\in I:\mathfrak{m}^k$ para algún $k\geqslant 1$ y dado que $I\subset J$ es inmediato que $I:\mathfrak{m}^k\subset J:\mathfrak{m}^k$, por lo que $f\in J:\mathfrak{m}^k$ y por tanto $f\in J^{sat}$.

III Queremos ver que $(I\cap J):\mathfrak{m}=I\cap J$. Sea $f\in(I\cap J):\mathfrak{m}$ y sea $g\in\mathfrak{m}$, entonces $fg\in I\cap J$, dado que I,J son saturados se sique que $f\in I\cap J$.

□

Ejemplo A.12.1. Consideremos el anillo de polinomios $R = \mathbb{Z}[x, y, z, w]$ y el ideal $I = \langle x^3 - yw^2, x^4 - zw^3 \rangle$. Para calcular su saturación, usamos `Macaulay2` [7], donde el código es el siguiente:

```
i1 : R=ZZ[x,y,z,w]

o1 = R

o1 : PolynomialRing

i2 : I=ideal(x^3-y*w^2,x^4-z*w^3)

              3      2   4      3
o2 = ideal (x  - y*w , x  - z*w )

o2 : Ideal of R

i3 : saturate(I)

              3      2        2      3   2   3    2 4   3 4      2 4
o3 = ideal (x  - y*w , x*y*w  - z*w , x z*w  - y w , y w  - x*z w )

o3 : Ideal of R
```

Por lo tanto, la saturación de I es

$$I^{\text{sat}} = \langle x^3 - yw^2, xyw^2 - zw^3, x^2zw^3 - y^2w^4, y^3w^4 - xz^2w^4 \rangle.$$

Recordemos que el *radical* de un ideal I de un anillo R es:

$$\sqrt{I} = \{f \in R : f^n \in I, \text{para algún entero } n > 0\}$$

$\sqrt{I}$ es un ideal. Decimos que I es radical si $I = \sqrt{I}$ y dado que $\sqrt{\sqrt{I}} = \sqrt{I}$ tenemos que $\sqrt{I}$ es un ideal radical, además es el ideal radical más pequeño que contiene a I.

Consideramos el anillo de polinomios $R = \mathbb{Q}[x, y, z]$ y el ideal $I = \langle x^3 - y^2, y^2z^2 \rangle$. Calculamos $\sqrt{I}$ con `Macaulay2` [7]. Por tanto, tenemos el siguiente código.

```

i1 : QQ[x,y,z]

o1 = QQ[x, y, z]

o1 : PolynomialRing

i2 : I=ideal(x^3-y^2,y^2*z^2)

              3    2   2 2
o2 = ideal (x  - y , y z )
```

```

o2 : Ideal of QQ[x, y, z]

i3 : radical I

                             3     2
o3 = ideal (y*z, x*z, - x  + y )
```

Así, el radical de I es $\sqrt{I} = \langle yz, xz, -x^3 + y^2 \rangle$

Bibliografía

[1] Arbarello, E., Cornalba M., Griffiths P.A., and Harris J. *Geometry of algebraic curves*, Volume I, Springer Science, New York, 1985.

[2] Atiyah, M., MacDonald I.G., *Introduction to Commutative Algebra*, Addison Wesley, 1969.

[3] Bruns, W., Conca, A. *Gröbner bases and determinantal ideals*, en: J. Herzog and V. Vuletescu (eds.), Commutative Algebra, Singularities and Computer Algebra 9–66, Kluwer Academic Pubs. NATO Science Series, 2003.

[4] Carrillo-Pacheco J., Zaldívar, F., *On Lagrangian-Grassmannian codes*, Designs, Codes and Cryptography 60, 291–298, 2011.

[5] Cox, D., Little J., and O'Shea D. *Ideals, Varieties and Algorithms*, Springer, 2010.

[6] Ene, V. and Herzog J., *Gröbner bases in Commutative Algebra*, AMS, Providence, Rhode Island, 2012.

[7] Grayson, D. R. and Stillman M. E., `Macaulay2, a software system for research in algebraic geometry`. Available at http://www.math.uiuc.edu/Macaulay2/.

[8] Harris, J., *Algebraic Geometry: A first course*, Springer Verlag, New York, 1992.

[9] Sturmfels, B., *Algorithms in Invariant Theory*, Springer, Berlín, 1993.

Índice alfabético

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE EXAMEN DE GRADO

No. 00220

Matrícula: 2183802308

Bases SAGBI para anillos de coordenadas de Grassmannianas.

Con base en la Legislación de la Universidad Autónoma Metropolitana, en la Ciudad de México se presentaron a las 16:00 horas del día 10 del mes de junio del año 2021 POR VÍA REMOTA ELECTRÓNICA, los suscritos miembros del jurado designado por la Comisión del Posgrado:

DR. PEDRO LUIS DEL ANGEL RODRIGUEZ
DR. ENRIQUE JAVIER ELIZONDO HUERTA
DR. FELIPE DE JESUS ZALDIVAR CRUZ

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron para proceder al Examen de Grado cuya denominación aparece al margen, para la obtención del grado de:

MAESTRO EN CIENCIAS (MATEMÁTICAS)

DE: MAGDIEL DELGADO CASTAÑEDA

y de acuerdo con el artículo 78 fracción III del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Casa abierta al tiempo
DIRECCIÓN DE SISTEMAS ESCOLARES

MAGDIEL DELGADO CASTAÑEDA
ALUMNO

REVISÓ

MTRA. ROSALIA SERRANO DE LA PAZ
DIRECTORA DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JESUS ALBERTO OCHOA TAPIA

PRESIDENTE

DR. PEDRO LUIS DEL ANGEL RODRIGUEZ

VOCAL

DR. ENRIQUE JAVIER ELIZONDO HUERTA

SECRETARIO

DR. FELIPE DE JESUS ZALDIVAR CRUZ