



Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

BASES DE GRÖBNER APLICADAS A LA
GEOMETRÍA EN CIENCIAS DE LA COMPUTACIÓN

Tesis presentada al

Colegio de Matemáticas

como requisito parcial para la obtención del grado de

LICENCIADO EN MATEMÁTICAS

por

Zaida Adriana Gárate Cahuantzi

Asesorada por

Ixchel Dzohara Gutiérrez Rodríguez

César Cejudo Castilla

Puebla Pue.
9 de mayo de 2023



Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas

BASES DE GRÖBNER APLICADAS A LA
GEOMETRÍA EN CIENCIAS DE LA COMPUTACIÓN

Tesis presentada al

Colegio de Matemáticas

como requisito parcial para la obtención del grado de

LICENCIADO EN MATEMÁTICAS

por

Zaida Adriana Gárate Cahuantzi

Asesorada por

Ixchel Dzohara Gutiérrez Rodríguez

César Cejudo Castilla

Puebla Pue.
9 de mayo de 2023

Título: BASES DE GRÖBNER APLICADAS A LA GEOMETRÍA
EN CIENCIAS DE LA COMPUTACIÓN

Estudiante: ZAIDA ADRIANA GÁRATE CAHUANTZI

COMITÉ

Agustín Contreras Carreto
Presidente

Carlos Guillén Galván
Secretario

Xabier García Martínez
Vocal

Ixchel Dzohara Gutiérrez Rodríguez
Asesor

César Cejudo Castilla
Asesor

"Mientras el álgebra y la geometría siguieron caminos separados, su avance fue lento y sus aplicaciones limitadas. Pero cuando estas ciencias se unieron, extrajeron una de la otra una nueva vitalidad y, desde entonces, marcharon a paso rápido hacia la perfección".

-Joseph-Louis Lagrange

Índice general

| | |
|--|------------|
| Introducción | 7 |
| I Fundamentos | 1 |
| 1. Preliminares | 3 |
| 1.1. Anillos de Polinomios | 3 |
| 1.2. Órdenes monomiales | 7 |
| 1.3. Algoritmo de la División en varias variables | 11 |
| 1.4. Ideales Monomiales | 17 |
| 2. Bases de Gröbner | 19 |
| 2.1. Definición y propiedades | 19 |
| 2.2. Algoritmo de Buchberger | 26 |
| 3. Variedades | 33 |
| 3.1. Variedades Irreducibles | 37 |
| II Aplicaciones | 41 |
| 4. Problema cinemático en los brazos de robots | 43 |
| 4.1. Problema cinemático directo | 47 |
| 4.2. Problema cinemático inverso | 53 |
| 5. Demostraciones automáticas en Geometría Euclideana | 67 |
| 6. Coloración de Grafos | 87 |
| 7. Conclusiones | 103 |
| Bibliografía | 105 |

Índice de figuras

| | |
|---|-----|
| 2.1. Código para generar una base de Gröbner Reducida | 31 |
| 4.1. Articulación de revolución plana | 44 |
| 4.2. Articulaciones prismáticas | 44 |
| 4.3. Brazo de robot | 45 |
| 4.4. Mano de robot | 46 |
| 4.5. Brazo de un robot en \mathbb{R}^2 | 47 |
| 4.6. Brazo de un robot en con cuatro articulaciones de revolución | 49 |
| 4.7. Brazo de robot del Ejemplo 4.3 | 50 |
| 4.8. Brazo de robot del Ejemplo 4.4 | 52 |
| 4.9. Brazo de Robot del ejemplo 4.5 | 54 |
| 4.10. Posiciones de la mano de robot | 57 |
| 4.11. Brazo de robot del Ejemplo 4.3 | 57 |
| 4.12. Posición del brazo del robot cuando $\theta_2 = 0$ | 61 |
| 4.13. Ejemplos de posiciones de el brazo de robot | 63 |
| 4.14. Ejemplos de posiciones de la mano del robot en el origen | 65 |
| 5.1. Paralelogramo | 69 |
| 5.2. Teorema del baricentro | 82 |
| 5.3. Teorema de Apolonio | 84 |
| 6.1. Grafo \mathcal{G} | 88 |
| 6.2. Coloración del grafo \mathcal{G} | 90 |
| 6.3. Grafo \mathcal{G}' | 91 |
| 6.4. Coloración del grafo \mathcal{G}' | 94 |
| 6.5. Segunda coloración del grafo \mathcal{G}' | 94 |
| 6.6. Tercera coloración del grafo \mathcal{G}' | 95 |
| 6.7. Grafo \mathcal{H} | 95 |
| 6.8. Primera coloración del grafo \mathcal{H} | 99 |
| 6.9. Segunda coloración del grafo \mathcal{H} | 100 |
| 6.10. Tercera coloración del grafo \mathcal{H} | 100 |
| 6.11. Grafo \mathcal{J} | 101 |

Introducción

Con la ayuda del álgebra podemos resolver problemas de la vida cotidiana, todo empieza con el hecho de poder representar el problema y sus hipótesis con expresiones algebraicas, de modo que se puede plantear un sistema de ecuaciones, en consecuencia se ha buscado la creación de diferentes métodos para resolver sistemas de ecuaciones. El objetivo principal de las bases de Gröbner es resolver sistemas de ecuaciones polinomiales para encontrar soluciones lo más exactas posibles sin importar el grado de complejidad del sistema de ecuaciones. Esto fue un gran avance para las matemáticas computacionales. Por su versatilidad y gran número de aplicaciones han permitido que dichas bases sean usadas para la investigación de diversas ramas de las matemáticas, como por ejemplo, el álgebra conmutativa, la geometría algebraica, teoría de grafos, teoría de códigos, criptografía, programación lineal entera, entre otras. Podemos considerar a las bases de Gröbner como el algoritmo de eliminación de Gauss en varias variables.

Históricamente, las bases de Gröbner surgen del teorema de la base de Hilbert donde nos dice que *Todo ideal $I \subseteq k[x_1, \dots, x_n]$ tiene un conjunto finito de generadores.* Este teorema surge como una solución a un problema de Paul Gordan en la teoría de variedades que trata sobre el cálculo de una base finita de invariantes para formas binarias de cualquier grado. La demostración del teorema de la base de Hilbert es existencial, en consecuencia varios expertos en el tema no aceptan la prueba, incluso Gordan dice la frase “¡esto no es matemáticas; es teología!”, sin embargo Hilbert continua trabajando su idea.

Posteriormente, en 1893, Hilbert envía una segunda evaluación de su trabajo [10], en donde logra demostrar su teorema usando teoría de anillos que habían sido estudiadas por Kronecker. En ese trabajo Hilbert demuestra el *Teorema Nullstellensatz* o *Teorema de los ceros de Hilbert*, estos teoremas son importantes en la teoría de variedades. Gordan reconocería la importancia del trabajo de Hilbert con la frase: “He de admitir que incluso la teología tiene sus ventajas.” y en [12] se publicó una versión del teorema propuesto por Hilbert en donde se introduce una idea similar a las de Bases de Gröbner titulado “*le systeme irréductible N*”.

En 1964, Wolfgang Gröbner trabaja en el problema que consiste en encontrar una base del k -espacio vectorial $\frac{k[x_1, \dots, x_n]}{I}$, siendo I un ideal de dimensión cero y le propone a su estudiante de doctorado, Bruno Buchberger continuar el problema que estaba trabajando. En 1965, Buchberger consigue crear la teoría de las bases de Gröbner junto con un algoritmo para calcularlas conocido actualmente como algoritmo de Buchberger, el cual fue publicado en su tesis doctoral [3]. En honor a su maestro, Buchberger le llamó a estos conjuntos: Bases de Gröbner. Las bases de Gröbner también son conocidas como bases de Groebner.

En el 2007, Buchberger recibió un premio de la Association for Computing Machinery's Paris Kanellakis Theory and Practice Award por su trabajo, reconociendo la importancia de su contribución a las matemáticas y a las ciencias computacionales.

El presente trabajo tiene como propósito un estudio introductorio a la teoría de las bases de Gröbner y algunas aplicaciones. En la primera parte se presentan los fundamentos, iniciando con la teoría básica de anillos de polinomios presentando a los ideales de un anillo y hablando de la pertenencia en un ideal, para ello hacemos uso del algoritmo de Euclides en varias variables y el Lemma de Dickson, y vemos que es necesario introducir los órdenes monomiales e ideales monomiales respectivamente.

En el Capítulo 2, se presentan el Teorema de la Base de Hilbert, para asegurar que todo ideal en el anillo $k[x_1, \dots, x_n]$ tiene un conjunto finito de generadores, en consecuencia se define la base de Gröbner. Mas aún, se introduce la definición de S -polinomio y usando el criterio de Buchberger se muestra si dada una base es de Gröbner, siguiendo esta idea se utiliza el algoritmo de Buchberger para calcular una base de Gröbner.

Una vez que se calcula la base de Gröbner para el ideal I podemos considerar el conjunto de todas las soluciones del sistema de ecuaciones polinómicas, es decir, consideramos la variedad del ideal I . En el Capítulo 3 estudiaremos la teoría de variedades del ideal I . Asimismo, se enuncian los Teoremas de los Ceros de Hilbert y un teorema que muestra la relación entre la base de Gröbner y la variedad, brindando información sobre la existencia de soluciones al sistema de ecuaciones polinómicas. Este capítulo aporta teoría importante que usaremos en las aplicaciones de este trabajo.

Asimismo, en la segunda parte de esta tesis se estudiarán tres aplicaciones en geometría algebraica en el área de las ciencias de la computación. En la primera aplicación se trata el problema cinemático inverso en los brazos de robots, se analizarán las variedades algebraicas para describir el espacio de configuraciones de mecanismos tales como brazos de robots y se usará este enfoque para resolver problemas cinemáticos de ciertos tipos de robots. Además, en el capítulo 5 se presentan dos métodos para demostraciones

automáticas de teoremas geométricos clásicos, cuya área es de gran interés para los investigadores en inteligencia artificial. Por último, en el capítulo 6 se utilizará la teoría de las bases de Gröbner para el estudio de la solución a problemas de coloración de grafos.

Parte I

Fundamentos

Capítulo 1

Preliminares

En este capítulo, se enunciarán las propiedades y definiciones básicas de los anillos de polinomios, junto con el algoritmo de la división en varias variables. Asimismo, se estudiarán los órdenes e ideales monomiales.

1.1. Anillos de Polinomios

En esta sección se estudiarán las definiciones y propiedades más importantes de los anillos de polinomios.

1.1 Definición. Un anillo k es un conjunto con dos operaciones binarias $+$: $k \times k \rightarrow k$ y \cdot : $k \times k \rightarrow k$ (llamadas suma y producto) que cumplen:

- (i) $(k, +, 0)$ es un grupo abeliano.
- (ii) $(k, \cdot, 1)$ es un monoide.
- (iii) $\forall a, b, c \in k : a \cdot (b + c) = a \cdot b + a \cdot c$.

Decimos que k es conmutativo si $\forall a, b \in k$ tal que $a \cdot b = b \cdot a$.

1.2 Ejemplo. \mathbb{Z} y $k[x_1, \dots, x_n]$

1.3 Definición. Sea k un anillo.

- (i) Un elemento $a \in k$ no cero es llamado divisor de cero si existe $b \in k \setminus \{0\}$ tal que $ab = 0$.
- (ii) Sea k un anillo con $1 \neq 0$. Un elemento $u \in k \setminus \{0\}$ es llamado unidad o invertible en k si existe $v \in k$ tal que $uv = 1$.

1.4 Definición. Diremos que k es dominio entero si cumple las siguientes condiciones:

- (i) Sean $a, b \in k$. Si existe $c \in k$ tal que $b = ac$, entonces diremos que a divide a b .
- (ii) Si $u \in k$ es una unidad, entonces u divide a 1.
- (iii) Dos elementos $a, b \in k$ son llamados asociados en k si $a = bu$ para algún $u \in k$ unidad.

1.5 Definición. Un subconjunto $I \subset k[x_1, \dots, x_n]$ es un **ideal** si satisface:

- (i) $0 \in I$.
- (ii) Si $f, g \in I$, entonces $f + g \in I$.
- (iii) Si $f \in I$ y $h \in k[x_1, \dots, x_n]$, entonces $hf \in I$.

1.6 Definición. Para f_1, \dots, f_s polinomios en $k[x_1, \dots, x_n]$, definimos el conjunto

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

$\langle f_1, \dots, f_s \rangle$ es un ideal.

1.7 Lema. Si $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, entonces $\langle f_1, \dots, f_s \rangle$ es un ideal de $k[x_1, \dots, x_n]$.

Diremos que $\langle f_1, \dots, f_s \rangle$ es el **ideal generado** por f_1, \dots, f_s .

Demostración. Demostremos que $\langle f_1, \dots, f_s \rangle$ es un ideal.

- (i) $0 \in \langle f_1, \dots, f_s \rangle$ ya que $0 = \sum_{i=1}^s 0f_i$
- (ii) Sean $f = \sum_{i=1}^s p_i f_i$ y $g = \sum_{i=1}^s q_i f_i$, entonces $f + g = \sum_{i=1}^s p_i f_i + \sum_{i=1}^s q_i f_i \in \langle f_1, \dots, f_s \rangle$
- (iii) Sean $f = \sum_{i=1}^s p_i f_i$ y $h \in k[x_1, \dots, x_n]$, así $hf = \sum_{i=1}^s (hp_i) f_i \in \langle f_1, \dots, f_s \rangle$

□

El ideal $\langle f_1, \dots, f_s \rangle$ tiene una buena interpretación en términos de ecuaciones polinómicas.

Dado $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, obtenemos el sistema de ecuaciones

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned}$$

Apartir de estas ecuaciones, se pueden derivar otras usando álgebra. Por ejemplo, si multiplicamos la primera ecuación por $h_1 \in k[x_1, \dots, x_n]$, la segunda por $h_2 \in k[x_1, \dots, x_n]$, así sucesivamente hasta la ecuación f_s por $h_s \in k[x_1, \dots, x_n]$ y sumamos las ecuaciones resultantes, obtenemos $h_1 f_1 + h_2 f_2 + \dots + h_s f_s = 0$.

Note que el lado izquierdo de la ecuación es un elemento del ideal $\langle f_1, \dots, f_s \rangle$. Así, podemos pensar de $\langle f_1, \dots, f_s \rangle$ como consistente en todas las “consecuencias polinómicas” de las ecuaciones $f_1 = f_2 = \dots = f_s = 0$.

Para ver lo que esto significa considere el ejemplo

$$\begin{cases} x = 1 + t \\ y = 1 + t^2 \end{cases} \quad (1.1)$$

Despejando t tenemos que $t = x - 1$, entonces $y = 1 + (x - 1)^2 = x^2 - 2x + 2$, así $x^2 - 2x + 2 - y = 0$.

Rehagamos este ejemplo igualando a cero las ecuaciones.

$$\begin{cases} x - 1 - t = 0 \\ y - 1 - t^2 = 0 \end{cases} \quad (1.2)$$

Para cancelar el término t multiplicamos la primera ecuación por $x - 1 + t$ y la segunda ecuación por -1

$$\begin{aligned} (x - 1 + t)(x - 1 - t) &= (x - 1)^2 - t^2 \\ (-1)(y - 1 - t^2) &= -y + 1 + t^2 \end{aligned}$$

Sumando las ecuaciones obtenemos $(x - 1)^2 - y + 1 = 0 = x^2 - 2x + 2 - y$.

En términos del ideal generado por las ecuaciones (1.2) podemos escribirlo como $x^2 - 2x + 2 - y = (x - 1 + t)(x - 1 - t) + (-1)(-y + 1 + t^2) \in \langle x - 1 - t, y - 1 - t^2 \rangle$.

De manera similar, cualquier otra “consecuencia polinomial” de (1.2), es decir, el sistema de ecuaciones igualadas a cero conduce a un elemento de este ideal.

1.8 Ejemplo. Tenemos el siguiente sistema de ecuaciones:

$$f = 2x^2 + 3y^2 - 11 = 0 \quad (1.3)$$

$$g = x^2 - y^2 - 3 = 0 \quad (1.4)$$

Veamos que $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$.

De la ecuación (1.4) despejamos y^2 y obtenemos $x^2 - 3 = y^2$, luego sustituimos en la ecuación (1.3) y tenemos

$$\begin{aligned} 2x^2 + 3(x^2 - 3) - 11 = 0 &\iff 2x^2 + 3x^2 - 9 - 11 = 0 \\ &\iff 5x^2 - 20 = 0 \\ &\iff x^2 - 4 = 0 \end{aligned}$$

Ahora, si despejamos x^2 de la ecuación (1.4) tenemos que $x^2 = y^2 + 3$, al sustituir x^2 en la ecuación (1.3) tenemos

$$\begin{aligned} 2(y^2 + 3) + 3y^2 - 11 = 0 &\iff 2y^2 + 6 + 3y^2 - 11 = 0 \\ &\iff 5y^2 - 5 = 0 \\ &\iff y^2 - 1 = 0 \end{aligned}$$

Note que $f = 2(x^2 - 4) + 3(y^2 - 1) = 2x^2 - 8 + 3y^2 - 3 = 2x^2 + 3y^2 - 11$ y $g = (x^2 - 4) - (y^2 - 1) = x^2 - 4 - y^2 + 1 = x^2 - y^2 - 3$. Por lo tanto, $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$.

1.9 Ejemplo. Sea $f_1 = y - z$, $f_2 = x + 2y + 3z$ y $f_3 = 3x - 4y + 2z$ polinomios en $\mathbb{Q}[x, y, z]$, consideremos el ideal $\langle f_1, f_2, f_3 \rangle$ y obtenemos el siguiente sistema de ecuaciones.

$$\begin{cases} y - z = 0 \\ x + 2y + 3z = 0 \\ 3x - 4y + 2z = 0 \end{cases} \quad (1.5)$$

La reducción de filas es la siguiente:

$$\begin{pmatrix} 0 & 1 & -1 \\ 1 & 2 & 3 \\ 2 & -4 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & -1 \\ 1 & 2 & 3 \\ 0 & -10 & -7 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & -1 \\ 1 & 2 & 3 \\ 0 & 0 & -17 \end{pmatrix}$$

Esto dice que se genera un nuevo conjunto para I que es $\{f_1, f_2, -17z\}$. Note que el polinomio $-17z$ se obtiene bajo la reducción

$$f_3 \xrightarrow{f_2} -10y - 7z \xrightarrow{f_1} -17z$$

El uso de estos pasos de reducción como el anterior se denotará por $f_3 \xrightarrow{f_1, f_2} -17z$.

Note que $f_3 = -10f_1 - 3f_2 - 17z$, tenga en cuenta que $-17z$ no se puede reducir más utilizando el principio de términos de f_1 y f_2 .

No es difícil ver que $f \in I = \langle f_1, f_2 \rangle = \langle f_1, f_3 \rangle$ si y sólo si el resto es cero, es decir, si el resto ya no se puede escribir en términos de los polinomios f_1 y f_2 .

1.2. Órdenes monomiales

Como observamos en los ejemplos anteriores de sistemas de ecuaciones polinómicas es necesario tener un orden en el método de la eliminación gaussiana y en el algoritmo de la división de polinomios para su resolución.

Para el algoritmo de división de polinomios, estamos tratando con el orden de grados en los monomios de una variable como:

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

y si hacemos eliminación gaussiana trabajando con ecuaciones lineales en $k[x_1, \dots, x_n]$, el orden suele ser:

$$x^n < \dots < x^2 < x$$

En esta sección, discutiremos las propiedades que debería tener tal ordenación.

Primero, observemos que en un monomio $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, los exponentes $\alpha = (\alpha_1, \dots, \alpha_n)$ son elementos de \mathbb{N}^n y entonces existe una correspondencia entre el conjunto de monomios y \mathbb{N}^n . En consecuencia, toda ordenación $>$ sobre el espacio \mathbb{N}^n induce una ordenación sobre los monomios, es decir, si $\alpha > \beta$, $x^\alpha > x^\beta$.

Dado que un polinomio es una suma de monomios, nos gustaría poder ordenar los términos en un polinomio sin ambigüedades en orden descendente (o ascendente). Para hacer esto, debemos poder comparar cada par de monomios para establecer su posiciones relativas adecuadas. Por tanto, exigiremos que nuestros ordenamientos sean lineales o totales, esto significa que para cada par de monomios x^α y x^β , se debe cumplir una de las tres situaciones: $x^\alpha > x^\beta$, $x^\alpha = x^\beta$ o $x^\alpha < x^\beta$.

1.10 Lema. Una relación de orden $<$ en \mathbb{N}^n es un buen orden si, y sólo si, toda sucesión decreciente de elementos de \mathbb{N}^n ,

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

es estacionaria, es decir, existe $n \in \mathbb{N}$ tal que $\alpha(n) = \alpha(m)$ para todo $n \leq m$.

Demostración. Demostraremos que $>$ no es un buen orden si, y sólo si, existe una sucesión infinita estrictamente decreciente de elementos de \mathbb{N} .

Si $>$ no es un buen orden en \mathbb{N}^n , existirá un subconjunto no vacío $S \subseteq \mathbb{N}^n$ que no tiene elemento mínimo. Como S es no vacío, podemos elegir un elemento $\alpha(1) \in S$; como $\alpha(1)$ no es el elemento mínimo de S , existe $\alpha(2) \in S$ tal que $\alpha(1) > \alpha(2)$; como $\alpha(2)$ no es el elemento mínimo de S , existe $\alpha(3) \in S$ tal que $\alpha(2) > \alpha(3)$. Continuando este proceso construimos una sucesión infinita estrictamente decreciente de elementos de \mathbb{N}^n . Recíprocamente, si existe una sucesión estrictamente decreciente de elementos de \mathbb{N}

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

entonces el subconjunto $S = \{\alpha(1), \alpha(2), \alpha(3), \dots\} \subset \mathbb{N}^n$ es no vacío y no posee un elemento mínimo, así que $>$ no puede ser un buen orden. □

1.11 Definición. Un orden monomial en $k[x_1, \dots, x_n]$ es una relación $>$ en \mathbb{N}^n , equivalentemente una relación en el conjunto de los monomios, que satisface las siguientes propiedades

- (i) La relación $>$ es un orden total (o lineal) en \mathbb{N}^n .
- (ii) Si $\alpha > \beta$, entonces $\alpha + \gamma > \beta + \gamma$ para $\gamma \in \mathbb{N}^n$.
- (iii) La relación $>$ es un buen ordenamiento en \mathbb{N}^n .

1.12 Definición. (Orden lexicográfico) Sean $\alpha, \beta \in \mathbb{N}^n$. Se dice que $\alpha >_{lex} \beta$ si en la diferencia $\alpha - \beta \in \mathbb{N}^n$ la primera componente es positiva y diferente de cero.

1.13 Ejemplo. Sean $f = xy^2$ y $g = y^3z^4$ polinomios en $k[x, y, z]$, entonces $\alpha = (1, 2, 0)$ y $\beta = (0, 3, 4)$. Así, $(1, 2, 0) >_{lex} (0, 3, 4)$, ya que $\alpha - \beta = (1, -1, -4)$.

1.14 Ejemplo. Si usamos el orden lexicográfico con $x < y$ en $k[x, y]$, entonces tenemos

$$1 < x < x^2 < x^3 < \dots < y < xy < x^2y < \dots < y^2 < \dots$$

1.15 Proposición. El orden lexicográfico en \mathbb{N}^n es un orden monomial.

Demostración. (a) $>_{lex}$ es un orden total, se sigue del orden total de \mathbb{N}^n .

- (b) Si $\alpha >_{lex} \beta$, entonces

$$\begin{aligned} x^\alpha \cdot x^\gamma &= x^{\alpha+\gamma} \\ x^\beta \cdot x^\gamma &= x^{\beta+\gamma} \end{aligned}$$
 Así, $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta > 0$.

(c) Supongamos que $>_{lex}$ no fuera un buen ordenamiento. Por el Lema 1.10 existe una sucesión estrictamente decreciente en \mathbb{N}^n . Mostraremos que esto conduce a una contradicción.

Considere las primeras entradas de los vectores $\alpha(i) \in \mathbb{N}^n$. Por la definición del orden lexicográfico, estas primeras entradas forman una sucesión no creciente de enteros no negativos. Dado que \mathbb{N}^n está bien ordenado, las primeras entradas de $\alpha(i)$ deben “estabilizarse” eventualmente. En otras palabras, existe l tal que todas las primeras entradas de $\alpha(i)$ con $i \geq l$ son iguales.

Comenzando en $\alpha(l)$, la segunda entrada y las subsiguientes entradas entran en juego determinando el orden lexicográfico. Las segundas entradas de $\alpha(l), \alpha(l+1), \dots$ formar una sucesión decreciente. Por el mismo razonamiento que antes, las segundas entradas se “estabilizan” eventualmente. Continuando el proceso, para algún m , $\alpha(m), \alpha(m+1), \dots$ formar una sucesión decreciente. Esto contradice el hecho de que $\alpha(m) > \alpha(m+1)$.

□

1.16 Observación. Hay muchos ordenes lexicográficos, para n variables x_1, \dots, x_n hay $n!$ órdenes lexicográficos.

Para nosotros el orden lexicográfico significará

$$x_1 > x_2 > x_3 > \dots > x_n$$

$$x > y > z$$

1.17 Definición. (Orden graduado lexicográfico)

Sean $\alpha, \beta \in \mathbb{N}^n$. Se dice que $\alpha >_{grlex} \beta$

si $|\alpha| = \sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i = |\beta|$ o $|\alpha| = |\beta|$ y $\alpha >_{lex} \beta$.

1.18 Ejemplo. Sean $f_1 = xy^2z^3$, $f_2 = x^3y^2$, $g_1 = xy^2z^4$ y $g_2 = xyz^5$ polinomios en $k[x, y, z]$.

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

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

1.19 Ejemplo. Usando el orden graduado lexicográfico en $k[x, y]$ con $x < y$ tenemos:

$$1 < x < y < x^2 < xy < y^2 < x^3 < x^2y < xy^2 < y^3 < \dots$$

1.20 Definición. (Orden graduado lexicográfico inverso)

Sean $\alpha, \beta \in \mathbb{N}^n$. Se dice que $\alpha >_{\text{grevlex}} \beta$

Si $|\alpha| = \sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i = |\beta|$ o $|\alpha| = |\beta|$ y la tercera componente del vector $\alpha - \beta \in \mathbb{N}^n$ es negativa y diferente de cero.

1.21 Ejemplo. Sean $f_1 = x^4y^7z$, $f_2 = x^4y^2z^3$, $g_1 = x^4yz^3$ y $g_2 = xy^5z^2$ polinomios en $k[x, y, z]$.

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

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

1.22 Ejemplo. Consideremos los polinomios $x_1^2x_2x_3 > x_1x_2^3$ con respecto al orden grlex con $x_3 < x_2 < x_1$.

$x_1^2x_2x_3 < x_1x_2^3$ con respecto al orden grevlex con $x_3 < x_2 < x_1$.

1.23 Ejemplo. Sea $f = 2x^2y^8 - 3x^5yz^4 + xyz^4 + 4x^6 - y^2 \in k[x, y, z]$. Vamos a ordenar a f respecto a los órdenes monomiales mencionados anteriormente con $x > y > z$.

(i) Respecto al orden lexicográfico (lex) reordenaríamos los términos de f en orden decreciente como:

$$f = 4x^6 - 3x^5yz^4 + 2x^2y^8 + xyz^4 + y^2.$$

(ii) Respecto al orden graduado lexicográfico (grlex) ordenamos a f como:

$$f = -3x^5yz^4 + 2x^2y^8 + 4x^6 + xyz^4 - y^2.$$

(iii) Respecto al orden graduado lexicográfico inverso (grevlex) ordenamos a f como:

$$f = 2x^2y^8 - 3x^5yz^4 + 4x^6 + xyz^4 - y^2.$$

1.24 Definición. Sea $f = \sum_{\alpha} a_{\alpha}x^{\alpha}$ un polinomio distinto de cero en $k[x_1, \dots, x_n]$ y sea $>$ un orden monomial. Definimos:

(i) El **multigrado** de f como: $\text{multideg}(f) = \max \{ \alpha \in \mathbb{N}^n : a_{\alpha} \neq 0 \}$.

El máximo se toma con respecto a $>$.

(ii) El **coeficiente principal** de f como: $LC(f) = a_{\text{multideg}(f)} \in k$.

(iii) El **monomio principal** de f como: $LM(f) = x^{\text{multideg}(f)}$.

(iv) El **término principal** de f como: $LT(f) = LC(f) \cdot LM(f)$.

1.25 Ejemplo. Sea $f = 2x^2y^8 - 3x^5yz^4 + 4x^6 + xyz^4 - y^2 \in k[x, y, z]$, de acuerdo al orden monomial tenemos:

Lex. $multideg(f) = (6, 0, 0)$, $LC(f) = 4$, $LM(f) = x^6$ y $LT(f) = 4x^6$.

Grlex. $multideg(f) = (5, 1, 4)$, $LC(f) = -3$, $LM(f) = x^5yz^4$ y $LT(f) = -3x^5yz^4$.

Grevlex. $multideg(f) = (2, 8, 0)$, $LC(f) = 2$, $LM(f) = x^2y^8$ y $LT(f) = 2x^2y^8$.

1.26 Lema. Sean $f, g \in k[x_1, \dots, x_n]$ polinomios distintos de cero. Entonces:

(i) $multideg(fg) = multideg(f) + multideg(g)$.

(ii) Si $f + g \neq 0$, $multideg(f + g) \leq \max\{multideg(f), multideg(g)\}$. Además se cumple la igualdad si $multideg(f) \neq multideg(g)$.

La demostración de este resultado es inmediata.

1.3. Algoritmo de la División en varias variables

En esta sección formularemos un algoritmo de división para polinomios en $k[x_1, \dots, x_n]$ que extiende el algoritmo para $k[x]$. En el caso general, el objetivo es dividir $f \in k[x_1, \dots, x_n]$ por $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Como veremos, esto significa expresar f en la forma

$$f = a_1f_1 + a_2f_2 + \dots + a_sf_s + r,$$

donde los "cocientes" a_1, \dots, a_s y el resto r están en $k[x_1, \dots, x_n]$. Aquí es donde usaremos los ordenes monomiales. Luego veremos cómo el algoritmo de división se aplica al problema de pertenecer al ideal.

1.27 Ejemplo. Sean $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ y $f_2 = y^2 - 1$, con el orden lexicográfico. Si dividimos f por f_1 . $LT(f)$ es múltiplo de $LT(f_1)$, así que primero dividimos f entre f_1

$$\begin{array}{r} \left| \begin{array}{l} xy - 1 \\ y^2 - 1 \end{array} \right| \\ \underline{ x} \\ f = x^2y + xy^2 + y^2 \\ \underline{-x^2y + x} \\ xy^2 + x + y^2 \end{array}$$

Como xy^2 es divisible por $LT(f_1)$, continuamos dividiendo entre f_1

$$\begin{array}{r}
 \overline{xy - 1} \mid \overline{y^2 - 1} \\
 x + y \\
 f = x^2y + xy^2 + y^2 \\
 \underline{-x^2y + x} \\
 xy^2 + x + y^2 \\
 \underline{-xy^2 + y} \\
 x + y^2 + y
 \end{array}$$

Note que $LT(x + y^2 + y) = x$ no es divisible por $LT(f_1) = xy$, ni por $LT(f_2) = y^2$. Sin embargo, $x + y^2 + y$ no es el resto pues $LT(f_2)$ divide a y^2 , así x forma parte del resto y continuamos dividiendo por f_2 .

$$\begin{array}{r}
 \overline{xy - 1} \mid \overline{y^2 - 1} \\
 x + y \qquad 1 \\
 f = x^2y + xy^2 + y^2 \\
 xy^2 + x + y^2 \\
 x + y^2 + y \\
 \underline{x - y^2 + 1} \\
 x + y + 1
 \end{array}$$

Como y y 1 no son divisibles por $LT(f_1)$ ni $LT(f_2)$ pasan al resto. Así, el resto es $x + y + 1$.

Por lo tanto, $x^2y + xy^2 + y^2 = (x + y)(xy - 1) + 1(y^2 - 1) + x + y + 1$.

1.28 Teorema. (Algoritmo de la división en $k[x_1, \dots, x_n]$)

Si la relación $>$ en \mathbb{N}^n es un orden monomial fijo y sea $F = (f_1, \dots, f_s)$ una s -tupla ordenada de polinomios en $k[x_1, \dots, x_n]$. Entonces, cada $f \in k[x_1, \dots, x_n]$ se puede escribir como

$$f = a_1f_1 + \dots + a_sf_s + r$$

donde $a_i, r \in k[x_1, \dots, x_n]$, y $r = 0$ o r es una combinación lineal de monomios con coeficientes en k , ninguno de los cuales es divisible por algún $LT(f_1), \dots, LT(f_s)$.

Además, si $a_if_i \neq 0$, tendremos que

$$\text{multideg}(f) \geq \text{multideg}(a_if_i).$$

Demostración. Demostraremos la existencia de los a_i y r , mediante un algoritmo:

Entrada: f_1, \dots, f_s, f

Salida: a_1, \dots, a_s, r

$a_1 := 0; \dots; a_s := 0; r := 0$

$p := f$

WHILE $p \neq 0$ **DO**

$i := 1$

ocurriodivision := falso

WHILE $i \leq s$ **AND** ocurriodivision := falso **DO**

IF $LT(f_i)$ divide a (p) **THEN**

$a_i := a_i + LT(p)/LT(f_i)$

$p := p - (LT(p)/LT(f_i))f_i$

ocurriodivision := verdadero

END IF

ELSE

$i := i + 1$

END WHILE

IF ocurriodivision := falso **THEN**

$r := r + LT(p)$

$p := p - LT(p)$

La variable “ocurriodivision” nos dice cuándo algún $LT(f_i)$ divide el término principal del dividendo intermedio, lo que nos lleva a dos casos:

1. Si algún $LT(f_i)$ divide a $LT(p)$, entonces el algoritmo procede como en el caso de una variable.
2. Si ningún $LT(f_i)$ divide a $LT(p)$, entonces el algoritmo suma $LT(p)$ al resto.

Para probar que el algoritmo funciona, primero mostraremos que

$$f = a_1 f_1 + \dots + a_s f_s + p + r \quad (1.6)$$

se cumple. En efecto, esto se cumple para los valores iniciales a_1, \dots, a_s, p y r . Ahora, supongamos que (1.6) se cumple en la primera iteración del algoritmo, si el siguiente paso es una división entonces alguna $LT(f_i)$ divide a $LT(p)$, y la igualdad

$$a_i f_i + p = (a_i + LT(p)/LT(f_i))f_i + (p - (LT(p)/LT(f_i))f_i)$$

muestra que $a_i f_i + p$ no cambia. Dado que todas las demás variables no se ven afectadas, 1.6 permanece cierto en este caso. Por otro lado, si el siguiente paso es un paso restante, entonces p y r cambiarán, pero la suma $p + r$ no cambia ya que

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

Como antes, la igualdad 1.6 aún se conserva.

A continuación, observe que el algoritmo se detiene cuando $p = 0$. En esta situación, (1.6) se convierte en

$$f = a_1 f_1 + \dots + a_s f_s + r$$

Dado que los términos se agregan a r solo cuando no son divisibles por ninguno de los $LT(f_i)$, se sigue que a_1, \dots, a_s y r tienen las propiedades deseadas cuando termina el algoritmo.

Finalmente, necesitamos mostrar que el algoritmo eventualmente termina. La clave es que cada vez que redefinimos la variable p , la disminución de los grados (relativo a nuestro ordenamiento) se convierte en 0. Para ver esto, primero suponga que durante alguna división, p se redefine como:

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

y tenemos que

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

de modo que p y $(LT(p)/LT(f_i))f_i$ tienen el mismo término principal. Por lo tanto, su diferencia p' debe tener un multigrado estrictamente más pequeño cuando $p' \neq 0$. A continuación, suponga que si la siguiente iteración es una iteración para el resto, p se redefine para ser

$$p' = p - LT(p)$$

Note que $multideg(p') < multideg(p)$ cuando $p' \neq 0$. Así, en cualquier caso, el multigrado debe disminuir. Si el algoritmo nunca terminara, entonces obtendríamos una secuencia decreciente infinita de multigrados. La propiedad de buen orden de $>$ muestra que esto no puede ocurrir. Por lo tanto, $p = 0$ debe ocurrir eventualmente, de modo que el algoritmo termina después de un número finito de pasos.

Ahora, estudiemos la relación entre $multideg(f)$ y $multideg(a_i f_i)$. Cada término en a_i es de la forma $LT(p)/LT(f_i)$ para algún valor de la variable p . El algoritmo comienza con

$p = f$ y mostramos que el multigrado de p decrece. Por lo tanto, $LT(p) < LT(f)$, usando la condición (ii) de la definición de un orden monomio se tiene que $multideg(a_i f_i) < multideg(f)$ cuando $a_i f_i \neq 0$. \square

1.29 Ejemplo. Sean $f = xy^2 - x$ y $f_1 = xy + 1$, $f_2 = y^2 - 1 \in k[x, y]$ con el orden lexicográfico $x > y$. Si dividimos f por $F = (f_1, f_2)$

$$\begin{array}{r} \quad \quad \quad \boxed{xy + 1} \mid y^2 - 1 \\ \quad \quad \quad \underline{} \\ \quad \quad \quad -xy^2 - y \\ \quad \quad \quad \underline{} \\ \quad \quad \quad -x - y \end{array}$$

Como ni $-xy - y$ son múltiplos de $LT(f_1)$ ni $LT(f_2)$, terminamos la división obteniendo

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

Ahora, si dividimos f por $F = (f_2, f_1)$

$$\begin{array}{r} \quad \quad \quad \boxed{xy + 1} \mid y^2 - 1 \\ \quad \quad \quad \underline{} \\ \quad \quad \quad -xy^2 + x \\ \quad \quad \quad \underline{} \\ \quad \quad \quad 0 \end{array}$$

Por lo tanto, $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$.

1.30 Ejemplo. Sea $f = x^2y + xy^2 + y^2$, dividamos a f entre $f_1 = y^2 - 1$ y $f_2 = xy - 1$ usando el orden lexicográfico $x > y$.

Si dividimos f por $F = (f_1, f_2)$, como $LT(f)$ no divide a $LT(f_1)$ pero si divide a $LT(f_2)$ comenzamos a dividir por f_2

$$\begin{array}{r} \quad \quad \quad \boxed{y^2 - 1} \mid xy - 1 \\ \quad \quad \quad \underline{} \\ \quad \quad \quad -x^2y + x \\ \quad \quad \quad \underline{} \\ \quad \quad \quad xy^2 + x + y^2 \end{array}$$

Luego, $LT(xy^2 + x + y^2)$ es divisible por $LT(f_1)$, entonces tenemos

$$\begin{array}{r} \begin{array}{|l} y^2 - 1 \\ \hline x \end{array} \quad \begin{array}{|l} xy - 1 \\ \hline x \end{array} \\ x^2y + xy^2 + y^2 \\ xy^2 + x + y^2 \\ \hline -xy^2 + x \\ 2x + y^2 \end{array}$$

$2x$ no es múltiplo de $LT(f_1)$ ni de $LT(f_2)$, así que $2x$ forma parte del resto y continuamos dividiendo

$$\begin{array}{r} \begin{array}{|l} y^2 - 1 \\ \hline x + 1 \end{array} \quad \begin{array}{|l} xy - 1 \\ \hline x \end{array} \\ x^2y + xy^2 + y^2 \\ xy^2 + x + y^2 \\ 2x + y^2 \\ \hline 2x - y^2 + 1 \\ 2x + 1 \end{array}$$

De igual manera 1 forma parte del resto. Por lo tanto,

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

Comparando con el Ejemplo 1.27 podemos observar que los restos de las divisiones son distintos.

Los Ejemplos 1.27 y 1.30 muestran que el orden de los s -tupla de polinomios (f_1, \dots, f_s) importa y si seguimos el algoritmo podemos notar que a_1, \dots, a_s y r están determinados si reordenamos f_1, \dots, f_s .

En $k[x]$ necesitamos que el resto sea cero para que f pertenezca al ideal I . En $k[x_1, \dots, x_n]$, si después de la división de f por F el resto igual a cero, entonces

$$f = a_1f_1 + \dots + a_sf_s$$

de modo que $f \in \langle f_1, \dots, f_s \rangle$. Por lo tanto, $r = 0$ es una condición suficiente para pertenecer al ideal. Sin embargo, en los Ejemplos 1.27 y 1.30 podemos notar que aunque el resto es distinto de cero, f pertenece al ideal generado por F . así, la condición de que f pertenece al ideal I si y sólo si $r = 0$, no es aplicable para el caso de varias variables.

1.4. Ideales Monomiales

1.31 Definición. Un ideal $I \subset k[x_1, \dots, x_n]$ es un *ideal monomial* si existe un subconjunto $A \subset \mathbb{N}^n$ (posiblemente infinito) tal que I está formado por todos los polinomios que son sumas finitas de la forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, donde $h_\alpha \in k[x_1, \dots, x_n]$. En este caso, escribimos

$$I = \{x^\alpha : \alpha \in A\}.$$

1.32 Lema. Sea $I = \{x^\alpha : \alpha \in A\}$ un ideal monomial, entonces el monomio x^β pertenece a I si y sólo si x^β es divisible por x^α para algún $\alpha \in A$.

Demostración. Si x^β es múltiplo de x^α , entonces $x^\beta \in I$ por definición de ideal. Ahora, si $x^\beta \in I$, entonces $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, donde $h_i \in k[x_1, \dots, x_n]$ y $\alpha(i) \in A$. Si desarrollamos cada h_i como una combinación lineal de monomios, vemos que cada término en el lado derecho de la ecuación es divisible por algún $x^{\alpha(i)}$. Por lo tanto, el lado izquierdo x^β debe tener la misma propiedad. \square

Note que x^β es divisible por x^α exactamente cuando $x^\beta = x^\alpha \cdot x^\gamma$ para algún $\gamma \in \mathbb{N}^n$, esto es equivalente a $\beta = \alpha + \gamma$, entonces tenemos el conjunto $\alpha + \mathbb{N}^n = \{\alpha + \gamma : \gamma \in \mathbb{N}^n\}$ que consta de los exponentes de todos los monomios divisibles por x^α .

1.33 Teorema. (Lema de Dickson).

Sea $I = \{x^\alpha : \alpha \in A\} \subseteq k[x_1, \dots, x_n]$ un ideal monomial. Entonces I se puede escribir de la forma $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$, donde $\alpha(1), \dots, \alpha(s) \in A$. En particular, I tiene una base finita.

Demostración. Realizaremos la demostración de este Lema por inducción sobre n , el número de variables

Si $n = 1$, entonces I está generado por el monomio x_1^α , donde $\alpha \in A \subset \mathbb{N}^n$. Si β es el elemento más pequeño en A , entonces $\beta \leq \alpha$ para todo $\alpha \in A$, por lo tanto, x_1^β divide a todos los demás generadores x_1^α . Así, $I = \langle x_1^\beta \rangle$.

Ahora, supongamos que $n > 1$ y que el teorema se cumple para $n - 1$. Escribiremos las variables como $x_1, x_2, \dots, x_{n-1}, y$, de modo que los monomios en $k[x_1, \dots, x_{n-1}, y]$ se pueden escribir como $x^\alpha y^m$, donde $m \in \mathbb{N}$ y $\alpha = (\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{N}^{n-1}$. Supongamos que $I \subset k[x_1, \dots, x_{n-1}, y]$ es un ideal monomial. Sea J el ideal en $k[x_1, \dots, x_{n-1}]$ generado por los monomios x^α para los cuales $x^\alpha y^m \in I$ para algún $m \geq 0$. Como J es un ideal monomial en $k[x_1, \dots, x_{n-1}]$, nuestra hipótesis inductiva implica que un número finito de los x^α genera a J , es decir, $J = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$.

Para cada i entre 1 y s , la definición de J nos dice que $x^{\alpha(i)} y^{m_i} \in I$ para algún $m_i \geq 0$. Sea m el máximo de los m_i , entonces para cada k entre 0 y $m - 1$, consideremos el ideal

$J_k \subset k[x_1, \dots, x_{n-1}]$ generado por los monomios x^β tal que $x^\beta y^k \in I$. Por nuestra hipótesis de inducción, J_k está generado por un número finito de elementos, $J_k = \langle x^{\alpha_k(1)}, \dots, x^{\alpha_k(s_k)} \rangle$.

I es generado por los siguientes monomios:

$$\begin{aligned} \text{Para } J: & \quad x^{\alpha(1)}y^m, \dots, x^{\alpha(s)}y^m \\ \text{Para } J_0: & \quad x^{\alpha_0(1)}, \dots, x^{\alpha_0(s_0)}, \\ \text{Para } J_1: & \quad x^{\alpha_1(1)}y, \dots, x^{\alpha_1(s_1)}y, \\ & \quad \vdots \\ \text{Para } J_{m-1}: & \quad x^{\alpha_{m-1}(1)}y^{m-1}, \dots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}. \end{aligned}$$

Primero veamos que todo monomio de I es divisible por alguno de los anteriores. Sea $x^\alpha y^p \in I$. Si $p \geq m$, entonces $x^\alpha y^p$ es divisible por algún $x^{\alpha(i)}y^m$ por construcción de J . Si $p \leq m-1$, entonces $x^\alpha y^p$ es divisible por algún $x^{\alpha_p(j)}y^p$ por construcción de J_p . Por el Lema 1.32, los monomios anteriores, generan un ideal que tiene los mismos monomios que I , así que tienen que ser iguales.

Finalmente, tenemos que demostrar que el conjunto finito de generadores, se puede escoger de entre un conjunto de generadores dados del ideal. Si volvemos a escribir las variables como x_1, \dots, x_n , nuestro ideal monomial es $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1, \dots, x_n]$. Como $I = \langle x^{\beta(1)}, \dots, x^{\beta(s)} \rangle$, para ciertos monomios $x^{\beta(i)} \in I$, por el Lema 1.32, cada $x^{\beta(i)}$ es divisible por $x^{\alpha(i)}$ para algún $\alpha(i) \in A$. De este modo, $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. \square

Capítulo 2

Bases de Gröbner

En este capítulo se define el objetivo principal de este trabajo, se estudia el teorema de la base de Hilbert, y en consecuencia se define la base de Gröbner y sus propiedades básicas. Asimismo, se introduce la definición de S -polinomio y el criterio de Buchberger con los cuales se muestra si una base dada es una base de Gröbner, esta idea conduce a un algoritmo conocido como el algoritmo de Buchberger para calcular una base de Gröbner.

2.1. Definición y propiedades

2.1 Definición. Sea $I \subset k[x_1, \dots, x_n]$ un ideal distinto del $\{0\}$:

(i) Definimos el conjunto de los términos principales de elementos de I como:

$$LT(I) = \{LT(f) = cx^\alpha : \text{existe } f \in I \setminus \{0\}\}.$$

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

Si I es el ideal generado por $\{f_1, \dots, f_s\}$, entonces $\langle LT(f_1), \dots, LT(f_s) \rangle \subset \langle LT(I) \rangle$. El siguiente ejemplo muestra que no siempre los ideales son iguales, es decir, no necesariamente los términos principales del ideal coinciden con el ideal generado por los términos principales de cada polinomio en I .

2.2 Ejemplo. Sea $I = \langle f_1, f_2 \rangle$, donde $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$. Si usamos el orden graduado lexicográfico en $k[x, y]$, tenemos que

$$x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^2,$$

tal que $x^2 \in \langle f_1, f_2 \rangle$, así, $x^2 \in \langle LT(I) \rangle$. Además, x^2 no es divisible por $LT(f_1) = x^3$ ni por $LT(f_2) = x^2y$, por lo tanto $LT(I) \not\subset \langle LT(f_1), LT(f_2) \rangle$.

2.3 Proposición. Sea $I \subset k[x_1, \dots, x_n]$ un ideal. Las siguientes aseveraciones son equivalentes.

- (i) $\langle LT(I) \rangle$ es un ideal monomial.
- (ii) Existen $g_1, \dots, g_s \in I$ tales que $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$.

Demostración. \implies] Supongamos que $\langle LT(I) \rangle$ es un ideal monomial. Por demostrar: Existen $g_1, \dots, g_s \in I$ tales que $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$.

Como $\langle LT(I) \rangle$ es un ideal monomial, por el lema de Dickson 1.33 $x^{\alpha(1)}, \dots, x^{\alpha(t)}$ generan a $\langle LT(I) \rangle$ y por el Lema 1.32 cada $x^{\alpha(i)} \in \langle LT(I) \rangle$ si y solo si es divisible por algún monomio monico que genera a $\langle LT(I) \rangle$, entonces $x^{\alpha(i)} = LM(g_i)$ para algún monomio $g_i \in I$.

\impliedby] Ahora, demostremos que $\langle LT(I) \rangle$ es ideal monomial.

Los monomios principales $LM(g)$ de elementos $g \in I \setminus \{0\}$ generan el ideal monomial $\langle LM(g) : g \in I \setminus \{0\} \rangle$, dado que $LM(g)$ y $LT(g)$ difieren de una constante distinta de cero el ideal $\langle LM(g) : g \in I \setminus \{0\} \rangle = \langle LT(I) \rangle$

□

2.4 Teorema. (Teorema de la Base de Hilbert)

Todo ideal $I \subset k[x_1, \dots, x_n]$ tiene un conjunto finito de generadores.

Demostración. Si $I = \{0\}$, el conjunto generador será $\{0\}$. Si $I \neq 0$, por la proposición anterior, existen polinomios $g_1, \dots, g_s \in I$ tales que $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$. Veamos que $I = \langle g_1, \dots, g_s \rangle$.

Es claro que $\langle g_1, \dots, g_s \rangle \subset I$, ya que cada $g_i \in I$. Para la otra contención, sea $f \in I$ un polinomio cualquiera. Aplicando el algoritmo de la división para dividir f entre $\langle g_1, \dots, g_s \rangle$, obtenemos

$$f = a_1g_1 + \dots + a_s g_s + r,$$

donde ningún término de r es divisible por ningún $LT(g_1), \dots, LT(g_s)$ y tenemos dos casos: $r \neq 0$ o $r = 0$, si $r = 0$ hemos terminado.

Note que si $r \neq 0$,

$$r = f - a_1g_1 - \dots - a_s g_s \in I$$

ya que f y g_1, \dots, g_s pertenecen a I , entonces $LT(r) \in \langle LT(g_1), \dots, LT(g_s) \rangle$, esto nos dice que el término principal de r es divisible por algún término principal de algún g_i , lo cual no es posible por el algoritmo de la división, de este modo $r = 0$, teniendo

$$f = a_1g_1 + \dots + a_s g_s + 0 \in \langle g_1, \dots, g_s \rangle$$

por lo tanto, $I \subset \langle g_1, \dots, g_s \rangle$.

□

La base utilizada en la demostración anterior tiene una propiedad especial, que es $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$. Esto nos lleva a la siguiente definición.

2.5 Definición. Fijado un orden monomial. Sea $G = \{g_1, \dots, g_s\}$ un conjunto finito de un ideal $I \subset k[x_1, \dots, x_n]$, se dice que es una base de Gröbner si

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

En el Ejemplo 2.2 nos muestra que la base $\{f_1, f_2\}$ no es una base de Gröbner para I , ya que $x^2 \in \langle LT(I) \rangle$, pero $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.

2.6 Corolario. Fijado un orden monomial, todo ideal $I \subset k[x_1, \dots, x_n]$ distinto del $\{0\}$ tiene una base de Gröbner. Además, cualquier base de Gröbner para un ideal I , es base de I .

Demostración. Dado un ideal distinto de $\{0\}$, el conjunto $G = \{g_1, \dots, g_s\}$ construido en la demostración del Teorema 2.4 es una base de Gröbner por definición. Si $\langle LT(g_1), \dots, LT(g_s) \rangle = \langle LT(I) \rangle$, el argumento dado en el Teorema 2.4 nos muestra que $I = \langle g_1, \dots, g_s \rangle$, de modo que G es una base para I . □

2.7 Teorema. (Condición de la Cadena Ascendente)

$$\text{Sea } I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

una cadena ascendente de ideales en $k[x_1, \dots, x_n]$. Existe $N \geq 1$ tal que

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

Demostración. Dada una sucesión ascendente $I \subseteq I_2 \subseteq I_3 \subseteq \dots$, consideremos el conjunto $I = \bigcup_{i=1}^{\infty} I_i$. Veamos que I es un ideal.

- (i) $0 \in I$, ya que $0 \in I_i$ para toda i .
- (ii) Sean $f, g \in I$, por definición $f \in I_i$ y $g \in I_j$ para $i \neq j$ tal que $i \leq j$. Como los ideales forman una cadena ascendente, $I_i \subseteq I_j$, así $f \in I_j$, de modo que $f + g \in I_j \subseteq I$.
- (iii) Sea $f \in I$ y $r \in k[x_1, \dots, x_n]$, entonces $f \in I_i$ para alguna i y $rf \in I_i \subseteq I$.

Por lo tanto (i), (ii) y (iii) muestran que I es un ideal. Ahora, por el Teorema de la Base de Hilbert 2.4, el ideal tiene un conjunto finito de generadores $I = \langle f_1, \dots, f_s \rangle$. Cada uno de los generadores pertenece a un I_j , es decir, $f_k \in I_{j_k}$. Si N es el máximo de los j_k , entonces por la definición de cadena ascendente tenemos que $I = \langle f_1, \dots, f_s \rangle \subset I_N \subseteq I_{N+1} \subseteq \dots \subseteq I$. □

A continuación estudiemos las propiedades básicas de la base de Gröbner.

2.8 Proposición. Si $G = \{g_1, \dots, g_s\}$ es una base de Gröbner del ideal $I \subset k[x_1, \dots, x_n]$ y $f \in k[x_1, \dots, x_n]$. Entonces existe un único $r \in k[x_1, \dots, x_n]$ que cumple las siguientes condiciones:

(i) Ningún término de r es divisible por ningún $LT(g_1), \dots, LT(g_s)$.

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

En particular, r es el resto de la división de f por G , sin importar como esten ordenados los elementos de G al aplicar el algoritmo de la división.

Demostración. Por el algoritmo de la división $f = a_1g_1 + \dots + a_tg_t + r$, esto demuestra la existencia de r . Para la unicidad, supongamos que $f = g + r = g' + r'$ satisfacen (i) y (ii), entonces $r - r' = g' - g \in I$, de modo que $r \neq r'$, entonces $LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$. Por el Lema 1.32 se sigue que $LT(r - r')$ es divisible por algún $LT(g_i)$, pero esto no puede ser ya que ningún término de r y r' es divisible por algún $LT(g_1), \dots, LT(g_t)$, por lo cual $r - r' = 0$, demostrando así la unicidad. \square

2.9 Corolario. Sea $G = \{g_1, \dots, g_s\}$ una base de Gröbner para el ideal $I \subset k[x_1, \dots, x_n]$ y sea $f \in k[x_1, \dots, x_n]$. Entonces $f \in I$ si y sólo si el resto r de la división de f por G es cero.

Demostración. Hemos observado que si el resto es cero $f \in I$. Ahora, si $f \in I$, entonces $f = g + r$ y $f = f + 0$ satisface las condiciones de la proposición anterior, de modo que cero es el resto de la división de f por G . \square

2.10 Definición. Denotamos por \overline{f}^F al resto de la división de f por la S -tupla ordenada $F = (f_1, \dots, f_s)$. Si F es una base de Gröbner podemos ver a F como un conjunto (sin ningún orden en particular), por la Proposición 2.8.

2.11 Definición. Sean $f, g \in k[x_1, \dots, x_n]$ polinomios no cero.

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

$$x^\gamma = \text{LCM}(LM(f), LM(g)).$$

El mínimo común múltiplo lo denotamos como LCM.

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

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

2.12 Ejemplo. Sean $f = 4x^2z - 7y^2$ y $g = xyz^2 + 3xz^4$ en $\mathbb{R}[x, y, z]$ con el orden graduado lexicográfico, entonces $\gamma = (2, 2, 4)$ y

$$S(f, g) = \frac{x^2yz^2}{4x^2z} \cdot f - \frac{x^2yz^2}{xyz^2} \cdot g = \frac{1}{4}yz(4x^2z - 7y^2) - x(xyz^2 + 3xz^4) = 3x^2z^4 + \frac{7}{4}y^3z.$$

Un S -polinomio $S(f, g)$ está “diseñado” para producir la cancelación de los términos principales.

2.13 Lema. Supongamos que tenemos una suma $\sum_{i=1}^s c_i f_i$, donde $c_i \in K$ y $\text{multideg}(f_i) = \delta \in \mathbb{N}^n$ para toda i . Si $\text{multideg}(\sum_{i=1}^s c_i f_i) < \delta$, entonces $\sum_{i=1}^s c_i f_i$ es una combinación lineal con coeficientes en k de los S -polinomios $S(f_j, f_k)$ para $1 \leq j, k \leq s$. Además, cada $S(f_j, f_k)$ tiene multigrado menor que δ .

Demostración. Escribimos a $f_i = x^{\alpha(i)} g_i$ y sea $d_i = LC(f_i)$, de modo que $c_i d_i$ es el coeficiente principal de $c_i f_i$, como $c_i f_i$ tiene multigrado δ y su suma es estrictamente menor que el multigrado δ se sigue que $\sum_{i=1}^s c_i d_i = 0$.

Ahora, definimos $p_i = f_i/d_i$, y note que el coeficiente principal de p_i es 1. Considere la suma

$$\begin{aligned} \sum_{i=1}^s c_i f_i &= \sum_{i=1}^s c_i d_i p_i \\ &= c_1 d_1 p_1 + c_2 d_2 p_2 + \dots + c_{s-1} d_{s-1} p_{s-1} + c_s p_s d_s \\ &= c_1 d_1 p_1 + c_1 d_1 p_2 - c_1 d_1 p_2 + \dots + c_1 d_1 p_{s-1} - c_1 d_1 p_{s-1} + c_1 d_1 p_s - c_1 d_1 p_s + \\ &\quad c_2 d_2 p_2 + c_2 d_2 p_3 - c_2 d_2 p_3 + \dots + c_2 d_2 p_{s-1} - c_2 d_2 p_{s-1} + c_2 d_2 p_s - c_2 d_2 p_s + \\ &\quad \dots + c_{s-1} d_{s-1} p_{s-1} + c_{s-1} d_{s-1} p_s - c_{s-1} d_{s-1} p_s + c_s d_s p_s \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2) (p_2 - p_3) + \dots + \\ &\quad (c_1 d_1 + \dots + c_{s-1} d_{s-1}) (p_{s-1} - p_s) + (c_1 d_1 + \dots + c_s d_s) p_s \end{aligned}$$

Además, $LT(f_i) = d_i x^\delta$ y $LM(f_k) = x^\delta$, esto implica que $LMC(LM(f_i), LM(f_k)) = x^\delta$, entonces

$$S(f_j, f_k) = \frac{x^\delta}{LT(f_j)} f_j - \frac{x^\delta}{LT(f_k)} f_k = \frac{x^\delta}{d_j x^\delta} f_j - \frac{x^\delta}{d_k x^\delta} f_k = p_j - p_k \quad (2.1)$$

Usando la ecuación (2.1) y que $\sum_{i=1}^s c_i d_i = 0$, tenemos que la suma

$$\begin{aligned} \sum_{i=1}^s c_i f_i &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) \\ &\quad + \dots + (c_1 d_1 + \dots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s). \end{aligned}$$

Dado que p_j y p_k tienen multigrado δ y coeficiente 1, la diferencia $p_j - p_k$ tiene multigrado menor que δ □

2.14 Teorema. (Criterio de Buchberger)

Sea I un ideal de $k[x_1, \dots, x_n]$. Una base $G = \{g_1, \dots, g_s\}$ de I es una base de Gröbner de I si y sólo si para todos los pares $p \neq q$, el resto de dividir $S(g_p, g_q)$ por G (listados en cualquier orden) es cero.

Demostración. \implies] Si G es una base de Gröbner, como $S(g_p, g_q) \in I$, por el Corolario 2.9 el resto de la división por G es cero.

[\Leftarrow Sea f un polinomio distinto de cero. Debemos demostrar que si todos los S -polinomios tiene resto cero en la división por G , entonces $LT(f) \in \langle LT(g_1), \dots, LT(g_t) \rangle$. Sea $f \in I = (g_1, \dots, g_t)$, existen polinomios $h_i \in k[x_1, \dots, x_n]$ tales que

$$f = \sum_{i=1}^t h_i g_i \tag{2.2}$$

Por el Lema 1.26 se sigue que

$$\text{multideg}(f) \leq \text{máx}(\text{multideg}(h_i g_i)) \tag{2.3}$$

Sea $m(i) = \text{multideg}(h_i g_i)$ y definimos $\delta = \text{máx}(m(1), \dots, m(t))$. Entonces la desigualdad (2.3) se convierte en

$$\text{multideg}(f) \leq \delta.$$

Ahora, consideremos todas las formas posibles en que f puede escribirse en la forma (2.2) y note que para cada expresión obtenemos un δ posiblemente diferente. Dado que un orden monomial es un buen orden, podemos seleccionar una expresión como en la ecuación (2.2) para f tal que δ sea de grado mínimo.

Si $\text{multideg}(f) = \delta$, la igualdad ocurre en (2.3), entonces $\text{multideg}(f) = \text{multideg}(h_i g_i)$ para algún i y se sigue que $LT(f)$ es divisible por $LT(g_i)$, así $LT(f) \in \langle LT(g_1), \dots, LT(g_t) \rangle$, que es lo que queremos demostrar.

Mostremos que $\text{multideg}(f) = \delta$. Probaremos esto por contradicción, supongamos que

$\text{multideg}(f) < \delta$ y escribamos a f como

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \end{aligned} \quad (2.4)$$

Las dos ultimas sumas del segundo renglón tienen $\text{multideg} < \delta$ y por hipótesis $\text{multideg}(f) < \delta$, entonces la primera suma también tiene $\text{multideg} < \delta$.

Sea $LT(h_i) = c_i x^{\alpha(i)}$, entonces $\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ tiene exactamente la forma descrita en el Lema 2.13 con $f_i = x^{\alpha(i)} g_i$. Entonces, el Lema 2.13 implica que la suma es una combinación lineal de los S -polinomios $S(x^{\alpha(p)} g_p, x^{\alpha(q)} g_q)$. Sin embargo,

$$\begin{aligned} S(x^{\alpha(p)} g_p, x^{\alpha(q)} g_q) &= \frac{x^\delta}{x^{\alpha(p)} LT(g_p)} x^{\alpha(p)} g_p - \frac{x^\delta}{x^{\alpha(q)} LT(g_q)} x^{\alpha(q)} g_q \\ &= x^{\delta-\gamma_{pq}} S(g_p, g_q), \end{aligned}$$

donde $x^{\gamma_{pq}} = LMC(LM(g_p), LM(g_q))$.

Entonces existen constantes $c_{pq} \in k$ tal que

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{pq} c_{pq} x^{\delta-\gamma_{pq}} S(g_p, g_q). \quad (2.5)$$

El siguiente paso es usar nuestra hipótesis de que el resto de $S(g_p, g_q)$ en la división por g_1, \dots, g_t es cero. Usando el algoritmo de la división, esto significa que cada S -polinomio se puede escribir en la forma

$$S(g_p, g_q) = \sum_{i=1}^t a_{ipq} g_i \quad (2.6)$$

donde $a_{ipq} \in k[x_1, \dots, x_n]$. El algoritmo de la división nos dice

$$\text{multideg}(a_{ipq} g_i) \leq \text{multideg}(S(g_p, g_q)) \text{ para todo } i, p, q \quad (2.7)$$

Multiplicando la expresión $S(g_p, g_q)$ por $x^{\delta-\gamma_{pq}}$ obtenemos

$$x^{\delta-\gamma_{pq}} S(g_p, g_q) = \sum_{i=1}^t b_{ipq} g_i, \text{ donde } b_{ipq} = x^{\delta-\gamma_{pq}} a_{ipq} \quad (2.8)$$

La desigualdad (2.7) y Lema 2.13 implican que

$$\text{multideg}(b_{ipq} g_i) \leq \text{multideg}(x^{\delta-\gamma_{pq}} S(g_p, g_q)) < \delta. \quad (2.9)$$

Si sustituimos la expresión (2.8) por $x^{\delta-\gamma_{pq}}S(g_p, g_q)$ en la ecuación (2.5) obtenemos la ecuación

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{p,q} c_{p,q}x^{\delta-\gamma_{pq}}S(g_p, g_q) = \sum_{p,q} c_{p,q} \left(\sum_i b_{ipq}g_i \right) = \sum_i \hat{h}_i g_i$$

Por la desigualdad (2.9) se tiene la propiedad de que para toda i ,

$$\text{multideg}(\hat{h}_i g_i) < \delta.$$

Para el paso final de la demostración vamos a sustituir

$$\sum_{m(i)} = LT(h_i)g_i = \sum_i^t \hat{h}_i g_i$$

en la ecuación (2.4) y obtenemos la expresión para f :

$$f = \sum_i^t \hat{h}_i g_i + \sum_{m(i)=\delta} (h_i - LT(h_i))g_i + \sum_{m(i)<\delta} h_i g_i \quad (2.10)$$

donde todos los términos tienen $\text{multideg} < \delta$. Esto contradice la minimalidad de δ y completa la demostración del teorema. \square

2.15 Ejemplo. Considere el ideal $I = \langle y - x^2, z - x^3 \rangle$. Afirmamos que $G = \{y - x^2, z - x^3\}$ es una base de Gröbner con el orden lexicográfico $y > z > x$.

Demostración. Para demostrar esto, consideremos el S -polinomio

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

Usando el algoritmo de la división tenemos que

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

De modo que $\overline{S(y - x^2, z - x^3)}^G = 0$. Por lo tanto, por el Criterio de Buchberger, G es una base de Gröbner para I . \square

2.2. Algoritmo de Buchberger

Usando la definición de S -polinomio y el criterio de Buchberger se puede probar si dada una base es una base de Gröbner, siguiendo esta idea, en 1965 Bruno Buchberger crea el algoritmo conocido como algoritmo de Buchberger para calcular bases de Gröbner.

2.16 Ejemplo. Considere el anillo $k[x, y]$ con el orden graduado lexicográfico y sea $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. En el Ejemplo (2.2) estudiamos que $\{f_1, f_2\}$ no es una base de Gröbner para I , ya que

$$S(f_1, f_2) = \frac{x^3y}{x^3}(x^3 - 2xy) - \frac{x^3y}{x^2y}(x^2y - 2y^2 + x) = y(x^3 - 2xy) - x(x^2y - 2y^2 + x)$$

entonces $LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.

El resto en la división por $F(f_1, f_2)$ es igual a $-x^2$, que es distinto de cero. Por lo tanto, deberíamos incluir ese resto como un nuevo generador $f_3 = -x^2$. Si establecemos $F = (f_1, f_2, f_3)$, podemos usar el Criterio de Buchberger 2.14 para probar si este nuevo conjunto es una base de Gröbner para I .

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

Por lo tanto, debemos agregar $f_4 = -2xy$ a nuestro conjunto de generadores. Si $F = (f_1, f_2, f_3, f_4)$, tenemos

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

Por lo tanto, añadimos $f_5 = -2y^2 + x$ al conjunto de generadores, haciendo $F(f_1, f_2, f_3, f_4, f_5)$ y haciendo los calculos correspondientes obtenemos que $\overline{S(f_i, f_j)}^F = 0$ para todo $1 \leq i < j \leq 5$. Por el Criterio de Buchberger se deduce que una base de Gröbner para I viene dada por

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

El ejemplo anterior muestra que se podría extender una base Gröbner F sumando sucesivamente restos distintos de cero de los S -polinomios. Esta idea es una consecuencia del Criterio de Buchberger y conduce al siguiente algoritmo para calcular una base de Gröbner.

2.17 Teorema. (Algoritmo de Buchberger)

Sea $I = \langle f_1, \dots, f_s \rangle \neq \{0\}$ un ideal de polinomios. Entonces se puede construir una base de Gröbner para I en un número finito de pasos mediante el siguiente algoritmo:

Input: $F = (f_1, \dots, f_s)$

Output: $G = (g_1, \dots, g_t), F \subset G$

```

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

```

Demostración. Primero mostraremos que $G \subset I$ se cumple en cada etapa de el algoritmo. Inicialmente G es un conjunto de generadores de I , con ello $G \subset I$. Además, añadimos a G el resto $S = \overline{S(p, q)}^{G'}$ para $p, q \in G$. Así, si $G \subset I$, entonces p, q y $S(p, q) \in I$ y como estamos dividiendo por $G' \subset I$, obtenemos $G \cup \{S\} \subset I$. También notamos que G contiene la base dada F de I , de modo que G es en realidad una base de I .

El algoritmo termina cuando $G = G'$, lo que significa que $S = \overline{S(p, q)}^{G'} = 0$ para todo $p, q \in G$. Por lo tanto, G es una base de Gröbner de $\langle G \rangle = I$ por el Criterio de Buchberger. Ahora, mostraremos que el algoritmo termina tras un número finito de pasos. Consideremos lo que sucede en cada iteración. El conjunto G está formado por G' (la anterior G) junto con los restos distintos de cero de S-polinomios de los elementos de G' . Entonces

$$\langle LT(G') \rangle \subset \langle LT(G) \rangle \quad (2.11)$$

ya que $G' \subset G$. Si $G' \neq G$, afirmamos que $\langle LT(G') \rangle$ es estrictamente menor que $\langle LT(G) \rangle$. Para probar esto, suponga que un resto r distinto de cero de un S-polinomio ha sido añadido a G . Dado que r es un resto de la división por G' , $LT(r)$ no es divisible por los términos principales de los elementos de G' , entonces $LT(r) \notin \langle LT(G') \rangle$. Sin embargo $LT(r) \in \langle LT(G) \rangle$, lo que prueba nuestra afirmación.

Por (2.11), los ideales $\langle LT(G') \rangle$ de las sucesivas iteraciones forman una cadena ascendente de ideales $k[x_1, \dots, x_n]$, la Condición de la Cadena Ascendente (Teorema 2.7) implica que después de un número finito de iteraciones la cadena se estabilizará, de modo que $\langle LT(G') \rangle = \langle LT(G) \rangle$ ocurre eventualmente. Esto implica que $G = G'$, por lo que el algoritmo debe terminar después de un número finito de pasos. \square

2.18 Lema. Sea G una base de Gröbner para el ideal de polinomios I . Sea $p \in G$ un polinomio tal que $LT(p) \in \langle LT(G - \{p\}) \rangle$. Entonces $G - \{p\}$ es también una base de Gröbner para I .

Demostración. Como $G = \{g_1, \dots, g_t, p\}$ una base de Gröbner para I se cumple que

$\langle LT(g_1), \dots, LT(g_t), LT(p) \rangle = \langle LT(I) \rangle$ y por hipótesis

$$LT(p) \in \langle LT(G - \{p\}) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$$

Así, $G - \{p\}$ es una base de Gröbner para I . □

2.19 Definición. Una base de Gröbner minimal para el ideal I es una base de Gröbner de I tal que

- (i) $LC(p) = 1$ para todo $p \in G$.
- (ii) Para todo $p \in G$, $LT(p) \notin \langle LT(G - \{p\}) \rangle$.

2.20 Ejemplo. Para construir una base de Gröbner minimal para un ideal distinto de cero, volvamos una vez más a la idea que estudiamos en el Ejemplo 2.16.

Usando el orden grlex, encontramos la base de Gröbner $F = \{f_1, f_2, f_3, f_4, f_5\}$ tal que

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

Dado que algunos de los coeficientes principales son diferentes de 1, el primer paso es multiplicar los generadores mediante constantes adecuadas para que 1 sea el coeficiente principal y tenemos

$$\begin{aligned} \tilde{f}_1 &= x^3 - 2xy \\ \tilde{f}_2 &= x^2y - 2y^2 + x \\ \tilde{f}_3 &= x^2 \\ \tilde{f}_4 &= xy \\ \tilde{f}_5 &= y^2 - (1/2)x \end{aligned}$$

Además, note que $LT(f_1) = x^3 = -x \cdot LT(f_3)$ y $LT(f_2) = x^2y = -(1/2)x \cdot LT(f_4)$ y por el Lema 2.18 podemos eliminar f_1 y f_2 de la base de Gröbner minimal. No hay más casos en los que el término principal de un generador divida el término principal de otro generador. Por eso, $\{\tilde{f}_3, \tilde{f}_4, \tilde{f}_5\}$ es una base de Gröbner minimal.

Un ideal puede tener muchas bases de Gröbner minimales, afortunadamente, podemos destacar una base de Gröbner minimal que sea mejor que las demás, lo que nos lleva a la siguiente definición.

2.21 Definición. Una base de Gröbner reducida para un ideal de polinomios I es una base de Gröbner G de I tal que:

- (i) $LC(p) = 1$ para todo $p \in G$.
- (ii) Para todo $p \in G$, ningún monomio de p pertenece a $\langle LT(G - \{p\}) \rangle$.

2.22 Proposición. Sea $I \neq \{0\}$ un ideal polinomial. Dado un orden monomial, I tiene una única base de Gröbner reducida.

Demostración. Sea G una base de Gröbner minimal de I . Decimos que $g \in G$ es reducido para G siempre que ningún monomio de g este en $\langle LT(G - \{g\}) \rangle$. Nuestro objetivo es modificar G hasta que todos sus elementos se reduzcan.

Una primera observación es que si g se reduce para G , entonces g también se reduce para cualquier otra base Gröbner minimal de I que contiene g y tiene el mismo conjunto de términos principales. Esto se deduce porque la definición de que reducido solo involucra los términos principales.

Dado $g \in G$, sean $g' = \overline{g}^{(G-\{g\})}$ y $G' = (G - \{g\}) \cup \{g'\}$. Afirmamos que G' es una base de Gröbner minimal para I . Para probar esto, primero note que $LT(g') = LT(g)$, ya que al dividir g por $G - \{g\}$, $LT(g)$ se añade al resto de la división dado que no es divisible por ningún elemento de $LT(G - \{g\})$. Esto muestra que $\langle LT(G') \rangle = \langle LT(G) \rangle$.

Como G' está claramente contenida en I , vemos que G' es una base de Gröbner y es minimal. Finalmente, g' se reduce para G' por construcción.

Ahora, tomemos los elementos de G y apliquemos el proceso anterior hasta que se reduzcan. La base de Gröbner puede cambiar cada vez que hacemos el proceso, pero nuestra observación anterior muestra que una vez que se reduce un elemento, permanece reducido ya que nunca cambiamos los términos principales de la base. Por lo tanto, terminamos con una base de Gröbner reducida.

Para probar la unicidad, supongamos que G y \tilde{G} son bases de Gröbner reducidas para I . Entonces, en particular, G y \tilde{G} son bases de Gröbner minimales, eso implica que tienen los mismos términos principales, es decir, $LT(G) = LT(\tilde{G})$. Entonces, dado $g \in G$, existe $\tilde{g} \in \tilde{G}$ tal que $LT(g) = LT(\tilde{g})$. Si probamos que $g = \tilde{g}$, entonces $G = \tilde{G}$.

Para probar que $g = \tilde{g}$, consideremos $g - \tilde{g} \in I$. Como G es una base de Gröbner tenemos que $\overline{g - \tilde{g}}^G = 0$. Además, $LT(g) = LT(\tilde{g})$, entonces los términos principales se cancelan en $g - \tilde{g}$ y los términos restantes no son divisibles por ninguno de los elementos de $LT(G) = LT(\tilde{G})$ ya que G y \tilde{G} son bases reducidas. Esto prueba que $\overline{g - \tilde{g}}^G = g - \tilde{g} = 0$ y así $g = \tilde{g}$. □

2.23 Ejemplo. Sea el ideal $I = \langle x^2 - 3y + z - 12, x - y + z - 9, x + y - z - 17 \rangle \subset k[x_1, \dots, x_n]$. Calculemos una base de Gröbner y una base de Gröbner reducida para el ideal I usando el programa Singular, en la Figura 2.1 se muestra el código.

```
call Singular
          SINGULAR
A Computer Algebra System for Polynomial Computations
          / Development
          / version 4.3.1
          0<
          \ Jun 2022
          \
by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann
FB Mathematik der Universitaet, D-67653 Kaiserslautern
// ** running in restricted mode: shell invocation and links are disallowed
> ring R=0, (x,y,z),lp;
> poly f = x^2-3y+z-12;
> poly g = x-y+z-9;
> poly h = x+y-z-17;
> ideal I = f,g,h;
> std(I);
_[1]=2z-145
_[2]=y-z-4
_[3]=x+y-z-17
> option(redSB);
> std(I);
_[1]=2z-145
_[2]=2y-153
_[3]=x-13
>
```

Figura 2.1: Código para generar una base de Gröbner Reducida

Capítulo 3

Variedades

En este capítulo se presenta la teoría básica de variedades y los teoremas de los ceros de Hilbert para el estudio de las aplicaciones de la base de Gröbner.

3.1 Definición. Sea un campo k y sean f_1, \dots, f_s polinomios en $k[x_1, \dots, x_n]$, entonces el conjunto

$$V(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0 \text{ para todo } 1 \leq i \leq s\}$$

A $V(f_1, \dots, f_s)$ lo llamaremos **variedad** o **variedad afin** definida por (f_1, \dots, f_s) .

Así, una variedad afin $V(f_1, \dots, f_s) \subset k^n$ es el conjunto de todas las soluciones del sistema de ecuaciones

$$f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0.$$

3.2 Proposición. $V(I)$ es una variedad. En particular, si $I = \langle f_1, \dots, f_s \rangle$, entonces

$$V(I) = V(f_1, \dots, f_s).$$

Demostración. Por el teorema de la base de Hilbert 2.4, $I = \langle f_1, \dots, f_s \rangle$ para algún conjunto generador finito. Afirmamos que $V(I) = V(f_1, \dots, f_s)$.

Primero, como $f_i \in I$, si $f(a_1, \dots, a_n) = 0$ para todo $f \in I$, entonces $f_i(a_1, \dots, a_n) = 0$, con ello $V(I) \subseteq V(f_1, \dots, f_s)$. Por otro lado, sean $(a_1, \dots, a_n) \in V(f_1, \dots, f_s)$ y $f \in I$. Si $I = \langle f_1, \dots, f_s \rangle$, podemos escribir a f como

$$f = \sum_{i=1}^s h_i f_i$$

para algún $h_i \in k[x_1, \dots, x_n]$. Entonces

$$f(a_1, \dots, a_n) = \sum_{i=1}^s h_i(a_1, \dots, a_n) f_i(a_1, \dots, a_n) = \sum_{i=1}^s h_i(a_1, \dots, a_n) \cdot 0 = 0.$$

Así, $V(f_1, \dots, f_s) \subseteq V(I)$ y, por tanto, son iguales. \square

3.3 Definición. Dado un subconjunto $V \subseteq k^n$ definimos el ideal $I(V)$ en $k[x_1, \dots, x_n]$ como

$$I(V) = \{f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ para todo } (a_1, \dots, a_n) \in V\}$$

3.4 Lema. Si $V \subset k^n$ es una variedad afin, entonces $I(V) \subset k[x_1, \dots, x_n]$ es un ideal.

Demostración. Demostremos que $I(V)$ es un ideal

- (i) $0 \in I(V)$, ya que el polinomio cero se anula en todo K^n .
- (ii) Supongamos que $f, g \in I(V)$ y sea (a_1, \dots, a_n) un punto arbitrario de V , entonces $f(a_1, \dots, a_n) + g(a_1, \dots, a_n) = 0 + 0 = 0$. Así $f + g \in I(V)$.
- (iii) Por último, supongamos que $f, g \in I(V)$ y $h \in k[x_1, \dots, x_n]$, entonces $h(a_1, \dots, a_n)f(a_1, \dots, a_n) = h(a_1, \dots, a_n)0 = 0$. De modo que $hf \in I(V)$.

Por lo tanto, $I(V)$ es un ideal. \square

3.5 Teorema. Sean V una variedad e I un ideal se cumple $V(I(V)) = V$.

Demostración. Sea $V = V(f_1, \dots, f_s)$ una variedad en k^n . Como $f \in I(V)$ es cero en V , la contención $V \subseteq V(I(V))$ se sigue directamente de la definición de V . Para la otra contención, note que $f_1, \dots, f_s \in I(V)$ por la definición de I , entonces $\langle f_1, \dots, f_s \rangle \subseteq I(V)$. Como V es inversora de inclusiones, tenemos que $V(I(V)) \subseteq V(\langle f_1, \dots, f_s \rangle) = V$. Así, $V(I(V)) = V$. \square

3.6 Lema. Sea V una variedad, Si $f^m \in I(V)$, entonces $f \in I(V)$.

Demostración. Sea $x \in V$. Si $f^m \in I(V)$, entonces $(f(x))^m = 0$. Pero esto puede ocurrir si $f(x) = 0$. Dado que $x \in V$ es arbitrario, tenemos que $f \in I(V)$. \square

3.7 Definición. Sea K un campo de extensión de k , es decir, K es un campo tal que $k \subseteq K$. Dado un subconjunto $S \subseteq k[x_1, \dots, x_n]$, definimos la variedad, $V_K(S)$, en K^n como

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

Por la Proposición 3.2, si $I = \langle f_1, \dots, f_s \rangle \subseteq k[x_1, \dots, x_n]$, entonces

$$V_K(I) = \{(a_1, \dots, a_n) \in K^n \mid f_i(a_1, \dots, a_n) = 0, 1 \leq i \leq s\} = V_K(f_1, \dots, f_s).$$

3.8 Ejemplo. Para $K = \mathbb{R}$ tenemos $V_{\mathbb{R}}(x^2 + y^2) = V_{\mathbb{R}}(x, y) = \{(0, 0)\} \subseteq \mathbb{R}^2$. Por otro lado, para $K = \mathbb{C}$ tenemos que $V_{\mathbb{C}}(x^2 + y^2)$ es la unión de dos rectas $y = \pm ix$, donde $i = \sqrt{-1}$, así que $V_{\mathbb{C}}(x, y)$ es $\{(0, 0)\}$.

3.9 Ejemplo. Consideremos el polinomio $f = x^2 + y^2 + 1$. Entonces para $K = \mathbb{R}$ vemos que $V_{\mathbb{R}}(f) = \emptyset$, mientras que $V_{\mathbb{C}}$ tiene un número infinito de puntos. La situación es similar para $f = x^4 + y^4 + 1$. De hecho, hay infinitos ideales de $\mathbb{R}[x, y]$ cuya variedad correspondiente en \mathbb{R}^2 es vacía.

Los Ejemplos 3.8 y 3.9 muestran que un sistema de ecuaciones puede tener “muy pocas soluciones” en k^n para darnos una idea de las propiedades algebraicas y geométricas de I y $V_K(I)$. En el Ejemplo 3.8, los ideales $\langle x^2 + y^2 \rangle$ y $\langle x + y \rangle$ dan lugar a la misma variedad sobre \mathbb{R} , pero son “esencialmente diferentes”. La misma situación se da en el Ejemplo 3.9. Ampliando el campo \mathbb{R} a \mathbb{C} , ideales “esencialmente diferentes” dará lugar a diferentes variedades.

Para enunciar el Teoremas de Hilbert Nullstellensatz, consideramos la cerradura algebraica del campo k , denotada \bar{k} . Recuerde que un campo K es algebraicamente cerrado si para cada polinomio $f \in K[x]$ en una variable, la ecuación $f = 0$ tiene solución en k . Cada campo k está contenido en un campo \bar{k} que es algebraicamente cerrado y tal que cada elemento en \bar{k} es la raíz de un polinomio distinto de cero en una variable con coeficientes en k .

3.10 Teorema. *Teorema Débil de los Ceros de Hilbert*

Sea I un ideal contenido en $k[x_1, \dots, x_n]$. Entonces $V_{\bar{k}}(I) = \emptyset$ si y sólo si $I = k[x_1, \dots, x_n]$.

3.11 Teorema. *Teorema de los Ceros de Hilbert*

Sea k un campo algebraicamente cerrado. Si $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$ tal que $f \in I(V(f_1, \dots, f_s))$, entonces existe un entero positivo $m \geq 1$ tal que

$$f^m \in \langle f_1, \dots, f_s \rangle$$

Demostración. Dado un polinomio f distinto de cero que desaparece en cada cero común de los polinomios f_1, \dots, f_s , debemos demostrar que existe un entero $m \geq 1$ y polinomios A_1, \dots, A_s tal que

$$f^m = \sum_{i=1}^s A_i f_i.$$

Considere el ideal $I' = \langle f_1, \dots, f_s, 1 - yf \rangle \subset k[x_1, \dots, x_n, y]$, donde f, f_1, \dots, f_s son polinomios descritos en el párrafo anterior. Afirmamos que $V(I') = \emptyset$.

Para probar esto, sea $(a_1, \dots, a_n, a_{n+1}) \in k^{n+1}$. Tenemos dos casos

- (a) (a_1, \dots, a_n) es un cero común de f_1, \dots, f_s .
 (b) (a_1, \dots, a_n) no es un cero común de f_1, \dots, f_s .

En el primer caso $f(a_1, \dots, a_n) = 0$ ya que f desaparece en cualquier cero común de f_1, \dots, f_s . Así, el polinomio $1 - yf$ toma el valor $1 - a_{n+1}f(a_1, \dots, a_n) = 1 \neq 0$ en el punto $(a_1, \dots, a_n, a_{n+1})$. En particular, $(a_1, \dots, a_n, a_{n+1}) \notin V(I')$. En el segundo caso, para algún $i, 1 \leq i \leq s$, debemos tener $f_i(a_1, \dots, a_n) \neq 0$. Pensando en f_i como una función de $n + 1$ variables que no depende de la última variable, tenemos $f_i(a_1, \dots, a_n, a_{n+1}) \neq 0$. En particular, de nuevo concluimos que $(a_1, \dots, a_n, a_{n+1}) \notin V(I')$. Dado que $(a_1, \dots, a_n, a_{n+1}) \in k^{n+1}$ era arbitrario, concluimos que $V(I') = \emptyset$.

Ahora, por El Teorema Débil de los Ceros de Hilbert 3.10 concluimos que $1 \in I'$. Eso es,

$$1 = \sum_{i=1}^s p_i(x_1, \dots, x_n, y)f_i + q(x_1, \dots, x_n, y)(1 - yf) \quad (3.1)$$

para algunos polinomios $p_i, q \in k[x_1, \dots, x_n, y]$. Ahora, si definimos $y = 1/f(x_1, \dots, x_n)$. Entonces, la ecuación (3.1) implica que

$$1 = \sum_{i=1}^s p_i(x_1, \dots, x_n, 1/f)f_i. \quad (3.2)$$

Multipliquemos ambos lados de esta ecuación por una potencia f^m , donde m se elige suficientemente grande para borrar todos los denominadores. Esto produce

$$f^m = \sum_{i=1}^s A_i f_i.$$

para algunos polinomios $A_i \in k[x_1, \dots, x_n]$, que es lo que teníamos que mostrar. \square

3.12 Definición. Para un ideal I de $k[x_1, \dots, x_n]$ definimos el radical de I , denotado por \sqrt{I} , como

$$\sqrt{I} = \{f \in k[x_1, \dots, x_n] \mid \text{existe } e \in \mathbb{N} \text{ tal que } f^e \in I\}$$

3.13 Lema. Si I es un ideal en $k[x_1, \dots, x_n]$, entonces \sqrt{I} también es un ideal en $k[x_1, \dots, x_n]$.

Demostración. Note que siempre se tiene que $I \subset \sqrt{I}$ ya que $f \in I$ implica $f^1 \in I$, por lo tanto, $f \in \sqrt{I}$ por definición.

Para mostrar que \sqrt{I} es un ideal, suponga $f, g \in \sqrt{I}$. Entonces hay enteros positivos m y l tal que $f^m, g^l \in I$. En el desarrollo del binomio $(f + g)^{m+l-1}$ todo término tiene un factor $f^i g^j$ con $i + j = m + l - 1$. Como $m \leq i$ o $l \leq j$, ya sea f^i o g^j está en I , donde $f^i g^j \in I$ y cada término de la expansión binomial está en I , por tanto, $(f + g)^{m+l-1} \in I$. Por lo tanto,

$$f + g \in \sqrt{I}.$$

Finalmente, supongamos que $f \in \sqrt{I}$ y $h \in k[x_1, \dots, x_n]$. Entonces $f^m \in I$ para algún entero $1 \leq m$. Dado que I es un ideal, tenemos $(h \cdot f)^m = h^m f^m \in I$. Por lo tanto, $hf \in \sqrt{I}$. Esto muestra que \sqrt{I} es un ideal. \square

3.14 Teorema. *El Teorema Fuerte de los Ceros de Hilbert*

Sea K un campo algebraicamente cerrado. Si I es un ideal en $k[x_1, \dots, x_n]$, entonces

$$I(V_{\bar{k}}(I)) = \sqrt{I} \text{ para todo } I \text{ en } k[x_1, \dots, x_n]$$

Demostración. Ciertamente tenemos $\sqrt{I} \subset I(V_{\bar{k}}(I))$ ya que $f \in \sqrt{I}$ implica que $f^m \in I$ para algún m . Por lo tanto, f^m es cero en $V_{\bar{k}}(I)$, lo que implica que f es cero en $V_{\bar{k}}(I)$. De este modo, $f \in I(V_{\bar{k}}(I))$.

Para la otra contención, suponga que $f \in I(V_{\bar{k}}(I))$. Entonces, por definición, f es cero en $V_{\bar{k}}(I)$. Por El Teorema de los Ceros de Hilbert 3.14, existe un entero $1 \leq m$ tal que $f^m \in I$. Pero esto significa que $f \in \sqrt{I}$. Como f era arbitraria, tenemos que $I(V_{\bar{k}}(I)) \subset \sqrt{I}$. Esto completa la prueba. \square

3.15 Teorema. $V_{\bar{k}}(I) = \emptyset$ si y sólo si $1 \in G$. Es decir, dados los polinomios f_1, \dots, f_s , entonces no hay soluciones para el sistema $f_1 = 0, f_2 = 0, \dots, f_s = 0 \in \bar{k}^n$ si y sólo si $G = \{1\}$.

Demostración. Por Teorema Débil de los Ceros de Hilbert 3.10, $V_{\bar{k}}(I) = \emptyset$ si y sólo si $1 \in I$. Pero la última condición es equivalente a $G = \{1\}$, ya que G es una base de Gröbner reducida. \square

3.1. Variedades Irreducibles

3.16 Definición. Una variedad $V \subseteq k^n$ es irreducible si V se escribe en de la forma $V = V_1 \cup V_2$, donde V_1 y V_2 son variedades, entonces $V_1 = V$ ó $V_2 = V$.

3.17 Definición. Un ideal $I \subseteq k[x_1, \dots, x_n]$ es primo si $f, g \in k[x_1, \dots, x_n]$ y $fg \in I$, entonces $f \in I$ o $g \in I$.

3.18 Proposición. Si $V \subseteq k^n$ una variedad. Entonces V es irreducible si y sólo si $I(V)$ es un ideal primo.

Demostración. Supongamos que V es una variedad irreducible y $f, g \in I(V)$ tal que $fg \in I(V)$. Sean $V_1 = V \cap V(f)$ y $V_2 = V \cap V(g)$ variedades, entonces $fg \in I(V)$ implica que $V = V_1 \cup V_2$. Dado que V es una variedad irreducible, tenemos dos casos $V = V_1$ o $V = V_2$. Si $V = V_1$, entonces $V = V_1 = V \cap V(f)$. De modo que f es cero en $V(f)$, así $f \in I(V)$. Análogamente, si $V = V_2$ implica que $V = V_2 = V \cap V(g)$. Entonces g es cero en $V(g)$, así

$g \in I(V)$. Por lo tanto, $I(V)$ es un ideal primo.

Ahora, supongamos que $I(V)$ es un ideal primo, $V = V_1 \cap V_2$ y $V \neq V_1$. Demostremos que $I(V) = I(V_2)$. Para demostrar esto, notemos que $I(V) \subseteq I(V_2)$ ya que $V_2 \subseteq V$. Asimismo, $I(V) \subsetneq I(V_1)$ dado que $V_1 \subsetneq V$. Así, podemos escoger $f \in I(V_1) \setminus I(V)$ y $g \in I(V_2)$. Como $V = V_1 \cup V_2$, se sigue que fg es cero en V , por lo tanto $fg \in I(V)$. Por hipótesis $I(V)$ es un ideal primo, esto implica que f o g pertenecen a $I(V)$. Sabemos que $f \notin I(V)$ y $g \in I(V)$. Esto demuestra que $I(V) = I(V_2)$, usando el Teorema 3.5 tenemos que $V = V_2$. Por lo tanto V es una variedad irreducible. \square

3.19 Teorema. (Condición de la Cadena Descendente)

$$\text{Sea } V_1 \supseteq V_2 \supseteq V_3 \supseteq \dots$$

una cadena descendentes de variedades en k^n . Entonces existe N un entero positivo tal que

$$V_N = V_{N+1} = V_{N+2} = \dots$$

Demostración. Usando el Teorema de la Cadena Ascendente de Ideales 2.7 tenemos que

$$I(V_1) \subseteq I(V_2) \subseteq I(V_3) \subseteq \dots,$$

entonces existe N tal que $I(V_N) = I(V_{N+1}) = I(V_{N+2}) = \dots$. Dado que $V(I(V)) = V$ para alguna variedad V , tenemos $V_N = V_{N+1} = V_{N+2} = \dots$ \square

Podemos usar esta proposición para demostrar el siguiente resultado básico sobre la estructura de las variedades.

3.20 Teorema. Sea $V \subseteq k^n$ una variedad. Entonces V se puede escribir como una unión finita

$$V = V_1 \cup \dots \cup V_m,$$

donde cada V_i es una variedad irreducible.

Demostración. Supongamos que V es una variedad que no se puede escribir como una unión finita de variedades irreducibles, entonces V no es irreducible, de modo que $V = V_1 \cup V'_1$, donde $V \neq V_1$ y $V \neq V'_1$. Mas aún, una de las variedades V_1 y V'_1 no es una unión de variedades irreducibles, ya que V no es una unión finita de variedades. De igual manera, como V_1 no es una unión de variedades irreducibles tenemos que $V_1 = V_2 \cup V'_2$, donde $V_1 \neq V_2$ y $V_1 \neq V'_2$, y V_2 no es una unión de variedades irreducibles. continuando el proceso tenemos una sucesión infinita de variedades

$$V \supseteq V_1 \supseteq V_2 \supseteq \dots$$

con $V \neq V_1 \neq V_2 \neq \dots$, esto contradice el Teorema de la cadena Descendente 2.7. \square

3.21 Definición. Sea $V \subseteq k^n$ una variedad. Una descomposición

$$V = V_1 \cup \dots \cup V_m,$$

donde V_i con $i = 1, \dots, m$ es una variedad irreducible, la llamaremos descomposición mínima o unión irredundante si $V_i \not\subseteq V_j$ para $i \neq j$. Además, cada variedad V_i se llama componente irreducible de V .

Esta definición nos introduce al siguiente teorema.

3.22 Teorema. Sea $V \subseteq k^n$ una variedad. Entonces V tiene una descomposición mínima

$$V = V_1 \cup \dots \cup V_m,$$

donde V_i con $i = 1, \dots, m$ es una variedad irreducible y $V_i \not\subseteq V_j$ para $i \neq j$. Mas aún, la descomposición mínima es única.

Demostración. Por el Teorema 3.20, V se puede escribir de la forma $V = V_1 \cup \dots \cup V_m$, donde cada V_i es una variedad irreducible. Además, si V_i está contenida en alguna V_j para $i \neq j$ podemos eliminar V_i de la unión. Repitiendo el proceso obtenemos una descomposición mínima de V .

Para demostrar la unicidad, supongamos que $V = V'_1 \cup \dots \cup V'_l$ es otra descomposición mínima de V . Entonces para cada V_i tenemos

$$V_i = V_i \cap V = V_i \cap (V'_1 \cup \dots \cup V'_l) = (V_i \cap V'_1) \cup \dots \cup (V_i \cap V'_l).$$

Como V_i es irreducible, se sigue que $V_i = V_i \cap V'_j$ para algún j , es decir, $V_i \subseteq V'_j$. Usando el mismo argumento para V'_j (usando las componentes V_i para descomponer V) tenemos que $V'_j \subseteq V_k$ para algún k , entonces

$$V_i \subseteq V'_j \subseteq V_k,$$

Por minimalidad, $i = k$, y se sigue que $V_i = V'_j$. Por lo tanto, cada V_i aparece en $V = V'_1 \cup \dots \cup V'_l$, lo que implica $m \leq l$, demostrando la unicidad. \square

Para un estudio más detallado ver [16].

Parte II

Aplicaciones

Capítulo 4

Problema cinemático en los brazos de robots

Nuestro propósito general es mostrar cómo las variedades afines se pueden utilizar para modelar los brazos de un robot y concretamente el papel de las bases de Gröbner en estos modelos.

Siempre consideraremos robots contruidos a partir de eslabones o segmentos rígidos que están conectados en serie, como en una extremidad humana. Un extremo de nuestro brazo del robot generalmente estará fijo en su posición. En el otro extremo estará la mano, que a veces se considerará como un segmento final del robot. En robots reales, esta mano podría estar provista de mecanismos para agarrar objetos o con herramientas para realizar alguna tarea. Por lo tanto, uno de los principales objetivos es poder describir y especificar la posición y orientación de la mano.

Los posibles movimientos de todo el ensamblaje del robot está determinado por los movimientos de las articulaciones. Muchos robots reales son contruidos usando diferentes tipos de articulaciones. En este trabajo se abordarán las siguientes articulaciones:

1. Articulación de revolución plana:

Es aquella que permite la rotación de un segmento con respecto a otro. Por simplicidad, vamos a suponer que ambos segmentos en cuestión se encuentran en un plano y todos los movimientos viven en dicho plano, es decir, el eje de rotación es perpendicular al plano en cuestión. Además, el ángulo θ es el ángulo medido desde el eslabón i hasta el eslabón $i + 1$ en sentido antihorario.

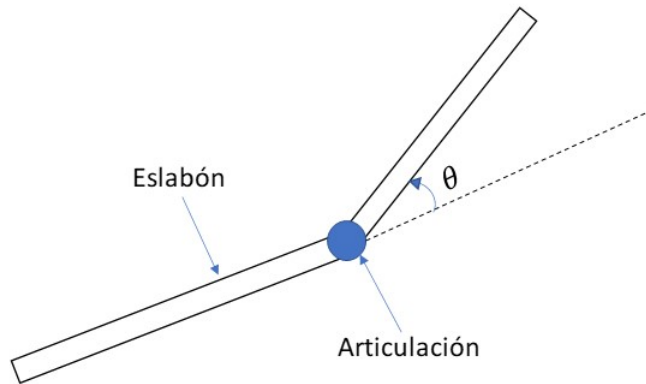


Figura 4.1: Articulación de revolución plana

2. Articulación prismática.:

Esta permite que un segmento de un robot se mueva a lo largo de un eje. En la Figura 4.2 se muestra una vista esquemática de una articulación prismática de un robot que se encuentra en un plano.

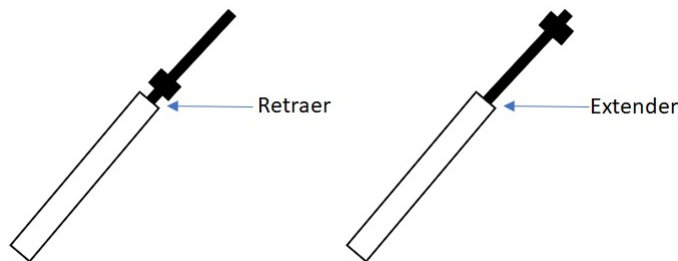


Figura 4.2: Articulaciones prismáticas

Si hay muchas articulaciones en un robot, asumiremos que las articulaciones se encuentran en el mismo plano, que los ejes de rotación de todas las articulaciones de revolución son perpendiculares a ese plano y que los ejes de traslación de las articulaciones prismáticas se encuentran en el plano de las articulaciones. Por lo tanto, todo movimiento tendrá lugar en un plano.

4.1 Ejemplo. Considere el siguiente brazo de robot plano con tres articulaciones de revolución y una articulación prismática. Todos los movimientos del robot tienen lugar en el mismo plano.

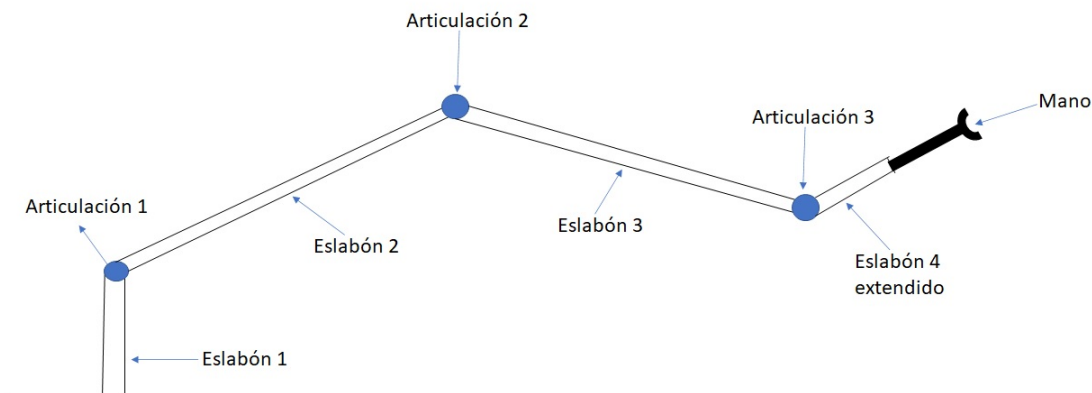


Figura 4.3: Brazo de robot

En general, la posición de una articulación de revolución entre los eslabones i e $i + 1$ se puede describir midiendo el ángulo θ (en sentido antihorario) desde el segmento i hasta segmento $i + 1$. Por lo tanto, la posición de tal articulación puede parametrizarse por un círculo S^1 en el intervalo $[0, 2\pi]$. Cabe señalar que, si existen obstáculos que no permitan girar el brazo en todo S^1 , entonces se parametriza cada posición en subconjuntos de S^1 . De igual manera, la posición de una articulación prismática que tiene longitud mínima m_1 y máxima m_2 , donde $m_1, m_2 \in \mathbb{R}$, puede parametrizarse en el intervalo $[m_1, m_2]$ y lo denotaremos como I_p .

Por otro lado, para un robot con r articulaciones de revolución y p articulaciones prismáticas, las posibles configuraciones de las articulaciones del robot estarán determinadas por el siguiente producto cartesiano:

$$J = \underbrace{S^1 \times \dots \times S^1}_{r \text{ veces}} \times I_1 \times \dots \times I_p$$

donde hay un factor S^1 por cada articulación de revolución e I_p por cada articulación prismática. Llamaremos a J el espacio articular del robot.

Fijando un sistema de coordenadas cartesianas en el plano $U \subseteq \mathbb{R}^2$, podemos representar las posibles posiciones de la mano por los puntos (a, b) . De manera similar, podemos representar la orientación de la mano dando un vector unitario alineado con alguna característica específica de la mano. Así, las posibles orientaciones de la mano están parametrizados por vectores u en $V = S^1$. Por ejemplo, si la mano está unida a una

articulación de revolución, entonces tenemos la siguiente imagen de la configuración de la mano:

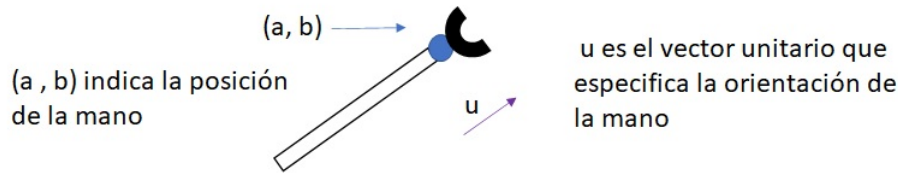


Figura 4.4: Mano de robot

Asimismo, consideraremos $C = U \times V$ como el espacio de configuraciones de la mano del robot.

Dado que los eslabones del robot son rígidos, cada colección de articulaciones colocará la mano en una única posición, con una única orientación. Por lo tanto, es posible definir una función:

$$f : J \rightarrow C$$

entre el espacio de articulaciones y el espacio de configuraciones del robot, esta función codifica las posibles posiciones de la mano.

Notemos que en el Ejemplo 4.1 el espacio articular es $J = S^1 \times S^1 \times S^1 \times [m_1, m_2]$ y $C = U \times S^1$.

Existen dos problemas básicos para describir las distintas posiciones y configuraciones de la mano y que pueden abordarse en términos de f :

1. Problema Cinemático Directo: ¿Es posible dar una descripción explícita para f en términos de las articulaciones (las coordenadas en J) y de los eslabones?
2. Problema Cinemático Inverso: ¿Dado $c \in C$, podemos determinar uno o todos los $j \in J$ tales que $f(j) = c$?

Notemos que en el problema inverso necesitamos resolver todas las soluciones para $f(j) = c$.

En la cinemática de los robots se tratan los aspectos geométricos del movimiento del robot con respecto a un sistema de referencia fijo sin considerar las fuerzas que causan tal movimiento y se estudia la configuración espacial del robot con las relaciones entre las variables del espacio de articulación, posición y orientación del robot.

4.1. Problema cinemático directo

En esta sección, presentaremos un método para abordar el problema cinemático directo. Dado un robot en el plano \mathbb{R}^2 , usaremos el sistema de coordenadas (x_1, y_1) para describir la posición y orientación de la mano. El origen del sistema de coordenadas se colocará en la articulación del brazo del robot, que también está fijo en su posición.

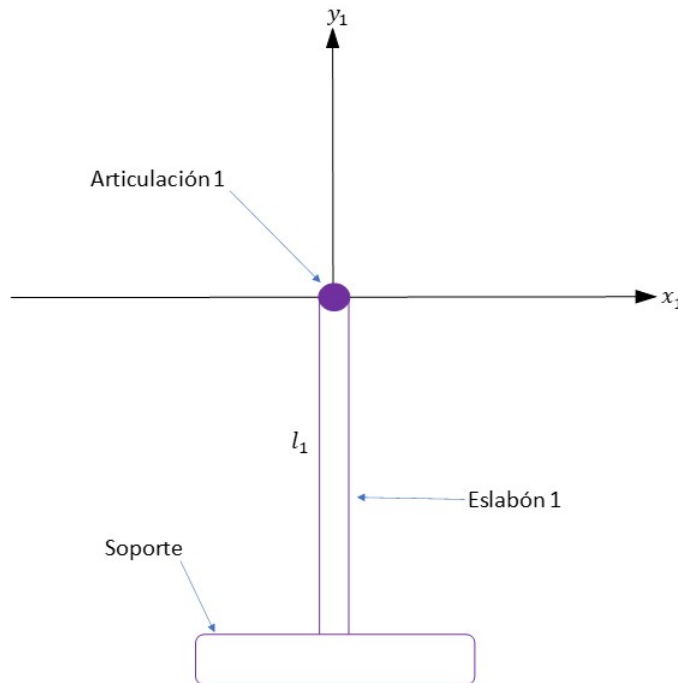


Figura 4.5: Brazo de un robot en \mathbb{R}^2

Además del sistema de coordenadas global (x_1, y_1) , introducimos un sistema de coordenadas en cada una de las articulaciones de revolución para describir las posiciones relativas de los eslabones que se encuentran en esa articulación. Naturalmente, estos sistemas de coordenadas cambian a medida que varía la posición del brazo.

En una articulación de revolución i , introducimos un sistema de coordenadas (x_{i+1}, y_{i+1}) , el origen se sitúa en la articulación i . Nótese que para cada $i \geq 2$, las coordenadas (x_i, y_i) de la articulación i son $(l_i, 0)$, donde l_i es la longitud del eslabón i .

Nuestro primer objetivo es relacionar las coordenadas (x_{i+1}, y_{i+1}) de un punto con las (x_i, y_i) coordenadas de ese punto. Sea θ_i el ángulo en sentido antihorario desde el eje x_i hasta el eje x_{i+1} .

Si un punto que tiene (x_{i+1}, y_{i+1}) coordenadas

$$q = (a_{i+1}, b_{i+1})$$

entonces para obtener las coordenadas (x_i, y_i) de q , digamos

$$q = (a_i, b_i),$$

rotamos por el ángulo θ_i para alinear los ejes x_i y x_{i+1} , y luego trasladamos el vector $(l_i, 0)$ para hacer coincidir los orígenes de los sistemas de coordenadas. La rotación por θ_i se logra multiplicando por la matriz de rotación

$$\begin{pmatrix} \cos \theta_i & -\text{sen } \theta_i \\ \text{sen } \theta_i & \cos \theta_i \end{pmatrix}.$$

También, la traslación se logra sumando el vector $(l_i, 0)$. De tal manera que, dado un punto $q = (a, b)$ en \mathbb{R}^2 , las coordenadas de q en términos de (x_i, y_i) están relacionadas con (x_{i+1}, y_{i+1}) por:

$$\begin{pmatrix} a_i \\ b_i \end{pmatrix} = \begin{pmatrix} \cos \theta_i & -\text{sen } \theta_i \\ \text{sen } \theta_i & \cos \theta_i \end{pmatrix} \begin{pmatrix} a_{i+1} \\ b_{i+1} \end{pmatrix} + \begin{pmatrix} l_i \\ 0 \end{pmatrix},$$

esta transformación de coordenadas también se escribe comúnmente en forma abreviada usando una matriz de 3×3 y vectores de 3 componentes:

$$\begin{pmatrix} a_i \\ b_i \\ 1 \end{pmatrix} = \begin{pmatrix} \cos \theta_i & -\text{sen } \theta_i & l_i \\ \text{sen } \theta_i & \cos \theta_i & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{pmatrix} = A_i \begin{pmatrix} a_{i+1} \\ b_{i+1} \\ 1 \end{pmatrix}.$$

Esto nos permite combinar la rotación por θ_i con la traslación a lo largo del segmento i en una única matriz A_i de 3×3 .

4.2 Ejemplo. Consideremos el siguiente brazo de robot con cuatro articulaciones de revolución.

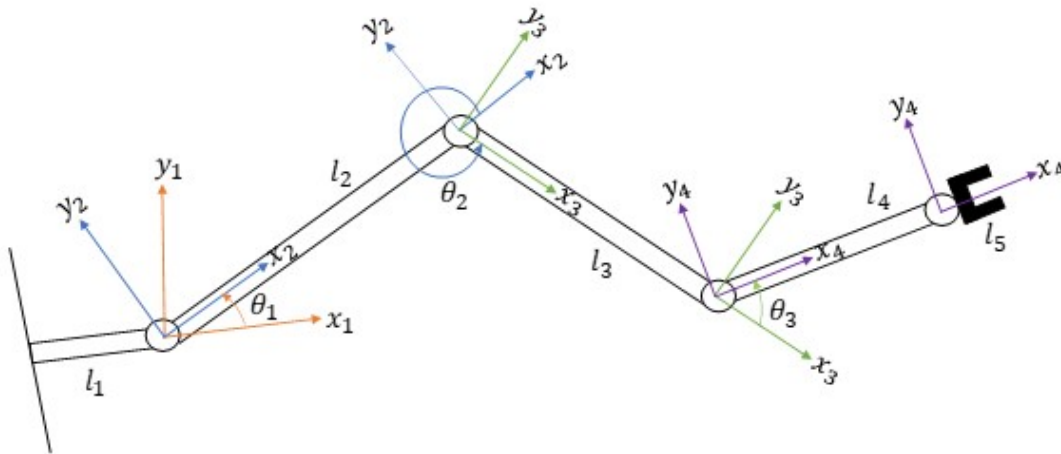


Figura 4.6: Brazo de un robot en con cuatro articulaciones de revolución

Observemos que

- (i) La mano es el eslabón 5 fijado por la articulación 4 con el eslabón 4
- (ii) El origen de sistema de coordenadas 1 y 2 coincide.
- (iii) El vector posición del origen del sistema de coordenadas 3 en el sistema de coordenadas 2 es $\begin{pmatrix} l_2 \\ 0 \end{pmatrix}$ y del sistema de coordenadas 4 en el sistema de coordenadas 3 es $\begin{pmatrix} l_3 \\ 0 \end{pmatrix}$.
En consecuencia, los problemas directos e inversos se formulan en términos de los movimientos relativos a esos sistemas de coordenadas.
- (iv) La rotación de la articulación $i + 1$ relativa a la articulación i se mide por el ángulo θ_i .
- (v) Por ejemplo, si P es un punto en la articulación 4 con posición del vector v_4 en el sistema de coordenadas 4, entonces el vector posición v_3 de P en el sistema de coordenadas 3 está relacionado con v_4 por la siguiente relación:

$$v_3 = \begin{pmatrix} \cos \theta_3 & -\text{sen } \theta_3 \\ \text{sen } \theta_3 & \cos \theta_3 \end{pmatrix} v_4 + \begin{pmatrix} l_3 \\ 0 \end{pmatrix},$$

$$\begin{pmatrix} v_3 \\ 1 \end{pmatrix} = \begin{pmatrix} \cos \theta_3 & -\text{sen } \theta_3 & l_3 \\ \text{sen} \theta_3 & \cos \theta_3 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} v_4 \\ 1 \end{pmatrix}.$$

Esta matriz permite cambiar de sistema de coordenadas 4 a 3.

4.3 Ejemplo. Consideremos el siguiente brazo de robot con 3 articulaciones.

Donde la mano es el eslabón 4 fijado por la articulación 3 con el eslabón 3, l_i es la longitud del eslabón i .

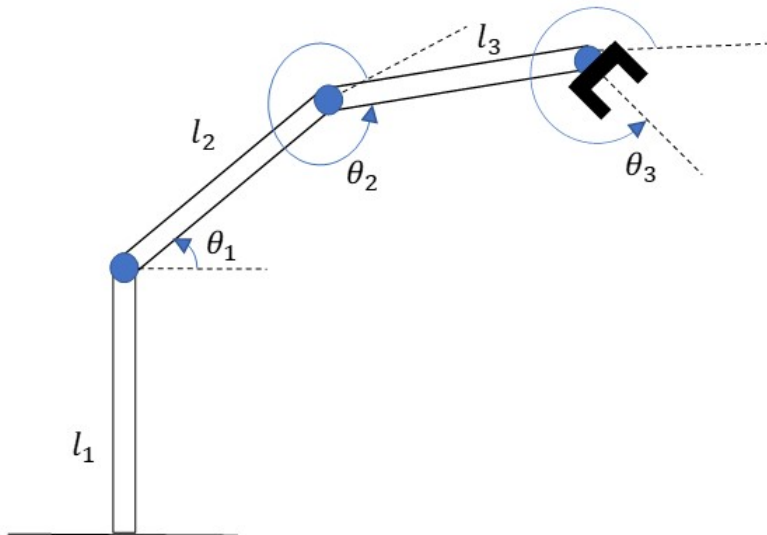


Figura 4.7: Brazo de robot del Ejemplo 4.3

Primero, consideremos la matriz (4.1)

$$A_i = \begin{pmatrix} \cos \theta_i & -\text{sen } \theta_i & l_i \\ \text{sen} \theta_i & \cos \theta_i & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ para } i = 1, 2, 3. \quad (4.1)$$

Además, las coordenadas de cualquier punto en la articulación i se pueden obtener comenzando en el sistema de coordenadas (x_i, y_i) al sistema de origen (x_1, y_1) mediante cada sistema de articulación. De manera que las coordenadas de un punto q en términos del sistema de origen (x_1, y_1) están relacionadas con el sistema de coordenadas (x_4, y_4)

mediante:

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = A_1 A_2 A_3 \begin{pmatrix} x_4 \\ y_4 \\ 1 \end{pmatrix},$$

usando las formulas trigonométricas obtenemos:

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = \begin{pmatrix} \cos(\theta_1 + \theta_2 + \theta_3) & -\sin(\theta_1 + \theta_2 + \theta_3) & l_3 \cos(\theta_1 + \theta_2) + l_2 \cos \theta_1 \\ \sin(\theta_1 + \theta_2 + \theta_3) & \cos(\theta_1 + \theta_2 + \theta_3) & l_3 \sin(\theta_1 + \theta_2) + l_2 \sin \theta_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_4 \\ y_4 \\ 1 \end{pmatrix}.$$

Como: $(x_4, y_4) = (0, 0)$ porque la mano está unida directamente a la articulación 3 se sigue que

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = \begin{pmatrix} l_3 \cos(\theta_1 + \theta_2) + l_2 \cos \theta_1 \\ l_3 \sin(\theta_1 + \theta_2) + l_2 \sin \theta_1 \\ 1 \end{pmatrix}. \quad (4.2)$$

Asimismo, la orientación de la mano está determinada por $\theta_1 + \theta_2 + \theta_3$. Si combinamos este hecho sobre la orientación de la mano con la matriz (4.2) para la posición de la mano, obtenemos una descripción explícita de la función $f : J \rightarrow C$ en términos de los ángulos articulares θ_1 y θ_2 . En consecuencia, la configuración de la mano está determinada por:

$$f(\theta_1, \theta_2, \theta_3) = \begin{pmatrix} l_3 \cos(\theta_1 + \theta_2) + l_2 \cos \theta_1 \\ l_3 \sin(\theta_1 + \theta_2) + l_2 \sin \theta_1 \\ \theta_1 + \theta_2 + \theta_3 \end{pmatrix}. \quad (4.3)$$

4.4 Ejemplo. Consideremos las mismas articulaciones del ejemplo anterior pero añadiremos una articulación prismática entre el segmento 4 y la mano como se muestra en la Figura 4.8. Así, el segmento 4 tendrá longitud variable y el segmento 5 será la mano.

Observaciones

- El eje de traslación de la articulación prismática se encuentra a lo largo de la dirección del eslabón 4.
- La articulación prismática puede cambiar la longitud del eslabón 4 a cualquier valor como:
 - (i) $l_4 = m_1$ para retraer o contraer.
 - (ii) $l_4 = m_2$ para extender.

- Las tres articulaciones de revolución pueden rotar libremente.

En consecuencia, el espacio articular J es $J = S^1 \times S^1 \times S^1 \times [m_1, m_2]$.

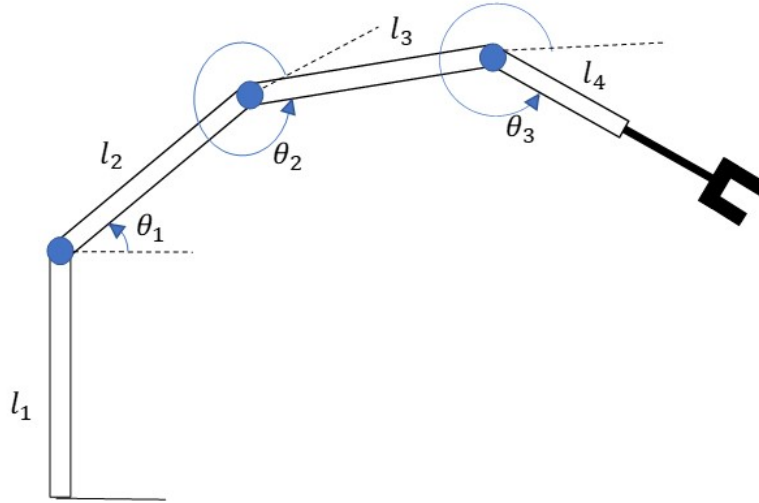


Figura 4.8: Brazo de robot del Ejemplo 4.4

Por el razonamiento dado en el Ejemplo 4.3, la posición de la mano se dará multiplicando la matriz producto $A_1A_2A_3$ por el vector (x_4, y_4) vector de coordenadas de la mano, a saber $(l_4, 0)$. De ello se deduce que la configuración de la mano está determinada por

$$g(\theta_1, \theta_2, \theta_3, l_4) = \begin{pmatrix} l_4 \cos(\theta_1 + \theta_2 + \theta_3) + l_3 \cos(\theta_1 + \theta_2) + l_2 \cos(\theta_1) \\ l_4 \sin(\theta_1 + \theta_2 + \theta_3) + l_3 \sin(\theta_1 + \theta_2) + l_2 \sin(\theta_1) \\ \theta_1 + \theta_2 + \theta_3 \end{pmatrix}, \quad (4.4)$$

donde l_2, l_3 son constantes de longitud fija y $l_4 \in [m_1, m_2]$. Asimismo, la orientación de la mano está determinada por $\theta_1 + \theta_2 + \theta_3$. Mas aún, dada la parametrización

$$\begin{aligned} x &= \cos(\theta), \\ y &= \sin(\theta), \end{aligned}$$

para una variedad algebraica $V(x^2 + y^2 - 1)$ en el plano. De tal manera que las funciones

$$\begin{aligned} c_i &= \cos(\theta_i), \\ s_i &= \sin(\theta_i), \end{aligned}$$

están sujetas a $c_i^2 + s_i^2 - 1 = 0$ para $i = 1, 2, 3$. De hecho la variedad está definida por las

tres ecuaciones anteriores en \mathbb{R}^6 y geoméricamente la variedad es el producto cartesiano de $S^1 \times S^1 \times S^1$.

Explícitamente, obtenemos de (4.3) una expresión para la posición de la mano como una función de las variables $c_1, s_1, c_2, s_2, c_3, s_3$. Dado que

$$\begin{aligned}\cos(\theta_1 + \theta_2) &= \cos(\theta_1)\cos(\theta_2) - \operatorname{sen}(\theta_1)\operatorname{sen}(\theta_2) = c_1c_2 - s_1s_2, \\ \operatorname{sen}(\theta_1 + \theta_2) &= \operatorname{sen}(\theta_1)\cos(\theta_2) + \operatorname{sen}(\theta_2)\cos(\theta_1) = s_1c_2 + s_2c_1,\end{aligned}$$

se obtiene que las coordenadas (x_1, y_1) de las posiciones de la mano están determinadas por

$$\begin{pmatrix} l_3(c_1c_2 - s_1s_2) + l_2c_1 \\ l_3(s_1c_2 + s_2c_1) + l_2s_1 \end{pmatrix}. \quad (4.5)$$

Del mismo modo, a partir de la función g del Ejemplo 4.4 la matriz en (4.4) se puede escribir de la forma:

$$\begin{pmatrix} l_4(c_1(c_2c_3 - s_2s_3) - s_1(c_2s_3 + c_3s_2)) + l_3(c_1c_2 - s_1s_2) + l_2c_1 \\ l_4(s_1(c_2c_3 - s_2s_3) + c_1(c_2s_3 + c_3s_2)) + l_3(s_1c_2 + s_2c_1) + l_2s_1 \end{pmatrix}.$$

En donde el espacio de articulaciones $J = V \times [m_1, m_2] \subset V \times \mathbb{R}$, con

$$V = V(x_1^2 + y_1^2 - 1, x_2^2 + y_2^2 - 1, x_3^2 + y_3^2 - 1).$$

4.2. Problema cinemático inverso

En esta sección continuaremos el estudio de los brazos de robot abordando el problema cinemático inverso en términos de un sistema de ecuaciones polinómicas de n variables con coeficientes reales, cuyo sistema puede resolverse con bases de Gröbner.

Dado un punto q con coordenadas $(a, b) \in \mathbb{R}^2$ y una orientación, nos gustaría determinar si es posible colocar la mano del robot en ese punto q y con esa orientación. Más aún, nos gustaría encontrar todas las combinaciones de las configuraciones que satisfagan esta condición.

En otras palabras, nos interesa determinar la imagen de la función

$$f : J \longrightarrow C$$

para este robot. En otras palabras, para cada c en la imagen de f , queremos determinar la imagen inversa $f^{-1}(c)$.

4.5 Ejemplo. Para ilustrarnos, consideremos el siguiente brazo de robot y obtengamos una descripción de las configuraciones de la mano.

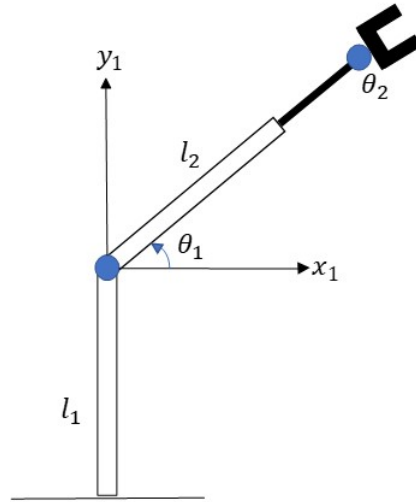


Figura 4.9: Brazo de Robot del ejemplo 4.5

Nuestro robot está compuesto de:

- Dos articulaciones de revolución en donde ambas pueden rotar libremente en el plano y la articulación 1 está centrada en el origen $(x_1, y_1) = (0, 0)$.
- Una articulación prismática que tiene una longitud mínima m_1 y longitud máxima m_2 .

En consecuencia, el espacio articular J es:

$$J = S^1 \times S^1 \times [m_1, m_2].$$

La coordenadas de un punto q en términos del sistema de origen (x_1, y_1) están relacionadas con (x_2, y_2) por:

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = A_1 A_2 \begin{pmatrix} x_2 \\ y_2 \\ 1 \end{pmatrix},$$

En consecuencia,

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = \begin{pmatrix} \cos \theta_1 & -\text{sen } \theta_1 & l_1 \\ \text{sen } \theta_1 & \cos \theta_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \cos \theta_2 & -\text{sen } \theta_2 & l_2 \\ \text{sen } \theta_2 & \cos \theta_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \\ 1 \end{pmatrix}.$$

Con el hecho de que $l_1 = 0$ por que centramos el origen (x_1, y_1) en la primera articulación y $(x_2, y_2) = (0, 0)$ por que la mano está unida directamente a la articulación 2 se sigue que

$$\begin{pmatrix} x_1 \\ y_1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & l_2 \cos \theta_1 \\ 0 & 0 & l_2 \sen \theta_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} l_2 \cos \theta_1 \\ l_2 \sen \theta_1 \\ 1 \end{pmatrix}.$$

Explícitamente, las configuraciones de la mano están descritas por la función $f : J \rightarrow C$, que se puede escribir como:

$$f(\theta_1, \theta_2, l_2) = \begin{pmatrix} l_2 \cos \theta_1 \\ l_2 \sen \theta_1 \\ \theta_1 + \theta_2 \end{pmatrix}. \quad (4.6)$$

Mas aún, pasamos de la matriz (4.6) a una matriz de ecuaciones parametrizadas por bajo la restricción

$$\begin{aligned} c_i &= \cos(\theta_i), \\ s_i &= \sen(\theta_i), \end{aligned}$$

$c_i^2 + s_i^2 - 1 = 0$ para $i = 1, 2$. Obteniendo que la posición de la mano está descrita por:

$$\begin{pmatrix} l_2 c_1 \\ l_2 s_1 \end{pmatrix}. \quad (4.7)$$

En nuestro ejemplo, la orientación de la mano es trivial. La última articulación de revolución no afecta la posición de la mano. Es decir, dado θ_1 una orientación $\alpha = \theta_1 + \theta_2$ está determinada por $\theta_2 = \alpha - \theta_1$ y por lo tanto sólo necesitamos conocer la posición de la mano.

De la matriz (4.6) las posiciones para colocar la mano en el punto (a, b) en las coordenadas (x_1, y_1) están descritas mediante el sistema de ecuaciones:

$$\begin{aligned} a &= l_2 c_1, \\ b &= l_2 s_1, \\ 0 &= c_1^2 + s_1^2 - 1. \end{aligned} \quad (4.8)$$

Para resolver este sistema de ecuaciones calculando una base de Gröbner usando el orden lexicográfico con el orden de las variables

$$c_1 > s_1 > l_2.$$

En este caso l_2 no es un segmento fijo, por lo tanto lo consideramos como una variable al igual que c_1 y s_1 . Generando el siguiente código para obtener nuestra base de Gröbner:

```
> ring R=(0,a,b),(c1,s1,l2),lp;
> poly f1 = l2*c1-a;
> poly f2 = l2*s1-b;
> poly f3 = s1^2+c1^2-1;
> ideal I = f1,f2,f3;
> std(I);
_[1]=l2^2+(-a^2-b^2)
_[2]=(a^2+b^2)*s1+(-b)*l2
_[3]=(a)*c1+s1^2*l2-l2
> option(redSB);
> std(I);
_[1]=l2^2+(-a^2-b^2)
_[2]=(a^2+b^2)*s1+(-b)*l2
_[3]=(a^2+b^2)*c1+(-a)*l2
```

Así, la base de Gröbner reducida en el anillo $\mathbb{R}(a,b)[c_1,s_1,l_2]$ para el ideal I generada por los polinomios de (4.8) está formada por:

$$\begin{aligned} -(a^2 + b^2) + l_2^2 &= 0, \\ -bl_2 + (a^2 + b^2)s_1 &= 0, \\ -al_2 + (a^2 + b^2)c_1 &= 0, \end{aligned} \tag{4.9}$$

con soluciones sobre \mathbb{R}

$$\left\{ c_1 = -\frac{a}{\sqrt{a^2 + b^2}}, s_1 = -\frac{b}{\sqrt{a^2 + b^2}}, l_2 = -\sqrt{a^2 + b^2} \right\}$$

$$\left\{ c_1 = \frac{a}{\sqrt{a^2 + b^2}}, s_1 = \frac{b}{\sqrt{a^2 + b^2}}, l_2 = \sqrt{a^2 + b^2} \right\}$$

Sin embargo, el primer conjunto solución queda descartado porque l_2 no puede ser un número negativo, es un número fijo positivo que toma valores entre un mínimo y máximo en el intervalo $[m_1, m_2]$. Por lo tanto, las soluciones a nuestro sistema son

$$0 < m_1 \leq l_2 = \sqrt{a^2 + b^2} \leq m_2,$$

$$0 < m_1^2 \leq l_2 = a^2 + b^2 \leq m_2^2.$$

En consecuencia, las posibles posiciones de la mano en el espacio de configuraciones describen un anillo con centro en el origen (x_1, y_1) como se muestra en la Figura 4.10

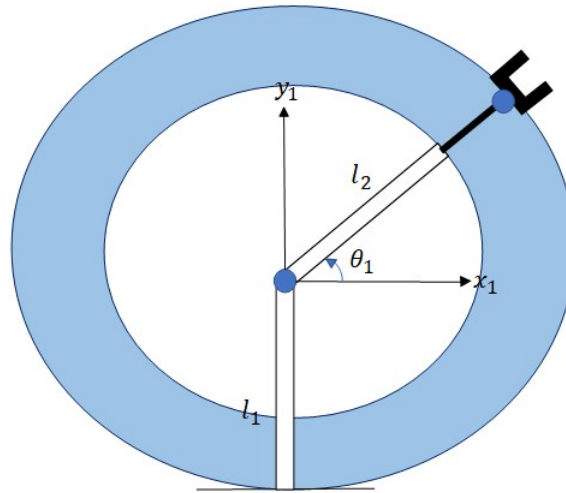


Figura 4.10: Posiciones de la mano de robot

4.6 Ejemplo. Consideremos el siguiente brazo de robot, observe que la mano es el eslabón 4 fijado por la articulación 3 con el eslabón 3.

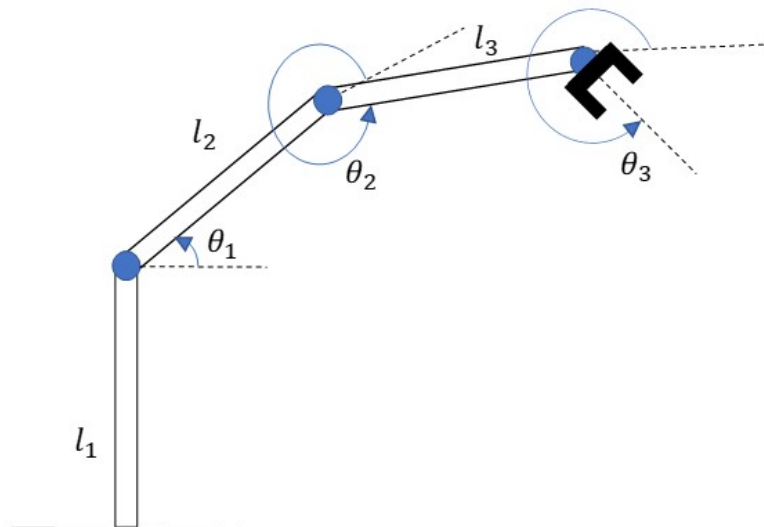


Figura 4.11: Brazo de robot del Ejemplo 4.3

De la matriz (4.5) se deduce que las posiciones posibles para colocar la mano en el punto dado (a, b) en coordenadas (x_1, y_1) están descritas por el siguiente sistema de

ecuaciones:

$$\begin{aligned}
 a &= l_3(c_1c_2 - s_1s_2) + l_2c_1 \\
 b &= l_3(c_1s_2 + c_2s_1) + l_2s_1 \\
 0 &= c_1^2 + s_1^2 - 1 \\
 0 &= c_2^2 + s_2^2 - 1
 \end{aligned} \tag{4.10}$$

Para resolver este sistema, calculamos una base de Gröbner con el orden graduado lexicográfico y con el orden en las variables

$$c_1 > s_1 > c_2 > s_2$$

En donde las soluciones dependen de los valores a, b, l_2, l_3 , los cuales aparecen como parámetros en los coeficientes de la base de Gröbner reducida en el anillo $\mathbb{R}(a, b, l_2, l_3)[s_1, c_1, s_2, c_2]$ para el ideal I generado por los polinomios de (4.10).

A continuación se muestra el código realizado con el programa Singular para calcular la base de Gröbner.

```

> ring R = (0, a, b, l2, l3), (c1, s1, c2, s2), dp;
> poly f1 = l3*(c1*c2 - s1*s2) + l2*c1 - a;
> poly f2 = l3*(c1*s2 + c2*s1) + l2*s1 - b;
> poly f3 = c1^2 + s1^2 - 1;
> poly f4 = c2^2 + s2^2 - 1;
> ideal I = f1, f2, f3, f4;
> std(I);
_[1]=(2*l2*l3)*c2+(-a^2-b^2+l2^2+l3^2)
_[2]=(2*a^2*l2+2*b^2*l2)*s1+(2*a*l2*l3)*s2+(-a^2*b-b^3-b*l2^2+b*l3^2)
_[3]=(b)*c1+(-a)*s1+(-l3)*s2
_[4]=(2*l2*l3^2)*s2^2+(a*l2^2-a*l3^2)*c1+(b*l2^2-b*l3^2)*s1
+(a^2*l3+b^2*l3)*c2+(-a^2*l2-b^2*l2)
> option(redSB);
> std(I);
_[1]=(2*l2*l3)*c2+(-a^2-b^2+l2^2+l3^2)
_[2]=(2*a^2*l2+2*b^2*l2)*s1+(2*a*l2*l3)*s2+(-a^2*b-b^3-b*l2^2+b*l3^2)
_[3]=(2*a^2*l2+2*b^2*l2)*c1+(-2*b*l2*l3)*s2+(-a^3-a*b^2-a*l2^2+a*l3^2)
_[4]=(4*l2^2*l3^2)*s2^2+(a^4+2*a^2*b^2-2*a^2*l2^2-2*a^2*l3^2+b^4
-2*b^2*l2^2-2*b^2*l3^2+l2^4-2*l2^2*l3^2+l3^4)

```

Así, nuestra base de Gröbner reducida está formada por los siguientes polinomios:

$$\begin{aligned} &(2a^2l_2 + 2b^2l_2)c_1 + (-2bl_2l_3)s_2 + (-a^3 - ab^2 - al_2^2 + al_3^2), \\ &(2a^2l_2 + 2b^2l_2)s_1 + (2al_2l_3)s_2 + (-a^2b - b^3 - bl_2^2 + bl_3^2), \\ &(2l_2l_3)c_2 + (-a^2 - b^2 + l_2^2 + l_3^2), \\ &(4l_2^2l_3^2)s_2^2 + (a^4 + 2a^2b^2 - 2a^2l_2^2 - 2a^2l_3^2 + b^4 - 2b^2l_2^2 - 2b^2l_3^2 + l_2^4 - 2l_2^2l_3^2 + l_3^4). \end{aligned}$$

Multiplicamos por $\frac{1}{2l_2(a^2 + b^2)}$, $\frac{1}{2l_2l_3}$, $\frac{1}{4l_2^2l_3^2}$ respectivamente y obtenemos la siguiente base de Gröbner reducida para el ideal I .

$$\begin{aligned} c_1 - \frac{2bl_2l_3}{2l_2(a^2 + b^2)}s_2 - \frac{a(a^2 + b^2 + l_2^2 - l_3^2)}{2l_2(a^2 + b^2)}, \\ s_1 + \frac{2al_2l_3}{2l_2(a^2 + b^2)}s_2 - \frac{b(a^2 + b^2 + l_2^2 - l_3^2)}{2l_2(a^2 + b^2)}, \\ c_2 - \frac{a^2 + b^2 - l_2^2 - l_3^2}{2l_2l_3}, \\ s_2^2 + \frac{(a^2 + b^2)^2 - 2(a^2 + b^2)(l_2^2 + l_3^2) + (l_2^2 - l_3^2)^2}{4l_2^2l_3^2}. \end{aligned} \tag{4.11}$$

donde los denominadores dependen solo de a, b, l_2, l_3 .

En la práctica, a, b, l_2 y l_3 tomarán ciertos valores y al sustituir su valor nos podemos preguntar si los polinomios generan un ideal en $\mathbb{R}[s_1, c_1, s_2, c_2]$. La pregunta es, ¿cuándo generan una base de Gröbner bajo estas situaciones?.

En general, reemplazar las variables a, b, l_2, l_3 por valores específicos en un campo se llama especialización. En consecuencia, uno se puede preguntar, ¿cómo se comporta una base de Gröbner bajo cierta especialización?.

Por ejemplo, si consideramos el polinomio

$$c_2 - \frac{a^2 + b^2 - l_2^2 - l_3^2}{2l_2l_3}$$

hay problemas si el denominador es cero.

En este caso debemos considerar $l_2 \neq 0, l_3 \neq 0$. De hecho para las Ecuaciones (4.11) consideramos $l_2 \neq 0, l_3 \neq 0, (a^2 + b^2) \neq 0$.

Analizando la Ecuaciones (4.10) se puede mostrar que el conjunto solución es finito. Si resolvemos la última ecuación de (4.11) podemos encontrar como máximo dos soluciones, bastaría ver cuáles soluciones son reales y estas serían las soluciones que buscamos para el robot.

Dado que $l_2, l_3 \neq 0$, vamos a sustituir $l_2 = l_3 = 1$ en (4.11), esto es:

$$\begin{aligned}
 c_1 - \frac{2bl_2l_3}{2l_2(a^2 + b^2)}s_2 - \frac{a(a^2 + b^2 + l_2^2 - l_3^2)}{2l_2(a^2 + b^2)} &= c_1 - \frac{b}{(a^2 + b^2)}s_2 - \frac{a}{2}, \\
 s_1 + \frac{2al_2l_3}{2l_2(a^2 + b^2)}s_2 - \frac{b(a^2 + b^2 + l_2^2 - l_3^2)}{2l_2(a^2 + b^2)} &= s_1 + \frac{a}{(a^2 + b^2)}s_2 - \frac{b}{2}, \\
 c_2 - \frac{a^2 + b^2 - l_2^2 - l_3^2}{2l_2l_3} &= c_2 - \frac{a^2 + b^2}{2}, \\
 s_2^2 + \frac{(a^2 + b^2)^2 - 2(a^2 + b^2)(l_2^2 + l_3^2) + (l_2^2 - l_3^2)^2}{4l_2^2l_3^2} &= s_2^2 + \frac{(a^2 + b^2)((a^2 + b^2) - 4)}{4}.
 \end{aligned}$$

De manera que obtenemos la siguiente base de Gröbner en $\mathbb{R}(a, b, l_2, l_3)[s_1, c_1, s_2, c_2]$:

$$\begin{aligned}
 c_1 - \frac{b}{(a^2 + b^2)}s_2 - \frac{a}{2}, \\
 s_1 + \frac{a}{(a^2 + b^2)}s_2 - \frac{b}{2}, \\
 c_2 - \frac{a^2 + b^2 - 2}{2}, \\
 s_2^2 + \frac{(a^2 + b^2)(a^2 + b^2 - 4)}{4}.
 \end{aligned} \tag{4.12}$$

Mas aún, (4.12) es una base de Gröbner para (4.10) para cualesquiera a, b tal que $a^2 + b^2 \neq 0$.

Si sustituimos $l_2 = l_3 = 1$ en (4.10) y calculamos una base de Gröbner con el orden graduado lexicográfico con $c_1 > s_1 > c_2 > s_2$ mediante el siguiente código:

```

> ring R = (0, a, b), (c1, s1, c2, s2), dp;
> poly f1 = (c1*c2 - s1*s2) + c1 -a;
> poly f2 = (c1*s2 + c2*s1) + s1 -b;
> poly f3 = c1^2+s1^2-1;
> poly f4 = c2^2+s2^2-1;
> ideal I = f1, f2, f3, f4;
> std(I);
_[1]=2*c2+(-a^2-b^2+2)
_[2]=(2*a^2+2*b^2)*s1+(2*a)*s2+(-a^2*b-b^3)
_[3]=(b)*c1+(-a)*s1-s2
_[4]=2*s2^2+(a^2+b^2)*c2+(-a^2-b^2)
> option(redSB);
> std(I);

```

$$-[1]=2*c_2+(-a^2-b^2+2)$$

$$-[2]=(2*a^2+2*b^2)*s_1+(2*a)*s_2+(-a^2*b-b^3)$$

$$-[3]=(2*a^2+2*b^2)*c_1+(-2*b)*s_2+(-a^3-a*b^2)$$

$$-[4]=4*s_2^2+(a^4+2*a^2*b^2-4*a^2+b^4-4*b^2)$$

la base de Gröbner reducida está formada por los siguientes polinomios:

$$2(a^2 + b^2)c_1 - 2bs_2 - a(a^2 + b^2),$$

$$2(a^2 + b^2)s_1 + 2as_2 + b(a^2 + b^2),$$

$$2c_2 - (a^2 + b^2 - 2),$$

$$4s_2^2 + (a^4 + 2a^2b^2 - 4a^2 + b^4 - 4b^2).$$

Multiplicando por $\frac{1}{2(a^2 + b^2)}$, $\frac{1}{2}$, $\frac{1}{4}$ respectivamente y agrupando obtenemos la base de Gröbner reducida (4.12). Esto significa que, ya sea sustituyendo $l_2 = l_3 = 1$ directamente en la ecuación o estableciendo $l_2 = l_3 = 1$ en la ecuación y volviendo a calcular una base de Gröbner en el anillo $\mathbb{R}(a, b)[c_1, s_1, c_2, s_2]$, obtenemos el mismo resultado.

Si resolvemos la última ecuación de (4.12) obtenemos que

$$s_2 = \pm \frac{1}{2} \sqrt{(a^2 + b^2)(4 - (a^2 + b^2))}$$

Note que las soluciones son reales si y sólo si $0 < a^2 + b^2 \leq 4$ y $a^2 + b^2 = 4$.

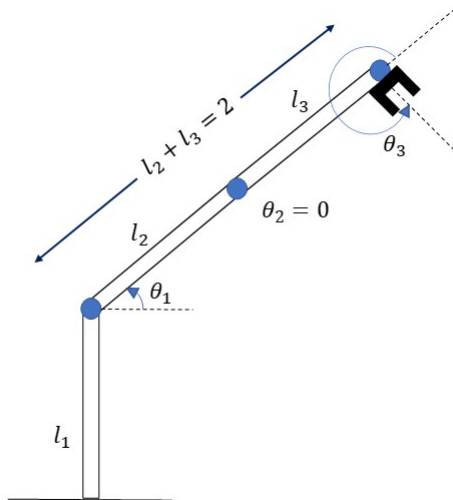


Figura 4.12: Posición del brazo del robot cuando $\theta_2 = 0$

Problema cinemático en los brazos de robots
4.2 Problema cinemático inverso

Geoméricamente, la distancia de la articulación 1 a la articulación 3 es como máximo $l_2 + l_3 = 2$ y las posiciones con $l_2 + l_3 = 2$ se pueden alcanzar de una sola manera: fijando $\theta_2 = 0$, de modo que l_2 y l_3 se encuentra en la misma posición como se muestra en la Figura 4.12.

Por otro lado, en el caso $0 < a^2 + b^2 < 4$, de nuestra base de Gröbner tenemos los siguientes conjuntos de soluciones:

$$\left\{ \begin{array}{l} \sqrt{2-b^2} = a, 2+2c_2 = a^2 + b^2, s_2 = \pm 1, s_1 = \frac{a^2b + b^3 - 2as_2}{2(a^2 + b^2)}, c_1 = \frac{a^3 + ab^2 + 2bs_2}{2(a^2 + b^2)} \end{array} \right\},$$

$$\left\{ \begin{array}{l} \sqrt{2-b^2} = -a, 2+2c_2 = a^2 + b^2, s_2 = \pm 1, s_1 = \frac{a^2b + b^3 - 2as_2}{2(a^2 + b^2)}, c_1 = \frac{a^3 + ab^2 + 2bs_2}{2(a^2 + b^2)} \end{array} \right\},$$

donde $-\sqrt{2} \leq b \leq \sqrt{2}$.

Ahora, sustituyamos a a en $a^2 + b^2 = 2 + 2c_2$, implica, $(2 - b^2) + b^2 - 2 = 0 = 2c_2$, entonces $\cos \theta_2 = 0$. Por otro lado, por los conjuntos solución sabemos que $\sin \theta_2 = \pm 1$, así $\theta_2 = \pi/2, 3\pi/2$.

Resolvamos para $s_1 = \frac{a^2b + b^3 - 2as_2}{2(a^2 + b^2)}$. Sea $a = \sqrt{2-b^2} = a$ en donde $-\sqrt{2} \leq b \leq \sqrt{2}$,

Caso (i) Si $s_2 = 1$, sustituyendo tenemos

$$s_1 = \frac{1}{4}(b(a^2 + b^2) - 2as_2) = \frac{1}{4}(2b - 2as_2) = \frac{1}{2}(b - \sqrt{2-b^2}(1)) = \frac{1}{2}(b - \sqrt{2-b^2}),$$

en los casos límite $-\sqrt{2}/2 \leq s_1 \leq \sqrt{2}/2$.

Caso (ii) Ahora, si $s_2 = -1$, entonces $s_1 = \frac{1}{2}(b - \sqrt{2-b^2}(-1)) = \frac{1}{2}(b + \sqrt{2-b^2})$, donde $-\sqrt{2} \leq b \leq \sqrt{2}$, tomando los casos límite $-\sqrt{2}/2 \leq s_1 \leq \sqrt{2}/2$.

Analógamente, resolvamos para $c_1 = \frac{a^3 + ab^2 + 2bs_2}{2(a^2 + b^2)}$. Sea $a = \sqrt{2-b^2}$ en donde $-\sqrt{2} \leq b \leq \sqrt{2}$,

Caso (i) Si $s_2 = 1$, sustituyendo tenemos

$$c_1 = \frac{1}{4}(a^3 + ab^2 + 2b) = \frac{1}{4}(a(a^2 + b^2) + 2b) = \frac{1}{4}(2a + 2b) = \frac{1}{2}(a + b) = \frac{1}{2}(\sqrt{2-b^2} + b),$$

tomando los casos límite, $-\sqrt{2}/2 \leq c_1 \leq \sqrt{2}/2$.

Caso (ii) Para $s_2 = -1$, $c_1 = \frac{1}{2}(a - b) = \frac{1}{2}(\sqrt{2-b^2} - b)$, de igual manera tomando los

Problema cinemático en los brazos de robots
4.2 Problema cinemático inverso

casos límite $\sqrt{2}/2 \leq c_1 \leq -\sqrt{2}/2$, esto nos dice que el movimiento de l_2 se mueve de derecha a izquierda.

En resumen, $-\sqrt{2}/2 \leq c_1, s_1 \leq \sqrt{2}/2$. Por lo tanto, θ_1 puede tomar cualquier valor en el intervalo $[0, 2\pi]$.

Mas aún, si $\sqrt{2-b^2} = -a$, en donde $-\sqrt{2} \leq b \leq \sqrt{2}$ se obtienen los mismos valores para θ_1 y θ_2 .

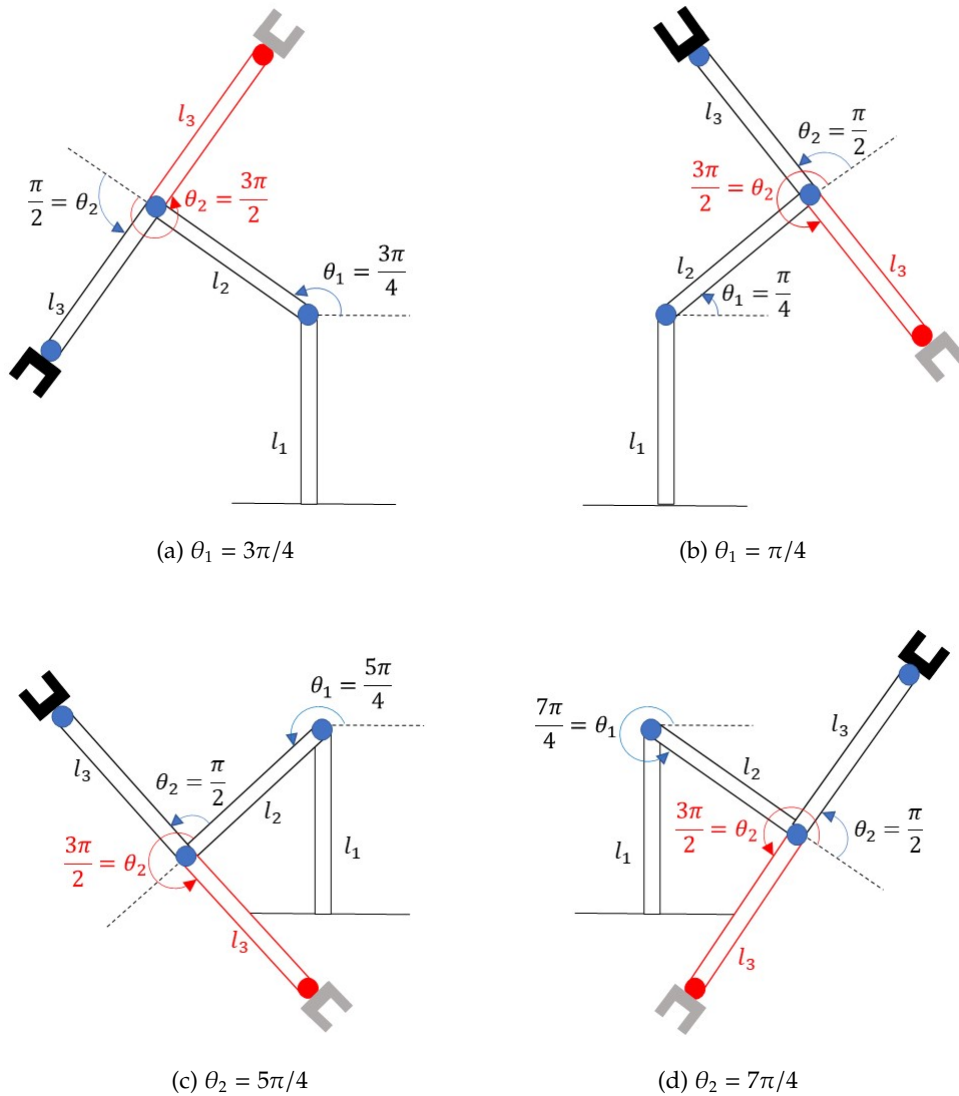


Figura 4.13: Ejemplos de posiciones de el brazo de robot

En la Figura 4.13 se muestran algunas posiciones de la mano del brazo del robot con algunos valores que toman θ_1 y θ_2 cuando $a^2 + b^2 < 4$.

Geoméricamente, considerando $l_2 = l_3 = 1$, las soluciones significan que la mano de nuestro robot puede colocarse en cualquier punto del disco cerrado de radio 2 centrado en la articulación 1, el origen de el sistema de coordenadas (x_1, y_1) .

¿Qué pasaría si $a = b = 0$?

Geoméricamente, esto pasa cuando la articulación 3 está en el origen del sistema de coordenadas $q = (x_1, y_1)$ en la misma posición que la articulación 1 y los polinomios en la base de Gröbner (4.11) no están bien definidos cuando $a = 0 = b$, entonces esta especialización falla. De hecho, haciendo $l_2 = l_3 = 1$ y $a = b = 0$ en el sistema original (4.10) calculamos la base de Gröbner usando el siguiente código:

```
> ring R=0, (c1,s1,c2,s2), dp;
> poly f1 = (c1*c2 - s1*s2) + c1;
> poly f2 = (c1*s2 + c2*s1) + s1;
> poly f3 = c1^2+s1^2-1;
> poly f4 = c2^2+s2^2-1;
> ideal I = f1,f2,f3,f4;
> std(I);
_[1]=s2
_[2]=c2+1
_[3]=c1^2+s1^2-1
> option(redSB);
> std(I);
_[1]=s2
_[2]=c2+1
_[3]=c1^2+s1^2-1
```

Por lo tanto, la base de Gröbner está formada por los polinomios:

$$\begin{aligned} c_1^2 + s_1^2 - 1, \\ c_2 + 1, \\ s_2. \end{aligned} \tag{4.13}$$

En donde el ángulo θ_1 toma un valor arbitrario y $\theta_2 = \pi$ ya que $\cos \theta_2 = -1$, resultando infinitas configuraciones posibles que colocarán la articulación 3 en la articulación 1. Por ejemplo, si $\theta_1 = 0$ y $\theta_2 = \pi$, el eslabón l_3 se dobla hacia atrás a lo largo de l_2 y la posición de la mano se colocará en $(a, b) = (0, 0)$, otra forma que colocará la mano en el origen se da cuando $\theta_1 = 3\pi/4$ y $\theta_2 = \pi$ como se muestra en la Figura 4.14.

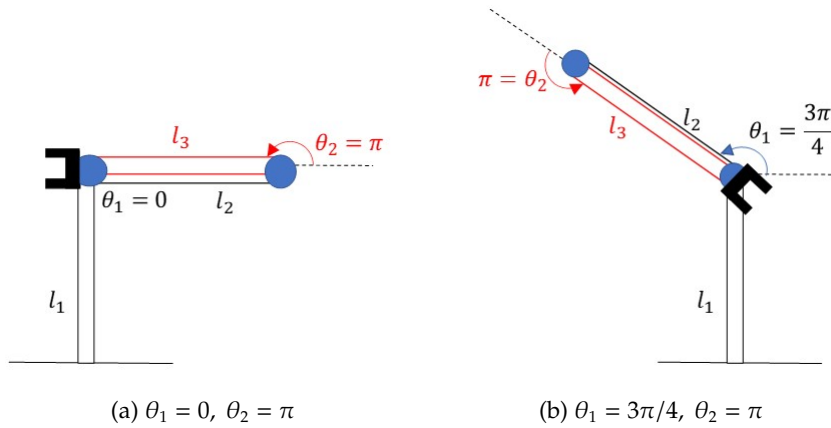


Figura 4.14: Ejemplos de posiciones de la mano del robot en el origen

Si $a = 0$ y $b \neq 0$, en general, la base de Gröbner para el ideal es diferente bajo esta especialización.

Resumiendo: dado (a, b) en coordenadas (x_1, y_1) y fijando la articulación 3 en (a, b) considerando $l_2 = l_3 = 1$:

1. Hay infinitas posiciones de la articulación 1 cuando $a^2 + b^2 = 0$. La mano del robot se coloca en el origen del disco cerrado de radio 1 en la articulación 1.
2. Hay dos configuraciones distintas de la articulación 1 para $a^2 + b^2 < 4$. La mano del robot puede colocarse en cualquier punto del disco cerrado de radio 2 centrado en la articulación 1.
3. Hay una configuración cuando $a^2 + b^2 = 4$. La mano del robot se coloca en cualquier punto de la circunferencia del disco cerrado de radio 2 centrado en la articulación 1.
4. No hay posiciones posibles de la articulación 1 cuando $a^2 + b^2 > 4$.

Los casos $a^2 + b^2 = 0, a^2 + b^2 = 4$ se conocen como singularidades cinemáticas.

Las descripciones de los posibles movimientos de robots como los que hemos desarrollado se utilizan de manera esencial en la planificación de los movimientos del robot necesarios para cumplir con las tareas que se le asignan. Los métodos que hemos esbozado se suelen utilizar para implementarlos en programas para controlar la automatización del movimiento del robot. El objetivo principal de dicho programa sería instruir al robot qué configuración debe realizar la articulación para llevar la mano de una posición a otra. Los problemas básicos a resolver aquí serían; primero, encontrar un camino parametrizado $c(t) \in C$ comenzando en la configuración inicial de la mano y terminando en la nueva

configuración deseada, y segundo, encontrar un camino correspondiente $j(t) \in J$ tal que $f(j(t)) = c(t)$ para todo t .

Además, es posible que deseemos imponer restricciones adicionales en las rutas utilizadas, como:

1. Si el espacio de configuraciones del camino $c(t)$ es cerrado (es decir, si el inicio y el final de las configuraciones son las mismas), también podríamos querer que el camino $j(t)$ sea un camino cerrado. Esto sería especialmente importante para los robots que realizan una tarea repetitiva como hacer una determinada soldadura en la carrocería de un automóvil. Asegurando que el camino de el espacio articular sea cerrado.
2. En cualquier robot real, nos gustaría limitar las velocidades conjuntas necesarias para realizar el movimiento prescrito. Los movimientos demasiado rápidos (o bruscos) podrían dañar los mecanismos.
3. Si queremos hacer el menor movimiento articular total posible para realizar cada movimiento.

Para los lectores que deseen profundizar en este tema, una referencia básica sobre robótica es el texto [14]. También se puede consultar [4] que contiene otra discusión sobre la teoría de la base de Gröbner para el problema cinemático inverso. Una introducción a los problemas de cinemática inversa se proporciona en [13].

Capítulo 5

Demostraciones automáticas en Geometría Euclidea

En esta sección, utilizaremos dos métodos para demostrar teoremas de geometría euclidea. Tales métodos son de interés de investigadores tanto en inteligencia artificial (IA) como en modelado geométrico porque se han utilizado en el diseño de programas que, en efecto, pueden probar o refutar teoremas.

Nuestro objetivo es escribir algebraicamente nuestras hipótesis y conclusiones para obtener una base de Gröbner y así probar o refutar los teoremas que se van a presentar.

5.1 Proposición. Sean $U = (u_1, u_2)$, $V = (v_1, v_2)$, $W = (w_1, w_2)$, $X = (x_1, x_2)$ puntos en el plano. Las siguientes propiedades pueden ser expresadas algebraicamente.

(i) UV es paralelo a WX :

$$(v_2 - u_2)(x_1 - w_1) - (v_1 - u_1)(x_2 - w_2) = 0,$$

(ii) UV es perpendicular a WX :

$$(v_1 - u_1)(x_1 - w_1) + (v_2 - u_2)(x_2 - w_2) = 0,$$

(iii) U, V y W son colineales:

$$(w_2 - u_2)(v_1 - u_1) = (v_2 - u_2)(w_1 - u_1),$$

(iv) La distancia de U a V es igual a la distancia de W a X , es decir, $UV = WX$:

$$(v_1 - u_1)^2 + (v_2 - u_2)^2 = (x_1 - w_1)^2 + (x_2 - w_2)^2,$$

(v) W es el punto medio del segmento UV :

Se cumple si se da que U, V y W son colineales y $UW = VW$.

Demostración. (i) Dos rectas son paralelas si y sólo si sus pendientes son iguales, entonces

$$\begin{aligned} UV \parallel WX : \frac{(v_2 - u_2)}{(v_1 - u_1)} = \frac{(x_2 - w_2)}{(x_1 - w_1)} &\iff (v_2 - u_2)(x_1 - w_1) = (v_1 - u_1)(x_2 - w_2) \\ &\iff (v_2 - u_2)(x_1 - w_1) - (v_1 - u_1)(x_2 - w_2) = 0. \end{aligned}$$

(ii) Dos segmentos son perpendiculares si y sólo si el producto de sus pendientes es -1 . Así,

$$\begin{aligned} UV \perp WX : \frac{(v_2 - u_2)}{(v_1 - u_1)} \cdot \frac{(x_2 - w_2)}{(x_1 - w_1)} &= -1 \\ &\iff \frac{(v_2 - u_2)}{(v_1 - u_1)} = -\frac{(x_1 - w_1)}{(x_2 - w_2)} \\ &\iff (v_2 - u_2)(x_2 - w_2) = -(x_1 - w_1)(v_1 - u_1) \\ &\iff (v_2 - u_2)(x_2 - w_2) + (x_1 - w_1)(v_1 - u_1) = 0. \end{aligned}$$

(iii) Para el caso cuando U, V y W son colineales, W pertenece al segmento \overline{UV} . La recta que pasa por U y V se puede expresar como:

$$b = \frac{v_2 - u_2}{v_1 - u_1}(a - u_1) + u_2 \iff (b - u_2)(v_1 - u_1) = (v_2 - u_2)(a - u_1).$$

Sea W en el segmento UV , obtenemos

$$(w_2 - u_2)(v_1 - u_1) = (v_2 - u_2)(w_1 - u_1).$$

$$\begin{aligned} \text{(iv)} \quad UV = WX &\iff \sqrt{(v_1 - u_1)^2 + (v_2 - u_2)^2} = \sqrt{(x_1 - w_1)^2 + (x_2 - w_2)^2} \\ &\iff (v_1 - u_1)^2 + (v_2 - u_2)^2 = (x_1 - w_1)^2 + (x_2 - w_2)^2 \end{aligned}$$

(v) Si W es un punto medio de UV significa que $UW = VW$ y que W es un punto en UV , esto se reduce a las ecuaciones de (iii) y (iv).

□

5.2 Ejemplo. Teorema: Sean A, B, C, D los vértices del paralelogramo. Entonces las diagonales \overline{AD} y \overline{BC} se cortan en un punto N que es el punto medio de ambas diagonales. Es decir, $AN = DN$ y $BN = CN$, donde XY denota la longitud del segmento \overline{XY} .

Las propiedades de los paralelogramos no cambian bajo traslaciones y rotaciones. Por lo tanto, podemos comenzar por trasladar y rotar el paralelogramo para colocarlo en

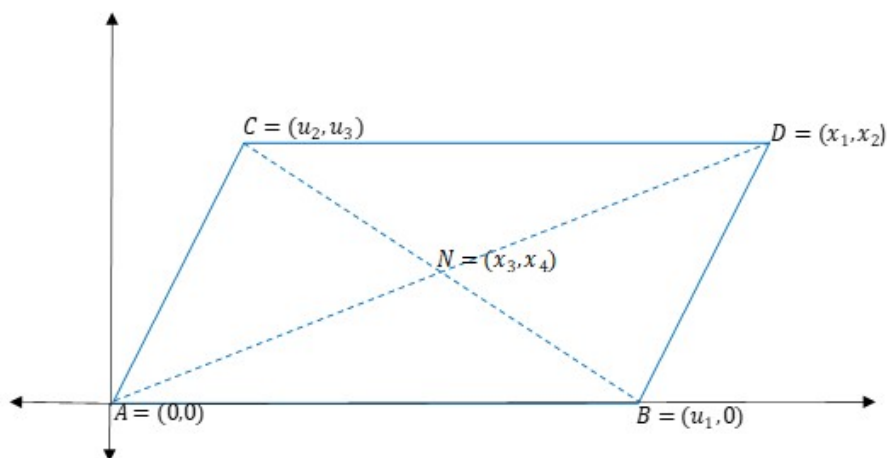


Figura 5.1: Paralelogramo

cualquier posición que queramos. Para simplificar, establecemos el vértice A en el origen, y el segmento \overline{AB} en el eje x . Así, los vértices A, B, C son de la forma

$$A = (0, 0), B = (u_1, 0), C = (u_2, u_3), \text{ para algún } u_1, u_2, u_3 \in \mathbb{R} \setminus \{0\}.$$

Note que las variables u_1, u_2, u_3 son variables arbitrarias y que las coordenadas de los vértices D y N dependen de las elecciones de las coordenadas de los vértices A, B, C . Por lo que, para las coordenadas arbitrarias, serán nombradas con las variables u_i y las coordenadas dependientes serán nombradas con las variables x_j . En consecuencia, $D = (x_1, x_2)$ y $N = (x_3, x_4)$. Una hipótesis de nuestro teorema, es que el cuadrilátero $ABCD$ es un paralelogramo, es decir, que los lados opuestos son paralelos. Con el hecho de que dos segmentos son paralelos si tienen la misma pendiente, vemos que podemos escribir estas declaraciones del siguiente modo:

$$\begin{aligned} \overline{AB} \parallel \overline{CD} : 0 &= \frac{x_2 - u_3}{x_1 - u_2}, \\ \overline{AC} \parallel \overline{BD} : \frac{u_3}{u_2} &= \frac{x_2}{x_1 - u_1}. \end{aligned}$$

Sacando denominadores, obtenemos

$$\begin{aligned} h_1 &= x_2 - u_3 = 0, \\ h_2 &= (x_1 - u_1)u_3 - x_2u_2 = 0. \end{aligned}$$

Otra hipótesis es que N es el punto de intersección de ambas diagonales, esto implica que N pertenece a los segmentos \overline{AD} y \overline{BC} , entonces, A, N, D y B, N, C son colineales. Usando

la fórmula de la pendiente, esto se puede escribir en ecuaciones polinómicas como

$$\begin{aligned} A, N, D \text{ colineales} &: \frac{x_4}{x_3} = \frac{u_3}{x_1}, \\ B, N, C \text{ colineales} &: \frac{x_4}{x_3 - u_1} = \frac{u_3}{u_2 - u_1}. \end{aligned}$$

Sacando denominadores, obtenemos

$$\begin{aligned} h_3 &= x_4x_1 - x_3u_3 = 0, \\ h_4 &= x_4(u_2 - u_1) - u_3(x_3 - u_1)u_3 = 0. \end{aligned}$$

Por lo tanto, las ecuaciones h_1, h_2, h_3 y h_4 describen las hipótesis de nuestro teorema. Asimismo, las conclusiones también se pueden escribir algebraicamente usando el Teorema de Pitágoras y elevando al cuadrado

$$\begin{aligned} AN = ND &: x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2, \\ BN = NC &: (x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2. \end{aligned}$$

Operando, obtenemos las ecuaciones

$$\begin{aligned} g_1 &= x_1^2 + x_2^2 - 2x_1x_3 - 2x_4x_2 = 0, \\ g_2 &= u_3^2 + u_2^2 - u_1^2 + 2x_3u_1 - 2x_3u_2 - 2x_4u_3 = 0. \end{aligned}$$

En conclusión, el teorema afirma que si se cumplen las ecuaciones h_1, h_2, h_3 y h_4 , entonces se satisfacen las ecuaciones g_1 y g_2 .

Se debe cumplir que el número de hipótesis y el número de variables dependientes x_j sea el mismo, como se muestra en el Ejemplo 5.2. En general, tendremos m variables arbitrarias que denotaremos por u_1, \dots, u_m , y n variables dependientes que denotaremos por x_1, \dots, x_n . En consecuencia, las n hipótesis se denotan como

$$\begin{aligned} h_1(u_1, \dots, u_m, x_1, \dots, x_n) &= 0, \\ &\vdots \\ h_n(u_1, \dots, u_m, x_1, \dots, x_n) &= 0. \end{aligned}$$

Por otro lado, las conclusiones del teorema se denota como

$$g(u_1, \dots, u_m, x_1, \dots, x_n) = 0.$$

Es suficiente considerar el caso en el que hay una sola conclusión, en caso contrario

podemos tratar el problema una por una.

La pregunta a responder es, ¿cómo podemos deducir g de h_1, \dots, h_n algebraicamente?. La idea básica es que queremos que g sea cero siempre que h_1, \dots, h_n sean cero. De tal manera que, las hipótesis nos definen una variedad

$$V = V(h_1, \dots, h_n) \subset \mathbb{R}^{m+n},$$

para formalizar esto, veamos la siguiente definición.

5.3 Definición. Diremos que la conclusión g se deduce estrictamente de las hipótesis h_1, \dots, h_n si $g \in I(V) \subset \mathbb{R}^{m+n}$, donde $V = V(h_1, \dots, h_n)$.

5.4 Teorema. Sea $I = \langle f_1, \dots, f_s \rangle$ un ideal en $k[x_1, \dots, x_n]$. Entonces $f \in \sqrt{I}$ si y sólo si $1 \in \langle f_1, \dots, f_s, 1 - yf \rangle \subset k[x_1, \dots, x_n, y]$, donde y es una nueva variable.

Demostración. Sea \bar{k} la cerradura algebraica de k , por el Teorema fuerte de los Ceros de Hilbert 3.14 tenemos que $\sqrt{I} = I(V_{\bar{k}}(I))$, y por lo tanto, $f \in \sqrt{I}$ si y sólo si $f(a_1, \dots, a_n) = 0$ para todo $(a_1, \dots, a_n) \in V_{\bar{k}}(I)$. Sea $f \in \sqrt{I}$. Si $(a_1, \dots, a_n, b) \in V(\langle f_1, \dots, f_s, 1 - yf \rangle)$, entonces

$$f_i(a_1, \dots, a_n) = 0 \text{ para todo } i = 1, \dots, s \text{ y } 1 - bf(a_1, \dots, a_n) = 0.$$

Como $(a_1, \dots, a_n) \in V_{\bar{k}}(I)$, tenemos que $f(a_1, \dots, a_n) = 0$ lo que es una contradicción ya que $1 - bf(a_1, \dots, a_n) = 1 \neq 0$. Entonces no hay puntos en $V_{\bar{k}}$, así que $1 \in \langle f_1, \dots, f_s, 1 - yf \rangle$. Recíprocamente, sea $1 \in \langle f_1, \dots, f_s, 1 - yf \rangle$, entonces

$$1 = \sum_{i=1}^s h_i + f_i + h(1 - yf), \text{ con } h_i, h \in k[x_1, \dots, x_n, y].$$

En consecuencia, para todo $(a_1, \dots, a_n) \in V_{\bar{k}}(I)$, tenemos que

$$1 = (1 - yf(a_1, \dots, a_n))h(a_1, \dots, a_n, y).$$

Si $f(a_1, \dots, a_n) \neq 0$, tomamos $y = \frac{1}{f(a_1, \dots, a_n)}$ y se obtiene una contradicción. Así, $f(a_1, \dots, a_n) = 0$, y por lo tanto $f \in \sqrt{I}$. □

Este teorema nos da un algoritmo para ver si un polinomio pertenece al radical de un ideal.

5.5 Proposición. Si $g \in \sqrt{\langle h_1, \dots, h_n \rangle}$, entonces g se deduce estrictamente de h_1, \dots, h_n .

Demostración. Si $g \in \sqrt{\langle h_1, \dots, h_n \rangle}$, implica que existe un s tal que $g^s \in \langle h_1, \dots, h_n \rangle$. Así, $g^s = \sum_{i=1}^n A_i h_i$, donde $A_i \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$. Entonces g^s es cero en los puntos donde h_1, \dots, h_n son cero, y por lo tanto g también es cero en dichos puntos. \square

El recíproco de esta proposición falla cuando $\sqrt{\langle h_1, \dots, h_n \rangle} \subsetneq I(V)$. Esta proposición junto con el algoritmo que obtenemos del Teorema 5.4, nos da un método para comprobar si una conclusión se deduce estrictamente. Mas aún, si $\bar{I} = \langle h_1, \dots, h_n, 1 - yg \rangle$ en $\mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$, el Teorema 5.4, implica que

$$g \in \sqrt{\langle h_1, \dots, h_n \rangle} \iff \{1\} \text{ es la base de Gröbner reducida de } \bar{I}.$$

Continuando con el Ejemplo 5.2, se tenían las hipótesis:

$$\begin{aligned} h_1 &= x_2 - u_3 = 0, \\ h_2 &= (x_1 - u_1)u_3 - x_2u_2 = 0, \\ h_3 &= x_4x_1 - x_3u_3 = 0, \\ h_4 &= x_4(u_2 - u_1) - u_3(x_3 - u_1) = 0. \end{aligned}$$

Una de las conclusiones que tenemos para comprobar el Teorema es

$$g = x_1^2 + x_2^2 - 2x_1x_3 - 2x_4x_2 = 0.$$

Para aplicar la Proposición 5.5, tenemos que calcular la base de Gröbner reducida de

$$\bar{I} = \langle h_1, \dots, h_4, 1 - yg \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4, y].$$

Calculamos la base de Gröbner reducida usando el siguiente código:

```
> ring R=0, (u1,u2,u3,x1,x2,x3,x4,y), lp;
> poly g = x1^2+x2^2-2*x1*x3-2*x4*x2;
> poly h1 = x2-u3;
> poly h2 = (x1-u1)*u3-x2*u2;
> poly h3 = x4*x1-x3*u3;
> poly h4 = x4*(u2-u1)-u3*(x3-u1);
> ideal I = h1,h2,h3,h4,1-y*g;
> std(I);
_[1]=x2^2*x3^2*y+x2^2*x4^2*y-2*x2*x3^2*x4*y-2*x2*x4^3*y-x4^2
_[2]=x1*x4-x2*x3
_[3]=x1*x2*x3*y-2*x1*x3*x4*y+x2^2*x4*y-2*x2*x4^2*y-x4
```

```

_[4]=x1^2*y-2*x1*x3*y+x2^2*y-2*x2*x4*y-1
_[5]=u3-x2
_[6]=u2*x4-u3*x1^2*x3*y-u3*x1*x2*x4*y+2*u3*x1*x3^2*y+u3*x1*x4^2*y
+u3*x2*x3*x4*y
_[7]=u2*x2-u3*x1^3*y+2*u3*x1^2*x3*y-u3*x1*x2^2*y+u3*x1*x2*x4*y
+u3*x2^2*x3*y
_[8]=u1*x4+u2*x2-u2*x4-u3*x1+u3*x3
_[9]=u1*x2-u1*x4+u2*x4-u3*x3
> option(redSB);
> std(I);
_[1]=x2^2*x3^2*y+x2^2*x4^2*y-2*x2*x3^2*x4*y-2*x2*x4^3*y-x4^2
_[2]=x1*x4-x2*x3
_[3]=x1*x2*x3*y+x2^2*x4*y-2*x2*x3^2*y-2*x2*x4^2*y-x4
_[4]=x1^2*y-2*x1*x3*y+x2^2*y-2*x2*x4*y-1
_[5]=u3-x2
_[6]=u2*x4-x2*x3
_[7]=u2*x2-x1*x2
_[8]=u1*x4
_[9]=u1*x2

```

Como podemos notar, la base de Gröbner no es $\{1\}$, pero el teorema es cierto, así que tenemos que descubrir en que falla el método. Si calculamos una base de Gröbner de $I = \langle h_1, h_2, h_3, h_4 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$, usando el orden lexicográfico con $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$. Calculamos la base de Gröbner reducida, usando el siguiente código

```

> ring R=0, (x1,x2,x3,x4,u1,u2,u3), lp;
> poly h1 = x2-u3;
> poly h2 = (x1-u1)*u3-x2*u2;
> poly h3 = x4*x1-x3*u3;
> poly h4 = x4*(u2-u1)-u3*(x3-u1);
> ideal I = h1,h2,h3,h4;
> std(I);
_[1]=x1*x4-x3*u3
_[2]=x1*u3-x2*u2-u1*u3
_[3]=x2-u3
_[4]=x3*u3+x4*u1-x4*u2-u1*u3
_[5]=2*x4*u1^2-2*x4*u1*u2-u1^2*u3+u1*u2*u3
_[6]=2*x4*u1*u3-u1*u3^2

```

```

> option(redSB);
> std(I);
_[1]=x1*x4+x4*u1-x4*u2-u1*u3
_[2]=x1*u3-u1*u3-u2*u3
_[3]=x2-u3
_[4]=x3*u3+x4*u1-x4*u2-u1*u3
_[5]=2*x4*u1^2-2*x4*u1*u2-u1^2*u3+u1*u2*u3
_[6]=2*x4*u1*u3-u1*u3^2

```

Por lo tanto, la base de Gröbner reducida está formada por los siguientes polinomios:

$$\begin{aligned}
 f_1 &= x_1x_4 + x_4u_1 - x_4u_2 - u_1u_3, \\
 f_2 &= x_1u_3 - u_1u_3 - u_2u_3 \\
 f_3 &= x_2 - u_3, \\
 f_4 &= x_3u_3 + x_4u_1 - x_4u_2 - u_1u_3, \\
 f_5 &= x_4u_1^2 - x_4u_1u_2 - \frac{1}{2}u_1^2u_3 + \frac{1}{2}u_1u_2u_3, \\
 f_6 &= x_4u_1u_3 - \frac{1}{2}u_1u_3^2.
 \end{aligned}$$

La variedad $V = V(h_1, h_2, h_3, h_4) = V(f_1, \dots, f_6) \subset \mathbb{R}^7$ definida por las hipótesis es reducible. Además, el polinomio f_2 se puede factorizar como $(x_1 - u_1 - u_2)u_3 = 0$, así que tenemos dos casos, $u_3 = 0$ o $(x_1 - u_1 - u_2) = 0$, lo que implica que

$$V = V_1(f_1, u_3, f_3, f_4, f_5, f_6) \cup V_2(f_1, x_1 - u_1 - u_2, f_3, f_4, f_5, f_6).$$

Veamos que la variedad V se puede descomponer en cuatro variedades irreducibles.

1. Caso $u_3 = 0$. Calculamos la base de Gröbner reducida del ideal $I = \langle f_1, u_3, f_3, f_4, f_5, f_6 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$ usando el orden lexicográfico con $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$ mediante el siguiente código:

```

> ring R=0, (x1, x2, x3, x4, u1, u2, u3), lp;
> poly f1 = x1*x4+x4*u1-x4*u2-u1*u3;
> poly f2 = u3;
> poly f3 = x2-u3;
> poly f4 = x3*u3+x4*u1-x4*u2-u1*u3;
> poly f5 = x4*u1^2-x4*u1*u2-1/2*u1^2*u3+ 1/2*u1*u2*u3;
> poly f6 = x4*u1*u3-1/2*u1*u3^2;
> ideal I = f1, f2, f3, f4, f5, f6;
> std(I);

```

```

_[1]=u3
_[2]=x4*u1-x4*u2-u1*u3
_[3]=x2-u3
_[4]=x1*x4+x4*u1-x4*u2-u1*u3
> option(redSB);
> std(I);
_[1]=u3
_[2]=x4*u1-x4*u2
_[3]=x2
_[4]=x1*x4

```

Por lo tanto, la base de Gröbner está formada por los polinomios

$$\begin{aligned}
 q_1 &= u_3, \\
 q_2 &= (u_1 - u_2)x_4, \\
 q_3 &= x_2, \\
 q_4 &= x_1x_4.
 \end{aligned}$$

Mas aún, el polinomio $q_2 = (u_1 - u_2)x_4 = 0$ nos dice que tenemos dos subcasos: $x_4 = 0$ y $u_1 - u_2 = 0$.

1.1 Caso $u_3 = 0, x_4 = 0$. Calculamos la base de Gröbner reducida del ideal $I = \langle q_1, x_4, q_3, q_4 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$ usando el orden lexicográfico con $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$ mediante el siguiente código:

```

> ring R=0, (x1, x2, x3, x4, u1, u2, u3), lp;
> poly q1 = u3;
> poly q2 = x4;
> poly q3 = x2;
> poly q4 = x1*x4;
> ideal I = q1, q2, q3, q4;
> option(redSB);
> std(I);
_[1]=u3
_[2]=x4
_[3]=x2

```

Así, la base de Gröbner está formada por

$$\begin{aligned} &u_3, \\ &x_4, \\ &x_2. \end{aligned}$$

Esta solución nos da la variedad $U_1 = V(x_2, x_4, u_3)$.

1.2 Caso $u_3 = 0, u_1 - u_2 = 0$. De igual modo, calculamos la base de Gröbner reducida del ideal $I = \langle q_1, u_1 - u_2, q_3, q_4 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$ usando el orden lexicográfico con $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$ mediante el siguiente código:

```
> ring R=0, (x1, x2, x3, x4, u1, u2, u3), lp;
> poly q1 = u3;
> poly q2 = u1-u2;
> poly q3 = x2;
> poly q4 = x1*x4;
> ideal I = q1, q2, q3, q4;
> option(redSB);
> std(I);
_[1]=u3
_[2]=u1-u2
_[3]=x2
_[4]=x1*x4
```

Entonces, los polinomios que pertenecen a la base de Gröbner reducida son

$$\begin{aligned} &u_3, \\ &u_1 - u_2, \\ &x_2, \\ &x_1x_4. \end{aligned}$$

Esta solución nos da la variedad $U_2 = V(u_3, u_1 - u_2, x_2, x_1x_4)$.

2. Caso $x_1 - u_1 - u_2 = 0, u_3 \neq 0$. Calculamos la base de Gröbner reducida del ideal $I = \langle f_1, x_1 - u_1 - u_2, f_3, f_4, f_5, f_6 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$ usando el orden lexicográfico con $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$ mediante el siguiente código:

```
> ring R=0, (x1, x2, x3, x4, u1, u2, u3), lp;
> poly f1 = x1*x4+x4*u1-x4*u2-u1*u3;
```

```

> poly f2 = x1-u1-u2;
> poly f3 = x2-u3;
> poly f4 = x3*u3+x4*u1-x4*u2-u1*u3;
> poly f5 = x4*u1^2-x4*u1*u2-1/2*u1^2*u3+ 1/2*u1*u2*u3;
> poly f6 = x4*u1*u3-1/2*u1*u3^2;
> ideal I = f1,f2,f3,f4,f5,f6;
> std(I);
_[1]=2*x4*u1-u1*u3
_[2]=x3*u3+x4*u1-x4*u2-u1*u3
_[3]=x2-u3
_[4]=x1-u1-u2
> option(redSB);
> std(I);
_[1]=2*x4*u1-u1*u3
_[2]=2*x3*u3-2*x4*u2-u1*u3
_[3]=x2-u3
_[4]=x1-u1-u2

```

Entonces, la base de Gröbner está formada por los polinomios

$$\begin{aligned}
 r_1 &= -u_1(u_3 - 2x_4), \\
 r_2 &= -u_1u_3 + 2u_3x_3 - 2u_2x_4, \\
 r_3 &= x_2 - u_3, \\
 r_4 &= x_1 - u_1 - u_2.
 \end{aligned}
 \tag{5.1}$$

Por el polinomio $r_1 = -u_1(u_3 - 2x_4)$ tenemos dos casos, $u_1 = 0$ o $u_3 - 2x_4 = 0$.

2.1 Caso $x_1 - u_1 - u_2 = 0, u_3 \neq 0, u_1 = 0$. Sustituimos $u_1 = 0$ en (5.1) y calculamos la base de Gröbner reducida del ideal $I = \langle -u_1, 2u_3x_3 - 2u_2x_4, r_3, x_1 - u_2 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$ usando el orden lexicográfico con $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$ mediante el siguiente código:

```

> ring R=0, (x1,x2,x3,x4,u1,u2,u3), lp;
> poly r1 = -u1;
> poly r2 = 2*u3*x3-2*u2*x4;
> poly r3 = x2-u3;
> poly r4 = x1-u2;
> ideal I = r1,r2,r3,r4;
> std(I);

```

```

_[1]=u1
_[2]=x3*u3-x4*u2
_[3]=x2-u3
_[4]=x1-u2
    
```

Así, los siguientes polinomios forman una base de Gröbner

$$\begin{aligned}
 &u_1, \\
 &x_3u_3 - x_4u_2, \\
 &x_2 - u_3, \\
 &x_1 - u_2.
 \end{aligned}$$

Esta solución nos da la variedad $U_3 = V(u_1, x_3u_3 - x_4u_2, x_2 - u_3, x_1 - u_2)$.

2.2 Caso $x_1 - u_1 - u_2 = 0, u_3 \neq 0, u_3 - 2x_4 = 0$. Por último, $u_3 - 2x_4 = 0$, esto implica que $u_3 = 2x_4$, si sustituimos u_3 en el polinomio r_2 de (5.1) tenemos el ideal $I = \langle u_3 - 2x_4, -u_1u_3 + 2u_3x_3 + u_3u_2, r_3, r_4 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$. Calculamos la base de Gröbner reducida de I usando el orden lexicográfico con $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$ mediante el siguiente código:

```

> ring R=0, (x1,x2,x3,x4,u1,u2,u3), lp;
> poly r1 = u3-2*x4;
> poly r2 = -u1*u3+2*u3*x3+u3*u2;
> poly r3 = x2-u3;
> poly r4 = x1-u1-u2;
> ideal I = r1,r2,r3,r4;
> std(I);
_[1]=2*x4-u3
_[2]=2*x3*u3-u1*u3+u2*u3
_[3]=x2-u3
_[4]=x1-u1-u2
    
```

En consecuencia, la base de Gröbner reducida está formada por los siguientes polinomios

$$\begin{aligned}
 &x_1 - u_1 - u_2, \\
 &x_2 - u_3, \\
 &u_3 \left(x_3 - \frac{u_1 + u_2}{2} \right), \\
 &x_4 - \frac{u_3}{2}.
 \end{aligned}$$

Además, el polinomio $u_3 \left(x_3 - \frac{u_1 + u_2}{2} \right) = 0$, implica que $\left(x_3 - \frac{u_1 + u_2}{2} \right) = 0$ ya que $u_3 \neq 0$, de modo que esta solución nos da la variedad

$$V' = V \left(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2} \right).$$

Por lo tanto, obtenemos la descomposición en variedades irreducibles

$$V = V' \cup U_1 \cup U_2 \cup U_3,$$

donde

$$V' = V \left(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2} \right),$$

$$U_1 = V(x_2, x_4, u_3),$$

$$U_2 = V(x_1, x_2, u_1 - u_2, u_3),$$

$$U_3 = V(x_1 - u_2, x_2 - u_3, x_3 u_3 - x_4 u_2, u_1).$$

Como ninguna variedad está contenida en otra, las variedades son componentes irreducibles en V .

En las variedades U_1 y U_2 , tenemos que $u_3 = 0$, esto es una contradicción, ya que u_3 arbitrario y diferente de cero. Mas aún, cuando $u_3 = 0$, el vértice C está en el eje x , esto implica que no existe el paralelogramo $ABCD$, de modo que tenemos un caso degenerado. Análogamente, tenemos $u_1 = 0$ en U_3 , este es otro caso degenerado.

Si evaluamos la conclusión g en la variedad U_1 , tenemos que $g = x_1^2 - 2x_1x_3$ es distinto de cero ya que x_1 y x_3 son arbitrarios. Por esta razón no fue posible demostrar el teorema. Si excluimos los casos degenerados U_1, U_2 y U_3 , tenemos que $g = (u_1 + u_2)^2 - (u_1 + u_2)^2 - u_3^2 + u_3^2 = 0$ en cualquier punto de V' .

Ahora, el objetivo en esta sección, es desarrollar un método general que pueda ser usado para demostrar teoremas sin tener que excluir los casos degenerados. Primero, escribimos $V = V(h_1, \dots, h_n) \subseteq \mathbb{R}^{m+n}$ como unión finita de variedades irreducibles.

$$V = V_1 \cup \dots \cup V_l. \tag{5.2}$$

Con el hecho de que las variables u_i son independientes, vamos a excluir estas variables en V . Así que introducimos la siguiente definición.

5.6 Definición. Sea W una variedad irreducible en el espacio \mathbb{R}^{m+n} con coordenadas $u_1, \dots, u_m, x_1, \dots, x_n$. Decimos que las funciones u_1, \dots, u_m son algebraicamente indepen-

dientes en W si ningún polinomio distinto de cero que solo tenga variables u_i sea cero en W , es decir si $I(W) \cap \mathbb{R}[u_1, \dots, u_m] = \{0\}$.

En consecuencia, en la descomposición de la variedad V dada en la ecuación (5.2), podemos reagrupar las componentes irreducibles de la forma

$$V = W_1 \cup \dots \cup W_p \cup U_1 \cup \dots \cup U_q, \quad (5.3)$$

donde u_1, \dots, u_m son algebraicamente independientes en las componentes W_i , y no lo son en las componentes U_j . Como los U_j representan casos “degenerados” de las hipótesis del teorema, consideraremos solamente la subvariedad

$$V' = W_1 \cup \dots \cup W_p \subseteq V.$$

5.7 Definición. Diremos que la conclusión g se deduce genéricamente de las hipótesis h_1, \dots, h_n si $g \in I(V') \subseteq \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$, donde como antes, $V' \subseteq \mathbb{R}^{m+n}$ es la unión de las componentes de la variedad $V = V(h_1, \dots, h_n)$ en las que u_i son algebraicamente independientes.

Decir que un teorema geométrico es cierto en el sentido usual significa que las conclusiones se deducen genéricamente de las hipótesis. Por lo tanto, debemos descomponer V , encontrar V' , calcular $I(V')$ y comprobar si $g \in I(V')$. Afortunadamente, es posible demostrar que g se deduce genéricamente de h_1, \dots, h_n sin conocer la descomposición de V dada en (5.2). Tenemos el siguiente resultado.

5.8 Proposición. En la situación descrita anteriormente, g se deduce genéricamente de h_1, \dots, h_n si existe un polinomio distinto de cero $p(u_1, \dots, u_m) \in \mathbb{R}[u_1, \dots, u_m]$ tal que

$$p \cdot m \in \sqrt{M},$$

donde M es el ideal generado por las hipótesis $h_n \in \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$.

Demostración. Sea V_j una componente irreducible de V' . Dado que $p \cdot g \in \sqrt{M}$, entonces $p \cdot g$ es cero en V y también en V_j . Entonces, $p \cdot g \in I(V_j)$, pero V_j es irreducible, de modo que $I(V_j)$ es un ideal primo por la Proposición 3.18. Así, $p \cdot g \in I(V_j)$ implica que $p \in I(V_j)$ o $g \in I(V_j)$. Note que $p \notin I(V_j)$ porque las funciones u_1, \dots, u_m son algebraicamente independientes en V_j . En consecuencia, $g \in I(V_j)$ y esto se cumple para todo elemento en V' , así $g \in I(V')$. □

Para poder aplicar esta proposición, necesitamos un criterio que nos diga cuándo existe el polinomio p .

Por la definición de radical, sabemos que $p \cdot g \in \sqrt{M}$ si y sólo si

$$(p \cdot g)^s = \sum_{j=1}^n A_j h_j,$$

con $A_j \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$ y $s \geq 1$. Si dividimos ambos lados entre p^s tenemos

$$g^s = \sum_{j=1}^n \frac{A_j}{p^s} h_j,$$

lo que demuestra que $g \in \sqrt{M}$ generado por las hipótesis h_1, \dots, h_n sobre el anillo $\mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$.

Recíprocamente, si $g \in \sqrt{M}$, entonces

$$g^s = \sum_{j=1}^n B_j h_j,$$

donde $B_j \in \mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$. Si definimos a p como mínimo común múltiplo de los denominadores, y multiplicamos ambos lados de la igualdad por p^s , tenemos

$$(p \cdot g)^s = \sum_{j=1}^n B'_j h_j,$$

con $B'_j \in \mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$ y p solo depende de u_i . Por lo tanto, $p \cdot g \in \sqrt{M}$.

5.9 Corolario. Considerando las condiciones de la proposición 5.8, las siguientes aseveraciones son equivalentes

- (i) Existe un polinomio distinto de cero $p \in \mathbb{R}[u_1, \dots, u_m]$ tal que $p \cdot g \in \sqrt{M}$.
- (ii) $g \in \sqrt{\tilde{M}}$, donde \tilde{M} es el ideal generado por los h_j en $\mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$.
- (iii) $\{1\}$ es la base de Gröbner reducida del ideal

$$\langle h_1, \dots, h_n, 1 - yg \rangle \subseteq \mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n, y].$$

Demostración. La demostración es una combinación del Teorema 5.4 y la Proposición 5.8 □

Si usamos este corolario y la proposición 5.8 obtenemos un método para probar teoremas de la geometría euclidea mediante las bases de Gröbner.

Para demostrar el teorema de el Ejemplo 5.2 usamos la Proposición 5.5 y concluimos que la base de Gröbner reducida no es $\{1\}$ aunque el teorema es cierto, por lo que el método fallaba. Ahora, para demostrar que el teorema es cierto, usando el Corolario 5.9, calculamos la base de Gröbner reducida del ideal generado por las hipótesis h_n y $1 - gy$ en el anillo $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4, y]$ usando el orden lexicográfico donde $x_1 > x_2 > x_3 > x_4 > y > u_1 > u_2 > u_3$ con el siguiente código:

```
> ring R=(0,u1,u2,u3),(x1,x2,x3,x4,y),lp;
> poly g = x1^2+x2^2-2*x1*x3-2*x4*x2;
> poly h1 = x2-u3;
> poly h2 = (x1-u1)*u3-x2*u2;
> poly h3 = x4*x1-x3*u3;
> poly h4 = x4*(u2-u1)-u3*(x3-u1);
> ideal I = h1,h2,h3,h4,1-y*g;
> option(redSB);
> std(I);
_[1]=1
```

Por lo tanto, la base de Gröbner reducida es $\{1\}$, esto demuestra que se cumple el teorema.

5.10 Ejemplo. (Teorema del Baricentro) Sea $\triangle ABC$ un triángulo cualquiera, si trazamos las medianas de cada lado estas se cortan en un punto $G = (x_1, x_2)$, este punto es llamado baricentro como se muestra en la Figura 5.2.

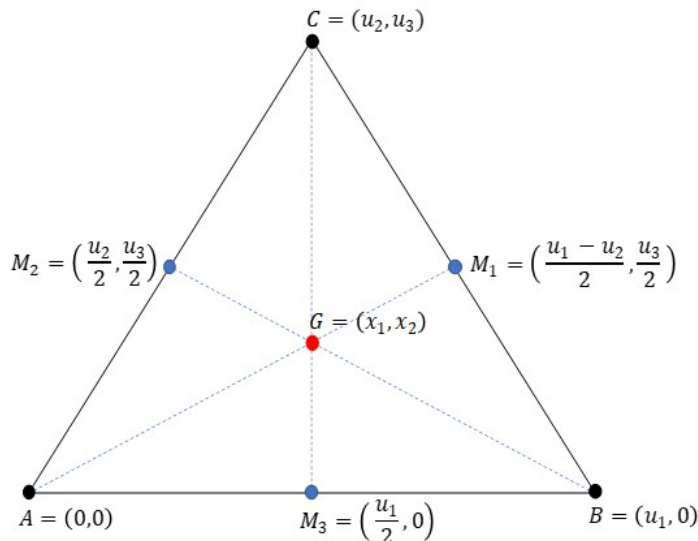


Figura 5.2: Teorema del baricentro

Establecemos el punto A en el origen $(0,0)$, así el segmento \overline{AB} está en el eje x . De modo que $B = (u_1, 0)$ y $C = (u_2, u_3)$. Mas aún, al trazar las medianas del triángulo obtenemos los tres puntos medios $M_1 = \left(\frac{u_1 - u_2}{2}, \frac{u_3}{2}\right)$, $M_2 = \left(\frac{u_2}{2}, \frac{u_3}{2}\right)$, y $M_3 = \left(\frac{u_1}{2}, 0\right)$.

Por hipótesis, el baricentro $G = (x_1, x_2)$ pertenece a la recta que pasa por los puntos A y M_1 , esto se puede escribir en ecuaciones polinómicas como

$$x_2 = \left(\frac{\frac{u_3}{2}}{\frac{u_1 - u_2}{2}}\right)x_1 \iff x_2 = \frac{u_3}{u_1 - u_2}x_1 \iff h_1 = u_3x_1 - (u_1 - u_2)x_2 = 0.$$

Similarmente, el baricentro $G = (x_1, x_2)$ pertenece a la recta que pasa por los puntos B y M_2 , esto se puede escribir en ecuaciones polinómicas como

$$x_2 = \left(\frac{\frac{u_3}{2}}{\frac{u_2}{2} - u_1}\right)(x_1 - u_1) \iff h_2 = u_3x_1 + (2u_1 - u_2)x_2 - u_3u_1 = 0.$$

Con el hecho de que Q es el punto de intersección de las rectas AM_1 y BM_2 , nuestra conclusión es que Q es un punto en la recta que pasa por C y M_3 , esto se puede escribir como

$$x_2 = \left(\frac{\frac{u_3}{2}}{u_2 - \frac{u_1}{2}}\right)\left(x_1 - \frac{u_1}{2}\right) \iff g = 2u_3x_1 + (u_1 - 2u_2)x_2 - u_3u_1 = 0.$$

Ahora, calculamos una base de Gröbner reducida para el ideal generado por $I = \langle h_1, h_2, 1 - gy \rangle$ sobre el anillo $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, y]$ con el orden lexicográfico usando el siguiente código

```
> ring R=(0,u1,u2,u3),(x1,x2,y),lp;
> poly h1 = u3*x1-(u1+u2)*x2;
> poly h2 = u3*x1+(2*u1-u2)*x2-u3*u1;
> poly g = 2*u3*x1+(u1-2*u2)*x2-u3*u1;
> ideal I = h1,h2,1-g*y;
> option(redSB);
> std(I);
_[1]=1
```

Obtenemos que la base es $\{1\}$, por el Colorario 5.9 queda probado el teorema.

5.11 Ejemplo. (Teorema del Círculo de Apolonio)

Sea $\triangle ABC$ un triángulo rectángulo en el plano con el ángulo recto en A . Sea H el punto de intersección de la altura con el segmento BC . Entonces, Los puntos medios de los tres lados y H están en una circunferencia, como se muestra en la Figura 5.3.

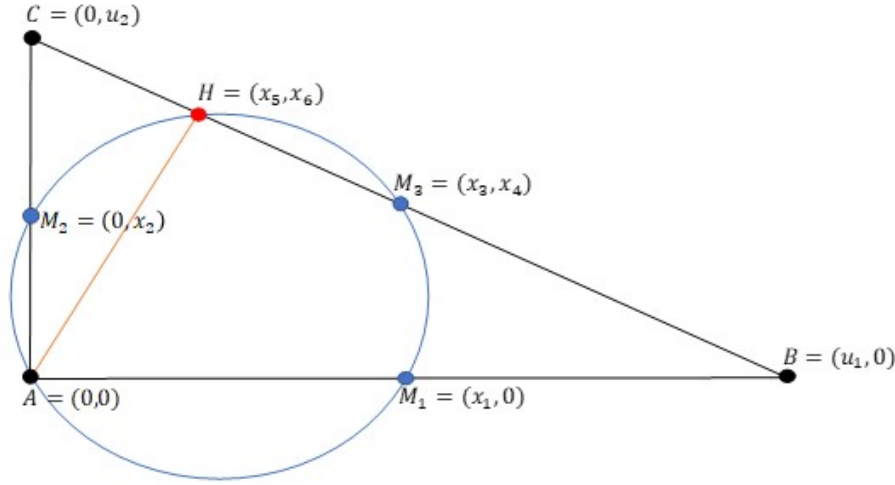


Figura 5.3: Teorema de Apolonio

Situamos el punto A en el origen, a los otros vértices del triángulo les asignamos las coordenadas $B = (u_1, 0)$ y $C = (0, u_2)$. Los puntos medios dependen de la distancia de los puntos A y B , entonces los puntos medios son $M_1 = (x_1, 0)$, $M_2 = (0, x_2)$ y $M_3 = (x_3, x_4)$. Con el hecho de que M_1 , M_2 y M_3 son puntos medios, usando (vi) de la Proposición 5.1 podemos escribir algebraicamente las hipótesis del siguiente modo:

$$\begin{aligned} AM_1 = M_1B : x_1^2 &= (x_1 - u_1)^2 \iff u_1(2x_1 - u_1) = 0 \iff h_1 = 2x_1 - u_1 = 0, \\ AM_2 = M_2C : x_2^2 &= (x_2 - u_2)^2 \iff u_2(2x_2 - u_2) = 0 \iff h_2 = 2x_2 - u_2 = 0, \\ CM_3 = M_3B : x_3^2 + (x_2 - u_2)^2 &= (x_3 - u_1)^2 + x_4^2 \iff u_2(2x_4 - u_2) = u_1(2x_3 - u_1). \end{aligned}$$

Si $u_2(2x_4 - u_2) = u_1(2x_3 - u_1) = 0$, entonces tenemos dos hipótesis, $h_3 = 2x_3 - u_1$ y $h_4 = 2x_4 - u_2 = 0$.

Mas aún, sea $H = (x_5, x_6)$ el punto de corte de la altura, usando (ii) y (iii) de la Proposición 5.1 tenemos

$$AH \perp BC : (x_5 - 0)(0 - u_1) + (x_6 - 0)(u_2 - 0) \iff h_5 = x_5u_1 - x_6u_2 = 0,$$

$$B, H, C \text{ son colineales} : (u_2 - 0)(x_5 - u_1) = (x_6 - 0)(0 - u_1) \iff h_6 = x_5u_2 + x_6u_1 - u_1u_2 = 0.$$

Por otro lado, sabemos que tres puntos no colineales se encuentran en la misma circunferencia, en este caso son los puntos medios M_1 , M_2 , M_3 , la conclusión es que el punto H se encuentra en esta circunferencia. Para expresar las hipótesis algebraicamente

necesitaremos el centro de la circunferencia $O = (x_7, x_8)$, entonces

$$M_1O = M_2O : h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0,$$

$$M_1O = M_3O : h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0.$$

Ahora, nuestra conclusión es que $HO = M_1O$, esto es

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0.$$

Notemos que en el Ejemplo 5.2 y en el Teorema del Círculo de Apolonio el número de hipótesis y el número de variables dependientes x_j son iguales.

Por último, calculamos la base de Gröbner reducida del ideal generado por las hipótesis h_i y $1 - gy$ en el anillo $\mathbb{R}(u_1, u_2)[x_1, \dots, x_8, y]$ usando el orden lexicográfico donde $x_1 > \dots > x_8 > y > u_1 > u_2$ con el siguiente código:

```
> ring R=(0,u1,u2),(x1,x2,x3,x4,x5,x6,x7,x8,y),lp;
> poly g = (x5-x7)^2+(x6-x8)^2-(x1-x7)^2-x8^2;
> poly h1 = 2*x1-u1;
> poly h2 = 2*x2-u2;
> poly h3 = 2*x3-u1;
> poly h4 = 2*x4-u2;
> poly h5 = x5*u1-x6*u2;
> poly h6 = x5*u2+x6*u1-u1*u2;
> poly h7 = (x1-x7)^2+x8^2-x7^2-(x8-x2)^2;
> poly h8 = (x1-x7)^2+x8^2-(x3-x7)^2-(x4-x8)^2;
> ideal I = h1,h2,h3,h4,h5,h6,h7,h8,1-g*y;
> option(redSB);
> std(I);
_[1]=1
```

Como la base de Gröbner reducida es $\{1\}$, por el Corolario 5.9 queda probado el teorema.

Capítulo 6

Coloración de Grafos

En esta sección queremos ilustrar cómo se puede aplicar la técnica de las bases de Gröbner para resolver un problema conocido en teoría de grafos: determinar si un grafo dado puede tener 3 colores. Ver [11] para más información.

Primero planteemos el problema con precisión. Dado un grafo \mathcal{G} con n vértices en donde como máximo existe una arista entre dos vértices cualesquiera. Queremos colorear los vértices de forma que solo se usen 3 colores, y no hay dos vértices adyacentes que se colorean de la misma manera. Si \mathcal{G} se puede colorear de esta forma, entonces \mathcal{G} se llama 3-coloreable. Se puede ver que esto es lo mismo que el problema de los 3 colores para un mapa: los vértices representan las regiones a colorear, y dos vértices que están conectados por una arista si las dos regiones correspondientes son adyacentes.

Primero, definimos $\xi = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ como la raíz cúbica de la unidad (es decir, $\xi^3 = 1$), donde cada raíz cubica de la unidad $1, \xi, \xi^2$ es un color. Ahora, sean x_1, \dots, x_n las variables que representan los distintos vértices del grafo \mathcal{G} . Cada vértice tiene asignado uno de los 3 colores. Esto puede ser representado por la siguientes n ecuaciones

$$x_i^3 - 1 = 0, \quad 1 \leq i \leq n. \quad (6.1)$$

Además, si los vértices x_i y x_j están conectados por una arista, deben tener un color diferente. Ya que $x_i^3 = x_j^3$, tenemos $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$. Por lo tanto x_i y x_j tendrán colores diferentes si y sólo si

$$x_i^2 + x_i x_j + x_j^2 = 0. \quad (6.2)$$

Sea I el ideal de $\mathbb{C}[x_1, \dots, x_n]$ generado por los polinomios de la Ecuación (6.1) y para cada par de vértices x_i y x_j que están conectados por una arista por los polinomios en la Ecuación (6.2). Consideraremos la variedad $V(I)$ contenida en \mathbb{C}^n y con el siguiente

Teorema podremos determinar si la gráfica \mathcal{G} es 3-coloreable.

6.1 Teorema. El grafo \mathcal{G} es 3-coloreable si y solo si $V(I) \neq \emptyset$.

Recordemos que si $1 \in G$, entonces $V(I) = \emptyset$, en caso contrario $V(I) \neq \emptyset$ (ver Teorema 3.15).

6.2 Ejemplo. Consideremos el grafo \mathcal{G} de la Figura 6.1

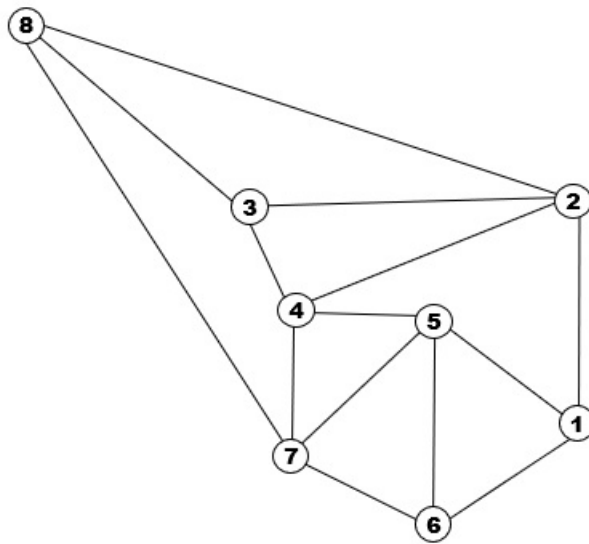


Figura 6.1: Grafo \mathcal{G}

Los polinomios correspondientes a \mathcal{G} son $x_i^3 - 1$, para $i = 1, \dots, 8$ y $x_i^2 + x_i x_j + x_j^2$, para las parejas $(i, j) \in \{(1, 2), (1, 5), (1, 6), (2, 3), (2, 4), (2, 8), (3, 4), (3, 8), (4, 5), (4, 7), (5, 6), (5, 7), (6, 7), (7, 8)\}$.

A continuación se muestra el código realizado en el programa Singular para calcular una base de Gröbner G para el ideal I , usando el orden lexicográfico con $x_1 > x_2 > \dots > x_8$.

```
> ring R=0, (x1,x2,x3,x4,x5,x6,x7,x8), lp;
> poly f1 = x1^3-1;
> poly f2 = x2^3-1;
> poly f3 = x3^3-1;
> poly f4 = x4^3-1;
> poly f5 = x5^3-1;
> poly f6 = x6^3-1;
```

```

> poly f7 = x7^3-1;
> poly f8 = x8^3-1;
> poly f9 = x1^2+x1*x2+x2^2;
> poly f10 = x1^2+x1*x5+x5^2;
> poly f11 = x1^2+x1*x6+x6^2;
> poly f12 = x2^2+x2*x3+x3^2;
> poly f13 = x2^2+x2*x4+x4^2;
> poly f14 = x2^2+x2*x8+x8^2;
> poly f15 = x3^2+x3*x4+x4^2;
> poly f16 = x3^2+x3*x8+x8^2;
> poly f17 = x4^2+x4*x5+x5^2;
> poly f18 = x4^2+x4*x7+x7^2;
> poly f19 = x5^2+x5*x6+x6^2;
> poly f20 = x5^2+x5*x7+x7^2;
> poly f21 = x6^2+x6*x7+x7^2;
> poly f22 = x7^2+x7*x8+x8^2;
> ideal I = f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, f13, f14, f15, f16, f17, f18,
f19, f20, f21, f22;
> std(I);
_[1]=x8^3-1
_[2]=x7^2+x7*x8+x8^2
_[3]=3*x6+x7^4-2*x7^3*x8+x7^2*x8^2
_[4]=3*x5-x6^3*x7-2*x6^2*x7^2+x6*x7^3+2*x7^4
_[5]=3*x4+x5^2*x6*x7-x5^2*x7^2-x6*x7^3+x7^4
_[6]=3*x3+x4^2*x8^2-x4*x5^2*x8-x4*x8^3+x5^2*x7*x8-x6^3*x8-x6^2*x7*x8
-x6*x8^3+3*x8^4
_[7]=3*x2-x3^3*x8-2*x3^2*x8^2+x3*x8^3+2*x8^4
_[8]=3*x1+x5^2*x7*x8-x5^2*x8^2-x6^2*x7*x8+x6^2*x8^2
> option(redSB);
> std(I);
_[1]=x8^3-1
_[2]=x7^2+x7*x8+x8^2
_[3]=x6-x8
_[4]=x5+x7+x8
_[5]=x4-x8
_[6]=x3-x7
_[7]=x2+x7+x8
_[8]=x1-x7

```

Así, $G = \{x_1 - x_7, x_2 + x_7 + x_8, x_3 - x_7, x_4 - x_8, x_5 + x_7 + x_8, x_6 - x_8, x_7^2 + x_7x_8 + x_8^2, x_8^3 - 1\}$. Como $1 \notin G$, tenemos que $V(I) \neq \emptyset$, y por tanto, por el Teorema 6.1, el grafo \mathcal{G} es 3-coloreable. Podemos usar la base de Gröbner G para dar una coloración explícita, ya que el sistema de ecuaciones representado por G resulta fácil de resolver. Supongamos que los 3 colores que estamos usando son azul, rojo y amarillo. Primero debemos elegir un color para x_8 , digamos rojo, ya que el único polinomio en una variable en G es $x_8^3 - 1$. Entonces debemos elegir un color diferente para x_7 , digamos azul, ya que $x_7^2 + x_7x_8 + x_8^2 \in G$. Entonces tenemos que x_1 y x_3 deben ser azules debido a los polinomios $x_1 - x_7 = 0$ y $x_3 - x_7 = 0$, de manera análoga $x_4 - x_8, x_6 - x_8 \in G$, entonces $x_4 - x_8 = 0$ y $x_6 - x_8 = 0$, por lo que x_4 y x_6 deben ser rojos. Finalmente, para los polinomios $x_2 + x_7 + x_8, x_5 + x_7 + x_8 \in G$, igualándolos a cero y restandolos obtenemos $x_2 - x_5 = 0$, así x_2 y x_5 tienen el mismo color, que es un color diferente de los colores asignados a x_7 y x_8 , asignaremos amarillo para x_2 y x_5 . Por lo tanto, el grafo \mathcal{G} queda coloreado de la siguiente forma:

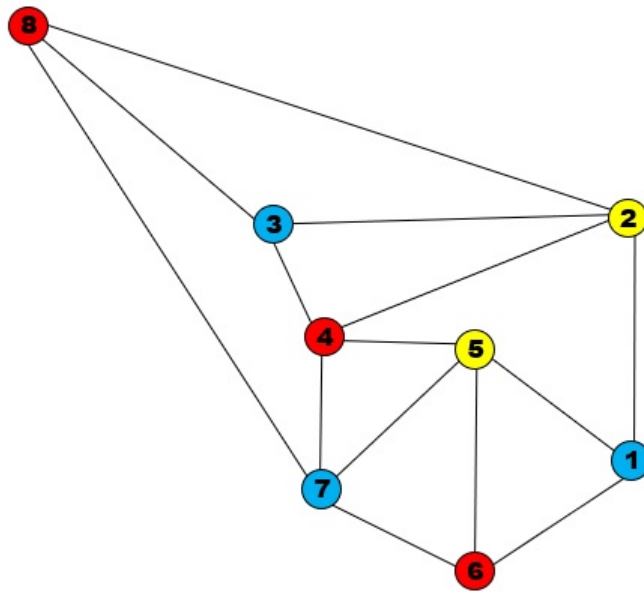


Figura 6.2: Coloración del grafo \mathcal{G}

Note que a partir de la base de Grobner se ha coloreado de manera única el grafo \mathcal{G} , salvo permutación de los colores. El siguiente ejemplo muestra la situación cuando hay más de una manera de colorear un grafo.

6.3 Ejemplo. Considere el grafo \mathcal{G}' de la Figura 6.3.

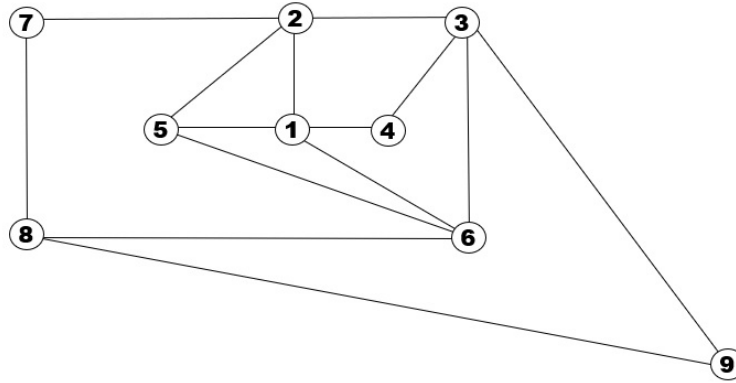


Figura 6.3: Grafo \mathcal{G}'

Los polinomios correspondientes a \mathcal{G}' son $x_i^3 - 1$, para $i = 1, \dots, 9$ y $x_i^2 + x_i x_j + x_j^2$, para las parejas $(i, j) \in \{(1, 2), (1, 4), (1, 5), (1, 6), (2, 3), (2, 5), (2, 7), (3, 4), (3, 6), (3, 9), (5, 6), (6, 8), (7, 8), (8, 9)\}$.

Ahora, calculamos una base de Gröbner G' para el ideal I' generado por los polinomios correspondientes usando el orden lexicográfico con $x_1 > x_2 > \dots > x_8 > x_9$.

```
> ring R=0, (x1,x2,x3,x4,x5,x6,x7,x8,x9), lp;
> poly f1 = x1^3-1;
> poly f2 = x2^3-1;
> poly f3 = x3^3-1;
> poly f4 = x4^3-1;
> poly f5 = x5^3-1;
> poly f6 = x6^3-1;
> poly f7 = x7^3-1;
> poly f8 = x8^3-1;
> poly f9 = x9^3-1;
> poly f10 = x1^2+x1*x2+x2^2;
> poly f11 = x1^2+x1*x4+x4^2;
> poly f12 = x1^2+x1*x5+x5^2;
> poly f13 = x1^2+x1*x6+x6^2;
> poly f14 = x2^2+x2*x3+x3^2;
> poly f15 = x2^2+x2*x5+x5^2;
> poly f16 = x2^2+x2*x7+x7^2;
```

```

> poly f17 = x3^2+x3*x4+x4^2;
> poly f18 = x3^2+x3*x6+x6^2;
> poly f19 = x3^2+x3*x9+x9^2;
> poly f20 = x5^2+x5*x6+x6^2;
> poly f21 = x6^2+x6*x8+x8^2;
> poly f22 = x7^2+x7*x8+x8^2;
> poly f23 = x8^2+x8*x9+x9^2;
> ideal I = f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, f13, f14, f15, f16, f17,
f18, f19, f20, f21, f22, f23;
> std(I);
_[1]=x9^3-1
_[2]=x8^2+x8*x9+x9^2
_[3]=x7^2+x7*x8+x8^2
_[4]=19260*x6+7670*x7^4*x9^3+13835*x7^3*x8*x9^3+16745*x7^3*x9^4
-10030*x7^3*x9+3520*x7^2*x8^2*x9^3+9775*x7^2*x8*x9^4-5440*x7^2*x8*x9
+3710*x7^2*x9^5-75*x7^2*x9^2+51470*x7*x8^3*x9^3-16571*x7*x8^2*x9^4
+25966*x7*x8^2*x9+8695*x7*x8*x9^5-10570*x7*x9^6-20730*x7*x9^3
+8281*x8^3*x9^4-15460*x8^3*x9-1164*x8^2*x9^2+4146*x8*x9^3
_[5]=x5^2+x5*x6+x6^2
_[6]=30*x4*x5*x7-10*x4*x5*x8^3*x9-30*x4*x5*x8^2*x9^2+10*x4*x5*x9^4
+8*x4*x6^3*x7*x8+36*x4*x6^3*x7*x9-80*x4*x6^3*x8*x9+2*x4*x6^3*x9^2
+12*x4*x6^2*x7*x8^2+23*x4*x6^2*x7*x8*x9+25*x4*x6^2*x7*x9^2
-12*x4*x6^2*x8^2*x9+89*x4*x6^2*x8*x9^2-30*x4*x6^2*x9^3+150*x4*x6^2
-3*x4*x6*x7^3*x9-5*x4*x6*x7^2*x8*x9-x4*x6*x7^2*x9^2-9*x4*x6*x7*x8*x9^2
+27*x4*x6*x7*x9^3+29*x4*x6*x8*x9^3-72*x4*x6*x9^4+26*x4*x7^3*x9^2
+22*x4*x7^2*x8*x9^2+68*x4*x7^2*x9^3-34*x4*x7^2-12*x4*x7*x8*x9^3
-60*x4*x7*x9^4-50*x4*x8*x9^4+10*x4*x9^5-60*x4*x9^2-20*x5^3*x6^2*x9
+20*x5^3*x6*x9^2+20*x5^2*x6^3*x9-30*x5^2*x6^2*x9^2+10*x5^2*x6*x9^3
-30*x5*x6^3*x9^2+40*x5*x6^2*x9^3-10*x5*x6*x9^4+20*x6^3*x8*x9^2
-40*x6^3*x9^3-70*x6^2*x8*x9^3+50*x6^2*x9^4-60*x6^2*x9+50*x6*x8*x9^4
-10*x6*x9^5+60*x6*x9^2
_[7]=3*x4^2+x4*x5^3*x9+2*x4*x5^2*x9^2+x4*x5*x6^2*x9-2*x4*x5*x9^3
-x4*x6^2*x8*x9+x4*x8*x9^3-2*x4*x9^4-x5^3*x6*x9+x5^2*x6^2*x9
-2*x5^2*x6*x9^2+2*x5*x6*x9^3+x6^2*x8*x9^2-2*x6^2*x9^3-x6*x8*x9^3
+2*x6*x9^4
_[8]=3*x3*x7-x3*x8^3*x9-2*x3*x8^2*x9^2+x3*x8*x9^3+2*x3*x9^4+x5^3*x8*x9
+2*x5^3*x9^2+x5^2*x6*x8*x9+2*x5^2*x6*x9^2+x5^2*x7*x8*x9+2*x5^2*x7*x9^2
-x5*x7^2*x8*x9-2*x5*x7^2*x9^2-x6^2*x8*x9^2-2*x6^2*x9^3+x6*x8*x9^3

```

```

+2*x6*x9^4+x7*x8*x9^3+2*x7*x9^4
_[9]=x3*x4-x3*x9+x4^2-x9^2
_[10]=x3^2+x3*x9+x9^2
_[11]=3*x2-3*x3^2*x6*x7+3*x3^2*x6*x9+3*x3^2*x7*x9-3*x3^2*x9^2+x5^3*x7
-3*x5^3*x9+x5^2*x6*x7-3*x5^2*x6*x9-3*x5^2*x7*x9+x5*x6^2*x7+3*x5*x7^2*x9
+3*x7^2*x9^2
_[12]=3*x1-x5^3*x6-2*x5^2*x6^2+x5*x6^3+2*x6^4
> option(redSB);
> std(I);
_[1]=x9^3-1
_[2]=x8^2+x8*x9+x9^2
_[3]=x7^2+x7*x8-x8*x9-x9^2
_[4]=x6+x7+x8
_[5]=x5^2-x5*x7-x5*x8+x7*x8
_[6]=x4*x5*x7+x4*x5*x8+x4*x5*x9-x4*x7*x9-x4*x8*x9-x4*x9^2
+x5*x7*x8+x5*x7*x9+x5*x8*x9-x7*x8*x9-x7*x9^2-x8*x9^2
_[7]=x4^2-x4*x5+x4*x7+x4*x8-x5*x7-x5*x8
_[8]=x3*x7+x3*x8+x3*x9-x7*x8+x9^2
_[9]=x3*x4-x3*x9+x4*x5-x4*x7-x4*x8+x5*x7+x5*x8-x9^2
_[10]=x3^2+x3*x9+x9^2
_[11]=x2+x7+x8
_[12]=x1+x5-x7-x8

```

Así, $G' = \{x_9^3 - 1, x_8^2 + x_8x_9 + x_9^2, (x_7 - x_9)(x_7 + x_8 + x_9), x_6 + x_7 + x_8, (-x_5 + x_7)(-x_5 + x_8), (x_5 - x_9)(x_4x_7 + x_4x_8 + x_7x_8 + x_4x_9 + x_7x_9 + x_8x_9), (x_4 - x_5)(x_4 + x_7 + x_8), x_3x_7 + x_3x_8 - x_7x_8 + x_3x_9 + x_9^2, x_3x_4 + x_4x_5 - x_4x_7 + x_5x_7 - x_4x_8 + x_5x_8 - x_3x_9 - x_9^2, x_3^2 + x_3x_9 + x_9^2, x_2 + x_7 + x_8, x_1 + x_5 - x_7 - x_8\}$. Como $1 \notin G'$, tenemos que $V(I') \neq \emptyset$, y por lo tanto, por el Teorema 6.1, el grafo \mathcal{G}' es 3-coloreable.

Esta base de Gröbner parece mucho más complicada que la del Ejemplo 6.2. Para colorear el grafo \mathcal{G}' supongamos que los 3 colores que estamos usando son amarillo, azul y rojo. Elegimos amarillo para x_9 , veamos que si $x_9^3 - 1 = 0$, tenemos $x_9 = 1$, entonces $x_8^2 + x_8x_9 + x_9^2 = x_8^2 + x_8 + 1 = 0$ y $x_3^2 + x_3x_9 + x_9^2 = x_3^2 + x_3 + 1 = 0$, así x_3 y x_8 se colorean del mismo color que será rojo. Luego, de los polinomios $(x_7 - x_9)(x_7 + x_8 + x_9)$, $(-x_5 + x_7)(-x_5 + x_8)$, $(x_5 - x_9)(x_4x_7 + x_4x_8 + x_7x_8 + x_4x_9 + x_7x_9 + x_8x_9)$, $(x_4 - x_5)(x_4 + x_7 + x_8) \in G$, obtenemos que $x_7 = x_9 = x_5 = x_4$, así x_4, x_5 y x_7 se colorean de amarillo. Al restar los polinomios $x_6 + x_7 + x_8 = 0$ y $x_2 + x_7 + x_8 = 0$, obtenemos que x_6 y x_2 son del mismo color, les asignaremos azul. Por último, $x_1 + x_5 - x_7 - x_8 = 0$, como x_5 y x_7 son iguales tenemos

que $x_1 - x_8 = 0$, coloreando a x_1 y x_8 de rojo.

Con lo anterior, en la Figura 6.4 se muestra una forma de colorear el grafo \mathcal{G}'

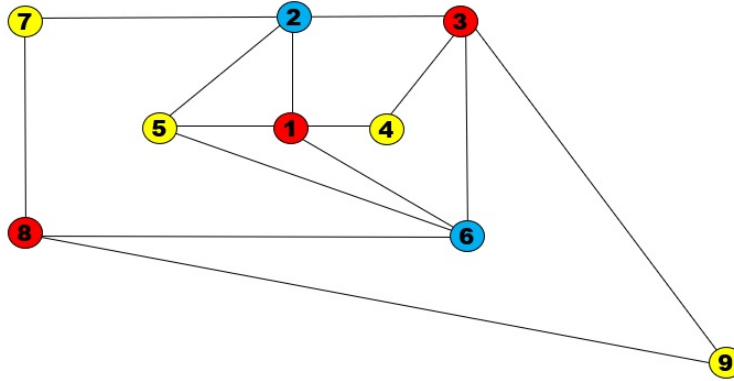


Figura 6.4: Coloración del grafo \mathcal{G}'

Mostraremos otras dos soluciones para nuestra base de Gröbner G' generada por los polinomios del grafo \mathcal{G}' , una de ellas es:

$$x_9 = -(-1)^{1/3} \text{ ó } x_9 = (-1)^{2/3}, x_8 = 1 \text{ ó } x_8 = -1 - x_9, x_7 = x_9, x_6 = -x_8 - x_9, \\ x_5 = x_9, x_4 = -x_8 - x_9, x_3 = x_8 \text{ y } x_1 = x_8.$$

Es decir, $x_9 = x_7 = x_5$, $x_2 = x_4 = x_6$ y $x_1 = x_3 = x_8$, donde les asignamos los colores rojo, amarillo y azul respectivamente obteniendo la siguiente coloración de la Figura 6.5

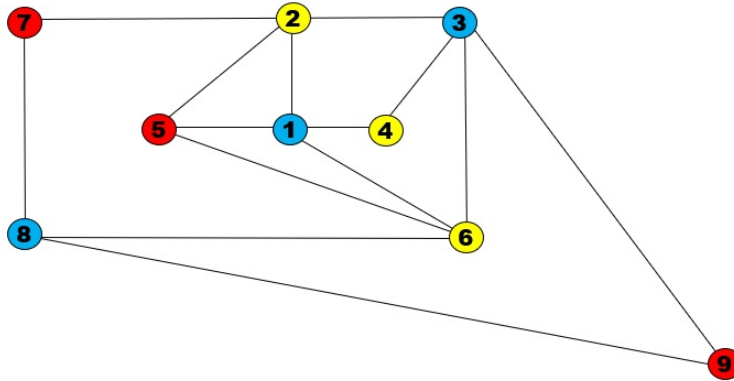


Figura 6.5: Segunda coloración del grafo \mathcal{G}'

Otra solución a la base de Gröbner es: $x_9 = -(-1)^{1/3} \text{ ó } x_9 = (-1)^{2/3}$, $x_8 = 1 \text{ ó } x_8 = -1 - x_9$, $x_7 = -x_8 - x_9$, $x_6 = x_9$, $x_5 = -x_8 - x_9$, $x_4 x_7 = -x_8 - x_9$, $x_4 = -x_8 - x_9$, $x_3 = x_8$, $x_2 = x_9$ y $x_1 = x_8$.

Se sigue que $x_1 = x_3 = x_8$, $x_2 = x_6 = x_9$ y $x_4 = x_5 = x_7$, asignando los colores amarillo, rojo y azul respectivamente, dando como resultado la siguiente coloración de la Figura 6.6

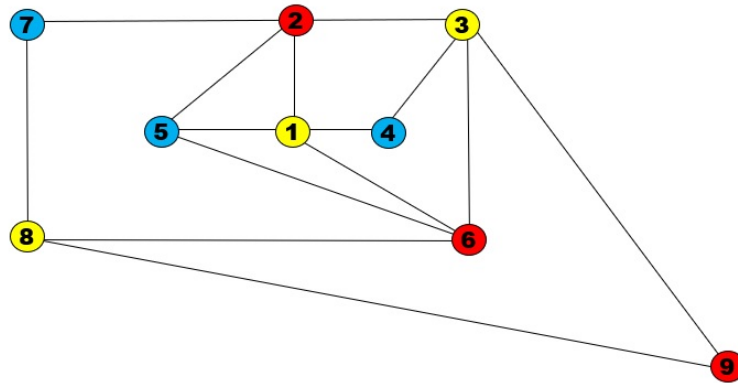


Figura 6.6: Tercera coloración del grafo \mathcal{G}'

Notemos que hemos obtenido distintas coloraciones no isomorfas para colorear el grafo \mathcal{G}' .

6.4 Ejemplo. Demostremos que si sumamos una arista entre x_2 y x_5 en la gráfica \mathcal{G} no es de 3-coloreable.

Si se añade una arista entre x_2 y x_5 en el grafo \mathcal{G} , obtenemos el grafo \mathcal{H} como muestra la Figura 6.7

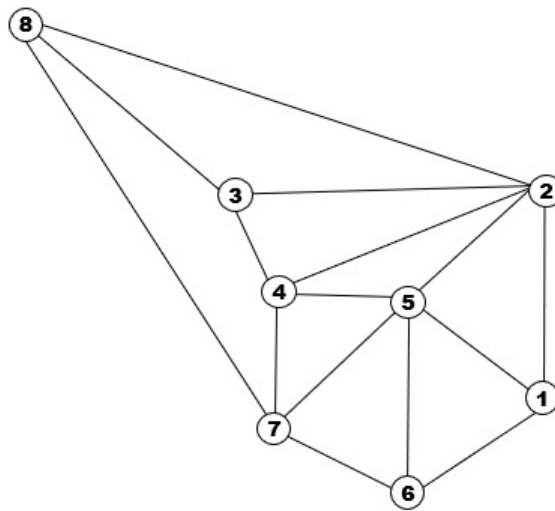


Figura 6.7: Grafo \mathcal{H}

Los polinomios correspondientes a \mathcal{H} son $x_i^3 - 1$, para $i = 1, \dots, 8$ y $x_i^2 + x_i x_j + x_j^2$, para las parejas $(i, j) \in \{(1, 2), (1, 5), (1, 6), (2, 3), (2, 4), (2, 8), (3, 4), (3, 8), (4, 5), (4, 7), (5, 2), (5, 6), (5, 7), (6, 7), (7, 8)\}$.

Notemos que los polinomios que corresponden al grafo \mathcal{H} son los mismos polinomios que corresponden al grafo \mathcal{G} y solo le añadimos el polinomio $x_5^2 + x_5x_2 + x_2^2$.

A continuación se muestra el código para obtener una base de Gröbner para el grafo \mathcal{H}

```
> ring R=0, (x1,x2,x3,x4,x5,x6,x7,x8), lp;
> poly f1 = x1^3-1;
> poly f2 = x2^3-1;
> poly f3 = x3^3-1;
> poly f4 = x4^3-1;
> poly f5 = x5^3-1;
> poly f6 = x6^3-1;
> poly f7 = x7^3-1;
> poly f8 = x8^3-1;
> poly f9 = x1^2+x1*x2+x2^2;
> poly f10 = x1^2+x1*x5+x5^2;
> poly f11 = x1^2+x1*x6+x6^2;
> poly f12 = x2^2+x2*x3+x3^2;
> poly f13 = x2^2+x2*x4+x4^2;
> poly f14 = x2^2+x2*x8+x8^2;
> poly f15 = x3^2+x3*x4+x4^2;
> poly f16 = x3^2+x3*x8+x8^2;
> poly f17 = x4^2+x4*x5+x5^2;
> poly f18 = x4^2+x4*x7+x7^2;
> poly f19 = x5^2+x5*x2+x2^2;
> poly f20 = x5^2+x5*x6+x6^2;
> poly f21 = x5^2+x5*x7+x7^2;
> poly f22 = x6^2+x6*x7+x7^2;
> poly f23 = x7^2+x7*x8+x8^2;
> ideal I = f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, f13, f14, f15, f16, f17,
f18, f19, f20, f21, f22, f23;
> std(I);
_[1]=1
```

Así, $G = \{1\}$, por Teorema 3.15 $V(I) = \emptyset$, se concluye que el grafo \mathcal{H} no es 3-coloreable.

6.5 Definición. Sea \mathcal{G} un grafo simple y no dirigido, con vértices $V_{\mathcal{G}} = \{1, \dots, n\}$ y aristas $E_{\mathcal{G}}$. Llamaremos ideal de q -coloraciones de el grafo \mathcal{G} al ideal $I_{\mathcal{G},q} \subset \mathbb{C}[x_1, \dots, x_n]$ generado por

$$x_i^q - 1, \text{ para todo } i \in V_{\mathcal{G}},$$

$$x_i^{q-1} + x_i^{q-2}x_j + \dots + x_ix_j^{q-2} + x_j^{q-1} \text{ para todo } (i, j) \in E.$$

6.6 Lema. $V(I_{\mathcal{G},q}) \subset \mathbb{C}^n$ está formado por todas las q -coloraciones de \mathcal{G} , siendo el conjunto de colores las q -ésimas raíces de la unidad.

Demostración. La variedad $V(I_{\mathcal{G},q})$ está formada por los puntos de \mathbb{C}^n que anulan todas las ecuaciones de polinomios de $I_{\mathcal{G},q}$, igualados a cero. El polinomio $x_i^q - 1$ se anula si y sólo si, el vértice i es una raíz q -ésima de la unidad, es decir, un color.

Además, los polinomios $x_i^{q-1} + x_i^{q-2}x_j + \dots + x_ix_j^{q-2} + x_j^{q-1}$ serán cero únicamente si los vértices i y j tienen colores distintos, ya que

$$x_i^{q-1} + x_i^{q-2}x_j + \dots + x_ix_j^{q-2} + x_j^{q-1} = \frac{(x_i^q - 1) - (x_j^q - 1)}{x_i - x_j}.$$

□

6.7 Ejemplo. Veamos que el grafo \mathcal{H} del ejemplo 6.4 es 4-coloreable.

Primero, introducimos los polinomios pertenecientes al grafo \mathcal{H} , generando el siguiente código:

```
> ring R=0, (x1,x2,x3,x4,x5,x6,x7,x8), lp;
> poly f1 = x1^4-1;
> poly f2 = x2^4-1;
> poly f3 = x3^4-1;
> poly f4 = x4^4-1;
> poly f5 = x5^4-1;
> poly f6 = x6^4-1;
> poly f7 = x7^4-1;
> poly f8 = x8^4-1;
> poly f9 = x1^3+x1^2*x2+x1*x2^2+x2^3;
> poly f10 = x1^3+x1^2*x5+x1*x5^2+x5^3;
> poly f11 = x1^3+x1^2*x6+x1*x6^2+x6^3;
> poly f12 = x2^3+x2^2*x3+x2*x3^2+x3^3;
> poly f13 = x2^3+x2^2*x4+x2*x4^2+x4^3;
> poly f14 = x2^3+x2^2*x5+x2*x5^2+x5^3;
> poly f15 = x2^3+x2^2*x8+x2*x8^2+x8^3;
> poly f16 = x3^3+x3^2*x4+x3*x4^2+x4^3;
> poly f17 = x3^3+x3^2*x8+x3*x8^2+x8^3;
> poly f18 = x4^3+x4^2*x5+x4*x5^2+x5^3;
```

```
> poly f19 = x4^3+x4^2*x7+x4*x7^2+x7^3;
> poly f20 = x5^3+x5^2*x6+x5*x6^2+x6^3;
> poly f21 = x5^3+x5^2*x7+x5*x7^2+x7^3;
> poly f22 = x6^3+x6^2*x7+x6*x7^2+x7^3;
> poly f23 = x7^3+x7^2*x8+x7*x8^2+x8^3;
> ideal I = f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, f13, f14, f15, f16, f17, f18,
f19, f20, f21, f22, f23;
```

Ahora, calculamos una base de Gröbner reducida para nuestra grafo \mathcal{H}

```
> option(redSB);
> std(I);
_[1]=x8^4-1
_[2]=x7^3+x7^2*x8+x7*x8^2+x8^3
_[3]=x6^3+x6^2*x7+x6*x7^2-x7^2*x8-x7*x8^2-x8^3
_[4]=x5^2+x5*x6+x5*x7+x6^2+x6*x7+x7^2
_[5]=x4^2+x4*x5+x4*x7-x5*x6-x6^2-x6*x7
_[6]=x3*x4*x6^2+x3*x4*x6*x7+x3*x4*x6*x8+x3*x4*x7^2+x3*x4*x7*x8+x3*x4*x8^2
-x3*x6^2*x8-x3*x6*x7*x8-x3*x6*x8^2-x3*x7^2*x8-x3*x7*x8^2-x3*x8^3
-x4*x5*x6^2-x4*x5*x6*x7-x4*x5*x6*x8-x4*x5*x7^2-x4*x5*x7*x8-x4*x5*x8^2
+x5*x6^2*x8+x5*x6*x7*x8+x5*x6*x8^2+x5*x7^2*x8+x5*x7*x8^2+x5*x8^3
_[7]=x3*x4*x5-x3*x4*x8-x3*x5*x8+x3*x8^2+x4*x5*x6+x4*x5*x7+x4*x5*x8+x4*x6^2
+x4*x6*x7+x4*x7^2-x5*x6*x8-x5*x7*x8-x5*x8^2-x6^2*x8-x6*x7*x8-x7^2*x8
_[8]=x3^2*x5*x6-x3^2*x5*x8+x3^2*x6^2+x3^2*x6*x7-x3^2*x7*x8-x3^2*x8^2
-x3*x4*x7^2-2*x3*x4*x7*x8-3*x3*x4*x8^2+2*x3*x5*x6*x8-2*x3*x5*x8^2
+2*x3*x6^2*x8+2*x3*x6*x7*x8+x3*x7^2*x8+x3*x8^3-x4*x5*x6*x7
+x4*x5*x6*x8+x4*x5*x7^2+3*x4*x5*x7*x8+2*x4*x5*x8^2-x4*x6^2*x7+x4*x6^2*x8
-x4*x6*x7^2+x4*x6*x7*x8+x4*x7^2*x8-x4*x8^3-x5*x6*x7^2-x5*x6*x7*x8
-x5*x6*x8^2-x5*x7*x8^2-2*x5*x8^3-x6^2*x7^2-x6^2*x7*x8-x6^2*x8^2
+x6*x8^3+x7^2*x8^2+x7*x8^3
_[9]=x3^2*x4-x3^2*x8-x3*x4*x7-x3*x4*x8+x3*x5*x6-x3*x5*x8+x3*x6^2+x3*x6*x7
+x4*x5*x6+2*x4*x5*x7+x4*x5*x8+x4*x6^2+x4*x6*x7+x4*x7^2-x5*x6*x7
-x5*x6*x8-x5*x7*x8-x5*x8^2-x6^2*x7-x6^2*x8-x6*x7^2-x6*x7*x8+x7*x8^2
_[10]=x3^3+x3^2*x8+x3*x8^2+x8^3
_[11]=x2*x5*x6-x2*x5*x8+x2*x6^2+x2*x6*x7-x2*x7*x8-x2*x8^2+x3*x5*x6
-x3*x5*x8+x3*x6^2+x3*x6*x7-x3*x7*x8-x3*x8^2+x4*x5*x6-x4*x5*x8+x4*x6^2
+x4*x6*x7-x4*x7*x8-x4*x8^2+x5*x6*x8-x5*x8^2+x6^2*x8+x6*x7*x8-x7*x8^2-x8^3
_[12]=x2*x4-x2*x8+x3*x4-x3*x8-x4*x5-x4*x7+x5*x6+x6^2+x6*x7-x8^2
_[13]=x2*x3-x2*x5+x3^2+x3*x4-x4*x5+x5*x6+x5*x7+x6^2+x6*x7+x7^2
```

$$\begin{aligned}
 _ [14] &= x_2^2 + x_2 * x_5 + x_2 * x_8 - x_3 * x_4 + x_3 * x_8 + x_4 * x_5 - x_5 * x_6 - x_5 * x_7 - x_6^2 - x_6 * x_7 - x_7^2 + x_8^2 \\
 _ [15] &= x_1 * x_6^2 + x_1 * x_6 * x_7 + x_1 * x_6 * x_8 + x_1 * x_7^2 + x_1 * x_7 * x_8 + x_1 * x_8^2 + x_2 * x_6^2 + x_2 * x_6 * x_7 \\
 &+ x_2 * x_6 * x_8 + x_2 * x_7^2 + x_2 * x_7 * x_8 + x_2 * x_8^2 + x_5 * x_6^2 + x_5 * x_6 * x_7 + x_5 * x_6 * x_8 + x_5 * x_7^2 \\
 &+ x_5 * x_7 * x_8 + x_5 * x_8^2 + x_6^2 * x_8 + x_6 * x_7 * x_8 + x_6 * x_8^2 + x_7^2 * x_8 + x_7 * x_8^2 + x_8^3 \\
 _ [16] &= x_1 * x_4 + x_1 * x_5 + x_1 * x_6 + x_1 * x_7 + x_2 * x_5 + x_2 * x_6 + x_2 * x_7 + x_2 * x_8 - x_3 * x_4 + x_3 * x_8 + 2 * x_4 * x_5 \\
 &+ x_4 * x_6 + x_4 * x_7 - x_6^2 - x_6 * x_7 - x_7^2 + x_8^2 \\
 _ [17] &= x_1 * x_3 * x_5 + x_1 * x_3 * x_6 + x_1 * x_3 * x_7 + x_1 * x_3 * x_8 - x_1 * x_5 * x_7 - x_1 * x_6 * x_7 - x_1 * x_7^2 \\
 &- x_1 * x_7 * x_8 - x_2 * x_5 * x_7 + x_2 * x_5 * x_8 - x_2 * x_6^2 - 2 * x_2 * x_6 * x_7 - 2 * x_2 * x_7^2 - x_2 * x_7 * x_8 \\
 &- x_3^2 * x_5 - x_3^2 * x_6 - x_3^2 * x_7 - x_3^2 * x_8 - x_3 * x_4 * x_6 - x_3 * x_4 * x_7 - 2 * x_3 * x_4 * x_8 + x_3 * x_5 * x_6 \\
 &+ x_3 * x_6 * x_8 - x_3 * x_7^2 + x_3 * x_8^2 + x_4 * x_5 * x_6 + x_4 * x_5 * x_7 + 2 * x_4 * x_5 * x_8 - x_5 * x_6^2 - 2 * x_5 * x_6 * x_7 \\
 &- 2 * x_5 * x_6 * x_8 - x_5 * x_7^2 - 3 * x_5 * x_7 * x_8 - x_5 * x_8^2 - 2 * x_6^2 * x_8 - 3 * x_6 * x_7 * x_8 - 3 * x_7^2 * x_8 \\
 &- x_7 * x_8^2 - x_8^3 \\
 _ [18] &= x_1 * x_3^2 + x_1 * x_3 * x_6 + x_1 * x_3 * x_8 - x_1 * x_6 * x_7 - x_1 * x_7^2 - x_1 * x_7 * x_8 - x_2 * x_5 * x_7 + x_2 * x_5 * x_8 \\
 &- x_2 * x_6^2 - 2 * x_2 * x_6 * x_7 - 2 * x_2 * x_7^2 - x_2 * x_7 * x_8 - x_3^2 * x_8 - x_3 * x_4 * x_6 - x_3 * x_4 * x_7 - 2 * x_3 * x_4 * x_8 \\
 &+ x_3 * x_5 * x_6 - x_3 * x_5 * x_7 + x_3 * x_6^2 + x_3 * x_6 * x_8 - x_3 * x_7^2 + x_3 * x_8^2 + x_4 * x_5 * x_6 + x_4 * x_5 * x_7 \\
 &+ 2 * x_4 * x_5 * x_8 - x_5 * x_6^2 - 2 * x_5 * x_6 * x_7 - 2 * x_5 * x_6 * x_8 - x_5 * x_7^2 - 3 * x_5 * x_7 * x_8 - x_5 * x_8^2 \\
 &- x_6^2 * x_7 - 2 * x_6^2 * x_8 - x_6 * x_7^2 - 3 * x_6 * x_7 * x_8 - 2 * x_7^2 * x_8 \\
 _ [19] &= x_1 * x_2 - x_1 * x_6 - x_2 * x_8 + x_3 * x_4 - x_3 * x_8 - x_4 * x_5 + x_5 * x_7 + x_6 * x_7 + x_7^2 - x_8^2 \\
 _ [20] &= x_1^2 + x_1 * x_5 + x_1 * x_6 - x_5 * x_7 - x_6 * x_7 - x_7^2
 \end{aligned}$$

Mostraremos algunas soluciones a la base de Gröbner reducida dado 4 colores, Sean verde, amarillo, azul y rojo.

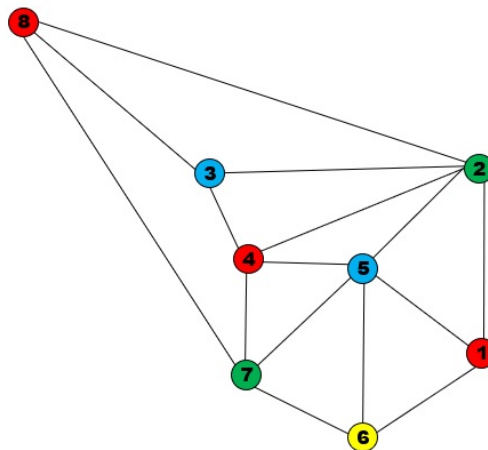


Figura 6.8: Primera coloración del grafo \mathcal{H}

- (i) En la primera solución obtenemos que $x_1 = 1$, $x_2 = -i$, $1 + x_3 = 0$, $x_4 = 1$, $1 + x_5 = 0$, $x_7 = -i$, $x_6 + x_7 = 0$ y $x_8 = 1$, entonces $x_1 = 1 = x_4 = x_8$, $x_2 = -i = x_7$, $x_3 = -1 = x_5$ y $x_6 = i = -x_7$. Por lo tanto, dado los 4 colores, a x_1 , x_4 y x_8 los coloreamos de

rojo, x_2 y x_7 los coloreamos de verde, x_3 y x_5 los coloreamos de azul y por último, coloreamos de amarillo a x_6 como se muestra en la Figura 6.8.

- (ii) Una segunda solución a la base de Gröbner reducida es $1 + x_2 = 0$, $x_5 = i$, $x_5 = x_3$, $x_1 + x_5 = 0$, $x_4 + x_5 = 0$, $x_6 = 1$, $1 + x_7 = 0$ y $x_8 = 1$. Así, $x_1 = -i = x_4$, $x_2 = -1 = x_7$, $x_5 = i = x_3$ y $x_6 = 1 = x_8$. Entonces, le asignamos el color verde a x_1 y x_4 , azul a x_2 y x_7 , rojo a x_3 y x_5 y amarillo para x_6 y x_8 como se muestra en la Figura 6.9

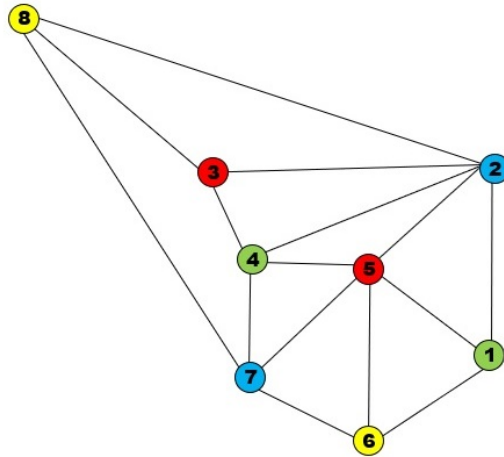


Figura 6.9: Segunda coloración del grafo \mathcal{H}

- (iii) Otra solución es $1 + x_3 = 0$, $x_2 + x_3 = 0$, $x_7 = 1$, $x_6 + x_7 = 0$, $x_8 = i$, $x_8 = x_5$, $x_1 + x_8 = 0$, $x_4 + x_8 = 0$, resultando $x_3 = 1 = x_7$, $x_2 = -1 = x_6$, $x_5 = i = x_8$ y $x_1 = -i = x_4$. Se concluye que x_3 y x_7 amarillos, x_2 y x_6 son rojos, x_5 y x_8 son verdes y x_1 y x_4 son azules. como se muestra en la Figura 6.10

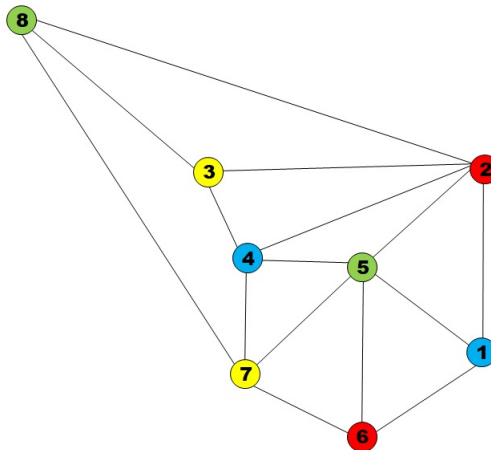


Figura 6.10: Tercera coloración del grafo \mathcal{H}

6.8 Ejemplo. Veamos que el grafo \mathcal{J} no es 4-coloreable.

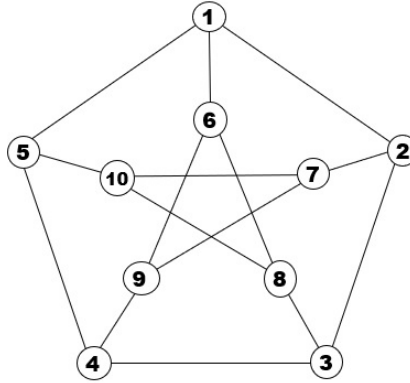


Figura 6.11: Grafo \mathcal{J}

```

> ring R=0, (x1,x2,x3,x4,x5,x6,x7,x8,x9,x10), lp;
> poly f1 = x1^4-1;
> poly f2 = x2^4-1;
> poly f3 = x3^4-1;
> poly f4 = x4^4-1;
> poly f5 = x5^4-1;
> poly f6 = x6^4-1;
> poly f7 = x7^4-1;
> poly f8 = x8^4-1;
> poly f9 = x9^4-1;
> poly f10 = x10^4-1;
> poly f11 = x1^3+x1^2*x2+x1*x2^2+x2^3;
> poly f12 = x1^3+x1^2*x5+x1*x5^2+x5^3;
> poly f13 = x1^3+x1^2*x6+x1*x6^2+x6^3;
> poly f14 = x2^3+x2^2*x3+x2*x3^2+x3^3;
> poly f15 = x2^3+x2^2*x7+x2*x7^2+x7^3;
> poly f16 = x3^3+x3^2*x4+x3*x4^2+x4^3;
> poly f17 = x3^3+x3^2*x8+x3*x8^2+x8^3;
> poly f18 = x4^3+x4^2*x5+x4*x5^2+x5^3;
> poly f19 = x4^3+x4^2*x9+x4*x9^2+x9^3;
> poly f20 = x5^3+x5^2*x10+x5*x10^2+x10^3;
> poly f21 = x6^3+x6^2*x8+x6*x8^2+x8^3;
> poly f22 = x6^3+x6^2*x9+x6*x9^2+x9^3;

```

```
> poly f23 = x7^3+x7^2*x9+x7*x9^2+x9^3;
> poly f24 = x7^3+x7^2*x10+x7*x10^2+x10^3;
> poly f25 = x8^3+x8^2*x10+x8*x10^2+x10^3;
> ideal I = f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, f13, f14, f15, f16, f17, f18,
f19, f20, f21, f22, f23, f24, f25;
> std(I);
_[1]=1
```

Así, $G = \{1\}$, por Teorema 3.15 $V(I) = \emptyset$, se concluye que el grafo \mathcal{H} no es 4-coloreable.

Capítulo 7

Conclusiones

Todo problema que pueda expresarse mediante ecuaciones polinómicas puede resolverse con la teoría de las bases de Gröbner.

Con el hecho de que todo ideal tiene un conjunto finito de generadores por el teorema de la base de Hilbert 2.4, uno de los principales objetivos del Capítulo 2 es definir y calcular bases de Gröbner, haciendo uso del Criterio de Buchberger, se puede mostrar si una base dada es de Gröbner. Mas aún, el algoritmo de Buchberger sigue la misma ideal que el criterio de Buchberger usando la definición de S -polinomio, a diferencia de que el algoritmo de Buchberger nos dice que se puede extender una base de Gröbner sumando sucesivamente los restos distintos de cero.

Por otro lado, la base de Gröbner no es única, puede cambiar dependiendo el orden de las variables sobre el anillo en el que estamos trabajando y el orden monomial. En este trabajo se puede observar que calculamos bases de Gröbner usando el orden lexicográfico si nuestro interés era eliminar variables y encontrar soluciones o el orden lexicográfico graduado si solo queremos generar una base. Mas aún, la base de Gröbner puede ser una base generada por una gran cantidad de polinomios y al calcular la base de Gröbner reducida simplificamos los polinomios que pertenecen a ella.

En el Capítulo 3 consideramos las variedades, y se presentaron los teoremas de los ceros de Hilbert en donde las demostraciones son mas sencillas de entender con nuestra teoría, en consecuencia se tiene el Teorema 3.15, este teorema es muy importante para saber el comportamiento entre la base de Gröbner generada por el ideal I y la variedad de I . Por ejemplo, en el Capítulo 6 el Teorema 6.1 nos dice que un grafo es coloreable si y sólo si la variedad del ideal es distinta de cero, este teorema junto con el Teorema 3.15 nos dice que si la base de Gröbner es $\{1\}$, entonces

no hay soluciones para el sistema de ecuaciones polinómicas, es decir, la variedad es igual al conjunto vacío y el grafo no es coloreable, en caso contrario, si la base de Gröbner no es $\{1\}$, entonces hay soluciones para el sistema de ecuaciones polinómicas, es decir, la variedad es distinta del conjunto vacío y en consecuencia el grafo es coloreable.

En el Capítulo 4 atendemos a dos problemas en los brazos de robot. En el problema cinemático directo obtenemos la configuración de la mano mediante un sistema de coordenadas y en el problema cinemático inverso nos interesa encontrar las posibles posiciones de la mano en el espacio de configuraciones usando la base de Gröbner, de modo que al tener valores arbitrarios como la longitud de eslabones y la coordenada de la mano entramos a un problema de especialización, y por cada condición tendremos una base de Gröbner resultando diferentes posiciones de la mano. El objetivo principal es instruir al robot qué configuración debe realizar la articulación para llevar la mano de una posición a otra.

Asimismo, en el Capítulo 5 se estudiaron dos métodos para poder probar la veracidad de un teorema. En el primer método, se tiene que hacer la descomposición minimal de la variedad y excluir los casos degenerados y en el segundo método se usa el Corolario 5.9, que es el resultado del Teorema 5.4 y la Proposición 5.8.

Mostramos que las bases de Gröbner inducen una variedad, por lo cual podemos usar bases de Gröbner para obtener componentes irreducibles de una variedad. Por otro lado, en el Capítulo 5 era necesario que la base de Gröbner fuese $\{1\}$ para que la conclusión se deduciera estrictamente de las hipótesis por el Teorema 5.4 y el Corolario 5.9, es decir, estamos hablando de pertenencia en el radical del ideal. Sin embargo, en el Capítulo 6 Coloración de Grafos al ser $\{1\}$ la base de Gröbner el grafo no es coloreable debido a que la variedad del ideal es igual al vacío por el Teorema 3.15, esto implicaba que no habían soluciones para nuestras variables. En resumen, podemos usar las bases de Gröbner para resolver sistemas de ecuaciones polinómicas, pertenencia a ideales, cálculo de componentes irreducibles de variedades y en demostraciones automáticas de teoremas.

Bibliografía

- [1] Adams, W.W. and Loustaunau, P. *An Introduction to Gröbner Bases*. American Mathematical Society, 1994.
- [2] Cox, D. Little, J. and O’Shea, D. *Ideals, Varieties, and algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Fourth edition, Undergraduate Texts in Mathematics, Springer, Cham, 2015.
- [3] B. Buchberger, *An algorithm for finding a basis for the residue class ring of a zero-dimensional ideal*, Ph. D. Thesis, Univ. of Innsbruck, Math. Inst., 1965.
- [4] B. Buchberger, *Groebner Bases: An Algorithmic Method in Polynomial Ideal Theory*, in *Multidimensional Systems Theory*, ed. by N.K. Bose (D. Reidel Publishing, Dordrecht, 1985), pp. 184–232
- [5] F. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. 26 (1927), 531–555.
- [6] W. Grobner, *uber die algebraischen Eigenschaften der Integrale von linearen Differentialgleichungen mit konstanten Koeffizienten*, Monatsh. der Math. 47 (1393), 247–284.
- [7] F. Bombai, *David Hilbert: La búsqueda de la certidumbre*, Rev. Real Academia de Ciencias Exactas, Físicas y Naturales de España, vol. 106 (2013).
- [8] D. S. Moran, *Una introducción a las Bases de Gröbner*. Boletín de Matemáticas, 26(2), 71–86. (2020). Disponible en <https://revistas.unal.edu.co/index.php/bolma/article/view/85543>
- [9] D. Hilbert, *“uber die theorie del algebraischen formen*, Math. Ann. 36 (1890), 473–534, Reprinted in *Gesammelte Abhandlungen*, Volume II, Chelsea, New York (1965).
- [10] D. Hilber, *uber die vollen invariantensysteme*, Math. Ann. 42 (1893), 313–373, Reprinted in: *Theory of Algebraic Invariants*, Cambridge University Press, Cambridge (1993).
- [11] D. Bayer, *The Division Algorithm and the Hilbert Scheme*, Ph.D. Thesis, Harvard University, Cambridge, MA, 1982.

- [12] P. Gordan, *Newer beweis des hilbertschen satzes über homogene funktionen*, Nachrichten Königl. Ges. Der. Wiss. Zu Göttingen, 1899, 240-242.
- [13] J. Baillieul et al., *Robotics. In: Proceedings of Symposia in Applied Mathematics*, vol. 41 (American Mathematical Society, Providence, Rhode Island, 1990)
- [14] R. Paul, *Robot Manipulators: Mathematics, Programming and Control* (MIT Press, Cambridge, MA, 1981)
- [15] Martínez, X. G. *Bases de Gröbner*, Tesis de Licenciatura, Universidad de Santiago de Compostela, Xullo, 2012.
- [16] Seidenberg, *Constructions in algebra*. Trans. Am. Math. Soc. 197, 273–313 (1974)
- [17] Windfeldt, T. *Computational Aspects of Graph Coloring and the Quillen–Suslin Theorem*. Ph. D. Thesis, University of Copenhagen, 2009.
- [18] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann. SINGULAR 4.3.1 A computer algebra system for polynomial computations. <https://www.singular.uni-kl.de:8003/>, 2022.