



Universidad de San Carlos de Guatemala
Escuela de Ciencias Físicas y Matemáticas
Departamento de Matemática

ABANICOS DE GRÖBNER DE VARIEDADES DE VERONESE

Cristian Yovanni Castañeda Paiz

Asesorado por Ing. Edgar Damián Ochoa Hernández

Guatemala, junio de 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



ESCUELA DE CIENCIAS FÍSICAS Y MATEMÁTICAS

**ABANICOS DE GRÖBNER DE VARIEDADES DE
VERONESE**

TRABAJO DE GRADUACIÓN
PRESENTADO A LA JEFATURA DEL
DEPARTAMENTO DE MATEMÁTICA
POR

CRISTIAN YOVANNI CASTAÑEDA PAIZ
ASESORADO POR ING. EDGAR DAMIÁN OCHOA HERNÁNDEZ

AL CONFERÍRSELE EL TÍTULO DE
LICENCIADO EN MATEMÁTICA APLICADA

GUATEMALA, JUNIO DE 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIAS FÍSICAS Y MATEMÁTICAS



CONSEJO DIRECTIVO INTERINO

Director	M.Sc. Jorge Marcelo Ixquiac Cabrera
Representante Docente	Arqta. Ana Verónica Carrera Vela
Representante Docente	M.A. Pedro Peláez Reyes
Representante de Egresados	Lic. Urías Amitaí Guzmán García
Representante de Estudiantes	Elvis Enrique Ramírez Mérida
Representante de Estudiantes	Oscar Eduardo García Orantes
Secretario	Ing. Edgar Damián Ochóa Hernández

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

Director	M.Sc. Jorge Marcelo Ixquiac Cabrera
Examinador	Lic. José Carlos Alberto Bonilla Aldana
Examinador	Ing. Edgar Damián Ochoa Hernández
Examinador	Lic. Ronald Oliverio Chubay Gallina
Secretario	Ing. Edgar Damián Ochoa Hernández

Escuela de Ciencias Físicas y Matemáticas

Ref. D.DTG. 001-2023
Guatemala 05 de junio de 2023

El Director de la Escuela de Ciencias Físicas y Matemáticas de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Coordinador de la Licenciatura en Matemática Aplicada, al trabajo de graduación titulado: "ABANICOS DE GRÖBNER DE VARIEDADES DE VERONESE", presentado por el estudiante universitario Cristian Yovanni Castañeda Paiz, autoriza la impresión del mismo.

IMPRÍMASE.



"ID Y ENSEÑAD A TODOS"



M.Sc. Jorge Marcelo Ixquiac Cabrera
Director

Escuela de Ciencias Físicas y Matemáticas

El jefe del Departamento de Matemática de la Escuela de Ciencias Físicas y Matemáticas de la Universidad de San Carlos de Guatemala, después de conocer el dictamen del asesor **Ing. Edgar Damián Ochoa Hernández**, al trabajo de graduación del estudiante **Cristian Yovanni Castañeda Paiz**, quien se identifica con carné: **2417 08419 0101** y registro académico no. **201213057**, titulado **“ABANICOS DE GRÖBNER DE VARIEDADES DE VERONESE”**, procede a la autorización del mismo.



Lic. William Roberto Gutiérrez Herrera
Jefe Departamento de Matemática



Guatemala, 01 de junio de 2023

Escuela de Ciencias Físicas y Matemáticas

Ref. ECFM.SAD-01.23
Guatemala, 12 de enero de 2023

Lic. William Gutiérrez
Jefe de departamento de la Licenciatura en Matemática Aplicada
Escuela de Ciencias Físicas y Matemáticas
Universidad de San Carlos de Guatemala
Presente

Estimado licenciado Gutiérrez:

Tengo el gusto de dirigirme a usted con la finalidad de informarle que he aceptado ser el asesor del trabajo de año de práctica del estudiante **Cristian Yovanni Castañeda Paiz** quién se identifica con carné número 201213057 y quién está inscrito en la carrera de Licenciatura en Matemática Aplicada en la Escuela No Facultativa de Ciencias Físicas y Matemáticas de la Universidad de San Carlos de Guatemala.

El título del Trabajo de Graduación que presenta es: **Abanicos de Gröbner de Variedades de Veronese**. Adjunto a esta carta encontrará el protocolo de dicho trabajo que ya cuenta con mi aprobación.

Atentamente,

“ID Y ENSEÑAD A TODOS”



Ing. Edgar Damián Ochoa Hernández
Secretario Académico
Escuela de Ciencias Físicas y Matemáticas



Cc. Archivo/DO

Guatemala, 14 de junio de 2023

Honorable Tribunal Examinador

Por este medio yo, Cristian Yovanni Castañeda Paiz, estudiante de la Licenciatura en Matemática Aplicada de la Escuela de Ciencias Físicas y Matemáticas, que me identifico con DPI 2417084190101 y registro académico 201213057, solicito aprueben mi tesis titulada "ABANICOS DE GRÖBNER DE VARIEDADES DE VERONESE".

A handwritten signature in black ink, consisting of a stylized 'C' and 'Y' intertwined.

Cristian Yovanni Castañeda Paiz

201213057

AGRADECIMIENTOS

A mi mamá Sandra Castañeda, por todo su apoyo y amor a lo largo de mi vida.
A mis amigos por siempre estar allí en todo momento y por siempre brindarme su apoyo y cariño cuando más lo he necesitado.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS	III
LISTA DE SÍMBOLOS	V
OBJETIVOS	VII
INTRODUCCIÓN	IX
1. CONCEPTOS PRELIMINARES	1
1.1. Teoría de anillos	1
1.1.1. Anillos	1
1.1.2. Ideales, anillo cociente y homomorfismos	3
1.1.3. Dominios especiales	7
1.1.4. Anillos conmutativos	9
1.2. Geometría algebraica	9
2. BASES DE GRÖBNER	13
2.1. Ordenes monomiales y bases de Gröbner	13
2.2. Ordenes monomiales y vectores de peso	21
3. GEOMETRÍA POLIEDRAL	23
4. ABANICOS DE GRÖBNER	31
5. VARIEDADES DE VERONESE	37
5.1. Espacio proyectivo y variedades proyectivas	37
5.2. Mapeo y variedad de Veronese	39
5.3. Abanicos de Gröbner de variedades de Veronese	41
CONCLUSIONES	47

RECOMENDACIONES	49
BIBLIOGRAFÍA	51

ÍNDICE DE FIGURAS

1.1. Círculo unitario	10
1.2. Cúbica abaleada	11
3.1. Cubo	24
3.2. Octaedro	24
3.3. Politopos P_1 , P_2 y Q	27
3.4. Suma de Minkowski del cubo y octaedro	27
3.5. Abanico normal de Q	28
3.6. Abanico normal del cubo	29

LISTA DE SÍMBOLOS

Símbolo	Significado
$\emptyset$	conjunto vacío
$k[x]$	anillo de polinomios de una variable del campo k
$k[x_1, \dots, x_n]$	anillo de polinomios de n variables del campo k
$\sqrt{I}$	ideal radical del ideal I
k^n	espacio afín de dimensión n del campo k
$V(f_1, \dots, f_n)$	variedad afín (o proyectiva) de los polinomios $f_1, \dots, f_n$
$V(S)$	variedad afín (o proyectiva) del conjunto $S \subset k[x_1, \dots, x_n]$
$I(V)$	ideal de la variedad afín (o proyectiva) V
$<, \leq$	orden monomial
$<_{lex}$	orden monomial lexicográfico
$<_{deglex}$	orden monomial lexicográfico graduado
$<_{revlex}$	orden monomial lexicográfico reverso
$<_{degrevlex}$	orden monomial lexicográfico reverso graduado
$\text{in}_{<}(f)$	forma inicial del polinomio f bajo el orden monomial $<$
$\text{in}_{<}(I)$	forma inicial del ideal I bajo el orden monomial $<$
$\mathbb{B}_{<}$	base de monomios estándar
G	base de Gröbner
$G_{red}(I; <)$	base de Gröbner reducida de I con respecto a $<$
$\text{in}_w(f)$	forma inicial del polinomio f bajo el vector de peso w
$\text{in}_w(I)$	forma inicial del ideal I bajo el vector de peso w
$\text{pos}(u_1, \dots, u_m)$	envolvente positiva de los puntos $u_1, \dots, u_m$
$\text{conv}(v_1, \dots, v_m)$	envolvente convexa de los puntos $v_1, \dots, v_m$
$\text{face}_w(P)$	cara de P con respecto al vector w
Δ	complejo poliédrico
$ \Delta $	soporte del complejo poliédrico Δ
$\mathcal{N}_P(F)$	cono normal de la cara F del poliedro P

Símbolo	Significado
$\text{New}(f)$	politopo de Newton del polinomio f
$C[w]$	clase de equivalencia de w
$GF(I)$	abanico de Gröbner del ideal I
$\text{State}_d(I)$	politopo de estado de grado d del ideal I
$\text{State}(I)$	politopo de estado del ideal I
$\mathbb{P}^n(k), \mathbb{P}^n$	espacio proyectivo sobre el campo k
$v_{n,d}$	mapeo de Veronese de grado d
$\mathbb{V}_{n,d}$	variedad de Veronese de grado d

OBJETIVOS

General

Calcular los abanicos de Gröbner de variedades de Veronese con el apoyo del software Macaulay2.

Específicos

1. Explicar los fundamentos de la geometría algebraica con el fin de sustentar el objeto de estudio.
2. Definir el concepto de bases de Gröbner como principal objeto de estudio en el desarrollo del trabajo de graduación.
3. Desarrollar los conceptos necesarios de la geometría poliedral y su conexión con las bases de Gröbner.
4. Estudiar los abanicos de Gröbner y su relación con los politopos de estado.
5. Establecer los conceptos de la geometría algebraica proyectiva que permitirán estudiar las variedades de Veronese.

INTRODUCCIÓN

La geometría algebraica tiene como principal área de estudio la conexión entre la geometría y el álgebra, es decir, el estudio de objetos geométricos utilizando conceptos e ideas que conciernen al álgebra abstracta. Esta conexión se logra por medio de lo que denominamos *variedades afines*, las cuales representan curvas y superficies de forma algebraica, a través del estudio de lo que denominamos *ideales* del anillo de polinomios [3]. En este trabajo nos centraremos principalmente en lo que denominamos *variedades de Veronese*, y en particular, estudiaremos los *abanicos de Gröbner* de estas variedades [20].

Para esto iniciaremos, en el capítulo 1, con una pequeña introducción a lo que es la teoría de anillos. Definiremos algunos conceptos de mucha importancia como lo son ideales, dominios íntegros o enteros, dominios de ideales principales; además de esto hablaremos brevemente sobre anillos Noetherianos [4] e introduciremos los conceptos de geometría algebraica más importantes y necesarios.

En el capítulo 2 se definirá el principal objeto de estudio de este trabajo, las *bases de Gröbner*, las cuales nos permiten resolver problemas polinomiales de forma computacional [3]; para esto discutiremos algunos conceptos como los *ordenes monomiales*, *formas iniciales*, entre otros. Esto nos permitirá facilitar la conexión entre *poliedros* [12] y sus principales propiedades (los cuales serán el principal objeto de estudio del capítulo 3) y los conceptos ya presentados de geometría algebraica.

A partir de los conceptos de los capítulos 2 y 3, de bases de Gröbner y geometría poliedral, podremos definir, en el capítulo 4, lo que denominamos como *abanicos de Gröbner* y un algoritmo para poder construirlos [20].

El capítulo 5 inicia presentando lo que denominamos como *espacio proyectivo*, *variedades proyectivas* y propiedades de estas últimas. A partir de esto presentaremos lo que es el *mapeo de Veronese*, el cual nos da una inclusión de variedades proyectivas [19] y nos permite construir las anteriormente mencionadas variedades de Veronese; estudiaremos algunas propiedades básicas de éstas y veremos ejemplos de mucha importancia. Por último procederemos a construir abanicos de Gröbner de

algunas variedades de Veronese, esto con el apoyo de un *sistema algebraico computacional* conocido como Macaulay2 o, simplemente, M2 [6], donde estudiaremos algunas propiedades algebraicas y geométricas vistas con anterioridad.

1. CONCEPTOS PRELIMINARES

1.1. Teoría de anillos

1.1.1. Anillos

El objeto de estudio más básico del presente trabajo de investigación es lo que conocemos como anillo. A continuación se presentarán definiciones básicas y algunos teoremas de importancia sobre la teoría de anillos.

1.1 Definición. Un conjunto no vacío A se llamará *anillo* si cuenta con dos operaciones binarias $+$ y $\cdot$, llamadas suma y multiplicación, tal que cumple con las siguientes propiedades:

1. $a, b \in A$ implica que $a + b \in A$.
2. $a + b = b + a$ para cada $a, b \in A$.
3. $(a + b) + c = a + (b + c)$ para cada $a, b, c \in A$.
4. Existe un elemento $0 \in A$ tal que $a + 0 = 0 + a = a$ para cada $a \in A$.
5. Dado $a \in A$, existe $b \in A$ tal que $a + b = 0$. (Escribiremos b como $-a$.)
6. $a, b \in A$ implica que $a \cdot b \in A$.
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para cada $a, b, c \in A$.
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$ para cada $a, b, c \in A$.

Estas son las propiedades básicas que debe cumplir un anillo, sin embargo, existen algunos casos especiales. En el caso en que la multiplicación sea conmutativa, es decir, $a \cdot b = b \cdot a$, lo llamaremos *anillo conmutativo*. También tenemos el caso en que existe $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in A$, entonces lo llamaremos *anillo con unidad*.

1.2 Ejemplo. Los conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ forman un anillo conmutativo con unidad bajo la suma y multiplicación usual. $2\mathbb{Z} = \{2p \mid p \in \mathbb{Z}\}$ forma un anillo conmutativo sin unidad.

1.3 Ejemplo. El conjunto de todos los polinomios con coeficientes reales, denotado por $\mathbb{R}[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in \mathbb{R}, n \in \mathbb{N}\}$, forma un anillo conmutativo con unidad.

Sabemos que un anillo es un conjunto con dos operaciones binarias así que es natural preguntarnos ¿qué pasa con un subconjunto de un anillo? ¿Es este un anillo también? Para esto veremos las condiciones necesarias que debe cumplir un subconjunto de un anillo bajo las dos operaciones dadas.

1.4 Definición. Sea A un anillo. Entonces un subconjunto B de A se dice que es *subanillo* si B es un anillo bajo las mismas operaciones del anillo A .

Sin embargo, el siguiente teorema nos muestra las condiciones que necesitamos para verificar si algún subconjunto del anillo A es un subanillo.

1.5 Teorema. Sea A un anillo y B un subconjunto de A . Entonces B es un subanillo de A si y solo si

1. $0 \in B$;
2. si $a, b \in B$, entonces $a - b \in B$; y
3. si $a, b \in B$, entonces $ab \in B$.

Demostración. Primero supongamos que B es un subanillo de A . Por la Definición 1.4, B es un anillo. Por la Definición 1.1 tenemos que $0 \in B$.

Supongamos que $a, b \in B$, por la Definición 1.1 tenemos que $-b \in B$, entonces $a + (-b) = a - b \in B$; y también tenemos que $ab \in B$.

Supongamos ahora que B cumple las propiedades (1) – (3). Entonces por (1) tenemos que $0 \in B$.

Supongamos que $a, b \in B$, entonces tenemos que $0 - a = -a \in B$ y de igual forma $-b \in B$. Con esto tenemos que $a - (-b) = a + b \in B$. Por (3) tenemos que $ab \in B$. Para la conmutatividad de la suma veamos que $(a + b) - (a + b) = a + b - a - b = 0$, entonces $a + b = b + a$. Y la asociatividad y distributividad se heredan de A . Por lo que B es un subanillo. $\square$

Algo importante que notar es que para todo anillo A , tenemos que $\{0\}$ y A son subanillos de A .

1.6 Ejemplo. Veamos que $2\mathbb{Z}$ es subanillo de $\mathbb{Z}$ que a su vez es subanillo de $\mathbb{Q}$ y estos a su vez son subanillos de $\mathbb{R}$.

Por el momento hemos definido lo que es un anillo, anillo conmutativo, anillo con unidad y subanillo. No obstante, existen algunos anillos especiales que examinaremos a continuación.

1.7 Definición. Un anillo conmutativo A es un *dominio de integridad* si $a \cdot b = 0$ en A implica que $a = 0$ o $b = 0$.

1.8 Nota. Algunos textos de álgebra indican que un dominio de integridad debe ser un anillo conmutativo con unidad.

1.9 Definición. Un anillo con unidad A se llama *anillo de división* si para cada $a \neq 0$ en A existe un elemento $b \in A$ (normalmente escrito como a^{-1}) tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

1.10 Definición. Un anillo A se llamará *campo* si A es un anillo de división conmutativo.

1.1.2. Ideales, anillo cociente y homomorfismos

En esta sección revisaremos algunos conceptos de mucha importancia en la teoría de anillos como lo son ideales, anillo cociente y homomorfismos entre anillos, además de estudiar algunas de sus propiedades básicas.

1.11 Definición. Sea A un anillo. Entonces un subanillo I de A se dice que es un *ideal* si $ia, ai \in I$ para todo $i \in I$ y todo $a \in A$.

Es decir que un ideal «absorbe» el producto del anillo. Y, así como el Teorema 1.5 para determinar subanillos, existe una forma de identificar ideales fácilmente.

1.12 Teorema. Sea A un anillo. Entonces un subconjunto I de A es un ideal si y solo si

1. $0 \in I$;
2. $i - j \in I$ para todo $i, j \in I$; y
3. $ia, ai \in I$ para todo $i \in I$ y todo $a \in A$.

Demostración. La demostración es bastante similar a la demostración del Teorema 1.5. □

1.13 Ejemplo. Sea n un entero. Entonces $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$. Notemos que $0 \in n\mathbb{Z}$. Si $na, nb \in n\mathbb{Z}$ para $a, b \in \mathbb{Z}$, entonces $na - nb = n(a - b) \in n\mathbb{Z}$. Además, si $na \in n\mathbb{Z}$, $na = an$ ya que los enteros conmutan, entonces $an \in n\mathbb{Z}$.

1.14 Ejemplo. Consideremos el conjunto I de polinomios $f(x) \in \mathbb{R}[x]$ tales que $f(0) = 0$. Entonces I es un ideal de $\mathbb{R}[x]$.

Claramente el polinomio cero está en I . Además, si $f(0) = g(0) = 0$, entonces $(f - g)(0) = f(0) - g(0) = 0$, por lo tanto $f(x) - g(x) \in I$. Ahora, si $f(0) = 0$ y $h(x) \in \mathbb{R}[x]$, entonces $h(0)f(0) = h(0)0 = 0$ y $f(0)h(0) = 0h(0) = 0$ por lo que $f(x)h(x), h(x)f(x) \in I$.

1.15 Ejemplo. Para cualquier anillo A , $\{0\}$ y A son ideales de A .

El siguiente teorema nos muestra una forma de encontrar nuevos ideales a partir de ideales que ya conozcamos. Es decir, que dados los ideales I, J de un anillo A , podemos formar un nuevo ideal como $I + J$ e IJ .

1.16 Teorema. Si I y J son ideales de un anillo A , entonces

$$I + J = \{i + j \mid i \in I, j \in J\},$$

$$IJ = \{i_1j_1 + \cdots + i_nj_n \mid i_k \in I, j_k \in J, n \in \mathbb{N}\},$$

son ideales también.

Demostración. Iniciaremos mostrando que $I + J$ es un ideal. Veamos que $0 \in I$ y $0 \in J$, por lo que $0 + 0 = 0 \in I + J$.

Ahora, sean $x, y \in I + J$, entonces $x = i + j$ y $y = i' + j'$ donde $i, i' \in I$ y $j, j' \in J$. Con esto tenemos que

$$\begin{aligned} x - y &= (i + j) - (i' + j') \\ &= i + j - i' - j' \\ &= (i - i') + (j - j'), \end{aligned}$$

donde $i - i' \in I$ y $j - j' \in J$, por lo que $x - y \in I + J$.

Por último consideremos que $x \in I + J$ y $a \in A$, donde $x = i + j$, $i \in I$ y $j \in J$. Con esto vemos que $ax = a(i + j) = ai + aj$ y también $xa = (i + j)a = ia + ja$, donde vemos que $ai, ia \in I$ y $aj, ja \in J$ por lo que $ax, xa \in I + J$.

Con esto tenemos que $I + J$ es un ideal.

Ahora mostraremos que IJ es un ideal. Notemos que $0 \in I$ y $0 \in J$ así que $0 \cdot 0 = 0 \in IJ$.

Si tenemos $i_k \in I$ y $j_k \in J$, entonces

$$\begin{aligned} & (i_1 j_1 + \cdots + i_m j_m) - (i_{m+1} j_{m+1} + \cdots + i_n j_n) \\ &= i_1 j_1 + \cdots + i_m j_m + (-i_{m+1}) j_{m+1} + \cdots + (-i_n) j_n \in IJ. \end{aligned}$$

Además, para todo $a \in A$ tenemos que

$$a(i_1 j_1 + \cdots + i_m j_m) = (ai_1)j_1 + \cdots + (ai_m)j_m,$$

pero $ai_k \in I$, por lo que $a(i_1 j_1 + \cdots + i_m j_m) \in IJ$. Así también tenemos que

$$(i_1 j_1 + \cdots + i_m j_m)a = i_1(j_1 a) + \cdots + i_m(j_m a),$$

pero $j_k a \in J$ así que $(i_1 j_1 + \cdots + i_m j_m)a \in IJ$. Y así concluimos que IJ es un ideal de A . $\square$

1.17 Definición. Sea X un subconjunto cualquiera de un anillo A . Entonces el *ideal generado por X* , denotado por (X) , es el ideal más pequeño de A que contiene a X . Si X es finito, diremos que (X) es *finitamente generado*.

Otra forma de ver al ideal generado por $X \subseteq A$, donde A es conmutativo, es

$$(X) = \{x_1 a_1 + \cdots + x_n a_n \mid x_i \in X, a_i \in A, n \in \mathbb{N}\}$$

Existe un tipo muy importante de ideal que definiremos a continuación.

1.18 Definición. Sea A un anillo conmutativo con unidad y $a \in A$. Entonces el *ideal principal* generado por a es (a) .

1.19 Ejemplo. En $\mathbb{Z}$, tenemos que $(n) = n\mathbb{Z}$ para $n \in \mathbb{Z}$.

1.20 Teorema. Si A es un anillo conmutativo con unidad, y $a \in A$, entonces (a) es un ideal de A ; ciertamente, (a) es la intersección de todos los ideales de A que contienen a a .

Demostración. Como $0 \in A$, $0a = 0 \in (a)$. Sean $x, y \in (a)$, entonces $x = ra$ y $y = r'a$, $r, r' \in A$; con esto vemos que $x - y = ra - r'a = (r - r')a \in (a)$. Sea $x \in (a)$, entonces $x = ra$, $r \in A$, y sea $s \in A$; con esto tenemos que $s(ra) = (ra)s = (rs)a \in (a)$. Por lo que (a) es un ideal de A .

Sea I un ideal de A tal que $a \in I$, por lo que para todo $r \in A$, $ra \in I$. Entonces (a) es un subconjunto de cualquier ideal de A que contenga a . Como (a) es un ideal que contiene a , tenemos que (a) es la intersección de todos los ideales que contienen a . $\square$

Dado un anillo y un ideal de éste, podremos definir nuevos anillos de mucha importancia conocidos como anillos cociente.

1.21 Definición. Sea A un anillo e I un ideal de A . Entonces, el *anillo cociente* A/I es el conjunto $\{a + I \mid a \in A\}$, junto con las operaciones $(a + I) + (b + I) = a + b + I$ y $(a + I)(b + I) = ab + I$, para todo $a, b \in A$.

Para cada anillo A y cualquier ideal I de este anillo, el anillo cociente A/I siempre formará un anillo con la suma y el producto como lo definimos anteriormente. Además también tenemos que si A es un anillo conmutativo, también lo es A/I ; y si A es un anillo con unidad, también lo es A/I .

Ahora nos preguntamos ¿qué pasa con funciones cuyo dominio y contradominio son anillos? Estas funciones reciben el nombre de homomorfismos y tienen la cualidad de respetar ambas operaciones del anillo.

1.22 Definición. Sean A y B anillos. Entonces un *homomorfismo de anillos* (o simplemente *homomorfismo*) de A a B es una función $\alpha: A \rightarrow B$ que satisface

$$\alpha(a_1 + a_2) = \alpha(a_1) + \alpha(a_2)$$

y

$$\alpha(a_1 a_2) = \alpha(a_1) \alpha(a_2)$$

para todo $a_1, a_2 \in A$.

Un concepto muy importante de homomorfismos es el de kernel (o núcleo), que en la teoría de anillos resulta ser un ideal del dominio. Además el kernel nos permite identificar si un homomorfismo es inyectivo o no, dado que $\ker(\alpha) = \{0\}$.

1.23 Definición. Sea $\alpha: A \rightarrow B$ un homomorfismo. Entonces el *kernel* de α es

$$\ker(\alpha) = \{a \in A \mid \alpha(a) = 0\}.$$

Algunas propiedades de los homomorfismos es que la imagen de un subanillo del dominio, será un subanillo del contradominio. Lo mismo sucede con los ideales.

La identidad de la suma del dominio se mapea en la identidad de la suma del contradominio (y si el anillo es un anillo con unidad, lo mismo sucede con la identidad del producto).

Si un homomorfismo es biyectivo lo llamaremos *isomorfismo* y un isomorfismo que tiene como dominio y contradominio al mismo anillo se llamará *automorfismo*.

A continuación se presentarán tres teoremas de mucha importancia sobre isomorfismo, cuya demostración puede ser encontrada en cualquier libro de álgebra abstracta como [4], [14] o [11].

1.24 Teorema (Primer Teorema de Isomorfismo). *Sea $\alpha: A \rightarrow B$ un homomorfismo. Entonces $A/\ker(\alpha)$ es isomorfo a $\alpha(A)$.*

1.25 Teorema (Segundo Teorema de Isomorfismo). *Sea A un anillo con ideales I y J . Entonces $I/(I \cap J)$ es isomorfo a $(I + J)/J$.*

1.26 Teorema (Tercer Teorema de Isomorfismo). *Sea A un anillo con ideales I y J tales que $I \subseteq J$. Entonces $(A/I)/(J/I)$ es isomorfo a R/J .*

1.1.3. Dominios especiales

Si recordamos el Ejemplo 1.3, el conjunto de todos los polinomios con coeficientes reales forman un anillo. Sin embargo, no es necesario considerar solo el conjunto de polinomios con coeficientes reales; en general si tenemos un anillo A , el conjunto de todos los polinomios con coeficientes en A con la suma y producto con el que ya estamos familiarizados, denotado por $A[x]$, es un anillo como veremos a continuación.

1.27 Teorema. *Si A es un anillo, su anillo de polinomios $A[x]$ también es un anillo.*

Demostración. Sean $f, g, h \in A[x]$ tales que

$$\begin{aligned} f(x) &= a_0 + \cdots + a_n x^n \\ g(x) &= b_0 + \cdots + b_m x^m \\ h(x) &= c_0 + \cdots + c_k x^k \end{aligned}$$

donde las a 's, b 's y c 's están en A .

El coeficiente x^i de $f(x) + g(x)$ es $a_i + b_i \in A$ por lo que $f(x) + g(x) \in A[x]$. Además $a_i + b_i = b_i + a_i$ que es el coeficiente x^i de $g(x) + f(x)$, por lo que $f(x) + g(x) = g(x) + f(x)$. Con esto tenemos que la suma es cerrada y conmutativa en

$A[x]$. Como los coeficientes son asociativos bajo la suma en A , $A[x]$ es asociativo. El polinomio 0 es la identidad de la suma. Para cada polinomio $f(x)$ como lo definimos anteriormente, existe su inverso $-f(x) = -a_0 - \cdots - a_n x^n$.

Ahora, el coeficiente x^i de $f(x)g(x)$ es $a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0 \in A$, así que $f(x)g(x) \in A[x]$. Por lo que $A[x]$ es cerrado bajo el producto. Veamos ahora que el coeficiente x^i de $f(x)(g(x) + h(x))$ es

$$\begin{aligned} & a_0(b_i + c_i) + a_1(b_{i-1} + c_{i-1}) + \cdots + a_i(b_0 + c_0) \\ &= (a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0) + (a_0 c_i + a_1 c_{i-1} + \cdots + a_i c_0) \end{aligned}$$

que es el coeficiente x^i de $f(x)g(x) + f(x)h(x)$, así que

$$f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x).$$

La otra ley distributiva se demuestra de forma similar.

Solo nos queda demostrar la asociatividad del producto. Si utilizamos la ley distributiva repetidas veces, reducimos el problema a mostrar que $(a_u x^u b_v x^v) c_w x^w = a_u x^u (b_v x^v c_w x^w)$, para todo $a_u, b_v, c_w \in A$; $u, v, w \geq 0$. Sin embargo, esta última ecuación es equivalente, en ambos lados, a $a_u b_v c_w x^{u+v+w}$. $\square$

También tenemos que si A es un anillo con identidad, un anillo conmutativo o un dominio de integridad, entonces $A[x]$ también lo es. En particular, si A es un campo tenemos que su anillo de polinomios $A[x]$ cumple con el algoritmo de la división.

1.28 Teorema. *Sea A un campo, sean $f(x)$ y $g(x)$ polinomios en $A[x]$ con $g(x) \neq 0$. Entonces existen polinomios únicos $q(x)$ y $r(x)$ en $A[x]$ tales que*

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

con $r(x) = 0$ o el grado de $r(x)$ es menor al grado de $g(x)$.

Demostración. Ver [14, p. 174] $\square$

Existen, además de anillos de polinomios, dominios de integridad especiales que cuentan con alguna propiedad especial. En particular nos interesan los dominios de ideales principales.

1.29 Definición. Un *dominio de ideales principales* es un dominio de integridad donde cada ideal es principal.

1.1.4. Anillos conmutativos

A partir de ahora, siempre que que hablemos de un anillo, nos referiremos a un anillo conmutativo con unidad. Veremos algunas definiciones y teoremas de importancia.

1.30 Definición. Un anillo A es *Noetheriano* si no existe una cadena creciente infinita de ideales en A , es decir, siempre que $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ sea una cadena creciente de ideales en A , entonces existe un entero positivo m tal que $I_k = I_m$ para todo $k \geq m$.

En otras palabras, un anillo Noetheriano es un anillo tal que sus ideales cumplen lo que se conoce como la condición de cadena ascendente.

Si tenemos un ideal I de un anillo Noetheriano A , su cociente A/I también será un anillo Noetheriano, y la imagen de un anillo Noetheriano bajo homomorfismo también lo será. Además, cada ideal de A es finitamente generado.

1.31 Ejemplo. Cualquier dominio de ideales principales es un anillo Noetheriano.

1.32 Ejemplo. Los enteros $\mathbb{Z}$, el anillo de polinomios $k[x]$ de un campo k y los enteros Gaussianos $\mathbb{Z}[i]$, son anillos Noetherianos.

1.33 Definición. Sea I un ideal de un anillo A . El *radical* de I , denotado por $\sqrt{I}$, es el conjunto

$$\sqrt{I} = \{a \in A \mid a^k \in I \text{ para algún } k \geq 1\}.$$

Si $I = \sqrt{I}$, diremos que I es un *ideal radical*.

Notemos que para cada ideal I , $\sqrt{I}$ también es un ideal y tenemos que $I \subseteq \sqrt{I}$.

1.34 Ejemplo. En el anillo de los enteros $\mathbb{Z}$, el ideal (a) es radical si y solo si a no es un cuadrado o es cero.

1.2. Geometría algebraica

En pocas palabras, y de manera muy simplificada, la geometría algebraica estudia objetos geométricos, que llamamos una variedad afín, que pueden ser descritos por ceros de polinomios. En esta sección se presentarán algunas definiciones, teoremas y propiedades básicas que serán de utilidad más adelante.

Supongamos que k es un campo, definiremos su *espacio afín* de dimensión n como

$$k^n = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in k\}.$$

Es decir que el espacio afín es el conjunto de n -tuplas de elementos de k . En particular, $k^1 = k$ se llama la recta afín y k^2 se llama el plano afín.

1.35 Definición. Sea k un campo y sea $S \subseteq k[x_1, \dots, x_n]$. Entonces el conjunto

$$V(S) = \{(a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \text{ para todo } f \in S\}$$

es una *variedad afín* definida por S . Si $S = \{f_1, \dots, f_n\}$, escribimos $V(f_1, \dots, f_n)$.

Es decir, que una variedad afín es el conjunto de soluciones en común de los polinomios del conjunto S . Además, notemos que $V(k[x_1, \dots, x_n]) = \emptyset$ y $V(0) = k^n$, es decir que la variedad de todo el anillo de polinomios es el vacío y la variedad del polinomio 0 es todo el espacio afín.

1.36 Ejemplo. Sea $f(x, y) = x^2 + y^2 - 1$ un polinomio de $\mathbb{R}[x, y]$. Entonces $V(f)$ es el círculo unitario centrado en el origen.

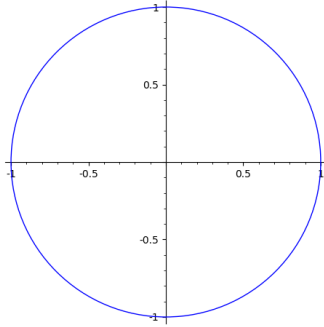


Figura 1.1. Círculo unitario. Fuente: elaboración propia utilizando SageMath.

1.37 Ejemplo. Consideremos los polinomios $f(x, y, z) = y - x^2$ y $g(x, y, z) = z - x^3$. La variedad afín $V(f, g)$ se conoce como la *cúbica abaleada* y la podemos observar en la Figura 1.2.

1.38 Teorema. Sean $S, T \subseteq k[x_1, \dots, x_n]$ y $V(S), V(T) \subseteq k^n$ variedades afín. Entonces

$$\begin{aligned} V(S) \cap V(T) &= V(S \cup T), \\ V(S) \cup V(T) &= V(\{fg \mid f \in S, g \in T\}) \end{aligned}$$

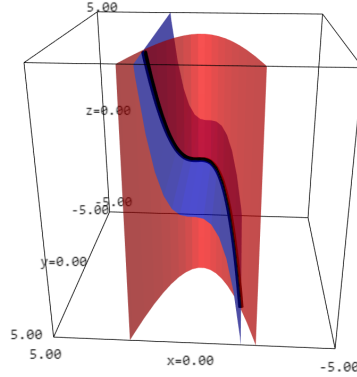


Figura 1.2. Cúbica abaleada. Fuente: elaboración propia utilizando SageMath.

también son variedades afín.

Demostración. Para demostrar la primer igualdad sea $x \in V(S) \cap V(T)$, si y solo si $x \in V(S)$ y $x \in V(T)$, si y solo si x es un cero de los polinomios de S y T , si y solo si $x \in V(S \cup T)$.

Para la segunda igualdad supongamos que $x \in V(S) \cup V(T)$, entonces $x \in V(S)$ o $x \in V(T)$. Supongamos que $x \in V(S)$, entonces x es un cero para cada $f \in S$, por lo que también lo es de fg , para cada $g \in T$; de forma similar cuando $x \in V(T)$. Con esto tenemos que $x \in V(\{fg \mid f \in S, g \in T\})$. Por otro lado supongamos que $y \in V(\{fg \mid f \in S, g \in T\})$. Si $y \in V(S)$ hemos terminado, de lo contrario tenemos que existe algún $f \in S$ tal que $f(y) \neq 0$. Esto implica que $y \in V(T)$, por lo que $y \in V(S) \cup V(T)$. $\square$

Este último teorema implica que la intersección arbitraria de variedades es una variedad y la unión finita de variedades es una variedad. En especial, el conjunto de variedades afín del espacio afín k^n forman el conjunto de cerrados de la llamada *topología de Zariski*.

Hasta ahora hemos visto las variedades afín $V(S)$, donde $S \subseteq k[x_1, \dots, x_n]$, sin embargo, si consideramos el ideal $I = (S)$ tenemos que $V(S) = V(I)$. Es decir, toda variedad afín está definida por un ideal del anillo de polinomios. Además si tenemos dos ideales I, J tales que $I \subseteq J$, entonces $V(I) \supseteq V(J)$.

1.39 Definición. Sea $V \subseteq k^n$ una variedad afín. Entonces definimos el conjunto

$$I(V) = \{f \in k[x_1, \dots, x_n] \mid f(x) = 0 \text{ para todo } x \in V\}.$$

1.40 Teorema. Si $V \subseteq k^n$ es una variedad afín, entonces $I(V)$ es un ideal de $k[x_1, \dots, x_n]$. Llamamos a $I(V)$ el ideal de V .

Demostración. Claramente $0 \in I(V)$, puesto que para cada $x \in V$ tenemos que $0(x) = 0$.

Sean $i, j \in I(V)$, entonces para cada $x \in V$ tenemos que $i(x) - j(x) = 0 - 0 = 0$, así que $i - j \in I(V)$.

Sea $i \in I(V)$ y $f \in k[x_1, \dots, x_n]$, entonces para todo $x \in V$ tenemos que $f(x)i(x) = f(x) \cdot 0 = 0$ y de igual forma $i(x)f(x) = 0 \cdot f(x) = 0$, por lo que $if, fi \in I(V)$. Con esto tenemos que $I(V)$ es un ideal de $k[x_1, \dots, x_n]$. $\square$

Algo importante que notar es que si tenemos un ideal $I = (S)$, $S \subseteq k[x_1, \dots, x_n]$, entonces $I \subseteq I(V(S))$. Es decir que el ideal generado por un conjunto está contenido en el ideal de la variedad de ese conjunto, sin embargo, el ideal de una variedad nos permite determinar la variedad de manera única por medio de la siguiente manera:

1. $V \subseteq W$ si y solo si $I(V) \supseteq I(W)$.
2. $V = W$ si y solo si $I(V) = I(W)$.

Otro resultado importante es el hecho que cualquier ideal de una variedad $I(V)$ es un ideal radical, es decir, $I(V) = \sqrt{I(V)}$.

1.41 Definición. Un campo k se dice que es algebraicamente cerrado si cada polinomio con coeficientes en k tiene sus raíces en k .

Por ejemplo, el campo de los números complejos, $\mathbb{C}$, es algebraicamente cerrado.

1.42 Teorema (Nullstellensatz de Hilbert). Sea I un ideal de $k[x_1, \dots, x_n]$, donde k es algebraicamente cerrado. Entonces $I(V(I)) = \sqrt{I}$.

Demostración. Ver [5, p. 10]. $\square$

2. BASES DE GRÖBNER

2.1. Ordenes monomiales y bases de Gröbner

Si consideramos el anillo de polinomios $k[x] = k[x_1, \dots, x_n]$ de un campo k , diremos que un *monomio* es un elemento de la forma

$$x^a := x_1^{a_1} \cdots x_n^{a_n},$$

donde $a = (a_1, \dots, a_n) \in \mathbb{Z}_{\geq 0}^n$ y sea $\text{Mon} \subset k[x]$ el conjunto de monomios.

2.1 Definición (Orden Monomial). Un *orden monomial* $\leq$ en Mon es aquel tal que para $x^a, x^b, x^c \in \text{Mon}$ tenemos que

1. $x^a \leq x^a$;
2. $x^a \leq x^b$ y $x^b \leq x^a$ implica que $x^a = x^b$;
3. $x^a \leq x^b$ y $x^b \leq x^c$ implica que $x^a \leq x^c$;
4. $x^a \leq x^b$ o $x^b \leq x^a$ para todo $x^a, x^b \in \text{Mon}$;
5. $1 \leq x^a$ para todos $1 \neq x^a \in \text{Mon}$;
6. si $x^a, x^b \in \text{Mon}$ y $x^a \leq x^b$ entonces $x^a x^c \leq x^b x^c$ para todo $x^c \in \text{Mon}$.

La siguiente propiedad es de mucha importancia cuando hablamos sobre un orden monomial.

2.2 Proposición. Sea $<$ un orden monomial. Para cada $x^a \in \text{Mon}$ tenemos que cada secuencia de la forma $x^a > x^{a_1} > x^{a_2} > \dots$ eventualmente termina.

Demostración. Supongamos que existe $x^a \in \text{Mon}$ tal que existe una cadena infinita la forma $x^a > x^{a_1} > x^{a_2} > \dots$. Notemos que existe una cantidad finita de monomios tales que $x^a > x^{a_1} > x^{a_2} > \dots > x^{a_n} > 1$, sin embargo, la cadena es infinita así que debe existir $x^b \in \text{Mon}$ tal que $1 > x^b$, lo cual es una contradicción. $\square$

Los siguientes son algunos ejemplos de ordenes monomiales.

- El *orden lexicográfico*, $<_{lex}$, está definido como $x^a <_{lex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \min\{i \mid a_i - b_i \neq 0\}$.
- El *orden lexicográfico graduado*, $<_{deglex}$, se define como $x^a <_{deglex} x^b$ si y solo si

1. $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$, o
2. $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ y $a_j - b_j < 0$ para $j = \min\{i \mid a_i - b_i \neq 0\}$.

- El *orden lexicográfico reverso*, $<_{revlex}$, se define como $x^a <_{revlex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \max\{j \mid a_i - b_i \neq 0\}$.
- El *orden lexicográfico reverso graduado*, $<_{degrevlex}$, lo definimos como $x^a <_{degrevlex} x^b$ si y solo si

1. $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$, o
2. $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ y $a_j - b_j < 0$ para $j = \max\{i \mid a_i - b_i \neq 0\}$.

2.3 Ejemplo. Consideremos los monomios $y^3, xz^2, xyz, xy, yz, z \in k[x, y, z]$ con $x > y > z$. Aplicando los ordenes monomiales anteriores tenemos

- Lex: $z < yz < y^3 < xz^2 < xy < xyz$.
- Deglex: $z < yz < xy < y^3 < xz^2 < xyz$.
- Revlex: $xy < y^3 < z < yz < xyz < xz^2$.
- Degrevlex: $xy < z < yz < y^3 < xyz < xz^2$.

La siguiente definición nos brindará terminología de importancia.

2.4 Definición. Sea $<$ un orden monomial y $f = \sum_{i=1}^m c_i x^{a_i} \in k[x]$, donde cada $c_i \in k$. Entonces la *forma inicial* de f bajo $<$ se define como $\text{in}_{<}(f) := c_j x^{a_j}$ con $x^{a_j} = \max_{<}\{x^{a_i} \mid c_i \neq 0\}$.

En la forma inicial $\text{in}_{<}(f) = c_j x^{a_j}$, c_j se denomina como *coeficiente principal* y x^{a_j} se conoce como *monomio principal*.

2.5 Ejemplo. Consideremos el polinomio $f = x^2 + xy + y^2 \in k[x, y]$, entonces

$$\begin{aligned}\text{in}_{<_{lex}}(f) &= x^2, \\ \text{in}_{<_{revlex}}(f) &= y^2.\end{aligned}$$

2.6 Definición. Sea $I \subseteq k[x]$ un ideal. Entonces definimos su *ideal inicial*, con respecto a $<$, como

$$\text{in}_<(I) := (\text{in}_<(f) \mid f \in I, f \neq 0).$$

Es decir que el ideal inicial es el ideal generado por todas las formas iniciales de los polinomios de un ideal. A continuación veremos algunas propiedades importantes sobre formas iniciales.

2.7 Proposición. Sean $x^a, x^b \in \text{Mon}$ y $f, g \in k[x]$. Entonces

1. si x^a divide a x^b , entonces $x^a \leq x^b$;
2. $\text{in}_<(x^a f) = x^a \text{in}_<(f)$;
3. $\text{in}_<(fg) = \text{in}_<(f) \text{in}_<(g)$;
4. $\text{in}_<(f + g) \leq \max\{\text{in}_<(f), \text{in}_<(g)\}$, donde la igualdad se alcanza cuando $\text{in}_<(f) \neq \text{in}_<(g)$.

La demostración de las primeras tres propiedades es directa. Sin embargo, la forma inicial de la suma solo nos da una cota superior debido a que si $\text{in}_<(f) + \text{in}_<(g) = 0$ la forma inicial de $f + g$ será menor.

Si tenemos un orden monomial $<$ y un ideal I , los monomios $x^a \notin \text{in}_<(I)$ se conocen como *monomios estándar*. Y el conjunto

$$\mathbb{B}_< := \{\bar{x}^a \in k[x]/I \mid x^a \notin \text{in}_<(I)\}$$

se llama una *base de monomios estándar*.

2.8 Proposición. $\mathbb{B}_<$ es una k -base (visto como espacio vectorial) de $k[x]/I$ y de $k[x]/\text{in}_<(I)$ para cada ideal I y cada orden monomial $<$.

La siguiente definición y, en general, el estudio de bases de Gröbner nos permite resolver problemas sobre ideales de polinomios de manera algorítmica. Algunos de estos problemas son: conocer si cada ideal del anillo de polinomios es finitamente generado; encontrar las soluciones en común de un sistema de polinomios; entre varios más.

2.9 Definición (Base de Gröbner). Sea $I \subseteq k[x]$ un ideal y $<$ un orden monomial. Un conjunto finito $\{g_1, \dots, g_s\}$ de elementos en I se llama *base de Gröbner* de I con respecto a $<$ si

$$\text{in}_<(I) = (\text{in}_<(g_1), \dots, \text{in}_<(g_s)).$$

2.10 Ejemplo. Consideremos el ideal $I = (x^2 - y, x^3 - z)$ en $k[x, y, z]$. El conjunto $G = \{y^3 - z^2, -y^2 + xz, xy - z, x^2 - y\}$ es una base de Gröbner de I bajo $<_{lex}$.

2.11 Ejemplo. Si tomamos el ideal $I = (xy^3 - x^2, x^3y^2 - y)$ en $k[x, y]$. Tomando $<_{deglex}$ tenemos que $G = \{xy - y^4, -x^2 + xy^3, -x^4 + y^2, -y + x^3y^2\}$ es una base de Gröbner de I .

2.12 Lema. Sea J un ideal generado por los monomios $\{x^{a_1}, \dots, x^{a_t}\}$, entonces un monomio $x^b \in J$ si y solo si existe un monomio x^c tal que $x^b = x^c x^{a_i}$, para algún $1 \leq i \leq t$.

Demostración. Si suponemos que existe x^c tal que $x^b = x^c x_i^a$, para algún $1 \leq i \leq t$, claramente $x^b \in J$ por definición de ideal.

Supongamos ahora que $x^b \in J$, entonces

$$x^b = \sum_{i=1}^t f_i x^{a_i} = \sum_{i=1}^t \left(\sum_j c_{i,j} x^{d_{i,j}} \right) x^{a_i} = \sum_{i,j} c_{i,j} x^{d_{i,j} + a_i}.$$

Luego de operar términos del mismo multigrado, tenemos que el lado derecho es divisible dentro de algún x^{a_i} , por lo que existe x^c tal que $x^b = x^c x^{a_i}$. $\square$

2.13 Teorema. Sea I un ideal en $k[x]$ y $G = \{g_1, \dots, g_s\}$ una base de Gröbner de I con respecto al orden monomial $<$. Entonces G genera al ideal I .

Demostración. Sea $f \in I$, $f \neq 0$. Entonces $\text{in}_<(f) \in \text{in}_<(I) = (\text{in}_<(g_1), \dots, \text{in}_<(g_s))$. Por el Lema 2.12 existe $g_{i_0} \in G$ tal que $\text{in}_<(g_{i_0})$ divide a $\text{in}_<(f)$, y sea $x^{a_0} \in \text{Mon}$ tal que $\text{in}_<(f) = c x^{a_0} \text{in}_<(g_{i_0})$ para algún $c \in k$.

Definamos

$$h_0 = f - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0} \in I$$

donde c_0, c_{i_0} son los coeficientes principales de f, g_{i_0} respectivamente. Con la Proposición 2.7 tenemos que $\text{in}_<(h_0) < \text{in}_<(f)$. Si $h_0 = 0$ tenemos que $f \in (g_1, \dots, g_s)$. Si $h_0 \neq 0$ realizamos el mismo procedimiento con h_0 en lugar de f .

Con eso tenemos que

$$h_1 = f - c_{i_1}^{-1} c_1 x^{a_1} g_{i_1} - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0}$$

donde $g_{i_1} \in G$ tal que $\text{in}_<(g_{i_1})$ divide a $\text{in}_<(h_0)$. Además c_{i_1}, c_1 son los coeficientes principales de g_{i_1}, h_0 respectivamente. Como antes, tenemos que $\text{in}_<(h_1) < \text{in}_<(h_0)$. Si $h_1 = 0$ tenemos que $f \in (g_1, \dots, g_s)$. Si $h_1 \neq 0$ continuamos el procedimiento.

Por la Proposición 2.2 sabemos que el procedimiento eventualmente termina, y obtenemos una expresión de la forma

$$f = \sum_{q=0}^N c_{i_q}^{-1} c_q x^{a_q} g_{i_q}.$$

Por lo que $f \in (g_1, \dots, g_s)$. □

Este teorema nos asegura que cada ideal I del anillo de polinomios $k[x]$ tiene una base de Gröbner, y como resultado inmediato tenemos el siguiente corolario.

2.14 Corolario (Teorema de la Base de Hilbert). *Cada ideal del anillo de polinomios tiene un conjunto de generadores finito.*

Este teorema recibe su nombre gracias al matemático David Hilbert,¹ quien hizo una primera demostración en el año 1888. Sin embargo esta demostración fue del tipo no constructiva, lo que provocó muchas críticas en ese entonces. Más adelante, con el desarrollo de las bases de Gröbner, se logró una demostración constructiva del teorema.

Existen varios tipos de bases de Gröbner, entonces una base de Gröbner $G = \{g_1, \dots, g_s\}$ se conoce como:

- *Reducida* si satisface que
 1. el coeficiente principal de g_i es 1 para $1 \leq i \leq s$, y
 2. si $i \neq j$, ningún monomio de g_j es divisible por $\text{in}_<(g_i)$.
- *Minimal* si ningún monomio en el conjunto $\{\text{in}_<(g) \mid g \in G\}$ es redundante.
- *Universal* si es una base de Gröbner para cada orden monomial $<$ simultáneamente.

Utilizamos la notación $G_{\text{red}}(I; <)$ para denotar la base de Gröbner reducida de I con respecto a $<$.

2.15 Teorema. *Para cada ideal I y cada orden monomial $<$, existe una única base de Gröbner reducida $G_{\text{red}}(I; <)$.*

¹**David Hilbert** (1862-1943), uno de los matemáticos más influyentes de finales del siglo XIX y principios del XX.

Demostración. Para la existencia, sea I un ideal no nulo de $k[x]$ y $\{u_1, \dots, u_s\}$ un sistema minimal de monomios generadores de $\text{in}_<(I)$. Entonces, para cada $i \neq j$, el monomio u_i no es divisible por u_j . Para cada $1 \leq i \leq s$, tomemos un polinomio $g_i \in I$ tal que $\text{in}_<(g_i) = u_i$.

Sea $g_1 = f_2g_2 + \dots + f_sg_s + h_1$ sea una expresión de g_1 con respecto a $g_2, \dots, g_s$, donde h_1 es un residuo. De esto tenemos que $\text{in}_<(g_1)$ debe coincidir con alguno de los monomios $\text{in}_<(f_2g_2), \dots, \text{in}_<(f_sg_s), \text{in}_<(h_1)$. Como $u_1 = \text{in}_<(g_1)$ no puede ser dividido por los monomios $\text{in}_<(g_2), \dots, \text{in}_<(g_s)$, tenemos que $\text{in}_<(g_1) = \text{in}_<(h_1)$. Por tanto $\{h_1, g_2, \dots, g_s\}$ es una base de Gröbner de I . Como h_1 es residuo de g_1 con respecto a $g_2, \dots, g_s$, entonces cada monomio de h_1 no es divisible entre los monomios $\text{in}_<(g_2), \dots, \text{in}_<(g_s)$.

De manera similar, si h_2 es un residuo de g_2 con respecto a $h_1, g_3, \dots, g_s$, entonces tenemos que $\text{in}_<(h_2) = \text{in}_<(g_2)$ y cada monomio de h_2 no es divisible por $\text{in}_<(h_1), \text{in}_<(g_3), \dots, \text{in}_<(g_s)$. En particular, $\{h_1, h_2, g_3, \dots, g_s\}$ es una base de Gröbner de I . Como $\text{in}_<(h_2) = \text{in}_<(g_2)$, cada monomio de h_2 no es divisible entre los monomios $\text{in}_<(h_1), \text{in}_<(g_3), \dots, \text{in}_<(g_s)$.

Continuando este proceso nos da los polinomios $h_3, \dots, h_s$ y obtenemos una base de Gröbner $\{h_1, \dots, h_s\}$ de I . Dividiendo cada h_i por el coeficiente de $\text{in}_<(h_i)$ para todo i , obtenemos una base de Gröbner reducida de I .

Para la unicidad, sean $\{g_1, \dots, g_s\}$ y $\{h_1, \dots, h_t\}$ bases de Gröbner reducidas de I . Como $\{\text{in}_<(g_1), \dots, \text{in}_<(g_s)\}$ y $\{\text{in}_<(h_1), \dots, \text{in}_<(h_t)\}$ son sistemas de monomios minimales que generan al ideal inicial $\text{in}_<(I)$ de I , podemos asumir que $s = t$ y que $\text{in}_<(g_i) = \text{in}_<(h_i)$ para todo i . Si $g_i \neq h_i$, entonces $0 \neq g_i - h_i \in I$ y que $\text{in}_<(g_i - h_i) < \text{in}_<(g_i)$. En particular $\text{in}_<(g_i)$ no divide a $\text{in}_<(g_i - h_i)$. Como $\text{in}_<(g_i - h_i)$ debe ser un monomio de g_i o h_i , tenemos que $\text{in}_<(g_i - h_i)$ no es divisible entre $\text{in}_<(g_j)$ con $i \neq j$. Por tanto $\text{in}_<(g_i - h_i) \notin \text{in}_<(I)$. Esto contradice que $g_i - h_i \in I$. $\square$

2.16 Corolario. Sean I, J ideales de $k[x]$. Entonces $I = J$ si y solo si $G_{\text{red}}(I; <) = G_{\text{red}}(J; <)$.

Por último veremos un resultado importante que nos permite generalizar el Teorema 1.28,

2.17 Teorema (Algoritmo de la División). Sea $<$ un orden monomial en $k[x]$. Sean $g_1, \dots, g_s \in k[x]$ polinomios no nulos. Entonces para cada polinomio no nulo $f \in k[x]$, existen polinomios $f_1, \dots, f_s, f' \in k[x]$ con

$$f = f_1g_1 + \dots + f_sg_s + f',$$

tal que se cumplen las siguientes condiciones:

1. si $f' \neq 0$, entonces para cada monomio x^a de f' , $x^a \notin (\text{in}_<(g_1), \dots, \text{in}_<(g_s))$;
2. si $f_i \neq 0$ tenemos que $\text{in}_<(f) \geq \text{in}_<(f_i g_i)$.

Llamaremos a la expresión $f = f_1 g_1 + \dots + f_s g_s + f'$ *forma estándar* de f con respecto a $g_1, \dots, g_s$, y diremos que f' es el residuo de f con respecto a $g_1, \dots, g_s$. Si $f' = 0$, decimos que f se *reduce a cero* con respecto a $g_1, \dots, g_s$.

Demostración. Sea $I = (\text{in}_<(g_1), \dots, \text{in}_<(g_s))$. Si ninguno de los monomios x^a de f está en I , entonces la expresión deseada sería $f = f'$ con $f_1 = \dots = f_s = 0$.

Ahora supongamos que algún monomio x^a de f está en I y escribamos x^{a_0} para denotar al monomio más grande con respecto a $<$ de los monomios de f que pertenecen a I . Digamos que $\text{in}_<(g_{i_0})$ divide a x^{a_0} y $x^{b_0} = x^{a_0} / \text{in}_<(g_{i_0})$. Escribimos

$$f = c'_0 c_{i_0}^{-1} x^{b_0} g_{i_0} + h_1,$$

donde c'_0 es el coeficiente de x^{a_0} en f y c_{i_0} es el coeficiente de $\text{in}_<(g_{i_0})$ en g_{i_0} . Tenemos que

$$\text{in}_<(x^{b_0} g_{i_0}) = x^{b_0} \text{in}_<(g_{i_0}) = x^{a_0} \leq \text{in}_<(f).$$

Si $h_1 = 0$ o, si $h_1 \neq 0$ pero ninguno de sus monomios está en I , entonces $f = c'_0 c_{i_0}^{-1} x^{b_0} g_{i_0} + h_1$ es una expresión estándar de f con respecto a $g_1, \dots, g_s$ y h_1 es el residuo de f .

Si un monomio de h_1 pertenece a I , y digamos que x^{a_1} es el más grande de ellos, entonces $x^{a_0} > x^{a_1}$. Notemos que ningún monomio de h_1 que pertenezca a I puede ser más grande que x^{a_0} y x^{a_0} no es monomio de h_1 .

Digamos que $\text{in}_<(g_{i_1})$ divide a x^{a_1} y que $x^{b_1} = x^{a_1} / \text{in}_<(g_{i_1})$. Entonces tenemos

$$f = c'_0 c_{i_0}^{-1} x^{b_0} g_{i_0} + c'_1 c_{i_1}^{-1} x^{b_1} g_{i_1} + h_2,$$

donde c'_1 es el coeficiente de x^{a_1} en h_1 y c_{i_1} es el coeficiente de $\text{in}_<(g_{i_1})$ en g_{i_1} . Y se tiene que

$$\text{in}_<(x^{b_1} g_{i_1}) < \text{in}_<(x^{b_0} g_{i_0}) \leq \text{in}_<(f).$$

Continuando el proceso nos da una sucesión de la forma

$$x^{a_0} > x^{a_1} > x^{a_2} > \dots$$

que por la Proposición 2.2 sabemos que el proceso termina luego de una cantidad finita de pasos. Supongamos que fueron N pasos, entonces obtenemos una expresión de la forma

$$f = \sum_{q=0}^{N-1} c'_q c_{i_q}^{-1} x^{b_q} g_{i_q} + h_N,$$

donde $h_N = 0$ o, en caso de que $h_N \neq 0$, ninguno de sus monomios pertenecen a I . Además también tenemos que

$$\text{in}_<(x^{b_q} g_{i_q}) < \dots < \text{in}_<(x^{b_0} g_{i_0}) \leq \text{in}_<(f).$$

Por lo que hemos encontrado una expresión $f = \sum_{i=1}^s f_i g_i + f'$ que satisface las condiciones deseadas. $\square$

2.18 Nota. Debemos de notar que el residuo, en este caso, no es único así como lo era en el caso de una variable.

2.19 Ejemplo. Sea $<_{lex}$ el orden lexicográfico en $k[x, y, z]$, inducido por $x > y > z$. Sea $g_1 = x^2 - z$, $g_2 = xy - 1$ y $f = x^3 - x^2 y - x^2 - 1$. Entonces tenemos que

$$f = (x - y - 1)g_1 + xz - yz - z - 1,$$

y también

$$f = (x - 1)g_1 - xg_2 + xz - x - z - 1.$$

2.20 Lema. Si $G = \{g_1, \dots, g_s\}$ es una base de Gröbner de $I = (g_1, \dots, g_s)$, entonces para cada polinomio no nulo $f \in k[x]$, existe un residuo único de f con respecto a $g_1, \dots, g_s$.

Demostración. Supongamos que existen residuos f' y f'' de f con respecto a $g_1, \dots, g_s$, con $f' \neq f''$. Como $0 \neq f' - f'' \in I$, el monomio $w = \text{in}_<(f' - f'') \in \text{in}_<(I)$. Sin embargo, como w debe ser un monomio de f' o de f'' , tenemos que ninguno de los monomios $\text{in}_<(g_1), \dots, \text{in}_<(g_s)$ divide a w . Por tanto $\text{in}_<(I) \neq (\text{in}_<(g_1), \dots, \text{in}_<(g_s))$, lo cual es una contradicción. $\square$

2.21 Corolario. Si $G = \{g_1, \dots, g_s\}$ es una base de Gröbner de $I = (g_1, \dots, g_s)$, entonces un polinomio no nulo $f \in k[x]$ pertenece a I si y solo si el residuo de f respecto de $g_1, \dots, g_s$ es cero.

2.2. Ordenes monomiales y vectores de peso

Hemos visto la forma inicial de un polinomio a partir de un orden monomial, sin embargo, también podemos definir las formas iniciales a partir de un vector de peso.

2.22 Definición. Sea $w \in \mathbb{R}^n$ un *vector de peso* y $f = \sum_{i=1}^m c_i x^{a_i} \in k[x]$. Definimos la *forma inicial de f con respecto a w* como

$$\text{in}_w(f) = \sum_j c_j x^{a_j},$$

donde j son todos los índices que cumplen con $\max\{w \cdot a_i\}$, para $i = 1, \dots, m$. El valor $w \cdot a \in \mathbb{R}$ se llama *w -peso* de x^a .

Anteriormente, cuando hablabamos de ordenes monomiales, la forma inicial de un polinomio era un monomio; sin embargo, en el caso de vectores de peso, la forma inicial de un polinomio no es un monomio necesariamente, puede ser otro polinomio. De manera similar, también tenemos el ideal inicial dado un vector de peso.

2.23 Definición. Para un ideal $I \subset k[x]$ el *ideal inicial* de I con respecto a w es

$$\text{in}_w(I) := (\text{in}_w(f) \mid 0 \neq f \in I).$$

Similarmente a los ordenes monomiales, tenemos $\text{in}_w(f \cdot g) = \text{in}_w(f) \cdot \text{in}_w(g)$ para cualesquiera $f, g \in k[x]$ y todo $w \in \mathbb{R}^n$, es decir que la forma inicial del producto de polinomios es igual al producto de formas iniciales de esos polinomios.

Algo importante que notar es que el ideal inicial con respecto a un vector de peso no necesariamente es un ideal monomial, es decir, no necesariamente es un ideal generado por monomios.

2.24 Ejemplo. Si tenemos el polinomio $x_1 - x_2^2$, su forma inicial con respecto al vector de peso $w = (2, 1)$ es $\text{in}_{(2,1)}(x_1 - x_2^2) = x_1 - x_2^2$.

Dado un orden monomial $<$ cualquiera, y para todo vector de peso $w = (w_1, \dots, w_n) \in \mathbb{R}_{\geq 0}^n$, podemos definir otro orden monomial $<_w$ como $x^a <_w x^b$ si y solo si

- $\sum_{i=1}^n w_i(a_i - b_i) < 0$, o
- $\sum_{i=1}^n w_i(a_i - b_i) = 0$ y $x^a < x^b$.

2.25 Teorema. Para cada ideal $I \subseteq k[x]$ tenemos que $\text{in}_<(\text{in}_w(I)) = \text{in}_{<_w}(I)$.

Demostración. Veamos que para cada $f \in k[x]$ tenemos que $\text{in}_<(\text{in}_w(f)) = \text{in}_{<_w}(f)$. Esto implica que $\text{in}_<(\text{in}_w(I))$ y $\text{in}_{<_w}(I)$ contienen los mismos monomios, y por lo tanto son iguales. $\square$

El teorema anterior implica los siguiente corolarios.

2.26 Corolario. Si $w \in \mathbb{R}_{\geq 0}^n$ y G una base de Gröbner del ideal I con respecto a $<_w$, entonces $\{\text{in}_w(g) \mid g \in G\}$ es una base de Gröbner para $\text{in}_w(I)$ con respecto a $<$.

2.27 Corolario. Si $w \in \mathbb{R}_{\geq 0}^n$ y $\text{in}_w(I)$ es un ideal monomial, entonces $\text{in}_w(I) = \text{in}_{<_w}(I)$.

3. GEOMETRÍA POLIEDRAL

Un hiperplano en $\mathbb{R}^n$ es el conjunto de puntos $x = (x_1, \dots, x_n)$ tales que cumplen $a \cdot x = a_1x_1 + \dots + a_nx_n = b$, para $a \in \mathbb{R}^n$ y $b \in \mathbb{R}$ fijo. Entonces diremos que un *semiespacio cerrado* son todos los puntos $y = (y_1, \dots, y_n) \in \mathbb{R}^n$ tal que

$$c \cdot y = c_1y_1 + \dots + c_ny_n \leq b,$$

donde $c \in \mathbb{R}^n$ y b es el mismo del hiperplano. Hay que notar que si cambiamos el lado de la desigualdad obtenemos otro semiespacio cerrado, y la intersección de estos dos semiespacios cerrados es el hiperplano.

3.1 Definición. Un *poliedro* es la intersección finita de semiespacios cerrados en $\mathbb{R}^n$. Entonces un poliedro puede ser descrito como $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$, donde $A \in \mathbb{R}^{m \times n}$ y $b \in \mathbb{R}^m$. Si P es acotado lo llamaremos *politopo*.

3.2 Ejemplo. Un ejemplo simple es el del cubo, que está dado por

$$C = \left\{ x \in \mathbb{R}^3 \mid \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} x \geq \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \end{pmatrix} \right\},$$

y podemos verlo en la figura 3.1.

3.3 Ejemplo. El octaedro está definido como

$$O = \left\{ x \in \mathbb{R}^3 \mid \begin{pmatrix} 2 & -2 & -2 \\ 2 & 2 & -2 \\ 2 & 2 & 2 \\ 2 & -2 & 2 \\ -2 & -2 & 2 \\ -2 & -2 & -2 \\ -2 & 2 & -2 \\ -2 & 2 & 2 \end{pmatrix} x \geq \begin{pmatrix} -3 \\ -3 \\ -3 \\ -3 \\ -3 \\ -3 \\ -3 \\ -3 \end{pmatrix} \right\},$$

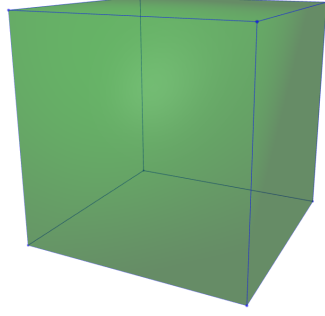


Figura 3.1. Cubo. Fuente: elaboración propia utilizando SageMath.

y se muestra en la figura 3.2.

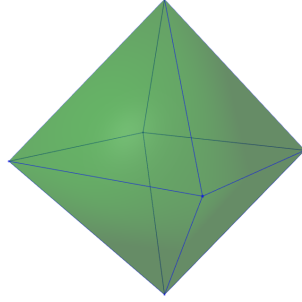


Figura 3.2. Octaedro. Fuente: elaboración propia utilizando SageMath.

Si en dado caso tenemos que $b = 0$, entonces existen vectores $u_1, \dots, u_m \in \mathbb{R}^n$ tales que

$$P = \text{pos}(u_1, \dots, u_m) := \{\lambda_1 u_1 + \dots + \lambda_m u_m \mid \lambda_1, \dots, \lambda_m \in \mathbb{R}_{\geq 0}\};$$

en este caso llamaremos a P *cono (poliedral)*.

Además, cada politopo Q puede ser escrito como la *envolvente convexa* de un conjunto finito de puntos, como:

$$Q = \text{conv}(v_1, \dots, v_m) := \left\{ \sum_{i=1}^m \lambda_i v_i \mid \lambda_i \in \mathbb{R}_{\geq 0} \text{ y } \sum_{i=1}^m \lambda_i = 1 \right\},$$

en particular, un politopo puede ser escrito como la envolvente convexa de sus vértices.

Sea $P \subseteq \mathbb{R}^n$ un poliedro y $w \in \mathbb{R}^n$, entonces definimos

$$\text{face}_w(P) := \{u \in P \mid w \cdot u \geq w \cdot v \text{ para todo } v \in P\}.$$

Cada subconjunto de P que tiene esta forma lo llamaremos una *cara* de P . Notemos que $\text{face}_0(P) = P$, por lo que el poliedro es una cara de sí mismo. Una identidad importante sobre las caras de un poliedro es que

$$\text{face}_{w'}(\text{face}_w(P)) = \text{face}_{w+\epsilon \cdot w'}(P),$$

para algún $\epsilon > 0$ lo suficientemente pequeño.

La *dimensión* de una cara de P es la dimensión del espacio afín que genera. La *codimensión* de una cara F de P se define como $\text{codim}_P(F) := \dim P - \dim F$, y una cara de codimensión 1 se llama *faceta*.

3.4 Ejemplo. Tanto el cubo del Ejemplo 3.2 y el octaedro del Ejemplo 3.3 cuentan con 27 caras en total.

- El poliedro: 1 cara;
- cada lado: 8 caras;
- cada arista: 12 caras;
- cada vértice: 6 caras;

para un total de 27 caras.

3.5 Definición. Para dos poliedros $P_1, P_2 \subseteq \mathbb{R}^n$ definimos su *suma de Minkowski* como

$$P_1 + P_2 := \{p_1 + p_2 \mid p_1 \in P_1, p_2 \in P_2\}.$$

3.6 Teorema. Sean $P_1, P_2 \subseteq \mathbb{R}^n$ y $w \in \mathbb{R}^n$, entonces tenemos que

$$\text{face}_w(P_1 + P_2) = \text{face}_w(P_1) + \text{face}_w(P_2).$$

Además, si v es un vértice de $P_1 + P_2$, entonces existen vértices únicos $p_1 \in P_1$ y $p_2 \in P_2$ tales que $v = p_1 + p_2$.

Demostración. Sea $x \in \text{face}_w(P_1 + P_2)$, entonces $x = x_1 + x_2$ con $x_1 \in P_1$ y $x_2 \in P_2$. Además tenemos que $x \cdot w \geq p \cdot w$ para todo $p \in P_1 + P_2$, por lo que $p = p_1 + p_2$ con $p_1 \in P_1$ y $p_2 \in P_2$, entonces

$$\begin{aligned} x \cdot w &\geq p \cdot w \\ (x_1 + x_2) \cdot w &\geq (p_1 + p_2) \cdot w \\ x_1 \cdot w + x_2 \cdot w &\geq p_1 \cdot w + p_2 \cdot w \\ (x_1 - p_1) \cdot w + (x_2 - p_2) \cdot w &\geq 0, \end{aligned}$$

de esto podemos ver, geométricamente, que $(x_1 - p_1) \cdot w \geq 0$ y $(x_2 - p_2) \cdot w \geq 0$, y por tanto tenemos que $x_1 \cdot w \geq p_1 \cdot w$ y $x_2 \cdot w \geq p_2 \cdot w$. Entonces $x_1 \in \text{face}_w(P_1)$ y $x_2 \in \text{face}_w(P_2)$, por lo que $x \in \text{face}_w(P_1) + \text{face}_w(P_2)$.

Por otro lado, sea $x \in \text{face}_w(P_1) + \text{face}_w(P_2)$, entonces tenemos que $x = x_1 + x_2$, donde $x_1 \in \text{face}_w(P_1)$ y $x_2 \in \text{face}_w(P_2)$. Con esto tenemos que $x_1 \cdot w \geq p_1 \cdot w$, para todo $p_1 \in P_1$, y $x_2 \cdot w \geq p_2 \cdot w$, para todo $p_2 \in P_2$. De estas desigualdades tenemos que

$$\begin{aligned} x_1 \cdot w + x_2 \cdot w &\geq p_1 \cdot w + p_2 \cdot w \\ (x_1 + x_2) \cdot w &\geq (p_1 + p_2) \cdot w \\ x \cdot w &\geq p \cdot w, \end{aligned}$$

donde $p \in P_1 + P_2$. Por lo tanto $x \in \text{face}_w(P_1 + P_2)$.

Por último, sea $w \in \mathbb{R}^n$ tal que $\text{face}_w(P_1 + P_2)$ es el vértice v . Por lo anterior sabemos que $\text{face}_w(P_1 + P_2) = \text{face}_w(P_1) + \text{face}_w(P_2)$, es decir que existen vértices tales que $v = p_1 + p_2$. Mostraremos que estos vértices son únicos. Supongamos que tenemos $p_1, p'_1 \in P_1$ y $p_2, p'_2 \in P_2$ vértices, tales que $v = p_1 + p_2 = p'_1 + p'_2$. Para algún $w \in \mathbb{R}^n$ tenemos que $p_1 \cdot w \geq p \cdot w$, para todo $p \in P_1$; en particular tenemos que $p_1 \cdot w \geq p'_1 \cdot w$. De forma similar tenemos que $p'_1 \cdot w \geq p_1 \cdot w$, entonces $p_1 \cdot w = p'_1 \cdot w$ y de forma análoga $p_2 \cdot w = p'_2 \cdot w$. Por lo tanto $p_1 = p'_1$ y $p_2 = p'_2$. $\square$

3.7 Ejemplo. Consideremos los politopos

$$P_1 = \text{conv}((0, 0), (0, 1)) \quad \text{y} \quad P_2 = \text{conv}((0, 0), (1, 0)).$$

Su suma de Minkowski es el cuadrado $P_1 + P_2 = Q = \text{conv}((0, 0), (0, 1), (1, 0), (1, 1))$, así como lo podemos observar en la Figura 3.3.

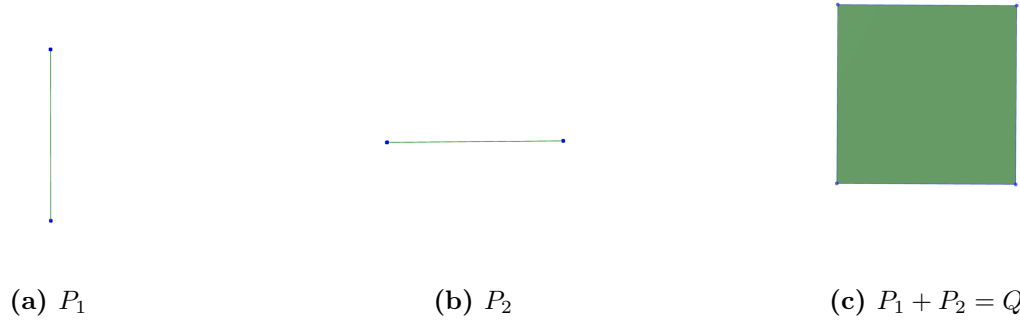


Figura 3.3. Politopos P_1 , P_2 y Q . Fuente: elaboración propia utilizando SageMath.

3.8 Ejemplo. Consideremos el cubo, C , del Ejemplo 3.2 y el octaedro, O , del Ejemplo 3.3. Su suma de Minkowski la podemos observar en la Figura 3.4.

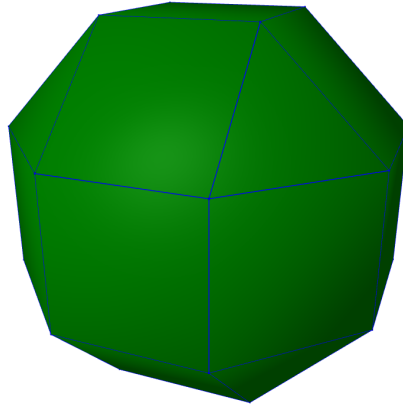


Figura 3.4. Suma de Minkowski del cubo y octaedro. Fuente: elaboración propia utilizando SageMath.

3.9 Definición. Un *complejo poliédrico* Δ es una colección finita de poliedra en $\mathbb{R}^n$ tal que

1. si $P \in \Delta$ y F es una cara de P , entonces $F \in \Delta$;
2. si $P_1, P_2 \in \Delta$, entonces $P_1 \cap P_2$ es una cara de P_1 y de P_2 .

El *soporte* Δ es $|\Delta| := \bigcup_{P \in \Delta} P$. Si cada $P \in \Delta$ es un cono, Δ se llama un *abanico*. Si un abanico Δ cumple que $|\Delta| = \mathbb{R}^n$ se llama *completo*.

Algo importante que notar es que podemos asociar un abanico a un poliedro tal que si $P \subseteq \mathbb{R}^n$ es un poliedro y F es una cara de P , el *cono normal* de F en P es:

$$\mathcal{N}_P(F) := \{w \in \mathbb{R}^n \mid \text{face}_w(P) = F\}.$$

Si tenemos que F y F' son dos caras del poliedro P , entonces F' es una cara de F si y solo si $\mathcal{N}_P(F)$ es una cara de $\mathcal{N}_P(F')$. La colección de conos normales $\mathcal{N}_P(F)$, donde F varía sobre las caras de P , es un abanico que llamamos *abanico normal de P* y lo denotamos como $\mathcal{N}(P)$.

3.10 Ejemplo. Si consideramos el cuadrado $Q = \text{conv}((0,0), (0,1), (1,0), (1,1))$ y la cara $F = \text{conv}((0,0), (1,0))$, tenemos que el cono normal de F en Q es $\mathcal{N}_Q(F) = \text{pos}((0,-1))$. Gráficamente podemos ver el abanico normal del cuadrado Q en la Figura 3.5.

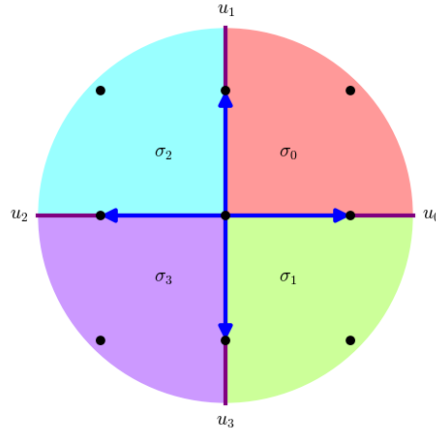


Figura 3.5. Abanico normal de Q . Fuente: elaboración propia utilizando SageMath.

3.11 Ejemplo. Consideremos el cubo del Ejemplo 3.2 tenemos que su abanico normal se muestra en la Figura 3.6.

3.12 Definición. Dos politopos Q y Q' se dice que son *fuertemente isomorfos* si $\mathcal{N}(Q) = \mathcal{N}(Q')$.

Recordemos que un monomio es un elemento del anillo de polinomios $k[x]$, donde k es un campo, de la forma

$$x^a = x_1^{a_1} \cdots x_n^{a_n} \text{ con } a = (a_1, \dots, a_n) \in \mathbb{Z}_{\geq 0}^n.$$

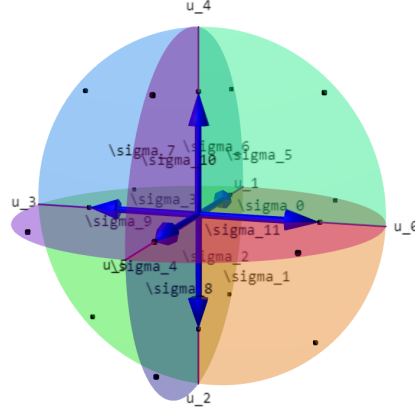


Figura 3.6. Abanico normal del cubo. Fuente: elaboración propia utilizando SageMath.

Para cada polinomio $f = \sum_{i=1}^m c_i x^{a_i} \in k[x]$ podemos asociarle su *politopo de Newton* de la siguiente manera

$$\text{New}(f) := \text{conv}(a_i \mid i = 1, \dots, m).$$

3.13 Lema. Para cada $w \in \mathbb{R}^n$ y cada $f \in k[x]$ tenemos que

$$\text{face}_w(\text{New}(f)) = \text{New}(\text{in}_w(f)).$$

Demostración. Mostraremos que $\text{face}_w(\text{New}(f))$ y $\text{New}(\text{in}_w(f))$ tienen los mismos vértices. Sea a_j , con j fijo, un vértice de $\text{face}_w(\text{New}(f))$, entonces $a_j \cdot w \geq x \cdot w$ para todo $x \in \text{New}(f)$. En particular tenemos que $a_j \cdot w \geq a_i \cdot w$ para todo $i \neq j$, por lo que a_j es la potencia de algún monomio de $\text{in}_w(f)$ y por tanto a_j es un vértice de $\text{New}(\text{in}_w(f))$. $\square$

3.14 Teorema. Para cada $f, g \in k[x]$ tenemos que $\text{New}(f \cdot g) = \text{New}(f) + \text{New}(g)$.

Demostración. Para mostrar la igualdad de los politopos, solo es necesario mostrar que sus vértices son iguales. Notemos que el teorema es cierto para monomios $f = x^a$ y $g = x^b$ ya que $x^a \cdot x^b = x^{a+b}$.

En caso de que f y g no sean monomios, tenemos que para todo $w \in \mathbb{R}^n$, tal

que $\text{face}_w(\text{New}(f \cdot g))$ y $\text{face}_w(\text{New}(f) + \text{New}(g))$ sean v rtices, se cumple que

$$\begin{aligned}
\text{face}_w(\text{New}(f \cdot g)) &= \text{New}(\text{in}_w(f \cdot g)) \\
&= \text{New}(\text{in}_w(f) \cdot \text{in}_w(g)) \\
&= \text{New}(\text{in}_w(f)) + \text{New}(\text{in}_w(g)) \\
&= \text{face}_w(\text{New}(f)) + \text{face}_w(\text{New}(g)) \\
&= \text{face}_w(\text{New}(f) + \text{New}(g)),
\end{aligned}$$

donde la primer igualdad es por el Lema 3.13; la segunda es una propiedad de las formas iniciales; la tercera debido a que son monomios; la cuarta por el Lema 3.13; y la quinta por el Teorema 3.6. Con esto se concluimos que ambos politopos tienen los mismos v rtices y, por tanto, son iguales. $\square$

4. ABANICOS DE GRÖBNER

Antes estudiamos el politopo de Newton y algunas propiedades de éste, sin embargo, nuestro objetivo es generalizarlo de polinomios a ideales. Para eso necesitaremos algunas definiciones y teoremas previos.

4.1 Definición. Sea $I \subseteq k[x]$ un ideal. Diremos que dos vectores de peso $v, w \in \mathbb{R}^n$ son *equivalentes*, con respecto a I , si $\text{in}_v(I) = \text{in}_w(I)$.

Al conjunto $C[w] := \{v \in \mathbb{R}^n \mid \text{in}_w(I) = \text{in}_v(I), I \text{ un ideal}\}$, para algún $w \in \mathbb{R}^n$, lo llamaremos la *clase de equivalencia de w* .

4.2 Proposición. Para cada $w \in \mathbb{R}^n$, su clase de equivalencia $C[w]$ es un cono convexo poliédrico relativamente abierto en $\mathbb{R}^n$.

Demostración. Sea $<$ un orden monomial y $<_w$ el orden inducido por $<$ y w . Sea G la base reducida de Gröbner de I con respecto a $<_w$. Queremos mostrar que

$$C[w] = \{w' \in \mathbb{R}^n \mid \text{in}_{w'}(g) = \text{in}_w(g) \text{ para todo } g \in G\}. \quad (4.1)$$

Esta expresión implica que $C[w]$ se representa como la intersección de hiperplanos y semiespacios abiertos. Para ver esto notemos que el lado derecho por las igualdades $w' \cdot a = w' \cdot b$ y las desigualdades $w' \cdot a \geq w' \cdot c$, donde x^a y x^b recorren los términos de $\text{in}_w(g)$ y x^c recorre los términos de g que no son parte de $\text{in}_w(g)$.

Primero supongamos que w' yace en el lado derecho de la ecuación 4.1, entonces $\text{in}_w(I) = (\text{in}_{w'}(g) \mid g \in G) \subseteq \text{in}_{w'}(I)$. Si esta contención fuera propia, entonces por el Teorema 2.25 tenemos que

$$\text{in}_{<_w}(I) = \text{in}_{<}(\text{in}_w(I)) \subset \text{in}_{<}(\text{in}_{w'}(I)) = \text{in}_{<_w}(I).$$

Pero, por la Proposición 2.8, sabemos que no puede haber una contención propia de dos ideales iniciales de I , por lo que $\text{in}_w(I) = \text{in}_{w'}(I)$.

Por otro lado, supongamos que $w' \in C[w]$. Por el Corolario 2.21, el conjunto $\text{in}_w(G) = \{\text{in}_w(g) \mid g \in G\}$ es la base de Gröbner reducida de $\text{in}_w(I) = \text{in}_{w'}(I)$

con respecto a $<$. Fijemos $g \in G$, entonces $\text{in}_{w'}(g)$ se reduce a cero con respecto de $\text{in}_w(G)$ y el orden monomial $<$. Esto implica que el monomio $m := \text{in}_{<_w}(g)$ debe aparecer en $\text{in}_{w'}(g)$, ya que los demás monomios de g no están en $\text{in}_{<_w} = \text{in}_{<}(\text{in}_w(I))$. Escribimos $\text{in}_w(g) = m + h$ y $\text{in}_{w'}(g) = m + h'$ donde h y h' son combinaciones lineales de monomios estándar. Luego del primer paso de la reducción a cero anterior obtenemos un polinomio $h' - h$, que yace en $\text{in}_w(I)$. Sin embargo, ninguno de los términos de $h' - h$ aparece en $\text{in}_{<_w}(I) = \text{in}_{<}(\text{in}_w(I))$. Por tanto, $h' - h$ es el polinomio cero, y concluimos que $\text{in}_{w'}(g) = \text{in}_w(g)$. $\square$

La ecuación 4.1 puede ser reformulada en términos de conos normales de politopos de Newton de una base de Gröbner reducida G como

$$C[w] = \mathcal{N}_Q(\text{face}_w(Q))$$

donde

$$Q := \text{New}\left(\prod_{g \in G} g\right) = \sum_{g \in G} \text{New}(g).$$

4.3 Definición. Sea $\overline{C[w]}$ la cerradura del cono $C[w]$ en $\mathbb{R}^n$. Definimos el *abanico de Gröbner* $\text{GF}(I)$ como el conjunto de conos cerrados $\overline{C[w]}$, para todo $w \in \mathbb{R}^n$.

4.4 Definición. Si existe un politopo P tal que $\text{GF}(I) = \mathcal{N}(P)$, P se llama *politopo de estado*.

4.5 Proposición. El abanico de Gröbner $\text{GF}(I)$ es un abanico.

Demostración. Sea $w' \in \overline{C[w]}$. Entonces $\text{in}_w(I)$ es un ideal inicial de $\text{in}_{w'}(I)$, y por tanto existe un orden monomial $<$ tal que $\text{in}_{<_w}(I) = \text{in}_{<_{w'}}(I)$. Sea G la base de Gröbner reducida de I con respecto a $<_w$, y sea $Q = \sum_{g \in G} \text{New}(g)$. Como G es la base de Gröbner reducida con respecto a $<_{w'}$ también, $C[w]$ y $C[w']$ son conos normales del mismo politopo

$$C[w] = \mathcal{N}_Q(\text{face}_w(Q)) \quad y \quad C[w'] = \mathcal{N}_Q(\text{face}_{w'}(Q)).$$

Nuestra hipótesis implica que el politopo $\text{face}_w(Q)$ es una cara del politopo $\text{face}_{w'}(Q)$, y por tanto, $\overline{C[w']}$ es una cara de $\overline{C[w]}$.

Ahora debemos mostrar que $\text{GF}(I)$ cumple los dos axiomas de un complejo poliédrico, en la Definición 3.9. Para verificar el primer axioma, sea F una cara de $\overline{C[w]}$. Si w' está en el interior relativo de F , entonces tenemos que $F = C[w']$ es una cara de $C[w]$. Para verificar el segundo axioma, sean $w, w' \in \mathbb{R}^n$ y consideremos

$P := \overline{C[w]} \cap \overline{C[w']}$. Sabemos que para cada $w'' \in P$, $\overline{C[w'']}$ es una cara de $\overline{C[w]}$ y de $\overline{C[w']}$. Por tanto P es una unión finita de caras en común. Pero una unión sin redundancia de caras de $\overline{C[w]}$ solo puede ser convexa si es un conjunto unitario. Por tanto concluimos que P es una cara de $\overline{C[w]}$ y de $\overline{C[w']}$. $\square$

Definiremos el *grado* de un monomio $x^a \in k[x]$ como $\deg(x^a) = \sum_{i=1}^n a_i$, y con I_d definimos al subespacio vectorial de polinomios homogéneos¹ de grado d en el ideal I . Entonces, para algún ideal monomial J definimos $\sum J_d$ como la suma de todos los vectores $a \in \mathbb{Z}_{\geq 0}^n$ tal que x^a es de grado d y $x^a \in J$.

4.6 Ejemplo. Consideremos el ideal $J = (x, y^2)$, entonces J_4 es el conjunto de polinomios homogéneos de grado 4. Notemos que J_4 tiene como base al conjunto $\{x^4, x^2y^2, y^4\}$. Entonces $\sum J_4 = (4, 0) + (2, 2) + (0, 4) = (6, 6)$.

4.7 Definición. Sea I un ideal y $\mathcal{U}$ una base de Gröbner universal minimal de I . Definimos

$$\text{State}_d(I) := \text{conv} \left\{ \sum \text{in}_{<}(I)_d \mid < \text{cualquier orden monomial} \right\}.$$

Sea $D = \max\{\deg(g) \mid g \in \mathcal{U}\}$. Definimos

$$\text{State}(I) := \sum_{d=1}^D \text{State}_d(I) = \text{State}_1(I) + \cdots + \text{State}_D(I).$$

4.8 Ejemplo. Sea $I = (g)$ y $g = xy^2 + x^2y + y^3$. En este caso solo tenemos tres ordenes monomiales de interés:

$$\text{in}_{<_1}(g) = xy^2, \text{in}_{<_2}(g) = x^2y, \text{in}_{<_3}(g) = y^3.$$

En particular, $\{g\}$ es una base de Gröbner universal minimal de I y notemos que $D = 3$. Tenemos que $\sum \text{in}_{<_1}(g) = (1, 2)$, $\sum \text{in}_{<_2}(g) = (2, 1)$ y $\sum \text{in}_{<_3}(g) = (0, 3)$. Entonces

$$\text{State}_3(I) = \text{conv}\{(1, 2), (2, 1), (0, 3)\}.$$

Notemos que $\text{State}_i(I) = \emptyset$ para $i < 3$. En este caso especial tenemos que $\text{State}(I) = \text{State}_3(I) = \text{New}(g)$.

Por el Lema 3.13, sabemos que para un polinomio $f \in k[x]$ y $w \in \mathbb{R}^n$ tenemos que $\text{face}_w(\text{New}(f)) = \text{New}(\text{in}_w(f))$. El siguiente lema nos generaliza este resultado.

¹Un polinomio homogéneo es tal que todos sus monomios tienen el mismo grado.

4.9 Lema. Para cada $w \in \mathbb{R}^n$ tenemos que $\text{face}_w(\text{State}_d(I)) = \text{State}_d(\text{in}_w(I))$.

Demostración. Primero probaremos el caso en el que $w \in \mathbb{R}^n$ tal que $\text{in}_w(I)$ es un ideal monomial y $\text{face}_w(\cdot)$ selecciona un vértice del politopo de estado. Sean $x^{a_1}, \dots, x^{a_m}$ todos los monomios de grado d , y sea $r := \dim(I_d) \leq m$. Sea $<$ algún orden monomial tal que $\text{in}_w(I) = \text{in}_{<}(I)$. Podemos suponer que $x^{a_1}, \dots, x^{a_r}$ son precisamente los monomios en $\text{in}_{<}(I)_d$. Ya que los monomios estándar forman una base módulo I , existen polinomios

$$x^{a_i} - \sum_{j=r+1}^m c_{ij} x^{a_j} \in I_d \quad \text{para } i = 1, \dots, r.$$

En cada una de estas r ecuaciones tenemos que el primer término es el más grande con respecto a w respectivamente, es decir, $w \cdot a_i \geq w \cdot a_j$ siempre que $c_{ij} \neq 0$. Observemos que $\text{State}_d(\text{in}_w(I)) = \{a_1 + \dots + a_r\}$ ya que $\text{in}_w(I)$ es monomial.

El vértice $\text{face}_w(\text{State}_d(I))$ es igual a $\sum \text{in}_{<'}(I)_d$ para algún orden monomial $<'$. Sean $x^{j_1}, \dots, x^{j_r}$ los monomios en $\text{in}_{<'}(I)_d$. Supongamos que el lema 4.9 es falso. Por definición de $\text{face}_w(\cdot)$ tenemos que $w \cdot (a_{j_1} + \dots + a_{j_r}) > w \cdot (a_1 + \dots + a_r)$. Por el lema de cambio de base de Steinitz aplicado al espacio vectorial $(k[x]/I)_d$, podemos pasar de la suma $a_1 + \dots + a_r$ a la suma $a_{j_1} + \dots + a_{j_r}$ con los cambios $a_i \mapsto a_j$ con $c_{ij} \neq 0$. Pero hemos visto que cada uno de estos reemplazos decrece el valor del funcional lineal w . Esto es una contradicción. Hemos mostrado que el lema 4.9 es verdadero para casi todos los $w \in \mathbb{R}^n$.

Para demostrar el Lema 4.9 en general, mostraremos que ambos politopos tienen los mismos vértices. Sea $w' \in \mathbb{R}^n$ como en la parte anterior. Entonces, para $\epsilon > 0$ lo suficientemente pequeño,

$$\begin{aligned} \text{face}_{w'}(\text{face}_w(\text{State}_d(I))) &= \text{face}_{w+\epsilon \cdot w'}(\text{State}_d(I)) \\ &= \text{State}_d(\text{in}_{w+\epsilon \cdot w'}(I)) \\ &= \text{State}_d(\text{in}_{w'}(\text{in}_w(I))) \\ &= \text{face}_{w'}(\text{State}_d(\text{in}_w(I))). \end{aligned}$$

Por lo que ambos politopos tienen los mismo vértices. □

4.10 Corolario. Si $< y <'$ son ordenes monomiales distintos, entonces

$$\text{in}_{<}(I)_d \neq \text{in}_{<'}(I)_d \iff \sum \text{in}_{<}(I)_d \neq \sum \text{in}_{<'}(I)_d.$$

Esto nos lleva al resultado más importante del capítulo.

4.11 Teorema. *Sea I un ideal homogéneo de $k[x]$. Existe un politopo $\text{State}(I) \subset \mathbb{R}^n$ cuyo abanico normal $\mathcal{N}(\text{State}(I))$ coincide con el abanico de Gröbner $\text{GF}(I)$.*

Demostración. Debemos mostrar que $\text{GF}(I) = \mathcal{N}(\text{State}(I))$. Notemos que, por la Proposición 4.5, $\text{GF}(I)$ es un complejo poliédrico. Todas las caras de un complejo poliédrico se determinan por sus caras maximales. Por lo tanto dos complejos poliédricos coinciden si y solo si sus caras maximales coinciden. Por lo tanto solo debemos mostrar que los conos maximales (abiertos) de $\text{GF}(I)$ y $\mathcal{N}(\text{State}(I))$ coinciden. De forma equivalente, debemos mostrar que $\text{in}_w(I) = \text{in}_{w'}(I)$ si y solo si $\text{face}_w(\text{State}(I)) = \text{face}_{w'}(\text{State}(I))$, para los vectores $w, w' \in \mathbb{R}^n$ tal que $\text{in}_w(I), \text{in}_{w'}(I)$ son ideales monomiales.

Dos ideales homogéneos son iguales si y solo si son iguales para cada grado. El número D es una cota universal para los grados de generadores minimales de I . Por tanto

$$\text{in}_w(I) = \text{in}_{w'}(I) \iff \text{in}_w(I)_d = \text{in}_{w'}(I)_d \quad (4.2)$$

para todo $d = 1, 2, \dots, D$. También notemos que, por el Teorema 3.6, tenemos que

$$\text{face}_w(\text{State}(I)) = \sum_{d=1}^D \text{face}_w(\text{State}_d(I)), \quad (4.3)$$

y de forma similar para w' . La dirección $\Rightarrow$ es una consecuencia directa de las ecuaciones 4.2, 4.3 y el Lema 4.9. Para la dirección $\Leftarrow$ supongamos que $\text{face}_w(\text{State}(I)) = \text{face}_{w'}(\text{State}(I))$, los cuales son vértices por como elegimos w y w' , y podemos sustituirlos por ordenes monomiales. Con esto $\Leftarrow$ se vuelve consecuencia directa del Corolario 4.10 y de la segunda parte del Teorema 3.6. $\square$

4.12 Proposición. *Sea f un polinomio homogéneo y $I = (f)$ su ideal principal. Entonces el politopo de Newton $\text{New}(f)$ es un politopo de estado de I .*

4.13 Corolario. *Sea $\mathcal{U}$ una base de Gröbner universal de I , que también es una base de Gröbner reducida de I para cada orden monomial. Entonces $\sum_{g \in \mathcal{U}} \text{New}(g)$ es un politopo de estado de I .*

5. VARIEDADES DE VERONESE

5.1. Espacio proyectivo y variedades proyectivas

Anteriormente hablamos sobre variedades afín y algunas propiedades de éstas. A continuación estudiaremos las variedades proyectivas; para esto debemos definir lo que es el espacio proyectivo, el cual se puede considerar como una compactificación de un espacio afín.

5.1 Definición. Sea k un campo cualquiera. El *espacio proyectivo* sobre k , denotado como $\mathbb{P}^n(k)$ o simplemente $\mathbb{P}^n$, es el conjunto de líneas que pasan por el origen de k^{n+1} .

Es decir, el espacio proyectivo lo vemos como el conjunto de clases de equivalencias definido de la siguiente forma

$$\mathbb{P}^n = \frac{k^{n+1} \setminus \{0\}}{\sim},$$

donde $\sim$ denota la relación de equivalencia $x \sim y$, para $x, y \in k^{n+1}$, si y solo si existe $\lambda \in k$ no cero tal que $y = \lambda x$. Entonces cada elemento $P \in \mathbb{P}^n$ se puede describir como la clase de equivalencia

$$P = [x_0 : x_1 : \cdots : x_n] = \{(\lambda x_0, \lambda x_1, \dots, \lambda x_n) \mid \lambda \in k, \lambda \neq 0\},$$

donde cada elemento se conoce como *coordenada homogénea de P* .

La Definición 1.35 nos indica que una variedad afín son las soluciones en común de un conjunto de polinomios, sin embargo, en el espacio proyectivo, un polinomio $f \in k[x_0, \dots, x_n]$ no nos define una función debido a la no unicidad de las coordenadas homogéneas. Podemos evitar este problema si nos centramos en cierto tipo de polinomios.

Decimos que un polinomio es homogéneo si todos sus términos tienen el mismo grado. Sea $F \in k[x_0, \dots, x_n]$ un polinomio homogéneo de grado d , entonces tenemos

que

$$F(\lambda x_0, \dots, \lambda x_n) = \lambda^d F(x_0, \dots, x_n).$$

Entonces $P \in \mathbb{P}^n$ es una solución de un polinomio homogéneo $F \in k[x_0, \dots, x_n]$ si para toda elección de coordenadas homogéneas de P tenemos que

$$F(P) = 0.$$

5.2 Definición. Sea $S \subset k[x_0, \dots, x_n]$ un conjunto de polinomios homogéneos. Entonces el conjunto

$$V(S) = \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ para todo } F \in S\}$$

es una *variedad proyectiva* definida por S .

De forma similar a las variedades afín, la unión y la intersección de variedades proyectivas es una variedad proyectiva; y el conjunto vacío y todo el espacio son variedades proyectivas. Además, las variedades proyectivas en $\mathbb{P}^n$ son los conjuntos cerrados en la topología de Zariski.

Sea $S \subset k[x_0, \dots, x_n]$ un conjunto de polinomios homogéneos, y sea $I = (S)$ un ideal homogéneo, entonces $V(S) = V(I)$. Además definimos el ideal de una variedad proyectiva como

$$I(V) = \{F \in k[x_0, \dots, x_n] \mid F(P) = 0 \text{ para todo } P \in V\}.$$

Notemos que $I(V)$ es un ideal homogéneo; también es fácil probar que $I(V)$ es un ideal radical y que es finitamente generado. Además si $F \in I(V)$, entonces cada término de F está en $I(V)$.

5.3 Teorema. Sea I un ideal de $k[x_0, \dots, x_n]$. Si $V(I) \neq \emptyset$, entonces $I(V(I)) = \sqrt{I}$.

Demostración. Ver [5, p. 46]. □

Por último discutiremos sobre mapeos entre variedades proyectivas.

5.4 Definición. Sean $V \subset \mathbb{P}^n$ y $W \subset \mathbb{P}^m$ variedades proyectivas, y consideremos el mapeo

$$\nu : V \longrightarrow W.$$

Decimos que ν es un *mapeo de variedades proyectivas* si: para cada $p \in V$, existen polinomios homogéneos $\nu_0, \dots, \nu_m \in k[x_0, \dots, x_n]$ tal que para alguna vecindad

abierto¹ no vacía $U \subseteq V$ de p , el mapeo $\nu|_U : U \rightarrow W$ concuerda con el mapeo polinomial

$$\begin{aligned} U &\longrightarrow \mathbb{P}^m \\ q &\longmapsto [\nu_0(q) : \cdots : \nu_m(q)] \end{aligned}$$

Algo importante, y que está implícito en la definición anterior, es el hecho que cada polinomio ν_i debe tener el mismo grado; de lo contrario no describirían un mapeo bien definido a $\mathbb{P}^m$. Es más, los ν_i no deben desvanecerse simultáneamente en la vecindad abierta U de p .

Como ejemplo consideremos el mapeo

$$\nu : \mathbb{P}^1 \longrightarrow \mathbb{P}^2,$$

definido de la siguiente forma

$$[s : t] \longmapsto [s^2 : st : t^2].$$

Este mapeo está bien definido, ya que si tomamos $[s : t] \in \mathbb{P}^1$, tenemos que

$$[s : t] = [\lambda s : \lambda t] \longmapsto [\lambda^2 s^2 : \lambda^2 st : \lambda^2 t^2] = [s^2 : st : t^2],$$

para cualquier constante $\lambda \neq 0$. Por lo que el mapeo no depende de nuestra elección de representante para los elementos de $\mathbb{P}^1$. Es más, al menos una de las coordenadas s^2 o t^2 de la imagen no es cero.

5.2. Mapeo y variedad de Veronese

Los mapeos que veremos a continuación son un ejemplo importante de morfismos de variedades proyectivas. Esto es debido a que estos mapeos hacen una inclusión de un espacio proyectivo $\mathbb{P}^n$ en uno de mayor dimensión de una forma no trivial.

5.5 Definición. El *mapeo de Veronese* de grado d es el morfismo

$$\nu_{n,d} : \mathbb{P}^n \longrightarrow \mathbb{P}^N,$$

¹Nos referimos a una vecindad abierta en el sentido topológico, dada la topología de Zariski.

dado por

$$[x_0 : \cdots : x_n] \longmapsto [\cdots : x^J : \cdots],$$

donde x^J varía sobre los monomios de grado d de las variables $x_0, \dots, x_n$ y

$$N = \binom{n+d}{d} - 1.$$

Este es un morfismo bien definido puesto que los polinomios de la imagen tienen el mismo grado y no todos se desvanecen simultáneamente en ningún punto de $\mathbb{P}^n$.

5.6 Proposición. *El mapeo de Veronese es una inclusión de variedades proyectivas.*

Demostración. Ver [19, p. 64]. □

5.7 Ejemplo. El mapeo de Veronese con $n = 1$ y $d = 2$, donde $N = \binom{1+2}{2} - 1 = 2$, es

$$\nu_{1,2} : \mathbb{P}^1 \longrightarrow \mathbb{P}^2$$

definido por

$$[x_0, x_1] \longmapsto [x_0^2, x_0x_1, x_1^2].$$

5.8 Ejemplo. El mapeo de Veronese con $n = 1$, $d = 3$ y $N = 3$ es

$$\nu_{1,3} : \mathbb{P}^1 \longrightarrow \mathbb{P}^3$$

dado por

$$[x_0, x_1] \longmapsto [x_0^3, x_0^2x_1, x_0x_1^2, x_1^3].$$

Las variedades proyectivas obtenidas a partir de estos mapeos se llaman *variedades de Veronese* y las denotaremos como $\mathbb{V}_{n,d}$. En general, la variedad de Veronese se puede definir a partir de las ecuaciones

$$\{z_I z_J - z_K z_L \mid I, J, K, L \in \mathbb{Z}_{\geq 0}^{n+1}, I + J = K + L\},$$

donde cada z_I son las coordenadas homogéneas de la imagen del mapeo de Veronese.

Es decir que, en el Ejemplo 5.7 tenemos que la variedad de Veronese está dada por

$$\mathbb{V}_{1,2}(xz - y^2),$$

donde $x = x_0^2$, $y = x_0x_1$, $z = x_1^2$.

De forma similar podemos ver la variedad de Veronese del ejemplo 5.8 es

$$\mathbb{V}_{1,3}(xw - yz, y^2 - xz, wy - z^2),$$

donde $x = x_0^3$, $y = x_0^2x_1$, $z = x_0x_1^2$, $w = x_1^3$.

5.3. Abanicos de Gröbner de variedades de Veronese

En esta última sección nos apoyaremos del software *Macaulay2* (M2) [6] para calcular los abanicos de Gröbner de algunas variedades de Veronese, es decir, tomaremos los polinomios que generan dichas variedades y estudiaremos el comportamiento de los abanicos de Gröbner del ideal generado por estos. Para lograr esto utilizaremos el apoyo de tres paquetes disponibles para Macaulay2 llamados *Resultants*, *StatePolytope* y *Polyhedra*.

5.9 Nota. Los cálculos realizados en Macaulay2 fueron hechos en el campo de los racionales $\mathbb{Q}$.

Iniciaremos estudiando el mapeo de Veronese

$$v_{1,2} : \mathbb{P}^1 \longrightarrow \mathbb{P}^2.$$

Iniciamos cargando los paquetes necesarios para realizar nuestros cálculos. *Resultants* nos permitirá generar los mapeos de Veronese y por consiguiente las variedades de Veronese con las que deseamos trabajar; *StatePolytope* nos permitirá calcular el politopo de estado de nuestra variedad de Veronese; *Polyhedra* lo usaremos para obtener nuestro abanico de Gröbner.

```
i1 : loadPackage "Polyhedra"
o1 = Polyhedra
o1 : Package

i2 : loadPackage "Resultants"
o2 = Resultants
o2 : Package

i3 : loadPackage "StatePolytope"
```

```
o3 = StatePolytope
o3 : Package
```

Luego de tener nuestros paquetes cargados calcularemos la variedad de Veronese de interés a partir de su mapeo de Veronese.

```
i4 : v12 = veronese(1,2)
                                2      2
o4 = map (QQ[t ..t ], QQ[x ..x ], {t , t t , t })
          0  1      0  2      0  0 1  1
o4 : RingMap QQ[t ..t ] <--- QQ[x ..x ]
          0  1      0  2
```

```
i5 : V12 = ker v12
      2
o5 = ideal(x  - x x )
          1    0 2
o5 : Ideal of QQ[x ..x ]
          0    2
```

A partir de esto podemos construir nuestro anillo de polinomios con el que trabajaremos y así generar el ideal con el cual realizaremos los cálculos que deseamos.

```
i6 : R = QQ[x_0..x_2]
o6 = R
o6 : PolynomialRing

i7 : I = ideal(x_1^2-x_0*x_2)
      2
o7 = ideal(x  - x x )
          1    0 2
o7 : Ideal of R
```

A continuación generaremos los vértices del politopo de estado del ideal en cuestión.

```
i8 : P = polymakeStatePolytope(I)
o8 = {{1, 0, 1}, {0, 2, 0}}
o8 : List
```

Dados los vértices podemos construir el politopo de estado a partir de su envolvente convexa.

```
i9 : M = transpose matrix P
o9 = | 1 0 |
      | 0 2 |
      | 1 0 |
           3      2
o9 : Matrix ZZ  <--- ZZ

i10 : Q = convexHull M
o10 = Q
o10 : Polyhedron
```

Con esto podemos notar, en la siguiente línea de código, que nuestro politopo de estado es de dimensión 1 y que no es de dimensión completa, es decir, estamos trabajando en un espacio de 3 dimensiones y la dimensión del politopo es menor.

```
i11 : dim Q
o11 = 1

i12 : isFullDimensional Q
o12 = false
```

Por último calcularemos el abanico normal del politopo de estado, que por el Teorema 4.11 coincide con el abanico de Gröbner de éste.

```
i13 : NF = normalFan Q
o13 = NF
o13 : Fan
```

De esto podemos ver que el abanico es completo, es decir, su soporte es igual a todo el espacio.

```
i14 : isComplete NF
o14 = true
```

Por último generaremos la lista de conos maximales y los rayos del abanico de Gröbner, para poder ver el comportamiento de dichos conos.

```

i15 : MC = maxCones NF
o15 = {{1}, {0}}
o15 : List

```

```

i16 : raysNF = rays NF
o16 = | 0 0 |
      | 1 0 |
      | 0 1 |
      3      2
o16 : Matrix ZZ <--- ZZ

```

```

i17 : apply(MC,mc -> raysNF_mc)
o17 = {| 0 |, | 0 |}
      | 0 | | 1 |
      | 1 | | 0 |
o17 : List

```

A continuación veremos el código para calcular el abanico de Gröbner del mapeo de Veronese

$$v_{1,3} : \mathbb{P}^1 \longrightarrow \mathbb{P}^3,$$

cuya variedad de Veronese es

$$\mathbb{V}_{1,3}(x_2^2 - x_1x_3, x_1x_2 - x_0x_3, x_1^2 - x_0x_2).$$

```

i18 : v13 = veronese(1,3)
      3      2      2      3
o18 = map (QQ[t ..t ], QQ[x ..x ], {t , t t , t t , t })
      0      1      0      3      0      0      1      0      1      1
o18 : RingMap QQ[t ..t ] <--- QQ[x ..x ]
      0      1      0      3

```

```

i19 : V13 = ker v13
      2      2
o19 = ideal (x  - x x , x x  - x x , x  - x x )
      2      1 3      1 2      0 3      1      0 2
o19 : Ideal of QQ[x ..x ]
      0      3

```

```

i20 : R = QQ[x_0..x_3]
o20 = R
o20 : PolynomialRing

i21 : I = ideal(x_2^2-x_1*x_3,x_1*x_2-x_0*x_3,x_1^2-x_0*x_2)
                2                2
o21 = ideal (x  - x x , x x  - x x , x  - x x )
                2      1 3      1 2      0 3      1      0 2
o21 : Ideal of R

i22 : P = polymakeStatePolytope(I)
o22 = {{11, 7, 7, 11}, {7, 15, 3, 11}, {4, 18, 6, 8}, {3, 18, 9, 6},
       {11, 3, 15, 7}, {8, 6, 18, 4}, {6, 9, 18, 3}, {3, 15, 15, 3}}
o22 : List

i23 : M = transpose matrix P
o23 = | 11 7  4  3  11 8  6  3 |
      | 7 15 18 18 3  6  9 15 |
      | 7  3  6  9 15 18 18 15 |
      | 11 11 8  6  7  4  3  3 |
                4      8
o23 : Matrix ZZ <--- ZZ

i24 : Q = convexHull M
o24 = Q
o24 : Polyhedron

i25 : dim Q
o25 = 2

i26 : isFullDimensional Q
o26 = false

i27 : NF = normalFan Q
o27 = NF

```

```

o27 : Fan

i28 : isComplete NF
o28 = true

i29 : MC = maxCones NF
o29 = {{6, 7}, {2, 6}, {2, 4}, {3, 7}, {0, 4}, {3, 5}, {1, 5}, {0, 1}}
o29 : List

i30 : raysNF = rays NF
o30 = | 0  0  0  0  0  0  0  0 |
      | 29 11  1 -2 11 -7 -1 -7 |
      | 4  22 -1 2  -5 13 -2 4  |
      | -21 -21 3  3  6  6 15 15 |
              4      8
o30 : Matrix ZZ <--- ZZ

i31 : apply(MC,mc -> raysNF_mc)
o31 = {| 0  0 |, | 0  0 |, | 0  0 |, | 0  0 |,
      | -1 -7 |, | 1  -1 |, | 1  11 |, | -2 -7 |
      | -2 4  |, | -1 -2 |, | -1 -5 |, | 2  4  |
      | 15 15 |, | 3  15 |, | 3  6  |, | 3  15 |

      | 0  0 |, | 0  0 |, | 0  0 |, | 0  0 |}
      | 29 11 |, | -2 -7 |, | 11 -7 |, | 29 11 |
      | 4  -5 |, | 2  13 |, | 22 13 |, | 2  22 |
      | -21 6 |, | 3  6  |, | -21 6 |, | -21 -21 |
o31 : List

```


CONCLUSIONES

1. La geometría algebraica estudia la representación de curvas y superficies geométricas de forma algebraica por medio de lo que denominamos variedades afines. Es decir, esta estudia la conexión entre la geometría y el álgebra.
2. El desarrollo de las bases de Gröbner ha brindado herramientas que permiten la resolución de varios problemas relacionados al estudio de polinomios de forma computacional.
3. Se estableció la conexión entre la geometría poliedral y el álgebra por medio del denominado politopo de Newton para polinomios y del politopo de estado para ideales del anillo de polinomios.
4. Se definió el abanico de Gröbner y se demostró que el abanico normal del politopo de estado de un ideal es equivalente éste.
5. Una variedad de Veronese se define como la imagen de un mapeo de Veronese, el cual es un mapeo entre espacios proyectivos, donde se estudiaron varias propiedades concernientes a su abanico de Gröbner, como su dimensión total, si es completo y la forma de sus conos dada de forma matricial.

RECOMENDACIONES

1. Estudiar más a fondo la relación entre ideales binomiales y las bases de Gröbner de variedades de Veronese.
2. Desarrollar el aprendizaje de herramientas como los sistemas algebraicos computacionales como apoyo al aprendizaje de estudiantes de matemática.
3. Investigar el comportamiento del abanico de Gröbner distintas variedades proyectivas, así como lo son las variedades de Veronese, la inclusión de Segre y otras.

BIBLIOGRAFÍA

- [1] BIGATTI, ANNA M; GIMENEZ, PHILIPPE y SÁENZ-DE CABEZÓN, EDUARDO: *Monomial ideals, computations and applications*. volumen 2083. Springer, 2013.
- [2] COSSIDENTE, ANTONIO; LABBATE, DOMENICO y SICILIANO, ALESSANDRO: «Veronese varieties over finite fields and their projections». *Designs, Codes and Cryptography*, 2001, **22(1)**, pp. 19–32.
- [3] COX, DAVID; LITTLE, JOHN; O'SHEA, DONAL y SWEEDLER, MOSS: «Ideals, varieties, and algorithms». *American Mathematical Monthly*, 1994, **101(6)**, pp. 582–586.
- [4] DUMMIT, DAVID STEVEN y FOOTE, RICHARD M: *Abstract algebra*. volumen 3. Wiley Hoboken, 2004.
- [5] FULTON, WILLIAM: «Algebraic curves». *An Introduction to Algebraic Geom*, 2008, p. 54.
- [6] GRAYSON, DANIEL R. y STILLMAN, MICHAEL E.: «Macaulay2, a software system for research in algebraic geometry». Disponible en <http://www.math.uiuc.edu/Macaulay2/>.
- [7] GRIFFITHS, PHILLIP y HARRIS, JOSEPH: *Principles of algebraic geometry*. John Wiley & Sons, 2014.
- [8] GRÜNBAUM, BRANKO; KLEE, VICTOR; PERLES, MICHA A y SHEPHARD, GEOFFREY COLIN: *Convex polytopes*. volumen 16. Springer, 1967.
- [9] HARRIS, JOE: *Algebraic geometry: a first course*. volumen 133. Springer Science & Business Media, 2013.
- [10] HARTSHORNE, ROBIN: *Algebraic geometry*. volumen 52. Springer Science & Business Media, 2013.

- [11] HERSTEIN, ISRAEL N: *Abstract algebra*. John Wiley & Sons, 1996.
- [12] HERZOG, JÜRGEN; HIBI, TAKAYUKI; HERZOG, JÜRGEN y HIBI, TAKAYUKI: *Monomial ideals*. Springer, 2011.
- [13] HERZOG, JÜRGEN; HIBI, TAKAYUKI y OHSUGI, HIDEFUMI: *Binomial ideals*. volumen 279. Springer, 2018.
- [14] LEE, GREGORY T: *Abstract algebra: An introductory course*. Springer, 2018.
- [15] MILNE, J: «Algebraic Geometry, Version 6.02». *Lecture Notes in Mathematics*, 2017.
- [16] PERRIN, DANIEL y otros: *Algebraic geometry: an introduction*. Springer, 2008.
- [17] SHAFAREVICH, IGOR R y REID, MILES: *Basic algebraic geometry 2*. volumen 2. Springer, 1997.
- [18] SHAFAREVICH, IGOR ROSTISLAVOVICH y REID, MILES: *Basic algebraic geometry 1*. volumen 2. Springer, 1994.
- [19] SMITH, KAREN; KAHANPÄÄ, LAURI; KEKÄLÄINEN, PEKKA y TRAVES, WILLIAM: *An invitation to algebraic geometry*. Springer Science & Business Media, 2004.
- [20] STURMFELS, BERND: *Grobner bases and convex polytopes*. volumen 8. American Mathematical Soc., 1996.
- [21] THOMAS, REKHA R: *Lectures in geometric combinatorics*. volumen 33. American Mathematical Soc., 2006.
- [22] ZHANG, SIMON: «What is the Veronese map?», 2016.
- [23] ZIEGLER, GÜNTER M: *Lectures on polytopes*. volumen 152. Springer Science & Business Media, 2012.