

UNIVERSIDAD DE EL SALVADOR  
FACULTAD MULTIDISCIPLINARIA ORIENTAL  
DEPARTAMENTO DE CIENCIAS NATURALES Y  
MATEMÁTICA  
SECCIÓN DE MATEMÁTICA



**INFORME FINAL DEL CURSO DE ESPECIALIZACIÓN:**  
VARIEDADES TÓRICAS Y ACCIONES DE GRUPOS ALGEBRAICOS

**TÍTULO DEL INFORME FINAL:**  
GRADO MÁXIMO PARA BASES DE GRÖBNER  
DE LOS IDEALES DE GRASSMANN-PLÜCKER

**PARA OPTAR AL GRADO ACADÉMICO DE:**  
LICENCIATURA EN MATEMÁTICA

**PRESENTADO POR:**  
WILL ALEXÁNDER TURCIOS FUENTES N° CARNET TF20001  
ROMEL ADILSON ÁVALOS RAMOS N° CARNET AR20013

**DOCENTE ASESOR:**  
DR. TOBÍAS HUMBERTO MARTÍNEZ LOVO

AGOSTO DE 2025  
SAN MIGUEL, EL SALVADOR, CENTROAMÉRICA

**UNIVERSIDAD DE EL SALVADOR**  
**AUTORIDADES**



**MSC. JUAN ROSA QUINTANILLA**  
**RECTOR**

**DRA. EVELYN BEATRIZ FARFÁN**  
**VICERRECTORA ACADÉMICA**

**MSC. ROGER ARMANDO ARIAS ALVARADO**  
**VICERRECTOR ADMINISTRATIVO**

**LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA**  
**SECRETARIO GENERAL**

**LIC. CARLOS ALMILCAR SERRANO RIVERA**  
**FISCAL GENERAL**

**UNIVERSIDAD DE EL SALVADOR**  
**FACULTAD MULTIDISCIPLINARIA ORIENTAL**  
**AUTORIDADES**



**MSC. CARLOS IVÁN HERNÁNDEZ FRANCO**  
**DECANO**

**DRA. NORMA AZUCENA FLORES RETANA**  
**VICEDECANA**

**LIC. CARLOS DE JESÚS SÁNCHEZ**  
**SECRETARIO**

**ING. DOLORES BENEDICTO SARAVIA MARTÍNEZ**  
**JEFE DEL DEPARTAMENTO DE CIENCIAS NATURALES Y**  
**MATEMÁTICA**

**LIC. SONIA DEL CARMEN MARTÍNEZ DE LÓPEZ**  
**COORDINADORA DEL PROCESO DE GRADO DEL**  
**DEPARTAMENTO DE CIENCIAS NATURALES Y**  
**MATEMÁTICA**

# Índice General

<b>1. Introducción</b>	<b>2</b>
<b>2. Preliminares</b>	<b>3</b>
2.1. Anillos de polinomios . . . . .	3
2.2. Ideales . . . . .	3
2.3. Ordenamientos Admisibles. . . . .	4
2.4. División Multivariantes . . . . .	6
2.5. Teorema de la Base de Hilbert . . . . .	10
2.6. Ideales Tóricos . . . . .	12
2.7. Álgebras A-graduadas . . . . .	13
<b>3. Bases de Gröbner</b>	<b>15</b>
3.1. Bases de Gröbner . . . . .	15
3.2. Algoritmo de Buchberger . . . . .	21
<b>4. Ideales de Grassman-Plücker</b>	<b>26</b>
4.1. El Grasmanniano . . . . .	26
4.2. Las relaciones de Plücker . . . . .	27
<b>5. Grado máximo para cualquier base de Gröbner reducida del ideal de Grassmann-Plücker</b>	<b>31</b>
5.1. El impacto del orden en el grado de las bases de Gröbner del ideal de Plücker	31

## Resumen

Se presenta el problema abierto de describir el grado máximo de una base de Gröbner para los ideales de Grassmann-Plücker, centrándonos en el ideal  $I_{2,s}$ , los cuales describen algebraicamente la Grassmanniana mediante las relaciones de Plücker.

**Palabras claves:** Base de Gröbner, Ideales de Grassmann-Plücker, Algoritmo de Buchberger, Grassmanniana, Relaciones de Plücker.

## Abstract

The open problem of describing the maximum degree of a Gröbner basis for Grassmann-Plücker ideals is presented, focusing on the ideal  $I_{2,s}$ , which algebraically describes the Grassmannian through the Plücker relations.

**Keywords:** Gröbner basis, Grassmann-Plücker ideals, Buchberger algorithm, Grassmannian, Plücker relations.

# 1. Introducción

El estudio de los ideales de Grassmann-Plücker y sus bases de Gröbner representa un tema fundamental en la geometría algebraica y el álgebra computacional. Estos ideales, generados por las relaciones de Plücker, describen algebraicamente la Grassmanniana, una variedad que parametriza los subespacios lineales de dimensión fija en un espacio vectorial. Las bases de Gröbner, por su parte, son herramientas esenciales para analizar la estructura de estos ideales, permitiendo resolver problemas como la pertenencia de polinomios a un ideal o la determinación de soluciones de sistemas de ecuaciones polinomiales.

En este trabajo, nos enfocamos en el estudio del grado máximo de las bases de Gröbner para los ideales de Grassmann-Plücker el cual aún es un problema abierto, con especial atención al caso  $I_{2,s}$ . Este problema no sólo tiene implicaciones teóricas en la comprensión de la estructura algebraica de la Grassmanniana, sino que también es relevante en aplicaciones computacionales, donde el grado de los polinomios en una base de Gröbner afecta directamente la eficiencia de los algoritmos.

El documento está organizado de la siguiente manera: en la Sección 2, se presentan los preliminares necesarios, incluyendo conceptos de anillos de polinomios, ideales y ordenamientos admisibles. La Sección 3 está dedicada a las bases de Gröbner, su construcción mediante el algoritmo de Buchberger y sus propiedades más relevantes. En la Sección 4, se introduce el ideal de Grassmann-Plücker y las relaciones de Plücker que lo definen. Finalmente, en la Sección 5, se aborda el problema central del trabajo: determinar cotas para el grado máximo de los generadores en las bases de Gröbner del ideal  $I_{2,s}$ .

Los resultados obtenidos proporcionan una visión más clara de la estructura algebraica de estos ideales y su relevancia en la representación de subespacios lineales, contribuyendo así al entendimiento de problemas abiertos en el área. Este estudio se enmarca dentro de los esfuerzos por caracterizar la complejidad algebraica de las bases de Gröbner y su relación con las propiedades geométricas de la Grassmanniana.

## 2. Preliminares

### 2.1. Anillos de polinomios

Sea  $K$  un cuerpo, denotemos por  $K[x]$  al anillo de polinomios en  $x$ . Veamos algunas definiciones, lemas y teoremas tomados de [\[Her96\]](#)

**Definición 1.** *Sea  $K$  un cuerpo. Se llaman polinomios de  $n$  variables sobre  $K$  a la suma finita de términos de la forma  $ax_1^{b_1} + x_2^{b_2} + \dots + ax_n^{b_n}$  con  $a \in K$  y  $b_i \in \mathbb{N}, i = 1, \dots, n$ , donde los  $a_i$ , llamados coeficientes del polinomio  $p(x)$ , están en  $K$ . En  $K[x]$  se definen igualdad, suma y producto de dos polinomios.*

**Lema 1.**  *$K[x]$  es un anillo conmutativo con unidad.*

Sea  $p(x)$  un polinomio en una variable  $x$ . Denotemos por  $\text{grd}(p(x))$  al grado del polinomio de  $p(x)$ , es decir, el exponente más alto de la variable  $x$  con coeficiente distinto de cero.

**Lema 2.** *Si  $p(x), q(x)$  son elementos de  $K[x]$  distintos de cero, entonces  $\text{grd}(p(x)q(x)) = \text{grd}(p(x)) + \text{grd}(q(x))$ .*

**Lema 3.**  *$K[x]$  es un dominio integral.*

**Teorema 1.** *Dados los polinomios  $f(x), g(x) \in K[x]$ , donde  $g(x) \neq 0$ , se cumple entonces que*

$$f(x) = q(x)g(x) + r(x),$$

donde  $q(x), r(x) \in K[x]$  y  $r(x) = 0$  o bien  $\text{grd}(r(x)) < \text{grd}(g(x))$ .

**Definición 2.** *Si  $f(x)$  y  $g(x) \neq 0 \in K[x]$ , entonces se dice que  $g(x)$  divide a  $f(x)$ , expresado como  $g(x)|f(x)$ , si  $f(x) = a(x)g(x)$  para algún  $a(x) \in K[x]$ .*

**Lema 4.** *Si  $f(x) \neq 0, g(x) \neq 0 \in K[x]$  y  $g(x)|f(x)$  y  $f(x)|g(x)$ , entonces  $f(x) = ag(x)$ , donde  $a \in K$ .*

### 2.2. Ideales

En el álgebra y geometría algebraica, los ideales son herramientas importantes para hablar de relaciones polinomiales y sirviendo como puente entre estructuras algebraicas y objetos geométricos. A continuación veremos unas definiciones y un lema tomados del libro [\[CLOS97\]](#)

**Definición 3.** Un subconjunto  $I \subseteq K[x_1, \dots, x_n]$  es un ideal si este satisface:

(i)  $0 \in I$ .

(ii) Si  $f, g \in I$ , entonces  $f + g \in I$ .

(iii) Si  $f \in I$  y  $h \in K[x_1, \dots, x_n]$ , entonces  $hf \in I$ .

**Definición 4.** Sea  $f_1, \dots, f_n$  polinomios en  $K[x_1, \dots, x_n]$ . Luego fijamos

$$\langle f_1, \dots, f_n \rangle = \left\{ \sum_{i=1}^s h_i f_i : h_1, \dots, h_s \in K[x_1, \dots, x_n] \right\}$$

El hecho crucial es que  $\langle f_1, \dots, f_n \rangle$  es un ideal.

**Lema 5.** Si  $f_1, \dots, f_s \in K[x_1, \dots, x_n]$ , entonces  $\langle f_1, \dots, f_n \rangle$  es ideal de  $K[x_1, \dots, x_n]$ . Llamaremos a  $\langle f_1, \dots, f_n \rangle$  el ideal generado por  $f_1, \dots, f_s$ .

Ahora por el libro de [Her96](#) podemos dar la siguiente definición de un ideal máximo

**Definición 5.** Un ideal propio  $\mathcal{M}$  de  $\mathcal{R}$  es un ideal máximo de  $\mathcal{R}$  si los únicos ideales de  $\mathcal{R}$  que contienen a  $\mathcal{M}$  son el mismo  $\mathcal{M}$  y  $\mathcal{R}$ .

### 2.3. Ordenamientos Admisibles.

Para estudiar polinomios de múltiples variables, en el contexto algebraico, es necesario establecer un criterio que nos permita comparar monomios entre sí. Esta comparación la logramos establecer haciendo uso de un orden monomial. En lo que sigue, presentaremos definiciones formales y propiedades fundamentales con ejemplos.

**Definición 6.** Un orden monomial  $>$  sobre  $K[x_1, \dots, x_n]$  es una relación  $>$  sobre  $\mathbb{Z}_{\geq 0}^n$ , o una equivalencia, una relación en el conjunto de monomios  $x^\alpha, \alpha \in \mathbb{Z}_{\geq 0}^n$ , satisfaciendo:

(i)  $>$  es un orden total (o lineal) en  $\mathbb{Z}_{\geq 0}^n$ .

(ii) Si  $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$ , entonces  $\alpha + \gamma > \beta + \gamma$ .

(iii)  $>$  es un buen orden en  $\mathbb{Z}_{\geq 0}^n$ . Esto significa que cada subconjunto no vacío tiene un elemento más pequeño bajo  $>$ . En otras palabras, si  $A \subset \mathbb{Z}_{\geq 0}^n$  es no vacío, entonces existe un  $\alpha \in A$  tal que  $\beta > \alpha$  para cada  $\beta \neq \alpha$  en  $A$ .

A continuación, definamos un lema para entender mejor el significado de la condición de buen orden de la Definición 6

**Lema 6.** Una relación de orden  $>$  en  $\mathbb{Z}_{\geq 0}^n$  es un buen orden si y sólo si para cada sucesión estrictamente decreciente en  $\mathbb{Z}_{\geq 0}^n$

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

eventualmente termina.

**Definición 7.** Sea  $\alpha = (\alpha_1, \dots, \alpha_n)$  y  $\beta = (\beta_1, \dots, \beta_n)$  en  $\mathbb{Z}_{\geq 0}^n$ . Diremos  $\alpha >_{lex} \beta$  si la entrada no nula más a la izquierda de la diferencia de vectores  $\alpha - \beta \in \mathbb{Z}^n$  es positiva. Diremos que  $x^\alpha >_{lex} x^\beta$  si  $\alpha >_{lex} \beta$

Ahora, veamos unos ejemplos del orden lexicográfico.

**Ejemplo 1.**  $(1, 2, 0) >_{lex} (0, 3, 4)$ , dado  $\alpha - \beta = (1, -1, -4)$

**Ejemplo 2.** En  $K[x, y, z]$  con el orden  $lex$  7 y donde fijamos  $x > y > z$ , tenemos

$$1 < z < z^2 < z^3 < \dots < y < yz < y^2 < \dots < x < x^2 < x^2y < x^2yz < \dots$$

sin embargo si fijamos  $y < x < z$

$$\begin{aligned} 1 < y < y^2 < y^3 < \dots < x < x^2 < x^2y < \dots \\ < z < yz < x^2yz < z^2 < z^3 < \dots \end{aligned}$$

**Ejemplo 3.** Veamos una forma más concreta de como se aplica este orden  $lex$ , asumiendo que  $x > y$ , y queremos comparar monomios en estas dos variables, por lo que lo primero que debemos hacer es comparar los exponentes de  $x$  y en caso de ser iguales tenemos que comparar los exponentes de  $y$ .

Sean  $p = x^2y^3$  y  $q = x^1y^4$ . Ahora comparemos los exponentes de  $x$ , entonces  $x^2$  vs  $x^1$  y como  $2 > 1$ , podemos decir que  $p >_{lex} q$  y no necesitamos comparar los exponentes de  $y$ , porque denotamos  $x > y$ .

**Definición 8.** Sea  $\alpha$  y  $\beta$ , como en la Definición 7. Si

$$|\alpha| = \sum_{i=1}^n a_i > |\beta| = \sum_{i=1}^n b_i$$

o

$$|\alpha| = |\beta| \text{ y } \alpha >_{lex} \beta,$$

entonces, diremos  $\alpha >_{grlex} \beta$ .  $|\alpha|$  se denota como el grado total.

**Ejemplo 4.** Dado  $x^4y^7z >_{grlex} x^4y^2z^3$ , entonces  $|(4, 7, 1)| = 12 > 9 = |(4, 2, 3)|$

**Ejemplo 5.** En  $K[x, y, z]$  con el orden  $grlex$  8 y donde fijamos  $z < y < x$ , tenemos

$$1 < z < y < x < z^2 < y^2 < x^2 < \dots < xy^2 < xy^2z < \dots < x^4 < \dots$$

sin embargo si fijamos  $y < x < z$

$$1 < x < y < z < y^2 < x^3 < x^2y < z^3 < z^4 < xy^3 < x^2yz < \dots$$

**Ejemplo 6.** Para ver un ejemplo en concreto del orden  $grlex$ , tomemos los mismos monomios definidos en el Ejemplos 3, es decir,  $p = x^2y^3$  y  $q = x^1y^4$ , tomando a  $x > y$ , y vamos a comparar estos dos monomios, por lo que lo primero que haremos será comparar el grado total (suma de exponentes). Si empatan usaremos el orden  $lex$

Haciendo la comparación del grado total tenemos  $p = x^2y^3 = 5 = x^1y^4 = q$ , dado que ambos tiene grado total 5, pasamos al orden  $lex$ , pero ya sabemos que  $p >_{lex} q$ , por lo que  $p >_{grlex} q$ .

Ahora bien, si los grados totales fueran diferentes, el mayor grado gana, por ejemplo,  $x^3 >_{grlex} x^1y^4$  porque  $3 > 5$  es falso, pero  $3 < 5$ , entonces  $x^3 <_{grlex} x^1y^4$

**Definición 9.** Sea  $f = \sum_{\alpha} a_{\alpha}x^{\alpha} = a_1x^{\alpha_1} + a_2x^{\alpha_2} + \dots + a_{n-1}x^{\alpha_{n-1}} + a_nx^{\alpha_n}$  un polinomio no cero en  $K[x_1, \dots, x_n]$  y sea  $>$  un orden monomial:

- (i)  $\text{multigrado}(f) = \max(\alpha \in \mathbb{Z}_{\geq 0}^n : a_{\alpha} \neq 0)$ , el multigrado de  $f$ . (El máximo esta dado con respecto a  $>$ )

(ii)  $LT(f) = a_1x^{\alpha_1}$ , el término líder de  $f$ .

(iii)  $LM(f) = x^{\alpha_1}$ , el producto de potencias líderes de  $f$ .

(iv)  $LC(f) = a_1$ , el coeficiente líder de  $f$ .

**Ejemplo 7.** Sea  $f = 2x^2y^2z^3 + x^6 + 7y^5z - 3xy \in \mathbb{R}[x, y, z]$ , donde fijamos el orden  $x > y > z$  en las variables. Utilizando el orden *lex*, tenemos que el polinomio  $f$  ordenado es  $x^6 + 2x^2y^2z^3 - 3xy + 7y^5z$

- $\text{multigrado}(f) = 6$ , el multigrado de  $f$ .
- $LT(f) = x^6$ , el término principal de  $f$ .
- $LM(f) = x^6$ , el producto de potencias principales de  $f$ .
- $LC(f) = 1$ , el coeficiente principal de  $f$ .

## 2.4. División Multivariables

En Anillos de polinomios realizamos una división entre polinomios con una única variable  $x$ . Para explorar este problema cuando hay más variables, necesitaremos formular el algoritmo de división polinomial en  $K[x_1, \dots, x_n]$  que extiende el algoritmo para  $K[x]$ .

El objetivo es dividir  $f \in K[x_1, \dots, x_n]$  entre  $f_1, f_2, \dots, f_s \in K[x_1, \dots, x_n]$ , en otras palabras expresaremos a  $f$  como:

$$f = q_1f_1 + \dots + q_sf_s + r,$$

donde los cocientes  $q_1, \dots, q_s$  y el residuo  $r$  están en  $K[x_1, \dots, x_n]$ .

Aquí tendremos cuidado al decidir cómo podemos describir el resto  $r \in K[x_1, \dots, x_n]$ , para este propósito utilizaremos los ordenamientos Admisibles anteriormente visto en [2.3](#). La idea básica del algoritmo es la misma que en el caso de una variable: Cancelar el término principal de  $f$  con respecto a un orden monomial fijo multiplicando por algún  $f_i$  por un monomio apropiado y restando. Entonces este monomio se convierte en un término correspondiente  $q_i$ .

**Teorema 2.** Sea  $>$  un orden monomial en  $\mathbb{Z}_{\geq 0}^n$ , y sea  $F = (f_1, \dots, f_s)$  una  $s$ -tupla ordenada de polinomios en  $K[x_1, \dots, x_n]$ . Entonces cada  $f \in K[x_1, \dots, x_n]$  se puede escribir como

$$f = q_1f_1 + \dots + q_sf_s + r,$$

donde  $q_i, r \in K[x_1, \dots, x_n]$ , y  $r = 0$  o  $r$  es una combinación lineal con coeficientes en  $K$  de monomios donde ninguno es divisible por  $LT(f_1), \dots, LT(f_s)$ . Llamamos a  $r$  un residuo de  $f$  en la división por  $F$ . Además, si  $q_i f_i \neq 0$ , entonces

$$\text{multigrado}(f) > \text{multigrado}(q_i f_i).$$

**Demostración.** Demostremos la existencia de  $q_1, \dots, q_s$  y  $r$  dando un algoritmo para su construcción y demostrando que funciona correctamente con cualquier entrada dada.

---

**Algorithm 1** División de un polinomio entre varios

---

**Require:**  $f_1, \dots, f_s, f$

**Ensure:**  $q_1, \dots, q_s, r$

```

1:  $q_1 := 0; \dots; q_s := 0$ 
2:  $r := 0$ 
3:  $p := f$ 
4: while  $p \neq 0$  do
5:    $i := 1$ 
6:   divisionoccurred := false
7:   while  $i \leq s$  and divisionoccurred = false do
8:     if  $LT(f_i)$  divide  $LT(p)$  then
9:        $q_i := q_i + LT(p)/LT(f_i)$ 
10:       $p := p - (LT(p)/LT(f_i))f_i$ 
11:      divisionoccurred := true
12:     else
13:        $i := i + 1$ 
14:     end if
15:   end while
16:   if divisionoccurred = false then
17:      $r := r + LT(p)$ 
18:      $p := p - LT(p)$ 
19:   end if
20: end while
21: return  $q_1, \dots, q_s, r$ 

```

---

Podemos relacionar que la variable  $p$  representa el dividendo, la variable  $r$  representa el residuo y las variables  $q_1, \dots, q_s$  son los cocientes enumerados. La variable booleana **divisionoccurred** indica si algún  $LT(f_i)$  divide el término principal del dividendo, lo cual se comprueba en cada iteración del ciclo principal.

**Paso 1 (División):** Si algún  $LT(f_i)$  divide a  $LT(p)$ , el algoritmo realiza la división correspondiente.

**Paso 2 (Residuo):** Si ningún  $LT(f_i)$  divide a  $LT(p)$ , entonces el algoritmo agrega  $LT(p)$  al residuo  $r$ .

Para demostrar que el algoritmo funciona, primero mostramos que

$$f = q_1f_1 + \dots + q_sf_s + p + r, \quad (1)$$

se mantiene en cada etapa. Esto es claramente cierto al inicio con los valores iniciales de  $q_i$ ,  $p$  y  $r$ .

Supongamos que la ecuación (1) se mantiene en un paso. Si el siguiente paso es de división, entonces

$$q_if_i + p = (q_i + LT(p)/LT(f_i))f_i + \left(p - \frac{LT(p)}{LT(f_i)}f_i\right),$$

lo que conserva la igualdad en la ecuación (1). Si el paso es de residuo, entonces

$$p + r = (p - LT(p)) + (r + LT(p)),$$

de modo que la igualdad en (1) también se conserva.

El algoritmo se detiene cuando  $p = 0$ , en cuyo caso la ecuación (1) se convierte en

$$f = q_1f_1 + \dots + q_sf_s + r.$$

Dado que los términos se añaden a  $r$  solo cuando no son divisibles por ninguno de los  $LT(f_i)$ , se deduce que  $q_i$  y  $r$  tienen las propiedades deseadas.

Para probar que el algoritmo termina, notamos que en cada paso el multigrado de  $p$  disminuye o se hace cero. Si nunca terminara, obtendríamos una secuencia infinita decreciente de multigrados, lo cual contradice la propiedad de buen orden del orden monomial (Lema 6).

Finalmente, para justificar que  $\text{multigrado}(q_if_i) < \text{multigrado}(f)$  cuando  $q_if_i \neq 0$ , recordamos que cada término en  $q_i$  proviene de divisiones de  $LT(p)$ , y que  $p$  comienza siendo  $f$  y su multigrado disminuye en cada paso. Así se deduce fácilmente que  $\text{multigrado}(q_if_i) \leq \text{multigrado}(f)$  y en particular, si  $q_if_i \neq 0$ , entonces  $\text{multigrado}(q_if_i) < \text{multigrado}(f)$ .

Esto completa la demostración del teorema. ■

Para observar esto de manera mas sencilla realizaremos un ejemplo

**Ejemplo 8.** *Primero dividiremos  $f = x^2yz - y^2$  entre  $f_1 = xy^2 + y^2$  y  $f_2 = xz + y$ , usando el orden lex con  $x > y > z$ . Queremos emplear el mismo*

esquema que para la división de polinomios de una variable, con la diferencia de que ahora hay varios divisores y cocientes. Enumerando los divisores  $f_1, f_2$  y los cocientes  $q_1, q_2$  verticalmente, tenemos la siguiente:

$$x^2yz - y^2 \left| \begin{array}{l} xz + y \\ \hline xy^2 + y^2 \\ q_1 : \\ q_2 : \end{array} \right.$$

El término  $LT(f_2) = xz$  divide al término principal  $LT(f) = x^2yz$ . Por lo tanto, dividimos  $x^2yz$  entre  $xz$ , dejando  $xy$ , y luego restamos  $xy \cdot f_2$  de  $f$ :

$$\begin{array}{r} x^2yz - y^2 \left| \begin{array}{l} xz + y \\ \hline xy^2 + y^2 \\ q_1 : \\ q_2 : xy \end{array} \right. \\ -x^2yz - xy^2 \\ \hline -xy^2 - y^2 \end{array}$$

Ahora repetimos el mismo proceso en  $-xy^2 - y^2$ , esta vez debemos usar  $f_1$  ya que  $LT(f_2) = xz$  no divide a  $LT(-xy^2 - y^2) = -xy^2$ . Obteniendo:

$$\begin{array}{r} x^2yz - y^2 \left| \begin{array}{l} xz + y \\ \hline xy^2 + y^2 \\ q_1 : -1 \\ q_2 : xy \end{array} \right. \\ -x^2yz - xy^2 \\ \hline -xy^2 - y^2 \\ +xy^2 + y^2 \\ \hline 0 \end{array}$$

Notemos que en este ejemplo  $r = 0$ . Por lo tanto hemos escrito  $f = x^2yz - y^2$  en la forma

$$x^2yz - y^2 = (-1)(xy^2 + y^2) + (xy)(xz + y).$$

Pero a diferencia de la división en una variables podremos encontrar algunas sutilezas inesperadas al tratar de dividir polinomios de mas de una variables, a modo de comprender esto haremos el ejemplo [9](#)

**Ejemplo 9.** Dividamos  $x^2y + xy^2 + y^2$  entre  $f_1 = xy - 1$  y  $f_2 = y^2 - 1$  usando el orden  $lex$   $x > y$ , los dos primeros pasos del algoritmo se desarrollan como de costumbre, lo que nos da la siguiente división parcialmente completada:

$$\begin{array}{r}
 x^2y + xy^2 + y^2 \left| \begin{array}{l} y^2 - 1 \\ xy - 1 \end{array} \right. \\
 \underline{-x^2y + x} \quad \begin{array}{l} q_1 : x + y \\ q_2 : \end{array} \\
 xy^2 + x + y^2 \\
 \underline{-xy^2 + y} \\
 x + y^2 + y
 \end{array}$$

Tenga en cuenta que ni  $LT(f_1) = xy$  ni  $LT(f_2) = y^2$  dividen a  $LT(x + y^2 + y) = x$ . Sin embargo,  $x + y^2 + y$  no es el resto, ya que  $LT(f_2)$  divide a  $y^2$ . Por lo tanto, si movemos  $x$  al resto, podemos continuar dividiendo. (Esto es algo que nunca sucede en el caso de una variable: una vez que el término principal del divisor ya no divide al término principal de lo que está al final de la división, el algoritmo termina). Para implementar esta idea, creamos una columna de resto  $r$ , a la derecha de la división, donde colocamos los términos que pertenecen al resto. Además, llamamos *dividendo intermedio* al polinomio al final de la división. Luego, continuamos dividiendo hasta que el dividendo intermedio sea cero. Este es el siguiente paso, donde movemos  $x$  a la columna de resto:

$$\begin{array}{r}
 x^2y + xy^2 + y^2 \left| \begin{array}{l} y^2 - 1 \\ xy - 1 \end{array} \right. \quad \begin{array}{l} r \\ \hline \end{array} \\
 \underline{-x^2y + x} \quad \begin{array}{l} q_1 : x + y \\ q_2 : \end{array} \\
 xy^2 + x + y^2 \\
 \underline{-xy^2 + y} \\
 x + y^2 + y \\
 y^2 + y \longrightarrow \quad x
 \end{array}$$

Ahora continuamos dividiendo.

Obteniendo:

$$\begin{array}{r}
x^2y + xy^2 + y^2 \left| \begin{array}{l} y^2 - 1 \\ xy - 1 \end{array} \right. \quad \frac{r}{\phantom{r}} \\
\hline
-x^2y + x \quad \begin{array}{l} q_1 : x + y \\ q_2 : 1 \end{array} \\
\hline
xy^2 + x + y^2 \\
\hline
-xy^2 + y \\
\hline
x + y^2 + y \\
\hline
y^2 + y \longrightarrow \phantom{x} \\
\hline
-y^2 + 1 \\
\hline
y + 1 \longrightarrow x + y + 1
\end{array}$$

Así el resto es  $x + y + 1$  y obtenemos:

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

Teniendo esto en cuenta ahora veremos algunas definiciones.

**Definición 10.** Sean  $f, g, h \in K[x_1, \dots, x_n]$  con  $g \neq 0$ , decimos que  $f$  es reducible en  $h$  módulo  $g$  en un paso y lo podemos denotar por

$$f \xrightarrow{g} h$$

si  $LM(g)$  divide a un término  $a_{\alpha_i}x^{\alpha_i}$ , con  $a_{\alpha_i} \neq 0 \in K$ , de  $f$  y se cumple

$$h = f - \frac{ax}{lt(g)}g.$$

**Definición 11.** Sean  $f, h$  y  $f_1, \dots, f_s \in K[x_1, \dots, x_n]$  con  $f_i \neq 0$  y sea  $F = \{f_1, \dots, f_n\}$  diremos que  $f$  es reducible en  $h$  módulo  $F$  y lo podemos denotar por

$$f \xrightarrow{F} h$$

si existe una secuencia de índices  $i_1, \dots, i_t \in \{1, \dots, s\}$  y una secuencia de polinomios  $h_1, \dots, h_{t-1} \in K_n[x_1, \dots, x_n]$  tal que

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \dots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

**Definición 12.** Decimos que un polinomio  $r$  está reducido respecto de  $F = \{f_1, \dots, f_n\}$  si no es reducible por  $F$ .

**Definición 13.** Si  $f \xrightarrow{F}_+ r$  y  $r$  está reducido respecto de  $F$ , se llama a  $r$  el resto de  $f$  respecto de  $F$ .

## 2.5. Teorema de la Base de Hilbert

Uno de los resultados más importantes en la geometría algebraica, es el Teorema de la Base de Hilbert, a grosso modo dice que aunque un ideal tenga infinitos polinomios, siempre existe un número finito de ellos a partir de los cuales se puede obtener todos los demás mediante combinaciones lineales con coeficientes en el anillo. Su relevancia se vuelve mayor en el estudio de las Bases de Gröbner, pues el teorema asegura que existe una base finita adecuada para describir cualquier ideal, por lo que este teorema no es solo una partida lógica, sino una piedra angular que posibilita y justifica el desarrollo del enfoque algorítmico que caracteriza el estudio de las bases de Gröbner, tema que se abordará en el capítulo 3.

Antes de enunciar este teorema de manera formal, empecemos por definir el ideal de términos principales, de la siguiente manera.

**Definición 14.** Sea  $I \subseteq K[x_1, \dots, x_n]$  un ideal distinto de  $\{0\}$  y fijemos un orden monomial sobre  $K[x_1, \dots, x_n]$ , entonces:

(i) Denotemos por  $LT(I)$  el conjunto de términos principales de los elementos no cero de  $I$ . Entonces,

$$LT(I) = \{cx^\alpha : \exists f \in I - \{0\}, LT(f) = cx^\alpha\}$$

(ii) Denotamos por  $\langle LT(I) \rangle$  el ideal generado por los elementos de  $LT(I)$ .

Antes de dar el siguiente resultado clave en esta sección, es necesario dar dos resultados previos, sobre los ideales monomiales.

**Definición 15.** Un ideal  $I \subseteq K[x_1, \dots, x_n]$  es un ideal monomial si existe un subconjunto  $A \subseteq \mathbb{Z}_{\geq 0}^n$  (podría ser infinito) tal que  $I$  consiste de todos los polinomios que se pueden expresar como una suma finita, de la siguiente forma  $\sum_{\alpha \in A} h_\alpha x^\alpha \in K[x_1, \dots, x_n]$ , en este caso escribiremos  $I = \langle x^\alpha : \alpha \in A \rangle$ .

**Lema 7.** Sea  $I = \langle x^\alpha : \alpha \in A \rangle$  un ideal monomial. Entonces, un monomio  $x^\beta$  vive en  $I$  si y sólo si  $x^\beta$  es divisible por  $x^\alpha$  para cada  $\alpha \in A$ .

**Proposición 1.** Sea  $I \subseteq K[x_1, \dots, x_n]$  un ideal diferente de  $\{0\}$ .

(i)  $\langle LT(I) \rangle$ , es un ideal monomial.

(ii) Existen  $g_1, \dots, g_t \in I$  tal que  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ .

Ahora bien, con la Proposición 1 y el algoritmo de la división multivariable, podemos asegurar la existencia de un conjunto generador finito de cada ideal polinomial, dando así el origen al Teorema de la Base de Hilbert.

**Teorema 3.** *Todo ideal  $I \in K[x_1, \dots, x_n]$  tiene un conjunto finitamente generador. En otras palabras  $I = \langle g_1, \dots, g_t \rangle$ , para algún  $g_1, \dots, g_t \in I$*

**Teorema 4.** *Sea*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

*una cadena ascendente de ideales en  $K[x_1, \dots, x_n]$ . Entonces, existe un  $N \geq 1$  tal que*

$$I_N = I_{N+1} = I_{N+2} = \dots$$

**Teorema 5.** *Cada ideal  $I \subseteq K[x_1, \dots, x_n]$ , tiene una cantidad finita de ideales de términos principales, distintos.*

Motivados por el Teorema de la Base de Hilbert 3, podemos introducir los siguientes dos resultados, en el sentido geométrico.

**Definición 16.** *Sea  $I \subseteq K[x_1, \dots, x_n]$  un ideal. Nosotros denotamos por  $V(I)$  el conjunto*

$$V(I) = \{(a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0 \quad \forall f \in I\}$$

**Proposición 2.**  *$V(I)$  es una variedad afín. En particular, si  $I = \langle f_1, \dots, f_n \rangle$  entonces,  $V(I) = V(f_1, \dots, f_n)$ .*

**Definición 17.** *Sea  $V \subseteq K^n$  una variedad algebraica. Entonces el conjunto*

$$I(V) = \{f \in K[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0, \forall (a_1, \dots, a_n) \in V\},$$

*es un ideal.*

**Lema 8.** *Sea  $V \subseteq K^n$  una variedad afín, entonces  $I(V)$  es un ideal. Llamaremos a  $I(V)$  el ideal de  $V$ .*

## 2.6. Ideales Tóricos

En esta sección estudiaremos un tipo especial de ideales en  $K[x] := K[x_1, \dots, x_n]$ . Fijemos un subconjunto  $\mathcal{A} = \{a_1, \dots, a_n\}$  de  $\mathbb{Z}^d$ . Cada vector  $a_i$  esta identificado con un monomio  $t^{a_i}$  en el polinomio de Laurent, en el anillo  $K[t^{\pm 1}] := K[t_1, \dots, t_n, t_1^{-1}, \dots, t_d^{-1}]$ . Consideremos el semigrupo de homomorfismos

$$\pi : \mathbb{N}^n \rightarrow \mathbb{Z}^d, \quad u = (u_1, \dots, u_n) \mapsto u_1 a_1 + \dots + u_n a_n.$$

La imagen de  $\pi$  es el semigrupo

$$\mathbb{N}\mathcal{A} = \{\lambda_1 a_1 + \dots + \lambda_n a_n : \lambda_1, \dots, \lambda_n \in \mathbb{N}\}.$$

El mapeo  $\pi$  es un homomorfismo de álgebras de semigrupo:

$$\hat{\pi} : K[x] \rightarrow K[t^{\pm 1}], \quad x_i \mapsto t^{a_i}.$$

El kernel de  $\hat{\pi}$  es denotado por  $I_{\mathcal{A}}$  y lo llamaremos el ideal tórico de  $\mathcal{A}$  y claramente  $I_{\mathcal{A}}$  es un ideal primo por lo que  $V(I_{\mathcal{A}})$  es una variedad afín irreducible de ceros en  $K^n$ .

**Lema 9.** *Todo ideal tórico  $I_{\mathcal{A}}$  es generado como un  $k$ -espacio vectorial por el conjunto de binomios*

$$\{x^u - x^v : u, v \in \mathbb{N}^n \text{ con } \pi(u) = \pi(v)\}.$$

Calculemos la dimensión de la variedad tórica  $V(I_{\mathcal{A}})$ . Escribiremos  $\mathbb{Z}\mathcal{A}$  para el látice generado por  $\mathcal{A}$  y  $\dim(\mathcal{A})$  para la detención de  $\mathbb{Z}\mathcal{A}$ .

Cada vector  $u \in \mathbb{Z}^n$  puede escribirse de manera única como  $u = u^+ - u^-$  donde  $u^+ - u^-$  son no negativos y tiene soporte disjuntos (en otras palabras, el conjunto de índices distintos de cero son disjuntos). Escribiremos como  $\ker(\pi)$  al sublátice de  $\mathbb{Z}^n$  que consisten de todos los vectores  $u$  tal que  $\pi(u^+) = \pi(u^-)$  y el Lema 9 podemos escribirlo de la siguiente manera.

**Corolario 1.**  $I_{\mathcal{A}} = \langle x^{u^+} - x^{u^-} : u \in \ker(\pi) \rangle$ .

**Corolario 2.** *Para cada orden de término  $<$ , existe un conjunto finito de vectores  $G_{<} \subset \ker(\pi)$  tal que la base reducida de Gröbner de  $I_{\mathcal{A}}$  con respecto a  $<$  es igual a  $\{x^{u^+} - x^{u^-} : u \in G_{<}\}$ .*

**Proposición 3.** *Para cada conjunto finito  $\mathcal{A} \subset \mathbb{Z}^d$  tenemos que  $\mathcal{C}_{\mathcal{A}} \subseteq \mathcal{U}_{\mathcal{A}} \subseteq Gr_{\mathcal{A}}$ .*

Aclaremos que  $\mathcal{C}_{\mathcal{A}}$  es el conjunto de los circuitos de  $I_{\mathcal{A}}$ ,  $\mathcal{U}_{\mathcal{A}}$  es la base universal de Gröbner (definida posteriormente en la Definición 19) de  $\mathcal{A}$  y  $Gr_{\mathcal{A}}$  es la base de Graver, que es el conjunto de binomios primitivos de una base de Gröbner de  $\mathcal{A}$ .

**Corolario 3.** *El ideal tórico  $I_{\mathcal{A}_{2,s}}$ , tiene las siguientes propiedades*

(a) *El conjunto de circuitos es igual a la base universal de Gröbner:*

$$[i_1 j_1][i_2 j_2] \cdots [i_v j_v] - [i_2 j_1][i_3 j_2] \cdots [i_1 j_v],$$

$$i_1, i_2 < j_1 \text{ y } i_2, i_3 < j_2 \text{ y } \dots \text{ y } i_v i_1 < j_v.$$

(b) *todo ideal inicial de  $I_{\mathcal{A}_{2,s}}$  es libre de cuadrados.*

Ahora, damos un algoritmo para encontrar la primera base de Gröbner de un ideal, diferente al algoritmo de Buchberger:

---

**Algorithm 2** Cálculo de una primera base de Gröbner de un ideal tórico

---

**Require:**  $n, d$ , puntos  $a_i$  para  $i = 1, \dots, n$

**Ensure:**  $\mathcal{G} \cap k[\mathbf{x}]$

- 1:  $T := \{t_0, t_1, \dots, t_d\}$  ▷ Variables auxiliares
- 2:  $X := \{x_1, \dots, x_n\}$  ▷ Variables originales
- 3: Elegir un orden de eliminación tal que  $T \succ X$
- 4: Definir el ideal  $I$  generado por:

$$I := \langle t_0 t_1 \cdots t_d - 1, x_1 \cdot \mathbf{t}^{a_1^-} - \mathbf{t}^{a_1^+}, \dots, x_n \cdot \mathbf{t}^{a_n^-} - \mathbf{t}^{a_n^+} \rangle$$

- 5:  $\mathcal{G} :=$  base de Gröbner reducida de  $I$  con respecto al orden elegido
  - 6:  $\mathcal{G}_{\text{red}} := \mathcal{G} \cap k[\mathbf{x}]$
  - 7: **return**  $\mathcal{G}_{\text{red}}$
- 

## 2.7. Álgebras A-graduadas

Sea  $\mathcal{A} = \{a_1, \dots, a_n\}$  un subconjunto de  $\mathbb{N}^d / \{0\}$ ,  $d = \dim(\mathcal{A})$ , y sea  $\mathbb{N}\mathcal{A}$  que denota el sub-semigrupo de  $\mathbb{N}^d$  generado por  $\mathcal{A}$ . Una álgebra A-

graduada, es una  $k$ -álgebra  $\mathbb{N}^d$ -graduada  $R = \bigoplus_b R_b$  con generadores homogéneos  $X_1, \dots, X_n$  con grados  $a_1, \dots, a_n$  tal que

$$\dim_K(R_b) = \begin{cases} 1 & \text{si } b \in \mathbb{N}\mathcal{A} \\ 0 & \text{en caso contrario} \end{cases} \quad \text{para todo } b \in \mathbb{N}^d.$$

Toda álgebra  $A$ -graduada  $\mathcal{R}$  tiene una presentación como un cociente de anillo de polinomios

$$0 \rightarrow I \rightarrow K[x] = K[x_1, \dots, x_n] \rightarrow \mathcal{R} \rightarrow 0.$$

La representación del ideal  $I = \ker(x_i \mapsto X_i)$  es llamado  $A$ -graduado. Es fácil notar que un ideal  $A$ -graduado  $I$  es generado por polinomios con máximo de dos término, es decir,  $I$  es un ideal binomial. El paradigma de una álgebra  $A$ -graduada es el semigrupo algebraico

$$K[\mathbb{N}\mathcal{A}] = K[t^{a_1}, \dots, t^{a_n}] = K[x]/I_{\mathcal{A}},$$

donde  $I_{\mathcal{A}}$  es un ideal tórico.

Dos álgebras  $A$ -graduadas  $\mathcal{R} = K[x]/I$  y  $\mathcal{R}' = K[x]/I'$  son isomorfas si existe un isomorfismo de álgebras graduadas de grado cero. Esto se cumple y sólo si para el correspondiente ideal  $I$  e  $I' \in K[x]$ , existe  $\lambda = (\lambda_1, \dots, \lambda_n) \in (K^*)^n$  tal que

$$I' = \lambda \cdot I := \{f(\lambda_1 x_1, \dots, \lambda_n x_n) : f \in I\}.$$

La teoría de las bases de Gröbner sugiere “pasar el límite tórico” como sigue:

Si  $I$  es un ideal  $A$ -graduado en  $K[x]$  y  $\omega \in \mathbb{Z}^n$ , entonces el ideal inicial  $LT_{\omega}(I)$  es  $A$ -graduado.

Llamaremos una álgebra  $A$ -graduada  $\mathcal{R} = K[x]/I$  coherente si existe  $\omega \in \mathbb{Z}^n$  tal que  $I$  es isomorfo a  $LT_{\omega}(I_{\mathcal{A}})$ .

**Lema 10.** *El grado de cada generador mínimo de un ideal  $A$ -graduado es un Graver grado.*

**Corolario 4.** *Sea  $d = 1$  y  $\mathcal{A} = \{a_1, < a_2 < \dots < a_n\} \subset \mathbb{N}$ . Entonces cada generador mínimo de un ideal  $A$ -graduado tiene grado como máximo  $a_{n-1} \cdot a_n$ .*

### 3. Bases de Gröbner

En el estudio de ideales de anillos de polinomios, especialmente en varias variables, surge la necesidad de encontrar representaciones que permitan trabajar de forma efectiva en dichos ideales. Una de las herramientas más poderosas desarrolladas para este propósito son las bases de Gröbner. Esta herramienta permiten generalizar el algoritmo de la división de una variable al caso multivariable y proporcionan métodos algorítmicos para resolver distintos problemas fundamentales de álgebra, tales como la pertenencia de un polinomio a un ideal, definir si dos ideales son iguales, resolución de ecuaciones no lineales y también sobre el problema abierto del ideal de Grassmann-Plücker, el cual estudiaremos en una de las secciones posteriores.

#### 3.1. Bases de Gröbner

Las bases de Gröbner, transforman los ideales en estructuras más manejables ya que trabajamos con representantes únicos de los elementos del ideal. Sin embargo, la construcción de estas bases dependen fuertemente de orden monomial elegido, siendo el orden lexicográfico y orden grado lexicográfico los usados en nuestro caso. En esta sección introduciremos la definición formal de una base de Gröbner y ejemplos que permitan comprender su utilidad y funcionamiento. Esta herramienta será importante en el desarrollo posterior, en el estudio del ideal de Grassmann-Plücker, donde su uso será muy importante para definir su estructura algebraica.

Habiendo introducido la teoría previa necesaria, ya contamos con las herramientas necesarias para introducir el concepto formal de base de Gröbner.

**Definición 18.** *Fijemos un orden monomial en el anillo de polinomios  $K[x_1, \dots, x_n]$ . Un subconjunto finito  $G = \{g_1, \dots, g_t\}$  de un ideal  $I \subseteq K[x_1, \dots, x_n]$  diferente de  $\{0\}$ , diremos que es una base de Gröbner, si*

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle.$$

*Usando la analogía  $\langle \emptyset \rangle$ , decimos que  $\emptyset$  es la base de Gröbner, del ideal  $\{0\}$*

Equivalentemente, pero manera más informal, el conjunto  $\{g_1, \dots, g_t\} \subseteq I$  es una base de Gröbner de  $I$  si y sólo si el término principal de cualquier elemento de  $I$ , es divisible por uno de los  $LT(g_i)$ . Esto se sigue del Lema 7.

**Corolario 5.** *Fijemos un orden monomial. Entonces, cada ideal  $I \subseteq K[x_1, \dots, x_n]$ , tiene una base de Gröbner. Además, cualquier base de Gröbner de un ideal  $I$  es una base para  $I$ .*

**Demostración.** Tomemos un ideal  $I$  no cero y sea  $G = \{g_1, \dots, g_t\}$  los generadores de  $I$ . Definiendo un orden monomial y el algoritmo de la división, entonces  $I$  es un ideal de términos principales  $\langle LT(I) \rangle$ . Por Proposición [1](#), existen  $g_1, \dots, g_t \in I$  tal que  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$  y ahora, por el Teorema [3](#), tenemos que  $I = \langle g_1, \dots, g_t \rangle$ . Además, es claro que  $\langle g_1, \dots, g_t \rangle \subseteq I$  dado  $g_i \in I$ , entonces, por Definición [18](#),  $G$  es una base de Gröbner. Ahora, para la segunda afirmación, notemos que  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ , y ya se vio que  $I = \langle g_1, \dots, g_t \rangle$ , por lo que  $G$ , es una base para  $I$ . ■

**Ejemplo 10.** *Consideremos el ideal  $J = \langle g_1, g_2 \rangle = \langle x+z, y-z \rangle$  y afirmamos que  $g_1$  y  $g_2$  forman una base Gröbner, usando el orden *lex* (lexicográfico)  $x > y > z$  en  $\mathbb{R}[x, y, z]$ .*

*Demostremos que el término principal de todo elemento de  $J$  no cero, vive en el ideal  $\langle LT(g_1), LT(g_2) \rangle = \langle x, y \rangle$ . Por le Lema [7](#), esto es equivalente a demostrar que el término líder de cada elemento no cero de  $J$  es divisible por  $x$  o  $y$ .*

*Tomemos a  $f = Ag_1 + Bg_2 \in J$ . Actuemos por contradicción, supongamos que  $f$  es no cero y que el  $LT(f)$  no es divisible ni por  $x$  ni por  $y$ . Entonces, por definición de orden lexicográfico,  $f$  debe ser un polinomio solo en  $z$  pero  $f$  se anula en el espacio lineal  $L = V(x+z, y-z) \subseteq \mathbb{R}^3$  dado  $f \in J$ . Es fácil notar que  $(x, y, z) = (-t, t, t) \in L$  para cada número real  $t$ . El único polinomio solo en  $z$  que se anula en todos estos puntos es el polinomio cero, y esto es una contradicción. Por lo que  $\{g_1, g_2\}$  es una base de Gröbner para  $J$ .*

En la siguiente sección nos encontraremos con una forma mecánica para saber si una base forma una base de Gröbner, por ahora, seguiremos estudiando más propiedades.

Motivados por el Teorema [5](#) y usando el libro [\[Stu96\]](#) nos permitimos dar la siguiente definición seguido de un corolario sobre las Bases de Gröbner finitas:

**Definición 19.** *Un subconjunto finito  $\mathcal{U} \subseteq I$  es llamado Base Universal de Gröbner si  $\mathcal{U}$  es una base de Gröbner de  $I$  con respecto a todos los órdenes monomiales  $<$  simultáneamente.*

**Corolario 6.** *Todo ideal  $I \subseteq K[x_1, \dots, x_n]$  posee una base universal  $\mathcal{U}$  finita.*

**Demostración.** Por el Teorema 5 existen solo una cantidad finita de bases de Gröbner distintas. Entonces su unión  $\mathcal{U}$  es finita, siendo esta una base universal de Gröbner. ■

Habiendo estudiado como es que el algoritmo de la división se aplica en el contexto de polinomios en  $K[x_1, \dots, x_n]$ , veamos una propiedad interesante en las bases de Gröbner, y es la existencia y unicidad del residuo al dividir un polinomio por una base de Gröbner, en la siguiente Proposición.

**Proposición 4.** *Sea  $I \subseteq K[x_1, \dots, x_n]$  un ideal y sea  $G = \{g_1, \dots, g_t\}$  una base de Gröbner para  $I$ . Dado  $f \in K[x_1, \dots, x_n]$ , entonces, existe un único  $r \in K[x_1, \dots, x_n]$ , que cumple las siguientes dos propiedades:*

- (i) *Ningún término de  $r$  es divisible por cada  $LT(g_1), \dots, LT(g_t)$ .*
- (ii) *Existe  $g \in I$  tal que  $f = g + r$ .*

*Es decir,  $r$  es el residuo de dividir  $f$  entre  $G$ , sin importar como se enumeren los elementos de  $G$  cuando se utilice el algoritmo de la división.*

**Demostración.** Notemos que por el algoritmo de la división, si tomamos a  $f = q_1g_1 + \dots + q_tg_t + r$ , donde  $r$  satisface la primera condición. También podemos satisfacer la segunda condición, tomando a  $g = q_1g_1 + \dots + q_tg_t \in I$ . Con esto, demostramos la existencia de  $r$ .

Ahora, para demostrar la unicidad, supongamos que  $f = g + r = g' + r'$  satisfaciendo la primera y segunda condición, por lo que tenemos que  $r - r' = g' - g \in I$ , si  $r \neq r'$ , tendremos que  $LT(r - r') \in \langle LT(g_1), \dots, LT(g_t) \rangle$ . Por Lema 7 se sigue que  $LT(r - r')$  es divisible por algún  $LT(g_i)$ . Esto es imposible, dado que ningún término de  $r, r'$  es divisible por algún  $LT(g_1), \dots, LT(g_t)$ , esto implica que  $r - r'$  debe ser cero, demostrando la unicidad de  $r$ . ■

**Corolario 7.** *Sea  $G = \{g_1, \dots, g_t\}$  una base de Gröbner de un ideal  $I \subseteq K[x_1, \dots, x_n]$  y sea  $f \in K[x_1, \dots, x_n]$ . Entonces  $f \in I$  si y sólo si el residuo de dividir  $f$  entre  $G$  es cero.*

**Demostración.** Si el residuo es cero, ya hemos visto que  $f \in I$ . Inversamente, tomemos a  $f \in I$ , entonces  $f = f + 0$ , satisfaciendo la segunda condición de la Proposición 4, de lo que se sigue, que cero, es el residuo de dividir  $f$  entre  $G$ . ■

Ya hemos visto que el residuo que se obtiene al dividir un polinomio entre una base de Gröbner, es único. Esta propiedad permite definir de manera precisa el residuo asociado a un conjunto de polinomios. La siguiente definición es una notación útil para referirte a este residuo, especialmente cuando trabajamos con varias variables y a menudo será usada esta notación en este trabajo.

**Definición 20.** *Escribiremos  $\overline{f}^F$  como el residuo de la división de  $f$  por la  $s$ -tupla ordenada  $F = (f_1, \dots, f_s)$ . Si  $F$  es una base de Gröbner para  $\langle f_1, \dots, f_s \rangle$ , entonces, podemos considerar a  $F$  como un conjunto (sin un orden) por la Proposición [4](#).*

**Ejemplo 11.** *Sea  $F = (x^2y - y^2, x^4y^2 - y^2) \subseteq K[x, y]$  usando el orden  $lex$ , tendremos*

$$\overline{x^5y}^F$$

*ya que el algoritmo de la división produce*

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

La cancelación de de términos líderes en combinaciones lineales de polinomios, es un fenómeno central en la teoría de las bases de Gröbner. En este contexto, introduciremos la siguiente definición, acompañada de los  $S$ -polinomios que son construcciones claves para este fenómeno y en el algoritmo de Buchberger, para la construcción de bases de Gröbner.

**Definición 21.** *Sea  $f, g \in K[x_1, \dots, x_n]$ , polinomios no cero.*

(i) *Si  $\text{multigrado}(f) = \alpha$  y  $\text{multigrado}(g) = \beta$ , entonces sea  $\gamma = (\gamma_1, \dots, \gamma_n)$ , donde  $\gamma_i = \max(\alpha_i, \beta_i)$  para cada  $i$ . Llamaremos a  $x^\gamma$  el mínimo común múltiplo de  $LM(f)$  y  $LM(g)$ , y escribiremos como  $x^\gamma = \text{lcm}(LM(f), LM(g))$ .*

(ii) *El  $S$ -polinomio de  $f$  y  $g$  es la combinación*

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

**Ejemplo 12.** Sea  $f = x^3y^2 - 4x^2y^3 + 2x$  y  $g = 5x^4y + y^2$  en  $\mathbb{R}[x, y]$  con el orden *grlex* (grado lexicográfico). Entonces  $\gamma = (4, 2)$ , entonces

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{5x^4y} \cdot g \\ &= x \cdot f - \frac{1}{5} \cdot y \cdot g \\ &= -4x^3y^3 + 2x^2 - \frac{1}{5}y^3. \end{aligned}$$

Antes de establecer un resultado crucial, en esta sección, como lo es el Teorema del Criterio de Buchberger, presentaremos un lema, el cual es un resultado técnico y clave para la demostración de dicho teorema, este lema nos permitirá tratar los casos en que se produce la cancelación entre los términos líderes de una combinación lineal. A continuación enunciamos y demostramos este lema que fue obtenido del artículo [Woo23].

**Lema 11.** Si  $\text{grd}(p_i) = \delta$  para todo  $i$  y  $\text{grd}(\sum_{p_i}^n p_i) < \delta$ , entonces, existe  $a_{ij} \in K$  tal que  $\sum_{i=1}^n p_i = \sum_{i,j} a_{i,j} S(p_i, p_j)$ .

**Demostración.** Sea  $S(p_i, p_j) = \frac{x^\delta}{LT(p_i)} \cdot p_i - \frac{x^\delta}{LT(p_j)} \cdot p_j$  donde  $LT(p_i) = b_i x^\delta$  y  $LT(p_j) = b_j x^\delta$ . Fijamos a  $j$ , entonces,

$$\begin{aligned} \sum_{i=1, i \neq j}^n b_i \left( \frac{p_i}{b_i} - \frac{p_j}{b_j} \right) &= \sum_{i=1, i \neq j}^n \left( p_i - \frac{b_i}{b_j} \cdot p_j \right) \\ &= \sum_{i=1, i \neq j}^n p_i - \frac{p_j}{b_j} \sum_{i=1, i \neq j}^n b_i \\ &= \sum_{i=1}^n p_i, \end{aligned}$$

donde  $\left( \frac{p_i}{b_i} - \frac{p_j}{b_j} \right) = S(p_i, p_j)$  y  $\sum_{i=1, i \neq j}^n b_i = 0$ , dado que la suma tiene grado menor que  $\delta$ . ■

De igual manera el siguiente teorema a sido extraído del artículo [Woo23].

**Teorema 6.** Sea  $I$  un ideal en  $K[x_1, \dots, x_n]$  tal que  $I = \langle g_1, \dots, g_d \rangle$ . Entonces  $G = \{g_1, \dots, g_d\}$  es una base de Gröbner si y sólo si  $\overline{S(g_i, g_j)}^G = 0$  para todo  $i, j \in \{1, \dots, d\}$ , donde  $\overline{S(g_i, g_j)}^G$  denota el residuo de  $S(g_i, g_j)$  dividido por  $G$ .

**Demostración.** Primero demosremos la condición necesaria, es decir, demostraremos que  $\langle LT(g_1), \dots, LT(g_d) \rangle = \langle LT(I) \rangle$ .

$\langle LT(g_1), \dots, LT(g_d) \rangle \subseteq \langle LT(I) \rangle$ , es claro que dado  $g_i$  en  $I$  implica que  $LT(g_i)$  esta en  $\langle LT(I) \rangle$  para todo  $i \in \{1, \dots, d\}$ . Así  $\langle LT(g_1), \dots, LT(g_d) \rangle \subseteq \langle LT(I) \rangle$ , dado que  $\langle LT(I) \rangle$  es cerrado bajo combinaciones lineales finitas y un elemento arbitrario de  $\langle LT(g_1), \dots, LT(g_d) \rangle$  se escribe como  $f_1 LT(g_1) + \dots + f_d LT(g_d)$  para todo  $f_i \in K[x_1, \dots, x_n]$ .

Queda por demostrar  $\langle LT(I) \rangle \subseteq \langle LT(g_1), \dots, LT(g_d) \rangle$  y por el mismo razonamiento anterior es suficiente demostrar que  $LT(I) \subseteq \langle LT(g_1), \dots, LT(g_d) \rangle$ . Sea  $f$  arbitrario en  $I$  y  $LT(f) = a_n x^{\alpha_n} \in LT(I)$ , escribimos

$$f = a_n x^{\alpha_n} + a_{n-1} x^{\alpha_{n-1}} + \dots + a_0 = \sum_{i=1}^n h_i g_i, h_i \in K[x_1, \dots, x_n].$$

A  $f$  se puede escribir así, dado que  $I = \langle g_1, \dots, g_n \rangle$ . Por Lema [7](#), necesitamos demostrar que  $a_n x^{\alpha_n}$  es divisible por alguno de los  $LT(g_i)$ ,  $i \in \{1, \dots, d\}$  y sea  $\delta = \max(\text{grd}(h_i, g_i))$ , por lo que tenemos dos casos

Caso 1:  $\delta = \text{grd}(f) = \alpha_n$ , este caso es cuando no ocurre cancelación en la suma de  $f$ .

Caso 2:  $\delta > \text{grd}(f)$ , este es el caso en que se cancela la suma de  $f$ .

Denotemos a  $f = \sum_{i=1}^d h_i^* g_i$  tal que  $\max(\text{grd}(h_i^*)) = \delta^*$  es estrictamente menor que  $\delta$ , podemos reducir inductivamente el caso 1.

Supongamos que  $f = h_1 g_1 + \dots + h_d g_d$  con  $\text{grd}(f) = \delta$  y  $\text{grd}(h_i g_i) \leq \delta$  (en el peor de los casos una igualdad). Entonces, para cada  $i \in \{1, \dots, d\}$ ,  $LM(f) = LM(h_i g_i) = LM(g_i) LM(h_i)$ . Ahora, tenemos que  $LM(g_i)$  divide a  $LM(f)$ , y estos nos da que  $LT(g_i)$  divide a  $LT(f)$  dado que  $LT(f) = x^\alpha = LM(h_i) LM(g_i)$  implica que

$$\begin{aligned} a_n x^\alpha &= a_n LM(h_i) LM(g_i) \\ &= \frac{a_n}{b_i} LM(h_i) \cdot b_i LM(g_i) \\ &:= \frac{a_n}{b_i} LM(h_i) LT(g_i), \end{aligned}$$

donde  $b_i \neq 0$  dado  $LT(g_i) \neq 0$ , demostrando el caso 1.

Ahora, veamos el caso 2. Escribamos a

$$f = \sum_{\text{grd}(h_i g_i) > \text{grd}(f)} h_i g_i + \sum_{\text{grd}(h_i g_i) \leq \text{grd}(f)} h_i g_i,$$

y dado  $\text{grd}(h_i g_i) = \delta$  entonces  $\text{grd}(LT(g_i)) = \delta$ , y por el buen orden tenemos

$$= \sum_{\text{grd}(h_i g_i) = \delta} LT(h_i)g_i + \sum_{\text{grd}(h_i g_i) = \delta} (h_i - LT(h_i))g_i + \sum_{\text{grd}(f) < \text{grd}(h_i g_i) < \delta} h_i g_i + \sum_{\text{grd}(h_i g_i) \leq \text{grd}(f)} h_i g_i,$$

donde la primera suma tiene un grado menor que  $\delta$  y la segunda suma, resta  $LT(h_i)$ , entonces, tiene un grado menor que  $\delta$ . Ahora por el Lema [11](#), existe  $a_{ij}$  tal que

$$\begin{aligned} \sum_{\text{grd}(h_i g_i) = \delta} LT(h_i)g_i &= \sum_{i,j}^d a_{ij} S(LT(h_i)g_i, LT(h_j)g_j) \\ &= \sum_{i,j}^d a_{ij} \left( \frac{x^\delta}{LT(h_i g_i)} LT(h_i)g_i - \frac{x^\delta}{LT(h_j g_j)} LT(h_j)g_j \right) \\ &= \sum_{i,j}^d \left( \frac{x^\delta}{LT(h_i)LT(g_i)} LT(h_i)g_i - \frac{x^\delta}{LT(h_j)LT(g_j)} LT(h_j)g_j \right) \\ &= \sum_{i,j}^d a_{ij} \left( \frac{x^\delta}{x^{\alpha_{ij}}} \frac{x^{\alpha_{ij}} g_i}{LT(g_i)} - \frac{x^\delta}{x^{\alpha_{ij}}} \frac{x^{\alpha_{ij}} g_j}{LT(g_j)} \right) \\ &= \sum_{i,j}^d \frac{x^\delta}{x^{\alpha_{i,j}}} a_{ij} S(g_i, g_j), \end{aligned}$$

donde usamos que  $LT(LT(h_k g_k)) = LT(h_k g_k)$  y  $LT(h_k g_k) = LT(h_k)LT(g_k)$ , por buen orden, y  $x^{\alpha_{ij}} = \text{lcm}(LM(g_i)LM(g_j))$ .

Ahora, por suposición  $\overline{S(g_i, g_j)}^G = 0$ , entonces,  $S(g_i, g_j) = \sum_{k=1}^d p_k g_k$  con  $\text{grd}(p_k g_k) \leq \text{grd}(S(g_i, g_j))$ , lo cual es estrictamente menor que  $\alpha_{ij}$ , donde la primera desigualdad sigue del algoritmo de la división y el segundo ya que  $S(g_i, g_j)$  cancela el término principal. Por lo que tenemos

$$\begin{aligned} \sum_{\text{grd}(h_i g_i) = \delta} LT(h_i)g_i &= \sum_{i,j}^d \frac{x^\delta}{x^{\alpha_{ij}}} a_{ij} \sum_{K=1}^d p_k g_k \\ &= \sum_{i,j}^d \sum_{k=1}^d \frac{x^\delta}{x^{\alpha_{ij}}} a_{ij} p_k g_k, \end{aligned}$$

con grado estrictamente menor que  $\delta$ . Esto demuestra el caso 2.

Habiendo quedado así demostrado el sentido suficiente, demos-tremos el sentido necesario, es decir, demos-tremos que  $\overline{S(g_i, g_j)}^G = 0 \forall (g_i, g_j) \in G$  donde asumimos que  $G = \{g_1, \dots, g_d\}$  es una base de Gröbner.

$S(g_i, g_j) = \frac{x^\gamma}{LT(g_i)} \cdot g_i - \frac{x^\gamma}{LT(g_j)} \cdot g_j$  en  $I$  implica que  $LT(S(g_i, g_j))$  en  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_d) \rangle$ , así podemos pasar al siguiente paso del algoritmo de la división por algún  $LT(g_k)$ , por Lema [7](#).

El siguiente paso es dividir  $S(g_i, g_j) - (\frac{LT(S(g_i, g_j))}{LT(g_k)} \cdot g_k)$  (en  $I$ ) por  $G$ . Por el mismo razonamiento que se menciona anteriormente se puede pasar al siguiente paso.

El algoritmo de división termina por el buen orden, por lo tanto concluimos que

$$\overline{S(g_i, g_j)}^G = 0,$$

y esto completa la demostración. ■

Con esto concluimos esta sección, habiendo estudiado propiedades cruciales de las bases de Gröbner y gracias a estos resultados, podemos dar el siguiente paso natural, la construcción efectiva de bases de Gröbner. En la siguiente sección estudiaremos a detalle el algoritmo de Buchberger, que aprovecha las ideas desarrolladas hasta aquí, para transformar cualquier conjunto de generadores de un ideal en una base de Gröbner.

## 3.2. Algoritmo de Buchberger

Por el Corolario [5](#) sabemos que todo ideal en  $K[x_1, \dots, x_n]$  tiene una base de Gröbner, aunque la prueba no es constructiva. Para obtener una base de Gröbner de cualquier ideal, utilizaremos el algoritmo de Buchberger. Pero antes veremos un ejemplo obtenido del libro [\[CLOS97\]](#).

**Ejemplo 13.** *Sea el anillo  $K[x, y]$  con el orden graduado lexicográfico, y sea  $I = \langle f_1, f_2 \rangle$ , siendo  $f_1 = x^3 - 2xy$  y  $f_2 = x^2y - 2y^2 + x$ . El conjunto  $\{f_1, f_2\}$  no es base de Gröbner, ya que  $S(f_1, f_2) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle$ . Para intentar construir una a partir de  $f_1$  y  $f_2$ , deberíamos añadir más generadores a la*

base. La idea, es añadir  $f_3 = -x^2$ , el resto de dividir  $S(f_1, f_2)$  entre  $(f_1, f_2)$ . Sea  $F = (f_1, f_2, f_3)$ , comprobemos los  $S$ -polinomios de nuestra nueva base de  $I$ .

$$\begin{aligned}\overline{S(f_1, f_2)}^F &= \overline{f_3}^F = 0, \\ \overline{S(f_1, f_3)}^F &= \overline{-2xy}^F \neq 0.\end{aligned}$$

Viendo esto añadimos al conjunto de generadores  $f_4 = -2xy$ . Entonces con  $F = (f_1, f_2, f_3, f_4)$  volveremos a comprobar

$$\begin{aligned}\overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = 0, \\ \overline{S(f_1, f_4)}^F &= \overline{-2xy^2}^F = \overline{yf_4}^F = 0, \\ \overline{S(f_2, f_3)}^F &= \overline{-2y^2 + x}^F \neq 0.\end{aligned}$$

Por tanto hay que añadir  $-2y^2 + x$  al conjunto de generadores. Así obtendríamos  $F = (f_1, f_2, f_3, f_4, f_5)$  al computarlos para todo  $1 \leq i \leq j \leq 5$  obtenemos que

$$\overline{S(f_i, f_j)}^F = 0.$$

Por el Teorema [6](#)  $F$  es una base de Gröbner para  $I$  con el orden graduado lexicográfico.

Con este ejemplo podemos tener una idea para obtener una base de Gröbner a partir de un conjunto de generadores y es justo lo que hace el algoritmo de Buchberger.

**Teorema 7.** Sea  $I = \langle f_1, \dots, f_s \rangle \neq \{0\}$  un ideal de  $K[x_1, \dots, x_n]$ . Entonces, el siguiente algoritmo nos construye una base de Gröbner tras un número finito de pasos.

---

**Algorithm 3** Algoritmo de Buchberger

---

```

1:  $a_1 := 0; \dots; a_s := 0; \quad r := 0$ 
2: repeat
3:    $G' := G$ 
4:   for all pares  $\{p, q\}$ , con  $p \neq q$  en  $G'$  do
5:      $S := \overline{S(p, q)}^{G'}$ 
6:     if  $S \neq 0$  then
7:        $G := G \cup \{S\}$ 
8:     end if
9:   end for
10: until  $G = G'$ 

```

---

**Demostración.** Veamos primero que  $G \subset I$  en todos los momentos del algoritmo. Inicialmente es cierto, y lo único que hacemos es añadir el  $S = \overline{S(p,q)}^{G'}$  para  $p, q \in G$ , y como dividimos entre  $G' \subset I$ ,  $G \cup \{S\} \subset I$ . Además, notemos que como  $G$  contiene a la base dada inicialmente,  $G$  es una base de  $I$ . El algoritmo termina cuando  $G = G'$ , lo que quiere decir que  $S = \overline{S(p,q)}^{G'} = 0$  para todo  $p, q \in G$ . Es decir, por el Teorema 6 el algoritmo termina cuando  $G$  es una base de Gröbner. Falta probar que el algoritmo termina en un número finito de pasos, para ver esto, tenemos que considerar que pasa después de cada iteración. El conjunto  $G$  está formado por  $G'$  (el antiguo  $G$ ) y los restos distintos de cero de los  $S$ -polinomios de los elementos de  $G'$ . Entonces

$$\langle LT(G') \rangle \subset \langle LT(G) \rangle \quad (2)$$

ya que  $G' \subset G$ . Si  $G' \neq G$ , podemos afirmar que  $\langle LT(G') \rangle \subsetneq \langle LT(G) \rangle$ . Para ver esto, suponemos un resto distinto de cero  $r$  de un  $S$ -polinomio que fue adjuntado a  $G$ . Como  $r$  es resto de la división entre  $G'$ ,  $LT(r)$  no es divisible por los  $LT$  de los elementos de  $G'$ , así que  $LT(r) \notin \langle LT(G') \rangle$ , pero  $LT(r) \in \langle LT(G) \rangle$ . De este modo por (2), los ideales  $\langle LT(G') \rangle$  de las sucesivas iteraciones, forman una cadena ascendente de ideales en  $K[x_1, \dots, x_n]$ , y por la Condición de Cadena Ascendente (Teorema 4) la cadena se estabilizará, por lo tanto  $G' = G$  para algún  $N$ , así que el algoritmo termina después de un número finito de pasos. ■

**Ejemplo 14.** Sea el ideal  $I = \langle x^3 - 2xy, x^2y + x - 2y^2 \rangle$  utilizando el orden lexicográfico  $x > y$  encontrar su Base de Gröbner. Con el siguiente código de SageMath, obtenemos una base de Gröbner para este ideal

```
sage: #Definir el anillo con orden lexicográfico (variable principal: x>y)
sage: R.<x,y>=PolynomialRing(QQ, order='lex')
sage: #Definir los polinomios
sage: f1=x^3-2*x*y
sage: f2=x^2 *y +x-2*y^2
sage: #Crear el Ideal
sage: I=Ideal([f1,f2])
sage: #Calcular la base de Gröbner
sage: G=I.groebner_basis()
sage: #mostrar resultados
sage: for g in G:
\dots.:     print(g)
```

\ldots :  
 $x - 2y^2$   
 $y^3$

Vemos que la base de Gröbner es  $G = \{x - 2y^2, y^3\}$ .

Ahora veamos un ejemplo de como podemos encontrar bases de Gröbner sin utilizar ningún programa de computadora

**Ejemplo 15.** Sea el ideal  $I = \langle f_1 = x^2 + y^2 - 1, f_2 = xy - 1 \rangle$  utilizando el orden lexicográfico  $x > y$  encontrar su Base de Gröbner. Calculemos  $S(f_1, f_2)$ , identifiquemos que  $LT(f_1) = x^2$  y  $LT(f_2) = xy$  además que el  $mcm(LM(f_1), LM(f_2)) = x^2y$ , entonces

$$\begin{aligned} S(f_1, f_2) &= \frac{x^2y}{x^2}(x^2 + y^2 - 1) - \frac{x^2y}{xy}(xy - 1) \\ &= y(x^2 + y^2 - 1) - x(xy - 1) \\ &= x^2y + y^3 - y - x^2y + x \\ &= y^3 - y + x. \end{aligned}$$

Observemos que  $LT(S(f_1, f_2)) = x$  no es divisible por  $f_1$  ni por  $f_2$  por ende agregamos este a  $G = \{f_1 = x^2 + y^2 - 1, f_2 = xy - 1, f_3 = y^3 - y + x\}$ . Veamos si la base de Gröbner está completa, calculemos  $S(f_1, f_3)$

$$\begin{aligned} S(f_1, f_3) &= \frac{x^2}{x^2}(x^2 + y^2 - 1) - \frac{x^2}{x}(y^3 - y + x) \\ &= x^2 + y^2 - 1 - xy^3 + xy - x^2 \\ &= -xy^3 + xy + y^2 - 1. \end{aligned}$$

Usando

$$f_2 = xy - 1 \implies xy = 1 \implies -xy^3 + xy + y^2 - 1 = -y^2(xy) + xy + y^2 - 1 = y^2(1) + 1 + y^2 - 1 = 0,$$

en este caso  $r = 0$ , ahora calculemos  $S(f_2, f_3)$ ,

$$\begin{aligned} S(f_2, f_3) &= \frac{xy}{xy}(xy - 1) - \frac{xy}{x}(y^3 - y + x) \\ &= xy - 1 - xy - y^4 + y^2 \\ &= -y^4 + y^2 - 1. \end{aligned}$$

Observemos que  $LT(S(f_2, f_3)) = -y^4$  no es divisible por ningún  $LT(f_i)$  donde  $1 \leq i \leq 3$ .

Así  $f_4 = -y^4 + y^2 - 1$ ,  $G = \{x^2 + y^2 - 1, xy - 1, y^3 - y + x, -y^4 + y^2 - 1\}$

Comprobemos si esta es la base de Gröbner, calculemos  $S(f_1, f_4)$ .

$$\begin{aligned} S(f_1, f_4) &= \frac{x^2y^4}{x^2}(x^2 + y^2 - 1) - \frac{x^2y^4}{-y^4}(-y^4 + y^2 - 1) \\ &= x^2y^4 + y^6 - y^4 - x^2y^4 + x^2y^2 - x^2 \\ &= x^2y^2 - x^2 + y^6 - y^4. \end{aligned}$$

$$\begin{array}{r|l} & -y^4 + y^2 - 1 \\ & x + y^3 - y \\ & xy - 1 \\ x^2y^2 - x^2 + y^6 - y^4 & \underline{x^2 + y^2 - 1} \\ -x^2y^2 + xy & q_1 := -1 \\ \hline xy - x^2 + y^6 - y^4 & q_2 := xy + 1 \\ -xy + 1 & q_3 := 0 \\ \hline -x^2 + y^6 - y^4 + 1 & q_4 := -y^2 \\ x^2 + y^2 - 1 & \\ \hline y^6 - y^4 + y^2 & \\ -y^6 + y^4 + y^2 & \\ \hline 0 & . \end{array}$$

Ahora calculemos  $S(f_2, f_4)$ .

$$\begin{aligned} S(f_2, f_4) &= \frac{xy^4}{xy}(xy - 1) - \frac{xy^4}{-y^4}(-y^4 + y^2 - 1) \\ &= xy^4 - y^3 - xy^4 + xy^2 - x \\ &= xy^2 - x - y^3. \end{aligned}$$

$$\begin{array}{r|l}
xy^2 - x - y^3 & \begin{array}{l} -y^4 + y^2 - 1 \\ x + y^3 - y \\ xy - 1 \\ \hline x^2 + y^2 - 1 \end{array} \\
\hline
-x y^2 + y & \begin{array}{l} q_1 := 0 \\ q_2 := y \end{array} \\
\hline
-x + y - y^3 & q_3 := -1 \\
+x + y^3 - y & q_4 := 0 \\
\hline
0 & .
\end{array}$$

Ahora calculemos  $S(f_3, f_4)$ .

$$\begin{aligned}
S(f_3, f_4) &= \frac{xy^4}{x}(x + y^3 - y) - \frac{xy^4}{-y^4}(-y^4 + y^2 - 1) \\
&= xy^4 + y^7 - y^5 - xy^4 + xy^2 - x \\
&= xy^2 - x + y^7 - y^5.
\end{aligned}$$

$$\begin{array}{r|l}
xy^2 - x + y^7 - y^5 & \begin{array}{l} -y^4 + y^2 - 1 \\ x + y^3 - y \\ xy - 1 \\ \hline x^2 + y^2 - 1 \end{array} \\
\hline
-x y^2 + y & \begin{array}{l} q_1 := 0 \\ q_2 := y \end{array} \\
\hline
-x + y^7 - y^5 + y & q_3 := -1 \\
+x + y^3 - y & q_4 := -y^3 \\
\hline
y^7 - y^5 + y^3 & \\
-y^7 + y^5 - y^3 & \\
\hline
0 & .
\end{array}$$

Debido a que todos los residuos son ceros podemos decir que la base de Gröbner es  $G = \{x^2 + y^2 - 1, xy - 1, y^3 - y + x, -y^4 + y^2 - 1\}$ .

**Definición 22.** Una base de Gröbner reducida para un ideal  $I \subset K[x_1, \dots, x_n]$  es una base de Gröbner  $G$  de  $I$  tal que

(i)  $LC(p) = 1$  para todo  $p \in G$ ;

(ii) Para todo  $p \in G$ , ningún monomio de  $p$  está en  $\langle LT(G - \{p\}) \rangle$ .

En el ejemplo [15](#) la base de Gröbner es  $G = \{x^2 + y^2 - 1, xy - 1, y^3 - y + x, -y^4 + y^2 - 1\}$ , tratemos de reducirla para esto hagamos todos los  $LC(p) = 1$  entonces

$$f_1 = x^2 + y^2 - 1,$$

$$f_2 = xy - 1,$$

$$f_3 = y^3 - y + x,$$

$$f_4 = -y^4 + y^2 - 1.$$

todos a excepción de  $f_4$  tienen  $LC(p) = 1$  entonces denotemos

$$\tilde{f}_4 = y^4 - y^2 + 1.$$

Notemos que hay monomios de  $f_1$  y  $f_2$  que están en  $f_4$ , por ende la base reducida de Gröbner es  $G = \{x + y^3 - y, y^4 - y^2 + 1\}$ .

## 4. Ideales de Grassman-Plücker

El estudio de subespacio lineales en un espacio vectorial conducen naturalmente a las variedades de Grassmannn, que las parametriza de manera algebraica. Para describir estos espacio se usan las coordenadas de Plücker, que permiten incrustar la Grassmanniana en un espacio proyectivo, pero la combinación de estas coordenadas deben cumplir las relaciones de Plücker. Estas relaciones, generan al ideal llamado Grassmann-Plücker, que codifica la estructura algebraica de la Grassmanniana. En este capítulo estudiaremos de manera organizada estos conceptos.

### 4.1. El Grasmanniano

La Grassmanniana, es la variedad que parametriza todos los subespacio lineales de dimensión fija en un espacio vectorial. Su estudio es fundamental para entender como representar algebraicamente estos subespacios mediante las coordenadas de Plücker, lo cual nos permitirá la construcción del ideal de Grassmann-Plücker que define su estructura en el espacio proyectivo.

Antes de introducir la definición formal de lo que es la Grassmanniana, introduciremos una definición previa, sobre la equivalencia de matrices que representan el mismo espacio lineal, dado que un subespacio de dimensión fija puede describirse mediante las filas de una matriz de rango máximo, buscamos una forma de identificar aquellas matrices cuyas filas generan el mismo subespacio. Esta relación de equivalencia será importante para definir la Grassmanniana como un espacio cociente de matrices, que es el punto de partida para su construcción algebraica.

**Definición 23.** *Sea  $K$  un cuerpo. Para  $k \leq n$  denotado por  $M(k, n)$  el espacio vectorial de  $k \times n$  – matrices sobre  $K$  y por  $M_k(k, n)$  el subconjunto de  $M(k, n)$  que consiste de las matrices de rango (máximo)  $k$ .*

Recordemos que  $M(k, n)$  es un espacio vectorial isomorfo a  $K^{kn}$ , ya que podemos considerar una  $k \times n$  – matriz como la  $kn$  – tupla donde las primeras  $n$  entradas son las primeras filas, las siguientes  $n$  entradas son la segunda fila y así sucesivamente.  $M_k(k, n)$  es un subconjunto abierto de  $M(k, n)$ , dado que su complemento consiste de todas las  $k \times n$  – matrices con todos los menores máximos iguales a 0. En otras palabras

$$M_k(k, n)^c = \{M \in M(k, n) : \det(M_I) = 0, \forall I = \{i_1, \dots, i_n\}\}.$$

Dado que este es el conjunto solución de una colección de polinomios en las entradas de la matriz, es cerrado, por lo tanto  $M_k(k, n)$  es abierto.

Ahora ya podemos definir la Grassmanniana

**Definición 24.** Sea la relación de equivalencia  $\sim$  definida sobre  $M_k(k, n)$  por

$$A \sim B \iff \exists X \in GL(k, K) : XB = A.$$

La Grassmanniana, es el espacio cociente

$$\text{Gr}(k, n) = M_k(k, n) / \sim.$$

Si  $V$  es cualquier  $K$ -espacio vectorial de dimensión  $n$  entonces existe un isomorfismo  $V \cong K^n$  que establece una biyección natural, entre los subespacios lineales de  $V$  y  $K^n$ . Por tanto, podemos resumir nuestra definición de Grassmanniana a subespacios de  $K^n$ , sin pérdida de generalidad. De ahora en adelante, nos referiremos a  $k \leq n$  cuando escribimos la matriz  $k \times n$ -matriz. Para los lectores familiarizados con el producto exterior de un espacio vectorial, aquí hay una forma más invariante de describir la Grassmanniana

$$\text{Gr}(k, n) = \{[v_1 \wedge \cdots \wedge v_k] \in \mathbb{P}(\bigwedge^k V) : v_1, \dots, v_k \in V \text{ linealmente independientes}\}.$$

**Ejemplo 16.** La Grassmanniana  $\text{Gr}(1, n+1)$  consta de  $1 \times (n+1)$ -matrices de rango máximo ( $(n+1)$ -tuplas con al menos una entrada distinta de cero) hasta la multiplicación con un elemento  $GL(1, K) = K^*$ . Por lo tanto,  $\text{Gr}(1, n+1) = KP^n$

**Ejemplo 17.** Consideremos  $\text{Gr}(2, 4)$ . La Grassmanniana, es el siguiente mapeo:

$$\begin{aligned} A = \begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix} &\mapsto ([12] : [13] : [14] : [23] : [24] : [45]) \\ &= (af - be : ag - ce : ah - de : bg - cf : bh - df : ch - dg) \in \mathbb{P}^5 \end{aligned}$$

Alternativamente, fijamos una base  $(v_1, v_2, v_3, v_4)$  de  $V$  y escribiremos

$$\begin{aligned} (av_1 + bv_2 + cv_3 + dv_4) \wedge (ev_1 + fv_2 + gv_3 + hv_4) &= (af - be)v_1 \wedge v_2 + (ag - ce)v_1 \wedge v_3 + \\ &+ (ah - de)v_1 \wedge v_4 + (bg - cf)v_2 \wedge v_3 + (bh - df)v_2 \wedge v_4 + (ch - dg)v_3 \wedge v_4. \end{aligned}$$

Esta Grassmanniana, tiene dimensión 4, es decir, es una hipersuperficie en  $\mathbb{P}^5$ . Escribiremos las coordenadas sobre  $\mathbb{P}^5$  como  $(p_{12} : p_{13} : p_{14} : p_{23}, p_{24}, p_{34})$ . Estos índices hacen referencia a las menores de una matriz  $2 \times 4$ .

**Definición 25.** *Los elementos de  $Gr(k, n)$  son clases de equivalencia de  $\sim$ . Nos referiremos a cualquier matriz en una clase de equivalencia, como coordenadas homogéneas generalizadas para el elemento. Es decir una matriz de  $k \times n$  (de rango máximo) hasta la multiplicación por la izquierda con una matriz  $k \times k$  invertible. La clase de equivalencia de matriz  $A$  se denota por  $[A]$ .*

## 4.2. Las relaciones de Plücker

Las relaciones de Plücker surgen en el estudio de la geometría de Grassmann, específicamente al describir algebraicamente los espacios proyectivos asociados a subespacios lineales. Estas relaciones son un conjunto de ecuaciones cuadráticas que satisfacen los menores de una matriz que representa un subespacio en el espacio de Grassmann. Son fundamentales para entender la estructura algebraica del Grassmanniano como una variedad algebraica, y permiten caracterizar qué conjuntos de coordenadas (llamadas coordenadas de Plücker) corresponden efectivamente a subespacios lineales válidos.

**Ejemplo 18.** *Trabajemos con un ejemplo  $Gr(2, 4)$  tomados del artículo [\[Bro24\]](#). Consideremos la matriz de rango máximo de la forma:*

$$A = \begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix}.$$

*Las coordenadas de Plücker de  $A$  serán todas las menores máximos de  $A$  ordenados, i.e.*

$$[af - be : ag - ce : ah - de : bg - cf : bh - df : ch - dg] \in \mathbb{P}(\Lambda^2(\mathbb{R}^4)).$$

*Sea  $[ij]$  las menores determinantes de la submatriz formada por las columnas  $i$ -ésimo y  $j$ -ésimo tales que  $i < j$ , como están relacionadas podríamos esperar encontrar algún tipo de relaciones entre ellas, por ejemplo supongamos que consideramos productos de menores tales que cada término contiene un índice de cada columna:*

$$[12][34] = (af - be)(ch - dg) = acfh - adfg - bceh + bdeg.$$

Intentemos sumar todas esas combinaciones, que en este ejemplo son tres:

$$\begin{aligned}
[12][34] + [13][24] + [14][23] &= (af - be)(ch - dg) + (ag - ce)(bh - df) \\
&\quad + (ah - de)(bg - cf) \\
&= (acfh - adfg - bceh + bdeg) \\
&\quad + (abgh - adfg - bceh + cdef) \\
&\quad + (abgh - acfh - bdeg + cdef) \\
&= (-adfg - bceh) + (abgh - adfg - bceh + cdef) \\
&\quad + (abgh + cdef).
\end{aligned}$$

Si cambiamos el signo del término  $[13][24]$  vemos que la suma total se convierte en

$$[12][34] - [13][24] + [14][23] = (af - be)(ch - dg) - (ag - ce)(bh - df) + (ah - de)(bg - cf) = 0$$

que es una ecuación polinómica de grado 2. En otras palabras, hemos encontrado una manera de caracterizar el Grassmanniano  $Gr(2, 4)$  como el conjunto de ceros del polinomio cuadrático homogéneo  $f(x_1, \dots, x_6) = x_1x_6 - x_2x_5 + x_3x_4 \in K\mathbb{P}^5$ . Dado que este es un espacio proyectivo de dimensión 5, y  $Gr(2, 4)$  tiene dimensión 4, esta ecuación elimina un nivel de libertad y, por lo tanto, es la única requerida.

En general los menores máximos satisfacen las siguientes relaciones no tan obvias, que probaremos más adelante.

**Observación 1.**  $[ii] = a_i b_i - a_i b_i = 0$  ya que desde el punto de vista geométrico no se puede formar un plano a partir de dos veces la misma dirección.

**Definición 26.** Sean  $[\dots : [l_1 \dots l_k] : \dots]$  coordenadas homogéneas en  $\mathbb{P}(\Lambda^k(K^n))$  y sean  $\{i_1, \dots, i_{k-1}\}$  y  $\{j_1, \dots, j_{k+1}\}$  dos conjuntos de índices estrictamente crecientes con  $1 \leq i_m, j_n \leq n$ . Definimos las relaciones de Plücker como el sistema de ecuaciones cuadráticas homogéneas

$$\sum_{t=1}^{k+1} (-1)^t [i_1 \dots i_{k-1} j_t] [j_1 \dots \hat{j}_t \dots j_{k+1}] = 0, \quad (3)$$

donde  $\hat{j}_t$  significa que  $j_t$  se ha eliminado de la secuencia.

**Ejemplo 19.** Considerando de nuevo  $Gr(2, 4)$ , nos gustaría ver que la ecuación encontrada en el ejemplo anterior corresponde a las relaciones de Plücker para este Grassmanniano. Como  $k = 2$ , obtenemos los posibles conjuntos de índices:

$$\begin{aligned} I_1 &= \{1\} & J_1 &= \{1, 2, 3\}, \\ I_2 &= \{2\} & J_2 &= \{1, 2, 4\}, \\ I_3 &= \{3\} & J_3 &= \{1, 3, 4\}, \\ I_4 &= \{4\} & J_4 &= \{2, 3, 4\}, \end{aligned}$$

con  $4 \cdot 4 = 16$  combinaciones  $(I_m, J_n)$ . Primero demostremos que si los dos conjuntos no son disjuntos, obtenemos la ecuación trivial, para ver esto, sean  $I = \{i\}$  y  $J = \{i, j_2, j_3\}$ , entonces

$$\sum_{t=1}^3 (-1)^t [i_1 j_t] [j_1 \cdots \hat{j}_t \cdots j_3] = -[i] [23] + [i j_2] [i j_3] - [i j_3] [i j_2] = 0,$$

donde el primer término es cero ya que  $[i] = 0$  y los dos términos restantes se cancelan. Por lo tanto, el único caso interesante es cuando  $I_m \cap J_n = \emptyset$ , lo que deja cuatro combinaciones. Solo consideramos el caso  $(I_1, J_4)$ :

$$\begin{aligned} \sum_{t=1}^3 (-1)^t [i_1 j_t] [j_1 \cdots \hat{j}_t \cdots j_3] &= 0 \\ &\iff \\ -[12][34] + [13][24] - [14][23] &= 0 \\ &\iff \\ [12][34] - [13][24] + [14][23] &= 0. \end{aligned}$$

**Definición 27.** El ideal de Plücker  $I_{r,s}$  que define al Grassmanniano  $G(r, s)$ , que parametriza todos los subespacios de dimensión  $r$  del espacio  $\mathbb{K}^s$ , donde  $\mathbb{K}$  es un cuerpo (típicamente  $\mathbb{C}$  ó  $\mathbb{Q}$ )

Hablaremos sobre las relaciones cuadráticas de Plücker basándonos en el libro de [\[Man01\]](#), así que de la fórmula general de las relaciones de Plücker  $G(r, s)$  [\(3\)](#), donde:

$$\begin{aligned} I &= \{i_1, \dots, i_{k-1}\} \subset [s], \\ J &= \{j_1, \dots, j_{k+1}\} \subset [s], \end{aligned}$$

notemos que al aplicar el caso para  $r = 2$ ,

$r - 1 = 1$  por tanto  $I = \{i\}$ ,

$r + 1 = 3$  por tanto  $J = \{j_1, j_2, j_3\}$ .

Entonces la relación se convierte en

$$\sum_{t=1}^3 (-1)^t [ij_t][j_1 \cdots \hat{j}_t \cdots j_3] = 0,$$

y esta es la formula explicita de

$$(-1)^1 [ij_1][j_2j_3] + (-1)^2 [ij_2][j_1j_3] + (-1)^3 [ij_3][j_1j_2],$$

es decir  $-[ij_1][j_2j_3] + [ij_2][j_1j_3] - [ij_3][j_1j_2] = 0$ , por el ejemplo [19](#) si multiplicamos por  $-1$  la igualdad sigue cumpliendo  $[ij_1][j_2j_3] - [ij_2][j_1j_3] + [ij_3][j_1j_2] = 0$ .

Podemos decir que el ideal  $I_{2,s}$  está generado por todas las relaciones cuadráticas de la forma

$$[ij][kl] - [ik][jl] + [il][jk] = 0,$$

para todos

$$1 \leq i \leq j \leq k \leq l \leq s.$$

Estas identidades se derivan del hecho de que los determinantes de submatrices de una matriz de rango  $\leq 2$  no son independientes. Geométricamente, esto refleja el hecho de que no todo punto en  $\mathbb{P}^{\binom{s}{2}-1}$  corresponde a una línea del espacio  $\mathbb{K}^s$ ; solo los que satisfacen las relaciones de Plücker lo hacen.

También es posible determinar el número total de relaciones cuadradas de Plücker para  $I_{2,s}$ , según el libro [\[MS21\]](#) y el artículo [\[Hu25\]](#), ya que El número total de relaciones de Plücker en  $I_{2,s}$  es igual al número de 4-subconjuntos de  $\{1, 2, \dots, s\}$ , es decir:  $\binom{s}{4}$  ya que cada conjunto de 4 índices  $\{i, j, k, l\}$  con  $i < j < k < l$  da lugar a una única relación:

$$[ij][kl] - [ik][jl] + [il][jk] = 0.$$

**Ejemplo 20.**  $I_{2,5}$  tenemos 5 relaciones cuadradas de Plücker, ya que  $\binom{5}{4} = 5$  donde estas son las siguientes:

$$[12][34] - [13][24] + [14][23],$$

$$[12][35] - [13][25] + [15][23],$$

$$[12][45] - [14][25] + [15][24],$$

$$[13][45] - [14][35] + [15][34],$$

$$[23][45] - [24][35] + [25][34].$$

De este ejemplo podemos destacar que el ideal

$$I_{2,5} = \{[12][34] - [13][24] + [14][23], [12][35] - [13][25] + [15][23], \\ [12][45] - [14][25] + [15][24], [13][45] - [14][35] + [15][34], \\ [23][45] - [24][35] + [25][34]\}.$$

## 5. Grado máximo para cualquier base de Gröbner reducida del ideal de Grassmann-Plücker

En el estudio de los Grassmannianos  $G(r, s)$ , las coordenadas de Plücker proporcionan una manera natural de describir algebraicamente los subespacios  $\mathbb{K}$ -dimensionales de un espacio vectorial  $n$ -dimensional. Estas coordenadas satisfacen un conjunto de relaciones polinómicas que generan el ideal de Plücker  $I_{r,s}$ , el cual define el Grassmanniano como una variedad algebraica en un espacio proyectivo.

Una herramienta fundamental en álgebra computacional para estudiar estos ideales es la base de Gröbner. Al cambiar el orden monomial, las bases de Gröbner ofrecen distintas representaciones de un mismo ideal, y permiten explorar sus propiedades algebraico-geométricas. Sin embargo, una característica importante de estas bases es su grado máximo, es decir, el mayor grado de los polinomios que las componen.

El problema del grado máximo busca determinar cuál es el mayor grado que puede alcanzar cualquier base de Gröbner reducida del ideal de Grassmann-Plücker  $I_{r,s}$ , al variar el orden monomial. Este problema es central en la teoría de la complejidad computacional de bases de Gröbner, ya que el grado de los polinomios afecta directamente la eficiencia de los algoritmos involucrados en su cálculo.

### 5.1. El impacto del orden en el grado de las bases de Gröbner del ideal de Plücker

Cuando se calcula una base de Gröbner del ideal de Plücker  $I_{r,s}$ , el orden monomial elegido influye fuertemente en los grados de los polinomios obtenidos. El orden lexicográfico, en particular, tiende a generar polinomios de mayor grado que otros órdenes, como el orden de grado inverso.

Esto ocurre porque el orden lexicográfico impone una prioridad muy estricta entre las variables (por ejemplo,  $[12] > [13] > \dots > [(s-1)s]$ ). Durante los pasos del algoritmo de Buchberger, esta jerarquía hace que los términos líderes se vuelvan más complejos, y para eliminarlos se necesitan multiplicaciones que aumentan el grado de los polinomios.

El ideal de Plücker, que ya tiene muchas simetrías, este efecto se amplifica: el orden lex rompe esas simetrías y produce relaciones más complicadas, con monomios de mayor grado.

**Observación 2.** *En los codigos de Sagemath vamos a cambiar la notación de las coordenadas de Plücker de la siguiente manera  $[ij] = p_{ij}$  con el objetivo de evitar que Sagemath lo tome como un numero.*

**Ejemplo 21.** *Retomando el ejemplo [20](#) encontremos la base reducida de Gröbner para  $I_{2,5}$  utilizando el orden lexicográfico en el software Sagemath*

```
sage:k = 2
....:n = 5
....: # Generar todas las variables Plücker ordenadas lex: p12 > p13 >...
....: > p(n-1)(n)
....: from itertools import combinations
....: nombres = ["p" + str(i+1) + str(j+1) for i, j in combinations(range(n), k)]
....:
....: # Ordenarlas lexicográficamente como p12 > p13 > p14 > ... > p(n-1)(n)
....: nombres.sort()
....:
....: R = PolynomialRing(QQ, nombres, order='lex')
....: p = R.gens()
....:
....: # Crear un diccionario para acceder fácilmente a los generadores
....: index_to_var = {}
....: for name, (i, j) in zip(nombres, combinations(range(n), k)):
....:     index_to_var[(i, j)] = R(name)
....:
....: #Generar todas las relaciones de Plücker para G(2,n)
....: def relaciones_plucker(k, n, ring, idx_var):
....:     relaciones = []
....:     if k != 2:
....:         raise NotImplementedError("Solo implementado para k = 2")
....:
....:     from itertools import combinations
....:
....:     for a, b, c, d in combinations(range(n), 4):
....:         ab = tuple(sorted([a, b]))
....:         ac = tuple(sorted([a, c]))
....:         ad = tuple(sorted([a, d]))
....:         bc = tuple(sorted([b, c]))
....:         bd = tuple(sorted([b, d]))
```

```

....     cd = tuple(sorted([c, d]))
.....:
....:     if all(tupla in idx_var for tupla in [ab, ac, ad, bc, bd, cd]):
....:         rel =idx_var[ab]*idx_var[cd]-idx_var[ac]*idx_var[bd]
....:         +idx_var[ad]*idx_var[bc]
....:         relaciones.append(rel)
....:
....:     return relaciones
.....:
....: # Obtener relaciones
....: relaciones = relaciones_plucker(k, n, R, index_to_var)
.....:
....: print(f"\nTotal de relaciones de Plücker para G({k},{n}):
....:{len(relaciones)}")
....: for i, rel in enumerate(relaciones, 1):
....:     print(f"Relación {i}: {rel}")
....:
....: I = R.ideal(relaciones)
.....:
....: print("\n¿Las relaciones generan el ideal de Grassmann-Plücker?")
....: print(I == R.ideal(relaciones))
.....:
....: print("\nBase de Gröbner del ideal:")
....: for g in I.groebner_basis():
....:     print(g)
.....:

```

Total de relaciones de Plücker para G(2,5): 5

Relación 1:  $p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23}$

Relación 2:  $p_{12}p_{35} - p_{13}p_{25} + p_{15}p_{23}$

Relación 3:  $p_{12}p_{45} - p_{14}p_{25} + p_{15}p_{24}$

Relación 4:  $p_{13}p_{45} - p_{14}p_{35} + p_{15}p_{34}$

Relación 5:  $p_{23}p_{45} - p_{24}p_{35} + p_{25}p_{34}$

¿Las relaciones generan el ideal de Grassmann-Plücker?

True

Base de Gröbner del ideal:

```

p12*p34 - p13*p24 + p14*p23
p12*p35 - p13*p25 + p15*p23
p12*p45 - p14*p25 + p15*p24
p13*p24*p35 - p13*p25*p34 - p14*p23*p35 + p15*p23*p34
p13*p45 - p14*p35 + p15*p34
p23*p45 - p24*p35 + p25*p34
sage:

```

Cabe recalcar que este código funciona para los ideales  $I_{2,s}$  haciendo una pequeña modificación en  $n = 5$  con el orden lexicográfico.

Así que la base de Gröbner es la siguiente

$$\{[12][34] - [13][24] + [14][23], [12][35] - [13][25] + [15][23], \\ [12][45] - [14][25] + [15][24], [13][24][35] - [13][25][34] - [14][23][35] + [15][23][34], \\ [13][45] - [14][35] + [15][34], [23][45] - [24][35] + [25][34]\}.$$

Podemos ver de manera sencilla que el grado máximo de la base de Gröbner reducida del ideal  $I_{2,5}$  es 3 por el polinomio

$$[13][24][35] - [13][25][34] - [14][23][35] + [15][23][34],$$

utilizando el orden lexicográfico.

Sea  $R$  la  $K$ -álgebra generada por los  $d \times d$ -menores de una  $n \times d$ -matriz  $(x_{ij})$  de indeterminados. Por lo tanto,  $Proj(\mathcal{R})$  es el Grassmanniano de subespacios lineales de dimensión  $d$  en  $K^n$ . Introducimos una variable  $[i_1, \dots, i_d]$  para cada menor maximal. El anillo polinómico en estas variables  $\binom{n}{d}$  se denota  $S$  y se llama anillo de corchetes [Stu08]. El núcleo  $I$  de la función natural de  $S$  sobre  $R$  es el ideal de Grassmann-Plücker. Por el Teorema 3.2.9 de [Stu08], los  $d \times d$ -menores son una base sagbi para la sub-álgebra  $R$  con respecto al “orden de términos diagonales” en  $K[x_{ij}]$ .

Los pesos que definen el orden del término diagonal se dan, por ejemplo, mediante la matriz de Vandermonde  $(w_{ij}) = (i^j)$ . Para la variable de corchete  $[i_1, i_2, \dots, i_d]$ , esto induce el peso en  $i_1 + i_2^2 + \dots + i_d^d$ . Los llamamos pesos de Vandermonde en el anillo de corchetes.

En el estudio de los ideales de Grassmann-Plücker  $I_{r,s}$ , que como sabemos, definen las coordenadas homogéneas de la Grassmanniana  $G(r, s)$ , un problema central es entender la complejidad algebraica de sus bases de Gröbner,

las cuales no son solo fundamentales en cálculos efectivos en la geometría algebraica, sino que también codifican propiedades combinatorias y geometría profunda. En particular, el grado máximo  $F(r, s)$  que aparece en cualquier base de Gröbner reducida para  $I_{r,s}$  es un invariante clave que refleja la no linealidad inherente al ideal.

Sobre este tema, existe un problema abierto, ya que  $F(r, s)$  está relacionado con los circuitos de la configuración  $\mathcal{A}_{r,s}$  asociada a las Grassmanniana, el cual se enuncia de la siguiente manera: ¿Cuál es el grado máximo  $F(r, s)$  que aparece en una base de Gröbner reducida para el ideal de Grassmann-Plücker  $I_{r,s}$ ?, donde sabemos que el ideal  $I_{r,s}$  está generado por las relaciones de Plücker, que son polinomios que surgen de condiciones de incidencia para las menores  $r \times r$  de una matriz  $r \times s$  y una base de Gröbner reducida de  $I_{r,s}$  depende del orden monomial elegido y su grado máximo  $F(r, s)$  mide la complejidad estructural del ideal.

Aunque se conocen cotas inferiores para  $F(r, s)$ , como  $F(2, s) \geq s - 2$ , el valor exacto y su comportamiento sigue siendo objeto de estudio. El desafío está en generalizar para  $r \geq 3$ , aunque existe la cota superior  $F(2, s) \geq s - 2$ , no está claro si esta cota es ajustada, por ejemplo, para  $s = 6$ , la base de Gröbner tiene grado 3, menor que  $s - 2 = 4$ . En este trabajo nos centraremos en el estudio del ideal de Grassmann-Plücker  $I_{2,s}$ .

Para comprender mejor este problema abierto, desarrollaremos un ejemplo concreto que nos permita visualizar su construcción y propiedades. A lo largo del análisis, nos apoyaremos en códigos propios implementados en Python, los cuales facilitarán la experimentación numérica y la verificación de resultados teóricos.

**Ejemplo 22.** *Para el Grassmanniano  $G(3, 5)$  que parametriza planos (3-subespacios) en  $\mathbb{C}^5$ , tomaremos un plano  $U \subset \mathbb{C}^5$  generados por 3 vectores linealmente independientes:*

$$v_1 = \langle 7, 1, 5, 7, 2 \rangle, \quad v_2 = \langle 7, 9, 3, 8, 7 \rangle, \quad v_3 = \langle 6, 4, 9, 3, 3 \rangle.$$

La matriz de base de  $U$  es:

$$\begin{bmatrix} 7 & 1 & 5 & 7 & 2 \\ 7 & 9 & 3 & 8 & 7 \\ 6 & 4 & 9 & 3 & 3 \end{bmatrix}.$$

Ahora vamos a calcular las coordenadas de Plücker que en este caso son las menores  $3 \times 3$ , hay  $\binom{5}{3} = 10$  menores:

$$[123] = \det \begin{bmatrix} 7 & 1 & 5 \\ 7 & 9 & 3 \\ 6 & 4 & 9 \end{bmatrix} = 308,$$

$$[124] = -190,$$

$$[125] = -38,$$

$$[134] = 9,$$

$$[135] = -183,$$

$$[145] = 114,$$

$$[234] = 445,$$

$$[235] = 89,$$

$$[245] = 0,$$

$$[345] = 267.$$

Para encontrar las relaciones de Plücker usaremos la ecuación [3](#), así que tomemos los siguientes conjuntos de índices:

$$I_1 = \{1, 2\} \quad J_1 = \{1, 2, 3, 4\}$$

$$I_2 = \{1, 3\} \quad J_2 = \{1, 2, 3, 5\}$$

$$I_3 = \{1, 4\} \quad J_3 = \{1, 2, 4, 5\}$$

$$I_4 = \{1, 5\} \quad J_4 = \{1, 3, 4, 5\}$$

$$I_5 = \{2, 3\} \quad J_5 = \{2, 3, 4, 5\}$$

$$I_6 = \{2, 4\}$$

$$I_7 = \{2, 5\}$$

$$I_8 = \{3, 4\}$$

$$I_9 = \{3, 5\}$$

$$I_{10} = \{4, 5\}$$

Notemos que por cada conjunto  $I_i$  tendremos únicamente 2 relaciones que no serán triviales ya que ambos no deben de aparecer en el conjunto  $J_j$  al menos

solo uno de los indices. Algunas de las relaciones de Plücker no triviales son:

$$\begin{aligned}
& [123][145] - [124][135] + [125][134], \\
& [123][245] - [124][235] + [125][234], \\
& [123][145] - [134][125] + [135][124], \\
& \quad - [123][345] - [134][235] + [135][234], \\
& [124][135] - [134][125] + [145][123], \\
& \quad \vdots \\
& \quad - [145][235] + [245][135] - [345][125].
\end{aligned}$$

El ideal  $I_{3,5}$  para este subespacio  $U$  está conformado por las relaciones de Plücker que son iguales a ceros, así que el Ideal  $I_{3,5}$  es:

$$\begin{aligned}
& [123][145] - [124][135] + [125][134] = (308)(114) - (-190)(-183) + (-38)(9) = 0, \\
& [123][245] - [124][235] + [125][234] = 0, \\
& [125][134] - [135][124] + [145][123] = 0, \\
& - [125][345] + [135][245] - [145][235] = 0, \\
& - [123][245] - [234][125] + [235][124] = 0, \\
& - [123][345] - [234][135] + [235][134] = 0, \\
& - [134][235] + [234][135] + [345][123] = 0, \\
& - [134][245] + [234][145] + [345][124] = 0, \\
& - [145][234] + [245][134] - [345][124] = 0, \\
& - [145][235] + [245][135] - [345][125] = 0.
\end{aligned}$$

La base de Gröbner para  $I_{3,5}$  utilizando el orden lexicográfico  $[123] > [124] > [125] > \dots > [345]$  es:

$$\begin{aligned}
& [125][345] - [135][245] + [145][235], \\
& [124][345] - [134][245] + [145][234], \\
& [123][345] - [134][235] + [135][234], \\
& [124][135][245] - [124][145][235] - [125][134][245] + [125][145][234], \\
& [123][245] - [124][235] + [125][234], \\
& [123][145] - [124][135] + [125][134].
\end{aligned}$$

Por tanto, el grado máximo de esta base de Gröbner es 3.

## Referencias

- [Bro24] Zakarias Brounéus. Projective spaces, grassmannians and the plücker embedding, 2024.
- [CLOS97] David Cox, John Little, Donal O’shea, and Moss Sweedler. *Ideals, varieties, and algorithms*. Springer, 1997.
- [Her96] Israel N Herstein. *Abstract algebra*. John Wiley & Sons, 1996.
- [Hu25] Yi Hu.  $\mathfrak{G}$ -quotients of grassmannians and equations, 2025.
- [Man01] Laurent Manivel. *Symmetric Functions, Schubert Polynomials, and Degeneracy Loci*, volume 3. American Mathematical Soc., 2001.
- [MS21] Mateusz Michałek and Bernd Sturmfels. *Invitation to nonlinear algebra*, volume 211. American Mathematical Soc., 2021.
- [Stu96] Bernd Sturmfels. *Grobner bases and convex polytopes*, volume 8. American Mathematical Soc., 1996.
- [Stu08] Bernd Sturmfels. *Algorithms in invariant theory*. Springer, 2008.
- [Woo23] Anwyn Woodyatt. An introduction to gröbner bases, 2023.