Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

TRIANGULACIÓN DE SISTEMAS DE ECUACIONES POLINÓMICAS

Autor: David Villacorta Nicolás

Tutor: José Ignacio Farrán Martín

Año: 2025

A Carmen y Miguel.
Sin vosotros no estaría aquí.

Resumen

Los sistemas de ecuaciones polinómicas suelen ser complejos y difíciles de resolver. En este trabajo se estudia la triangulación, una técnica algebraica que permite transformar estos sistemas en una colección de sistemas triangulares, en los que cada ecuación involucra un número creciente de variables. Para ello, se abordará primero el estudio de las bases de Groebner, una herramienta fundamental en álgebra computacional que sirve como punto de partida para los algoritmos de triangulación considerados. Estos algoritmos son dos: el algoritmo de Lazard y el de Möller, ambos con implementaciones en el software algebraico `SINGULAR`. Para cada uno de ellos se estudia su marco teórico, ilustrándolos con ejemplos concretos en `SINGULAR`.

Palabras clave: Sistemas de ecuaciones polinómicas, Triangulación, Sistemas triangulares, Ideales, Bases de Groebner, Algoritmo de Möller, Algoritmo de Lazard, `SINGULAR`.

Abstract

Polynomial equation systems are often complex and difficult to solve. This work studies triangulation, an algebraic technique that transforms such systems into a collection of triangular systems, where each equation involves an increasing number of variables. To this end, we first address the study of Gröbner bases, a fundamental tool in computational algebra that serves as the starting point for the triangulation algorithms considered. These algorithms are Lazard's algorithm and Möller's algorithm, both implemented in the algebraic software `SINGULAR`. For each of them, we examine their theoretical foundations, illustrating them with concrete examples in `SINGULAR`.

Keywords: Polynomial systems, Triangulation, Triangular systems, Ideals, Gröbner bases, Möller's algorithm, Lazard's algorithm, `SINGULAR`.

Índice general

Índice de figuras

Capítulo 1
Introducción

1.1. Motivación

Los sistemas de ecuaciones polinómicas son fundamentales en la modelización de diversos fenómenos de la física, la ingeniería o las matemáticas aplicadas, como por ejemplo el estudio de trayectorias de un objeto o el diseño de algoritmos criptográficos basados en dichas ecuaciones. Por ello, su resolución constituye un aspecto clave en numerosos problemas científicos y tecnológicos. Sin embargo, la complejidad inherente a los sistemas de ecuaciones polinómicas hace que resolverlos sea, en muchos casos, computacionalmente inviable. En algunos campos, encontrar soluciones exactas o aproximadas a estos sistemas es crucial para la toma de decisiones y la optimización de procesos. Pero la resolución de sistemas no lineales no solo implica desafíos teóricos, sino también dificultades computacionales significativas, ya que los métodos numéricos tradicionales pueden ser ineficaces ante la presencia de múltiples soluciones.

Por ello, el desarrollo de estrategias algebraicas que permitan simplificar estos sistemas ha cobrado gran relevancia en los últimos años. Una de ellas es la triangulación, una técnica algebraica que permite descomponer un sistema de ecuaciones en uno o varios sistemas más simples, que pueden ser resueltos de manera secuencial. Esta técnica será el eje principal de este trabajo.

1.2. Estructura del trabajo

En este primer capítulo, se realiza una introducción al tema principal del trabajo: triangulación de sistemas de ecuaciones polinómicas. Se ilustra brevemente qué es triangular un sistema, junto con otras alternativas posibles a la triangulación.

En el segundo capítulo, se desarrollará el marco teórico necesario para contextualizar el estudio de las bases de Groebner y los algoritmos de triangulación. Se revisarán conceptos fundamentales del álgebra de polinomios, así como las herramientas algebraicas necesarias para abordar los capítulos siguientes.

El tercer capítulo estará dedicado al estudio de las bases de Groebner, necesarias para la comprensión y desarrollo de los algoritmos de triangulación estudiados en este trabajo. Dado que una base de Groebner se calcula a partir de un orden monomial fijado, en este capítulo se estudiará los órdenes monomiales en $K[x_1, \ldots, x_n]$. También se estudiarán los principales aspectos de los ideales polinómicos, así como el teorema de la Base de Hilbert para garantizar la existencia de bases de Groebner de un ideal de polinomios, y el algoritmo de Buchberger para construirlas. Finalmente, y dado que los algoritmos de triangulación estudiados parten de una base de Groebner con el orden monomial lexicográfico, se estudiará cómo obtener una base de Gröbner para un nuevo orden monomial a partir de otra ya calculada.

El cuarto capítulo estará dedicado al análisis del algoritmo de triangulación propuesto por Daniel Lazard en su artículo *Solving Zero-dimensional Algebraic Systems* [13]. Este método es clave en la resolución de sistemas de ecuaciones polinómicas y se explicarán en detalle tanto los fundamentos teóricos que lo sustentan como los pasos necesarios para su ejecución. A través del estudio de este algoritmo, se verá cómo es posible descomponer un sistema de polinomios en subsistemas más sencillos que puedan resolverse de forma progresiva, facilitando así el proceso de resolución.

En el quinto capítulo, se estudiará un segundo algoritmo de triangulación, propuesto por Michael Möller en su artículo *On Decomposing Systems of Polynomial Equations With Finitely Many Solutions* [14]. Este método presenta una alternativa al enfoque de Lazard, y nos permitirá comprender mejor diferentes estrategias existentes para abordar la triangulación de sistemas polinómicos.

1.3. Descripción del problema

1.3.1. Caso lineal

Uno de los enfoques más efectivos y conocidos para simplificar el proceso de resolución de un sistema de ecuaciones lineales es el de triangular el sistema. Consiste en transformar el sistema de ecuaciones en una forma jerárquica o escalonada, de manera que se pueda resolver secuencialmente, variable por variable. Consideremos un sistema de ecuaciones lineales en tres variables x, y, y z:

$$\begin{cases} x + 2y + 3z = 6 \\ 2x + 3y + z = 4 \\ 3x + y + 2z = 5 \end{cases} \tag{1.1}$$

Aplicamos la eliminación de Gauss [15] para transformar el sistema (1.1) a una forma escalonada en la que la última ecuación solo involucre la variable z, y la penúltima ecuación solo las variables y y z.

$$\begin{cases} x + 2y + 3z = 6 \\ y + 5z = 8 \\ z = \dfrac{3}{2} \end{cases} \tag{1.2}$$

De este modo, la resolución secuencial de (1.2) es directa:

- De la tercera ecuación obtenemos $z = \frac{3}{2}$.
- Sustituimos z en la segunda ecuación para obtener $y = \frac{1}{2}$.
- Finalmente, sustituimos y y z en la primera ecuación para obtener $x = \frac{1}{2}$.

Hemos triangulado el sistema original y, tras una simple sustitución, obtenemos el valor de todas las incógnitas. En el caso no lineal veremos cómo este proceso no es tan sencillo.

1.3.2. Caso mo lineal

La resolución de sistemas de ecuaciones polinómicas es un proceso más complejo que el de los sistemas lineales debido a la mayor variedad de posibles soluciones. A diferencia del caso lineal, en el que para garantizar una solución única el número de ecuaciones debe ser igual al número de variables y deben ser linealmente independientes, en los sistemas polinómicos no siempre se cumple esta correspondencia. Puede haber más ecuaciones que variables, menos ecuaciones que variables o incluso la misma cantidad, sin que ello garantice una solución única.

A esta dificultad se suma el reto de calcular raíces de polinomios en una variable. Una vez que el sistema ha sido triangulado, el procedimiento consiste en resolver primero la ecuación con una sola incógnita. Luego, se utilizan sus soluciones para resolver, de forma sucesiva, las ecuaciones que contienen más variables, hasta determinar completamente todas las incógnitas. El principal obstáculo de este enfoque es precisamente encontrar los valores de las incógnitas, ya que implica resolver polinomios en una variable. Si se busca una solución simbólica, este proceso requiere factorizar dichos polinomios, lo cual puede resultar complicado y no siempre es inmediato.

Nota 1.1. Cabe destacar que este trabajo se centra en sistemas cuyo conjunto de soluciones es finito. Si no fuese así, el estudio del conjunto de soluciones presentaría una mayor dificultad, pues este dependería de uno o varios parámetros. Por otro lado, salvo indicación en contra, supondremos que las soluciones de los sistemas considerados pertenecen a un cuerpo K, el cual no se especificará de manera explícita si no es necesario

Mostremos ahora lo sencillo que puede ser resolver un sistema de ecuaciones polinómicas si encontramos un sistema triangular con sus mismas soluciones, lo cual evidentemente no es inmediato. Supongamos que queremos resolver el siguiente sistema:

$$\begin{cases} 3x - 1 + 3y - 2y^2 - 2yz + 3z + z^3 - 2z^2 = 0 \\ 2x + y^2 + 2y + yz + z^2 + 2z = 0 \\ x - 1 + y + z^3 + z = 0 \end{cases} \tag{1.3}$$

Consideremos el siguiente sistema:

$$\begin{cases} x + y + z = 0 \\ y^2 + yz + z^2 = 0 \\ z^3 - 1 = 0 \end{cases} \tag{1.4}$$

Sin entrar en demasiado detalle, pues se explicará más adelante, las ecuaciones de (1.4) constituyen una base de Gröbner para el ideal generado por los polinomios del sistema (1.3). Esto garantiza que ambos sistemas comparten exactamente las mismas soluciones.

Dado que el sistema (1.4) es triangular, es decir, cada ecuación involucra progresivamente menos variables, es sencillo calcular sus soluciones de forma secuencial. Acudiendo a la tercera ecuación podemos calcular los valores de z. Después, acudimos a la primera ecuación de (1.4) para expresar y en función de x como:

$$y = -z - x \tag{1.5}$$

A continuación, podemos sustituir y en la segunda ecuación de (1.4) para conocer el valor de x. Como z es conocida, en este último paso encontramos la dificultad comentada anteriormente: la búsqueda de raíces de un polinomio en una variable, en este caso en x:

$$(-z - x)^2 + (-z - x)z + z^2 = 0 \tag{1.6}$$

Comenzamos resolviendo la ecuación cúbica:

$$z^3 - 1 = 0$$

cuyas soluciones son las raíces cúbicas de la unidad:

$$z_1 = 1, \quad z_2 = \omega = \frac{-1 + \sqrt{3}i}{2}, \quad z_3 = \omega^2 = \frac{-1 - \sqrt{3}i}{2}$$

Sustituyendo secuencialmente estos valores en (1.6) y aplicando la fórmula general de ecuaciones cuadráticas obtenemos los valores de x:

$$x_1 = zw, \quad x_2 = zw^2$$

Finalmente sustituimos los valores de x y z en (1.5), y obtenemos los seis elementos de $\mathbb{C}^3$ que solucionan (1.4), y con ello el sistema original (1.3):

$$\begin{array}{c} (\omega,\ \omega^2,\ 1)\,,\ (\omega^2,\ \omega,\ 1)\,,\ (1,\ \omega^2,\ \omega)\,, \\ (\omega^2,\ 1,\ \omega)\,,\ (1,\ \omega,\ \omega^2)\,,\ (\omega,\ 1,\ \omega^2) \end{array}$$

1.4. Alternativas a la Triangulación

La falta de técnicas directas, como la eliminación de Gauss en el caso lineal, hace que el tratamiento de los sistemas de ecuaciones polinómicas requiera herramientas más avanzadas. En este trabajo nos centraremos en la triangulación de estos sistemas, pero cabe mencionar que existen otros enfoques como las bases de Groebner, teoría de eliminación, teoría de resultantes o descomposición primaria [2]. Sin entrar mucho en detalle, porque no son el objetivo de este trabajo, se presentan a continuación.

1.4.1. Bases de Groebner

En el Capítulo 3 entraremos, con rigor, en más detalle sobre las bases de Groebner, dado que para la triangulación nos apoyaremos en ellas. Sin embargo, por el momento mencionaremos que una base de Groebner (ver Definición 2.10) es un conjunto particular de polinomios que genera el mismo ideal que los polinomios de un sistema de ecuaciones polinómicas dado, pero con una estructura más manejable para su resolución. Si se usa el orden monomial lexicográfico, que se definirá en el Capítulo 3, para calcular la base de Groebner, el sistema toma una forma escalonada, lo que facilita la eliminación de variables y con ello la resolución.

Aunque, en general, las bases de Groebner son un elemento auxiliar para otras técnicas, por sí solas pueden simplificar un sistema de ecuaciones hasta el punto de convertir su resolución en un proceso sencillo. De hecho, el ejemplo puesto es una muestra de ello. Como se comentó previamente, la base de Groebner del ideal generado por las ecuaciones del sistema (1.3) es precisamente el ideal generado por las ecuaciones del sistema (1.4). Como se mencionó, esto hace que (1.3) y (1.4) tengan las mismas soluciones.

1.4.2. Teoría de Eliminación

La teoría de eliminación es una técnica algebraica utilizada para eliminar variables en un sistema de ecuaciones polinómicas, con el objetivo de reducir el problema a una forma más manejable. El proceso de eliminación también se basa en la construcción de una base de Groebner, permitiendo obtener ecuaciones que involucran cada vez menos variables.

Ejemplo 1.1. Sin entrar demasiado en detalle en esta técnica, ilustrémosla con un sencillo ejemplo. Consideremos el siguiente sistema de ecuaciones polinómicas:

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

El objetivo es eliminar variables para encontrar soluciones más fácilmente. Si tomamos el ideal asociado:

$$I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$$

y calculamos una base de Groebner (en el Capítulo 3 se mostrará cómo hacerlo), obtenemos el siguiente conjunto de polinomios:

$$\begin{cases} h_1 = x + y + z^2 - 1 \\ h_2 = y^2 - y - z^2 + z \\ h_3 = 2yz^2 + z^4 - z^2 \\ h_4 = z^6 - 4z^4 + 4z^3 - z^2 \end{cases}$$

El último polinomio, h_4, solo involucra la variable z, lo que nos permite encontrar sus posibles valores. Resolviendo la ecuación:

$$z^6 - 4z^4 + 4z^3 - z^2 = 0$$

obtenemos que los valores posibles de z son $0, 1, -1 \pm \sqrt{2}$. Luego, podemos eliminar la variable z sustituyendo uno a uno sus valores en h_2 y en h_3 para determinar los valores de y y finalmente acudir a h_1 para encontrar los valores de x.

Nota 1.2. Este proceso ilustra la potencia de la teoría de eliminación: al calcular los valores de z hemos reducido el problema de un sistema de tres variables a uno de dos. Para saber más acerca de la Teoría de Eliminación se puede consultar [1].

1.4.3. Teoría de Resultantes

La teoría de resultantes es una técnica algebraica utilizada en la eliminación de variables dentro de sistemas de ecuaciones polinómicas. Permite determinar si dos ecuaciones tienen soluciones comunes y, en caso afirmativo, encontrar ecuaciones equivalentes en menos variables. La herramienta principal de esta teoría es el resultante de Sylvester, el cual se basa en la construcción de un determinante a partir de los coeficientes de los polinomios involucrados.

Definición 1.1. Sea $f(x)$ y $g(x)$ dos polinomios en una variable con coeficientes en un anillo R:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \tag{1.7}$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0. \tag{1.8}$$

El *resultante* de $f(x)$ y $g(x)$, $\mathrm{Res}(f, g)$, se define como el determinante de la *matriz de Sylvester*, que es la matriz $(m + n) \times (m + n)$ construida con los coeficientes de ambos polinomios del siguiente modo:

$$S = \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & \cdots & 0 & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & b_m & b_{m-1} & \cdots & \cdots & b_0 \end{pmatrix}$$

El resultado es un escalar que caracteriza cuándo los polinomios tienen una raíz común. Si $\mathrm{Res}(f, g) = 0$, entonces los polinomios tienen al menos un factor común, es decir, comparten una raíz.

Ejemplo 1.2. Consideremos los siguientes polinomios en x:

$$f(x) = x^2 + x - 2, \tag{1.9}$$

$$g(x) = x^2 - 3x + 2. \tag{1.10}$$

La matriz de Sylvester asociada es:

$$S = \begin{pmatrix} 1 & 1 & -2 & 0 \\ 0 & 1 & 1 & -2 \\ 1 & -3 & 2 & 0 \\ 0 & 1 & -3 & 2 \end{pmatrix}. \tag{1.11}$$

Calculamos el determinante:

$$\mathrm{Res}(f, g) = \det(S) = \begin{vmatrix} 1 & 1 & -2 & 0 \\ 0 & 1 & 1 & -2 \\ 1 & -3 & 2 & 0 \\ 0 & 1 & -3 & 2 \end{vmatrix} = 0. \tag{1.12}$$

Dado que $\mathrm{Res}(f, g) = 0$, esto indica que $f(x)$ y $g(x)$ tienen una raíz común. Resolviendo cada ecuación, encontramos que ambos polinomios tienen la raíz $x = 1$, confirmando el resultado del cálculo del resultante.

Nota 1.3. La teoría de resultantes permite eliminar variables de sistemas de ecuaciones polinómicas y detectar soluciones comunes de manera eficiente.

Ejemplo 1.3. Consideremos el siguiente sistema de ecuaciones polinómicas en las variables x e y:

$$\begin{cases} f(x, y) = x^2 + y^2 - 1 = 0, \\ g(x, y) = x^2 + 2y^2 - 1 = 0. \end{cases} \tag{1.13}$$

Queremos eliminar la variable x para obtener una ecuación en términos únicamente de y. Para ello, consideramos y como un parámetro fijo y tratamos f y g como polinomios en $\mathbb{R}[x]$.

$$\begin{cases} f_y(x) = x^2 + 0x + (y^2 - 1) = 0, \\ g_y(x) = x^2 + 0x + (2y^2 - 1) = 0. \end{cases} \tag{1.14}$$

El resultante de Sylvester se construye entonces como:

$$S_y = \begin{pmatrix} 1 & 0 & y^2 - 1 & 0 \\ 0 & 1 & 0 & y^2 - 1 \\ 1 & 0 & 2y^2 - 1 & 0 \\ 0 & 1 & 0 & 2y^2 - 1 \end{pmatrix} \tag{1.15}$$

Calculamos su determinante:

$$\text{Res}(f, g) = \det(S_y) = y^4 \tag{1.16}$$

Se anula en $y = 0$, lo quiere decir que los polinomios $f_0(x)$ y $g_0(x)$ tienen raíces en común. Calculemos las raíces de $f(x, 0)$ y $g(x, 0)$:

$f(x, 0) = g(x, 0) = x^2 - 1$, luego $f(x, 0) = 0 \Rightarrow x = \pm 1$.

Las soluciones del sistema original son (1, 0) y (-1, 0).

Nota 1.4. Este sencillo ejemplo muestra cómo los resultantes pueden usarse para eliminar variables en sistemas de ecuaciones polinómicas sin necesidad de sustitución directa. Para saber más acerca de la Teoría de Resultantes se puede consultar [2].

1.4.4. Descomposición Primaria

La descomposición primaria es una técnica en álgebra computacional que permite descomponer un ideal en una intersección de ideales primarios. Esta técnica es útil en álgebra conmutativa y geometría algebraica, ya que permite estudiar la estructura de los conjuntos algebraicos asociados a un ideal. Si I es un ideal en un anillo de polinomios $K[x_1, \ldots, x_n]$, su descomposición primaria es una expresión de la forma:

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_r, \tag{1.17}$$

donde cada Q_i es un ideal primario, es decir, si $ab \in Q_i$, entonces $a \in Q_i$ o $b^m \in Q_i$ para algún $m \geq 1$.

Ejemplo 1.4. Consideremos el ideal en $K[x, y]$:

$$\begin{cases} f(x, y) = x^2 + y^2 - 1 = 0, \\ g(x, y) = x^2 + 2y^2 - 1 = 0. \end{cases} \tag{1.18}$$

El ideal asociado al sistema es:

$$I = \langle x^2 + y^2 - 1, x^2 + 2y^2 - 1 \rangle. \tag{1.19}$$

No siempre es sencillo encontrar la descomposición en ideales primarios (consultar [2]), pero en este caso se puede probar que:

$$I = \langle x - 1, y \rangle \cap \langle x + 1, y \rangle. \tag{1.20}$$

Nota 1.5. La idea es que al descomponer el ideal de un sistema en la intersección de ideales, el conjunto de soluciones del sistema es la unión de los conjuntos de soluciones de los sistemas asociados a cada ideal de la intersección, que, en general, son más sencillos de calcular. En este caso, $(1, 0)$ es un cero común a todos los polinomios del ideal $\langle x - 1, y \rangle$ y $(-1, 0)$ lo es para los polinomios del ideal $\langle x + 1, y \rangle$, luego el conjunto de soluciones del sistema original es $\{(1, 0)\} \cup \{(-1, 0)\} = \{(1, 0), (-1, 0)\}$.

Capítulo 2
Conceptos previos

En este capítulo, abordaremos los conceptos matemáticos fundamentales necesarios para una mejor comprensión de los capítulos siguientes. El estudio de estas bases conceptuales es esencial para profundizar en las técnicas de álgebra computacional más avanzadas de este trabajo, tales como el uso de bases de Groebner y las técnicas de triangulación.

2.1. Polinomios y Espacio Afín

Para comenzar, estudiaremos algunas estructuras algebraicas junto con otros conceptos como el de polinomio y espacio afín.

Definición 2.1. Un **anillo** es un conjunto A junto con dos operaciones binarias: la suma $(+)$ y el producto $(\cdot)$, tales que se cumplen las siguientes propiedades:

1. Cerrado para la suma y producto: Para todo $a, b \in A$, tanto $a+b \in A$ como $a \cdot b \in A$.
2. Asociatividad de la suma y el producto: Para todo $a, b, c \in A$, se cumple que $(a + b) + c = a + (b + c)$ y $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Elemento neutro para la suma: Existe un elemento $0 \in A$ tal que para todo $a \in A$, $a + 0 = a$.
4. Inverso para la suma: Para todo $a \in A$, existe un elemento $-a \in A$ tal que $a + (-a) = 0$.
5. Conmutatividad de la suma: Para todo $a, b \in A$, se cumple que $a + b = b + a$.
6. Distributividad: Para todo $a, b, c \in A$, se cumple que $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(a + b) \cdot c = a \cdot c + b \cdot c$.

Nota 2.1. Si además existe un elemento $1 \in A$ tal que para todo $a \in A$, $a \cdot 1 = a$, se dice que el anillo es un **anillo con unidad**.

Nota 2.2. Si además la multiplicación es conmutativa, es decir, si para todo $a, b \in A$, se cumple que $a \cdot b = b \cdot a$, se dice que el anillo es un **anillo conmutativo**.

Definición 2.2. Un **cuerpo** es un conjunto K junto con dos operaciones binarias: la suma $(+)$ y el producto $(\cdot)$, tales que se cumplen las siguientes propiedades:

1. Cerrado para la suma y el producto: Para todo $a, b \in K$, tanto $a + b \in K$ como $a \cdot b \in K$.
2. Asociatividad: Para todo $a, b, c \in K$, se cumple que $(a + b) + c = a + (b + c)$ y $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Elemento neutro para la suma y producto: Existen elementos $0 \in K$ y $1 \in K$ (con $0 \neq 1$) tales que para todo $a \in K$, $a + 0 = a$ y $a \cdot 1 = a$.
4. Inverso para la suma: Para todo $a \in K$, existe un elemento $-a \in K$ tal que $a + (-a) = 0$.
5. Conmutatividad: Para todo $a, b \in K$, se cumple que $a + b = b + a$ y $a \cdot b = b \cdot a$.
6. Inverso para el producto: Para todo $a \in K$, con $a \neq 0$, existe un elemento $a^{-1} \in K$ tal que $a \cdot a^{-1} = 1$.
7. Distributividad: Para todo $a, b, c \in K$, se cumple que $a \cdot (b + c) = a \cdot b + a \cdot c$.

Ahora podemos definir el concepto de polinomio en varias variables. Necesitaremos trabajar con polinomios en n variables $x_1, x_2, \ldots, x_n$ con coeficientes en un cuerpo arbitrario K. Comenzamos definiendo monomios:

Definición 2.3. Un **monomio** en $x_1, \ldots, x_n$ es un producto de la forma

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

donde todos los exponentes $\alpha_1, \ldots, \alpha_n$ son enteros no negativos. El **grado total** de este monomio se define como la suma $\alpha_1 + \cdots + \alpha_n$.

Para abreviar la notación definimos los monomios de la siguiente manera: sea $\alpha = (\alpha_1, \ldots, \alpha_n)$ un n-tupla de enteros no negativos. Entonces definimos

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

En particular, si $\alpha = (0, \ldots, 0)$, entonces $x^\alpha = 1$. Denotamos el grado total del monomio x^α por $|\alpha| = \alpha_1 + \cdots + \alpha_n$

Definición 2.4. Un **polinomio** en $x_1, \ldots, x_n$ con coeficientes en un cuerpo K es una combinación lineal finita de monomios. Un polinomio f puede escribirse como

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in K,$$

donde la suma es sobre un número finito de n-tuplas $\alpha = (\alpha_1, \ldots, \alpha_n)$. El conjunto de todos los polinomios en $x_1, \ldots, x_n$ con coeficientes en K se denota por $K[x_1, \ldots, x_n]$.

Definición 2.5. Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio en $K[x_1, \ldots, x_n]$.

(i) Llamamos a_α al **coeficiente** del monomio x^α.

(ii) Si $a_\alpha \neq 0$, entonces llamamos a $a_\alpha x^\alpha$ un **término** de f.

(iii) El **grado total** de f, denotado $\deg(f)$, es el máximo de los grados totales de todos los monomios de f. En otras palabras, es el máximo $|\alpha|$ tal que el coeficiente a_α es no nulo. El grado total del polinomio cero es indefinido.

Ejemplo 2.1. Por ejemplo, el polinomio $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ tiene cuatro monomios y grado total seis. Observemos que hay dos monomios de grado total máximo, lo cual es algo que no puede ocurrir en polinomios de una sola variable.

Nota 2.3. La suma y el producto de dos polinomios es nuevamente un polinomio. Decimos que un polinomio f *divide* a un polinomio g si existe un polinomio $h \in K[x_1, \ldots, x_n]$ tal que $g = fh$.

Observación 2.1. Bajo la suma y la multiplicación, $K[x_1, \ldots, x_n]$ satisface todos los axiomas de cuerpo excepto la existencia de inversos multiplicativos (porque, por ejemplo, $1/x_1$ no es un polinomio). Por tanto, $K[x_1, \ldots, x_n]$ es un *anillo conmutativo*.

Definición 2.6. Dado un cuerpo K y un número entero positivo n, definimos el **espacio afín** n-dimensional sobre K como el conjunto

$$K^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in K\}.$$

Como ejemplo de espacio afín, consideremos el caso $K = \mathbb{R}$. Aquí obtenemos el espacio familiar $\mathbb{R}^n$. En general, llamamos a $K^1 = K$ la **línea afín** y a K^2 el **plano afín**.

2.1.1. Polinomios en una variable

En esta subsección, estudiaremos los polinomios en una variable y mostraremos el *Algoritmo de División* de álgebra básica, que utilizaremos más adelante.

Nota 2.4. De manera informal, un algoritmo es un conjunto específico y finito de instrucciones para manipular datos simbólicos o numéricos. Un algoritmo tiene entradas, que son los objetos utilizados por el algoritmo, y salidas, que son los resultados del algoritmo. En cada etapa de la ejecución, el algoritmo debe especificar exactamente cuál será el siguiente paso. Cuando estudiemos un algoritmo, usualmente se presentará un "pseudocódigo", lo cual hará que la estructura formal sea más fácil de entender. El pseudocódigo es similar a muchos lenguajes de programación comunes e indica cómo puede programarse el algoritmo en una computadora.

Comenzamos con el Algoritmo de División para polinomios en $K[x]$. Un elemento clave de este algoritmo es la noción de "término líder" de un polinomio en una variable.

Definición 2.7. Dado un polinomio no nulo $f \in K[x]$, sea

$$f = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0,$$

donde $c_i \in K$ para cada $1 \leq i \leq n$, y $c_n \neq 0$ (de modo que $n = \deg(f)$). Entonces decimos que $c_n x^n$ es el **término líder** de f, y lo denotamos por $\mathrm{LT}(f) = c_n x^n$.

Proposición 2.1 (Algoritmo de División)**.** *Sea K un cuerpo y sea g un polinomio no nulo en $K[x]$. Entonces todo $f \in K[x]$ puede escribirse como*

$$f = qg + r,$$

donde $q, r \in K[x]$, y $r = 0$ o bien $\deg(r) < \deg(g)$. Además, q y r son únicos, y existe un algoritmo para encontrar q y r.

El Algoritmo 1, presentado en pseudocódigo, garantiza la existencia de q y r. La demostración de finitud y resultado esperado del algoritmo puede consultarse en [1].

Algoritmo 1 Algoritmo de División

- **Entrada**: g, f
- **Salida**: q, r

1: $q := 0$; $r := f$;
2: **while** $r \neq 0$ **AND** $\mathrm{LT}(g)$ divide $\mathrm{LT}(r)$ **do**
3: $\quad q := q + \mathrm{LT}(r)/\mathrm{LT}(g)$;
4: $\quad r := r - (\mathrm{LT}(r)/\mathrm{LT}(g))\, g$;
5: **end while**
6: **return** q, r;
7: **end**

2.2. Variedades afines

Podemos ahora definir los objetos geométricos básicos que utilizaremos.

Definición 2.8. Sea K un cuerpo, y sean $f_1, \ldots, f_s$ polinomios en $K[x_1, \ldots, x_n]$. Entonces definimos

$$\mathcal{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ para todo } 1 \leq i \leq s\}.$$

Llamamos a $\mathcal{V}(f_1, \ldots, f_s)$ la **variedad afín** definida por $f_1, \ldots, f_s$.

Observación 2.2. Una variedad afín $\mathcal{V}(f_1, \ldots, f_s) \subseteq K^n$ es el conjunto de todas las soluciones del sistema de ecuaciones $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$.

Nota 2.5. En general, usaremos las letras V o W para denotar a una variedad afín, como por ejemplo $V = \mathcal{V}(f_1, \ldots, f_s)$.

A continuación, daremos algunos ejemplos de variedades en dimensiones superiores. Un caso familiar proviene del álgebra lineal. Fijemos un cuerpo K y consideremos un sistema de m ecuaciones lineales en n incógnitas $x_1, \ldots, x_n$, con coeficientes en K:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1, \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m. \end{cases} \tag{2.1}$$

Las soluciones de estas ecuaciones forman una variedad afín en K^n, a la que llamaremos *variedad lineal*. Así, las líneas y planos son variedades lineales, y existen ejemplos de dimensión arbitrariamente grande.

2.3. Ideales

A continuación, definiremos los objetos algebraicos básicos que utilizaremos.

Definición 2.9. Un subconjunto $I \subseteq K[x_1, \ldots, x_n]$ 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 $h \in K[x_1, \ldots, x_n]$, entonces $hf \in I$.

A lo largo de esta sección veremos cómo los ideales se relacionan con las variedades afines. La verdadera importancia de los ideales radica en que nos proporcionarán un lenguaje para calcular variedades afines.

El primer ejemplo natural de un ideal es el ideal generado por un número finito de polinomios.

Definición 2.10. Sean $f_1, \ldots, f_s$ polinomios en $K[x_1, \ldots, x_n]$. Entonces definimos

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \;\middle|\; h_1, \ldots, h_s \in K[x_1, \ldots, x_n] \right\}.$$

y lo llamamos el **ideal generado por** $f_1, \ldots, f_s$.

Veamos que $\langle f_1, \ldots, f_s \rangle$ es un ideal.

Lema 2.2. *Si $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, entonces $\langle f_1, \ldots, f_s \rangle$ es un ideal de $K[x_1, \ldots, x_n]$.*

Demostración.

Primero, $0 \in \langle f_1, \ldots, f_s \rangle$ ya que $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Supongamos ahora que $f = \sum_{i=1}^{s} p_i f_i$ y $g = \sum_{i=1}^{s} q_i f_i$, y sea $h \in K[x_1, \ldots, x_n]$. Entonces las igualdades

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i,$$

$$hf = \sum_{i=1}^{s} (hp_i) f_i$$

completan la demostración de que $\langle f_1, \ldots, f_s \rangle$ es un ideal. □

Observación 2.3. El ideal $\langle f_1, \ldots, f_s \rangle$ tiene una interpretación interesante en términos de ecuaciones polinómicas. Dados $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, obtenemos el sistema de ecuaciones

$$f_1 = 0,$$

$$\vdots$$

$$f_s = 0.$$

A partir de estas ecuaciones, se pueden derivar otras. Por ejemplo, si multiplicamos la primera ecuación por $h_1 \in K[x_1, \ldots, x_n]$, la segunda por $h_2 \in K[x_1, \ldots, x_n]$, etc., y luego sumamos las ecuaciones resultantes, obtenemos

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0,$$

lo cual es una "consecuencia" de nuestro sistema original. Notemos que el lado izquierdo de esta ecuación es exactamente un elemento del ideal $\langle f_1, \ldots, f_s \rangle$. Por lo tanto, podemos pensar en $\langle f_1, \ldots, f_s \rangle$ como el conjunto de todas las "consecuencias polinómicas" de las ecuaciones $f_1 = f_2 = \cdots = f_s = 0$.

Definición 2.11. Decimos que un ideal I es **finitamente generado** si existen $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ tales que $I = \langle f_1, \ldots, f_s \rangle$, y decimos que $f_1, \ldots, f_s$ son una **base** de I.

Nota 2.6. En el Capítulo 3 mostraremos que se puede elegir un tipo de base especialmente útil, llamada *base de Groebner*.

La siguiente proposición aclara el papel que juegan los ideales: una variedad depende únicamente del ideal generado por las ecuaciones que lo definen.

Proposición 2.3. *Si $f_1, \ldots, f_s$ y $g_1, \ldots, g_t$ son bases del mismo ideal en $K[x_1, \ldots, x_n]$, es decir, $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, entonces tenemos $\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(g_1, \ldots, g_t)$.*

Demostración.

Sea $I = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$ el ideal generado por $f_1, \ldots, f_s$ y $g_1, \ldots, g_t$ en $K[x_1, \ldots, x_n]$. Queremos demostrar que $\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(g_1, \ldots, g_t)$.

Recordemos que, por definición,

$$\mathcal{V}(f_1, \ldots, f_s) = \{x \in K^n \mid f_1(x) = 0, \ldots, f_s(x) = 0\},$$

$$\mathcal{V}(g_1, \ldots, g_t) = \{x \in K^n \mid g_1(x) = 0, \ldots, g_t(x) = 0\}.$$

Ahora, tomemos un punto $x \in \mathcal{V}(f_1, \ldots, f_s)$. Esto significa que:

$$f_1(x) = 0,\ f_2(x) = 0,\ \ldots,\ f_s(x) = 0.$$

Dado que $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, cualquier elemento de I, en particular los generadores $g_1, \ldots, g_t$, puede escribirse como una combinación lineal de $f_1, \ldots, f_s$. Así, existe un conjunto de polinomios $p_{ij} \in K[x_1, \ldots, x_n]$ tales que

$$g_j = \sum_{i=1}^{s} p_{ij} f_i \quad \text{para cada } j = 1, \ldots, t.$$

Por lo tanto, evaluando en el punto x, tenemos que

$$g_j(x) = \sum_{i=1}^{s} p_{ij}(x) f_i(x) = \sum_{i=1}^{s} p_{ij}(x) \cdot 0 = 0.$$

Esto muestra que $g_j(x) = 0$ para todos $j = 1, \ldots, t$, y por lo tanto $x \in \mathcal{V}(g_1, \ldots, g_t)$. Razonando de manera análoga, podemos tomar cualquier punto $y \in \mathcal{V}(g_1, \ldots, g_t)$ y demostrar que $y \in \mathcal{V}(f_1, \ldots, f_s)$. Por tanto, hemos probado que $\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(g_1, \ldots, g_t)$.

□

A continuación, veremos cómo las variedades afines dan lugar a una interesante clase de ideales.

Definición 2.12. Sea $V \subseteq K^n$ una variedad afín. Definimos el conjunto

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

Lema 2.4. *Si $V \subseteq K^n$ es una variedad afín, entonces el conjunto $I(V) \subseteq K[x_1, \ldots, x_n]$ es un ideal.*

Demostración.

Observemos que $0 \in I(V)$ ya que el polinomio cero se anula en todo K^n y, en particular, se anula en V. Ahora, supongamos que $f, g \in I(V)$ y que $h \in K[x_1, \ldots, x_n]$.

Sea $(a_1, \ldots, a_n)$ un punto arbitrario de V. Entonces

$$f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0,$$

$$h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0,$$

y de esto se deduce que $I(V)$ es un ideal. □

Nota 2.7. A la vista del Lema 2.4, diremos que el conjunto $I(V)$ es el ideal de V.

Ejemplo 2.2. Como ejemplo del ideal de una variedad, consideremos la variedad $\{(0,0)\}$ que consiste en el origen en K^2. Entonces su ideal $I(\{(0,0)\})$ consiste en todos los polinomios que se anulan en el origen, y afirmamos que

$$I(\{(0,0)\}) = \langle x, y \rangle.$$

Una dirección de la demostración es trivial, ya que cualquier polinomio de la forma $A(x,y)x + B(x,y)y$ obviamente se anula en el origen. En la otra dirección, supongamos que $f = \sum_{i,j} a_{ij} x^i y^j$ se anula en el origen. Entonces $a_{00} = f(0,0) = 0$ y, por consiguiente,

$$\begin{aligned} f &= a_{00} + \sum_{i,j \neq 0,0} a_{ij} x^i y^j \\ &= 0 + \left(\sum_{i>0} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \\ &\in \langle x, y \rangle. \end{aligned}$$

Observación 2.4. Sea $f, g \in K[x]$ dos polinomios en una variable. Si aplicamos el Algoritmo de División de f entre g, obtenemos una expresión de la forma

$$f = qg + r,$$

donde $q, r \in K[x]$ y el grado de r es estrictamente menor que el grado de g, o bien $r = 0$. En este contexto, $f \in \langle g \rangle$ si, y solo si, el resto r es cero. Es decir, f pertenece al ideal generado por g si puede escribirse como un múltiplo de g. Por tanto, el Algoritmo de División nos permite comprobar si un polinomio pertenece al ideal generado por otro en $K[x]$.

Finalicemos este capítulo introduciendo el concepto de dimensión de ideal y la relación entre ideales de dimensión cero y que su sistema de ecuaciones asociado tenga un número finito de soluciones.

Definición 2.13. Sea A un anillo conmutativo con unidad. Un ideal $\mathfrak{p} \subsetneq A$ se dice **primo** si, para todo $a, b \in A$, se cumple que

$$ab \in \mathfrak{p} \;\Rightarrow\; a \in \mathfrak{p} \text{ o } b \in \mathfrak{p}.$$

Definición 2.14. La **dimensión de un ideal** I en un anillo A se define como la dimensión de Krull del anillo cociente A/I. La dimensión de Krull de un anillo es el supremo de las longitudes de las cadenas estrictamente crecientes de ideales primos:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

La siguiente observación pretende relacionar el concepto de dimensión cero de un ideal con que su sistema de ecuaciones asociado tenga un conjunto finito de soluciones.

Observación 2.5. Decimos que un ideal tiene **dimensión cero** si la dimensión de Krull del anillo cociente A/I es cero, es decir, si todos los ideales primos de A/I son ideales maximales. En el contexto de anillos de polinomios sobre un cuerpo de característica cero, los ideales maximales de $A = K[x_1, \ldots, x_n]$ corresponden a evaluaciones en puntos del espacio afín, es decir, ideales de la forma $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$, pues K es cuerpo y

$$K[x_1, \ldots, x_n] \Big/ \langle x_1 - a_1, \ldots, x_n - a_n \rangle \cong K$$

Por tanto, decir que un ideal tiene dimensión cero equivale a decir que su variedad algebraica asociada consiste en un número finito de puntos. Esto justifica el uso del término "dimensión cero" para describir ideales cuyo sistema de ecuaciones asociado tiene un conjunto finito de soluciones.

Observación 2.6. En este trabajo, cuando consideremos un cuerpo K será de característica cero, pero cabe destacar que en cuerpos finitos todo sistema de polinomios con solución tiene un número finito de soluciones porque el cuerpo base tiene cardinalidad finita, sin que esto implique que el ideal tenga dimensión cero.

Considérese el sistema de ecuaciones en dos variables:

$$\begin{cases} x + y = 0 \\ 2x + 2y = 0 \end{cases}$$

Sobre un cuerpo de característica cero, como $\mathbb{Q}$, este sistema tiene infinitas soluciones de la forma $(x, y) = (-t, t)$ con $t \in \mathbb{Q}$. El ideal generado por estas ecuaciones es $\langle x+y \rangle \subset \mathbb{Q}[x, y]$, que tiene dimensión 1, ya que su variedad asociada es una recta en el plano afín.

Sin embargo, si trabajamos sobre un cuerpo finito, como $\mathbb{F}_5$, el número de soluciones es finito. En este caso, las soluciones son:

$$(0, 0),\ (1, 4),\ (2, 3),\ (3, 2),\ (4, 1)$$

Aunque el ideal $\langle x + y \rangle \subset \mathbb{F}_5[x, y]$ sigue teniendo dimensión 1, la variedad asociada contiene solo cinco puntos, debido a que el cuerpo base es finito. Por tanto, en cuerpos de característica cero un ideal de dimensión cero equivale a un número finito de soluciones del sistema asociado al ideal, pero en cuerpos finitos no es equivalente dado que el recíproco no es cierto.

Capítulo 3
Bases de Groebner

En este capítulo, estudiaremos las bases de Groebner, que nos permitirán resolver problemas relacionados con ideales de polinomios. Además, son el punto de partida para los dos algoritmos de triangulación que se estudiarán en los Capítulos 4 y 5.

3.1. Órdenes monomiales en $K[x_1, \ldots, x_n]$

Observación 3.1. Si examinamos el algoritmo de división en $K[x]$ podemos observar que una noción de orden monomial en polinomios es clave.

Para el algoritmo de división en polinomios de una sola variable, usamos el orden monomial por grados de los monomios en una sola variable:

$$\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1.$$

El éxito del algoritmo depende de trabajar sistemáticamente con los términos líderes en f y g, y de no eliminar términos arbitrarios de f utilizando términos arbitrarios de g.

En esta subsección, veremos las propiedades deseables que debería tener dicho orden monomial, y construiremos varios órdenes monomiales diferentes. Cada uno será útil en diferentes contextos.

Definición 3.1. Sea A un conjunto. Una relación binaria $\leq$ sobre A se dice que es una **relación de orden** (o un **orden**) si verifica las siguientes propiedades, para todos $a, b, c \in A$:

- **Reflexividad**: $a \leq a$.
- **Antisimetría**: Si $a \leq b$ y $b \leq a$, entonces $a = b$.
- **Transitividad**: Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

Definición 3.2. Sea A un conjunto. Una relación binaria $<$ sobre A se dice que es una **relación de orden estricto** si satisface las siguientes propiedades, para todos $a, b, c \in A$:

- **Irreflexividad**: No se verifica $a < a$ para ningún $a \in A$.
- **Asimetría**: Si $a < b$, entonces no se cumple $b < a$.
- **Transitividad**: Si $a < b$ y $b < c$, entonces $a < c$.

Observación 3.2. Primero, notemos que podemos reconstruir el monomio $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ a partir de la n-tupla de exponentes $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. Esta observación establece una correspondencia uno a uno entre los monomios en $K[x_1, \ldots, x_n]$ y $\mathbb{Z}_{\geq 0}^n$. Además, cualquier orden $<$ que establezcamos en el espacio $\mathbb{Z}_{\geq 0}^n$ nos dará un orden monomial en los monomios: si $\alpha < \beta$ según este orden, también diremos que $x^\alpha < x^\beta$.

Nota 3.1. Las expresiones $a > b$ y $b < a$ son equivalentes. Respetando la notación seguida en la bibliografía, concretamente en [1], se escribirá el símbolo $>$.

Dado que un polinomio es una suma de monomios, queremos poder organizar los términos de un polinomio de manera inequívoca en orden descendente o ascendente. Para hacer esto, debemos poder comparar cada par de monomios para establecer sus posiciones relativas.

Definición 3.3. Sea A un conjunto, y $>$ un orden en A. Se dice que es un orden **total** si para cada $\alpha, \beta \in A$ exactamente una de las siguientes tres afirmaciones es verdadera:

$$\alpha > \beta, \quad \alpha = \beta, \quad \text{o} \quad \beta > \alpha.$$

Definición 3.4. Un **orden monomial** $>$ en $K[x_1, \ldots, x_n]$ es una relación $>$ en $\mathbb{Z}_{\geq 0}^n$, o equivalentemente, una relación en el conjunto de monomios x^α, donde $\alpha \in \mathbb{Z}_{\geq 0}^n$, que satisface:

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

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

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

Observación 3.3. De las propiedades (i) y (iii) de la Definición 3.4 se deduce que todo orden monomial es un **buen orden**, pues precisamente esa es su definición.

Nota 3.2. Dado un orden monomial $>$, decimos que $\alpha \geq \beta$ cuando $\alpha > \beta$ o $\alpha = \beta$.

El siguiente lema nos ayudará a entender qué significa la condición de orden bien fundado en la parte (iii) de la Definición 3.4.

Lema 3.1. *Una relación de orden $>$ en $\mathbb{Z}_{\geq 0}^n$ es un orden bien fundado si, y solo si, toda sucesión estrictamente decreciente en $\mathbb{Z}_{\geq 0}^n$ es finita.*

Demostración.

Demostraremos el contrarrecíproco: $>$ no es un orden bien fundado si y solo si existe una sucesión estrictamente decreciente infinita en $\mathbb{Z}_{\geq 0}^n$.

$\boxed{\Rightarrow}$ Si $>$ no es un orden bien fundado, entonces algún subconjunto no vacío $S \subseteq \mathbb{Z}_{\geq 0}^n$ no tiene un elemento mínimo. Ahora elijamos $\alpha(1) \in S$. Dado que $\alpha(1)$ no es el menor elemento, podemos encontrar $\alpha(2) > \alpha(1)$ en S. Como $\alpha(2)$ tampoco es el menor elemento, podemos encontrar $\alpha(3) > \alpha(2)$ en S. Continuando de esta manera, obtenemos una sucesión estrictamente decreciente infinita:

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots .$$

$\boxed{\Leftarrow}$ Por el contrario, si existe tal sucesión infinita, entonces el conjunto $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ es un subconjunto no vacío de $\mathbb{Z}_{\geq 0}^n$ sin un elemento mínimo, lo que implica que $>$ no es un orden bien fundado. □

El primero de los órdenes que presentaremos es el **orden lexicográfico**.

Definición 3.5 (Orden Lexicográfico)**.** Sean $\alpha = (\alpha_1, \ldots, \alpha_n)$ y $\beta = (\beta_1, \ldots, \beta_n)$ en $\mathbb{Z}^n_{\geq 0}$. Decimos que $\alpha >_{\text{lex}} \beta$ si la primera entrada no nula del vector diferencia, $\alpha - \beta \in \mathbb{Z}^n$, es positiva. Escribiremos $x^\alpha >_{\text{lex}} x^\beta$ si $\alpha >_{\text{lex}} \beta$.

Observación 3.4. Las variables $x_1, \ldots, x_n$ están ordenadas de la manera usual por el orden lexicográfico:

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

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

En la práctica, cuando trabajamos con polinomios en dos o tres variables, llamaremos a las variables x, y, z en lugar de x_1, x_2, x_3. Además, asumiremos que el orden alfabético $x > y > z$ en las variables se usa para definir el orden lexicográfico.

Proposición 3.2. *El orden lexicográfico en $\mathbb{Z}^n_{\geq 0}$ es un orden monomial.*

Demostración.

(i) Que $>_{\text{lex}}$ sea un orden total se deduce directamente de la definición y del hecho de que el orden numérico usual en $\mathbb{Z}_{\geq 0}$ es un orden total.

(ii) Si $\alpha >_{\text{lex}} \beta$, entonces la entrada no nula más a la izquierda en $\alpha - \beta$, digamos $\alpha_i - \beta_i$, es positiva. Pero $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ y $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Entonces en $(\alpha+\gamma)-(\beta+\gamma) = \alpha-\beta$, la entrada no nula más a la izquierda sigue siendo $\alpha_i - \beta_i > 0$, luego $(\alpha + \gamma) >_{\text{lex}} (\beta + \gamma)$.

(iii) Supongamos que $>_{\text{lex}}$ no es un orden bien fundado. Entonces por el Lema 3.1, existiría una sucesión estrictamente decreciente infinita:

$$\alpha(1) >_{\text{lex}} \alpha(2) >_{\text{lex}} \alpha(3) >_{\text{lex}} \cdots$$

de elementos de $\mathbb{Z}^n_{\geq 0}$. Mostraremos que esto lleva a una contradicción. Consideremos las primeras entradas de los vectores $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Por la definición del orden lexicográfico, estas primeras entradas forman una secuencia no creciente de enteros no negativos. Dado que $\mathbb{Z}_{\geq 0}$ es bien fundado, las primeras entradas de los $\alpha(i)$ eventualmente se estabilizan. En otras palabras, existe un ℓ tal que todas las primeras

entradas de $\alpha(i)$ con $i \geq \ell$ son iguales. A partir de $\alpha(\ell)$, las segundas y subsecuentes entradas entran en juego. Las segundas entradas de $\alpha(\ell), \alpha(\ell+1), \ldots$ forman una secuencia no creciente. Por el mismo razonamiento anterior, las segundas entradas también eventualmente se estabilizan. Continuando de la misma manera, vemos que para algún m, $\alpha(m), \alpha(m+1), \ldots$ son todas iguales. Esto contradice el hecho de que $\alpha(m) >_{\text{lex}} \alpha(m+1)$.

□

En el orden lexicográfico, notemos que una variable domina a cualquier monomio que involucre únicamente variables más pequeñas, sin importar su grado total. Por ejemplo, para el orden lexicográfico con $x > y > z$, tenemos $x >_{\text{lex}} y^5 z^3$.

Para algunos propósitos, también podríamos querer tomar en cuenta los grados totales de los monomios y ordenar primero los monomios de mayor grado total. Una forma de hacer esto es utilizando el orden monomial **orden lexicográfico graduado** (o **orden grlex**).

Definición 3.6 (Orden Lexicográfico Graduado)**.** Sea $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Decimos que $\alpha >_{\text{grlex}} \beta$ si

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|,$$

o bien

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

Escribiremos $x^\alpha >_{\text{grlex}} x^\beta$ si $\alpha >_{\text{grlex}} \beta$.

Ejemplo 3.1. Se tiene que $xy^2 >_{\text{grlex}} xy$ por el primer caso de la Definición 3.6 y $xy >_{\text{grlex}} yz$ por el segundo caso.

Otro orden monomial es el **orden lexicográfico graduado inverso** (o **orden grevlex**). Se ha demostrado que, para algunas operaciones, el orden grevlex es el más eficiente para realizar cálculos.

Definición 3.7 (Orden Lexicográfico Graduado Inverso)**.** Sea $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Decimos que $\alpha >_{\text{grevlex}} \beta$ si

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|,$$

o bien

$$|\alpha| = |\beta| \text{ y la entrada no nula más a la derecha de } \alpha - \beta \in \mathbb{Z}^n \text{ es negativa.}$$

Ejemplo 3.2. Consideremos el polinomio $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$. Entonces:

- Con respecto al orden lexicográfico ($>_{\text{lex}}$), reordenaríamos los términos de f en orden decreciente como:
$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2.$$
- Con respecto al orden grlex ($>_{\text{grlex}}$), tendríamos:
$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2.$$
- Con respecto al orden grevlex ($>_{\text{grevlex}}$), tendríamos:
$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2.$$

Usaremos la siguiente terminología.

Definición 3.8. Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio no nulo en $K[x_1, \ldots, x_n]$, y sea $>$ un orden monomial.

(i) El **multigrado** de f es

$$\text{multideg}(f) = \text{máx}\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\}$$

(el máximo se toma con respecto a $>$).

(ii) El **coeficiente líder** de f es

$$\text{LC}(f) = a_{\text{multideg}(f)} \in K.$$

(iii) El **monomio líder** de f es

$$\mathrm{LM}(f) = x^{\mathrm{multideg}(f)}$$

(con coeficiente 1).

(iv) El **término líder** de f es

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

Ejemplo 3.3. Sea $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ y sea $>_{\mathrm{lex}}$ el orden lexicográfico. Entonces:

$$\mathrm{multideg}(f) = (3, 0, 0),$$
$$\mathrm{LC}(f) = -5,$$
$$\mathrm{LM}(f) = x^3,$$
$$\mathrm{LT}(f) = -5x^3.$$

Lema 3.3. *Sean $f, g \in K[x_1, \ldots, x_n]$ polinomios no nulos. Entonces:*

(i) $\mathit{multideg}(fg) = \mathit{multideg}(f) + \mathit{multideg}(g)$.

(ii) Si $f + g \neq 0$, entonces

$$\mathit{multideg}(f + g) \leq \max(\mathit{multideg}(f), \mathit{multideg}(g)).$$

Además, si $\mathit{multideg}(f) \neq \mathit{multideg}(g)$, entonces se alcanza la igualdad.

Demostración.

Sea $f = \sum_\alpha a_\alpha x^\alpha$ y $g = \sum_\beta b_\beta x^\beta$ polinomios en $K[x_1, \ldots, x_n]$, donde $a_\alpha, b_\beta \in K$ y $a_\alpha \neq 0, b_\beta \neq 0$.

(i) Consideremos el producto fg:

$$fg = \sum_{\alpha,\beta} a_\alpha b_\beta x^{\alpha+\beta}.$$

El multigrado de fg, $\mathrm{multideg}(fg)$, corresponde al máximo de los vectores $\alpha + \beta$, donde $\alpha = \mathrm{multideg}(f)$ y $\beta = \mathrm{multideg}(g)$. Por definición, esto implica que

$$\mathrm{multideg}(fg) = \mathrm{multideg}(f) + \mathrm{multideg}(g).$$

(ii) Los términos de grado más alto en f y g determinan el multigrado de $f+g$, pues si no se cancelan al calcular $f+g$, se daría la igualdad. Pero si se cancelan, se daría la desigualdad estricta. Por tanto:

$$\text{multideg}(f+g) \leq \text{máx}(\text{multideg}(f), \text{multideg}(g)).$$

Si $\text{multideg}(f) \neq \text{multideg}(g)$, los términos líderes de f y g no se cancelan, lo que implica que

$$\text{multideg}(f+g) = \text{máx}(\text{multideg}(f), \text{multideg}(g)).$$

Esto prueba la igualdad en el caso indicado.

□

3.2. Algoritmo de División en $K[x_1, \ldots, x_n]$

En la Sección 2.3, del capítulo anterior, vimos cómo el algoritmo de división puede utilizarse para resolver el problema de pertenencia a ideales en el caso de polinomios en una sola variable. Para estudiar este problema cuando hay más variables, formularemos un algoritmo de división en $K[x_1, \ldots, x_n]$. El objetivo es dividir $f \in K[x_1, \ldots, x_n]$ por $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. Como veremos, esto significa expresar f en la forma:

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

donde los elementos $q_1, \ldots, q_s$ y el resto r pertenecen a $K[x_1, \ldots, x_n]$. La idea básica del algoritmo es la misma que en el caso de una variable: queremos cancelar el término líder de f (con respecto a un orden monomial fijo) multiplicando algún f_i por un monomio apropiado y restando. Ese monomio se convierte entonces en un término del cociente correspondiente q_i.

Teorema 3.4 (Algoritmo de División en $K[x_1, \ldots, x_n]$)**.** *Sea $>$ un orden monomial sobre $\mathbb{Z}^n_{\geq 0}$, y sea $F = (f_1, \ldots, f_s)$ una s-tupla ordenada de polinomios en $K[x_1, \ldots, x_n]$. Entonces para todo $f \in K[x_1, \ldots, x_n]$, se puede escribir:*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

*donde $q_i, r \in K[x_1, \ldots, x_n]$, y se cumple que $r = 0$ o bien r es una combinación lineal, con coeficientes en K, de monomios que no son divisibles por ninguno de los términos líderes $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. A este r lo llamamos un **resto** de f al dividirlo por F.*

Además, si $q_i f_i \neq 0$, entonces $\mathrm{multideg}(f) \geq \mathrm{multideg}(q_i f_i)$.

Proporcionaremos un algoritmo para la construcción de $q_1, \ldots, q_s$ y r, lo que automáticamente garantiza su existencia (ver Algoritmo 2). La demostración de su finitud y resultado esperado puede consultarse en [1].

Algoritmo 2 Algoritmo de División en $K[x_1, \ldots, x_n]$

- **Entrada**: $f_1, \ldots, f_s, f \in K[x_1, \ldots, x_n]$
- **Salida**: $q_1, \ldots, q_s, r$

$q_1 := 0;\ \ldots;\ q_s := 0;\ r := 0;$
$p := f;$
while $p \neq 0$ **do**
  $i := 1;$
  `division_ocurrida` := `falso`;
  while $i \leq s$ **and** `division_ocurrida` = `falso` **do**
    if $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$ **then**
      $q_i := q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i);$
      $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))\, f_i;$
      `division_ocurrida` := `verdadero`;
    else
      $i := i + 1;$
    end if
  end while
  if `division_ocurrida` = `falso` **then**
    $r := r + \mathrm{LT}(p);$
    $p := p - \mathrm{LT}(p);$
  end if
end while
return $q_1, \ldots, q_s, r;$
end

3.3. Ideales monomiales

Para comenzar, definimos los ideales monomiales en $K[x_1, \ldots, x_n]$.

Definición 3.9. Un ideal $I \subseteq K[x_1, \ldots, x_n]$ es un **ideal monomial** si existe un subconjunto $A \subseteq \mathbb{Z}^n_{\geq 0}$ (posiblemente infinito) tal que I consiste en todos los polinomios que son sumas finitas de la forma

$$\sum_{\alpha \in A} h_\alpha x^\alpha,$$

donde $h_\alpha \in K[x_1, \ldots, x_n]$. En este caso, escribimos

$$I = \langle x^\alpha \mid \alpha \in A \rangle.$$

Ejemplo 3.4. Un ejemplo de un ideal monomial está dado por

$$I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle \subseteq K[x, y].$$

Primero necesitamos caracterizar todos los monomios que pertenecen a un ideal monomial dado.

Lema 3.5. *Sea $I = \langle x^\alpha \mid \alpha \in A \rangle$ un ideal monomial. Entonces un monomio x^β pertenece a I si y solo si x^β es divisible por x^α para algún $\alpha \in A$.*

Demostración.

$\boxed{\Leftarrow}$ Si x^β es un múltiplo de x^α para algún $\alpha \in A$, entonces $x^\beta \in I$ por la definición del ideal.
$\boxed{\Rightarrow}$ Recíprocamente, si $x^\beta \in I$, entonces

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)},$$

donde $h_i \in K[x_1, \ldots, x_n]$ y $\alpha(i) \in A$. Si expandimos cada h_i como una suma de términos, obtenemos

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} = \sum_{i=1}^{s} \left(\sum_j c_{i,j} x^{\beta(i,j)} \right) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}.$$

Después de agrupar términos del mismo multigrado, 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. □

Observación 3.5. Nótese que x^β es divisible por x^α exactamente cuando $x^\beta = x^\alpha \cdot x^\gamma$ para algún $\gamma \in \mathbb{Z}^n_{\geq 0}$. Esto es equivalente a $\beta = \alpha + \gamma$. Por lo tanto, el conjunto

$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma \mid \gamma \in \mathbb{Z}^n_{\geq 0}\}$$

consiste en los exponentes de todos los monomios divisibles por x^α.

Sea $f \in K[x_1, \ldots, x_n]$. Mostraremos que determinar si un polinomio f pertenece a un ideal monomial se puede determinar analizando los monomios de f.

Lema 3.6. *Sea I un ideal monomial y sea $f \in K[x_1, \ldots, x_n]$. Entonces las siguientes afirmaciones son equivalentes:*

1. *$f \in I$.*
2. *Cada monomio de f pertenece a I.*
3. *f es una combinación K-lineal de los monomios en I.*

Corolario 3.7. *Dos ideales monomiales son iguales si y solo si contienen los mismos monomios.*

Nota 3.3. El resultado principal de esta sección es que todos los ideales monomiales de $K[x_1, \ldots, x_n]$ son finitamente generados.

Teorema 3.8 (Lema de Dickson)**.** *Sea $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$ un ideal monomial. Entonces I puede escribirse en la forma*

$$I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle,$$

donde $\alpha(1), \ldots, \alpha(s) \in A$. En particular, I tiene una base finita.

Nota 3.4. La demostración de 3.6, 3.7, y 3.8 puede consultarse en [1].

También podemos usar el Lema de Dickson para demostrar el siguiente hecho importante sobre los órdenes monomiales en $K[x_1, \ldots, x_n]$.

Proposición 3.9. *Un ideal monomial $I \subseteq K[x_1, \ldots, x_n]$ tiene una base $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ con la propiedad de que $x^{\alpha(i)}$ no divide a $x^{\alpha(j)}$ para $i \neq j$. Además, esta base es única y se llama* ***base mínima*** *de I.*

Demostración.

Por el Teorema 3.8, I tiene una base finita que consiste en monomios. Si un monomio en esta base divide a otro, entonces podemos descartarlo y aún así tener una base. Repetir este proceso prueba la existencia de una base mínima $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$.

Para la unicidad, supongamos que $x^{\beta(1)}, \ldots, x^{\beta(t)}$ es una segunda base mínima de I. Entonces $x^{\alpha(1)} \in I$ y el Lema 3.5 implica que $x^{\beta(i)} \mid x^{\alpha(1)}$ para algún i. Cambiando a la otra base, $x^{\beta(i)} \in I$ implica que $x^{\alpha(j)} \mid x^{\beta(i)}$ para algún j. Así, $x^{\alpha(j)} \mid x^{\alpha(1)}$, lo cual, por minimalidad, implica $j = 1$, y $x^{\alpha(1)} = x^{\beta(i)}$ sigue fácilmente. Continuando de esta manera, vemos que la primera base está contenida en la segunda. Luego, la igualdad sigue al intercambiar ambas bases. □

3.4. Teorema de la Base de Hilbert y Bases de Groebner

Una vez que elegimos un órden monomial, cada $f \in K[x_1, \ldots, x_n]$ no nulo tiene un término líder único $LT(f)$. Entonces para cualquier ideal I, podemos definir su ideal de términos líderes.

Definición 3.10. Fijado un orden monomial en $K[x_1, \ldots, x_n]$, y sea $I \subseteq K[x_1, \ldots, x_n]$ un ideal distinto de $\{0\}$. Entonces:

1. Denotamos por $LT(I)$ al **conjunto de términos líderes de los elementos no nulos de I**. Así,

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

2. Denotamos por $\langle LT(I) \rangle$ al **ideal generado por los elementos de LT(I)**.

Observación 3.6. Si tenemos un conjunto finito de generadores para I, $I = \langle f_1, \ldots, f_s \rangle$, entonces $\langle LT(f_1), \ldots, LT(f_s) \rangle$ y $\langle LT(I) \rangle$ pueden ser ideales diferentes. Es cierto que dado $1 \leq i \leq s$, $LT(f_i) \in LT(I) \subseteq \langle LT(I) \rangle$ por definición, lo que implica $\langle LT(f_1), \ldots, LT(f_s) \rangle \subseteq \langle LT(I) \rangle$. Sin embargo, $\langle LT(I) \rangle$ puede ser estrictamente mayor.

Ejemplo 3.5. Para aclarar la observación anterior, consideremos el siguiente ejemplo. Sea $I = \langle f_1, f_2 \rangle$, donde $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$, y usemos el orden grlex en los monomios de $K[x, y]$. Entonces

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

de modo que $x^2 = x \cdot f_2 - y \cdot f_1$, luego $x^2 \in I$. Por lo tanto, $x^2 = LT(x^2) \in \langle LT(I) \rangle$. Sin embargo, x^2 no es divisible por $LT(f_1) = x^3$ ni por $LT(f_2) = x^2y$, por lo que $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$ según el Lema 3.5.

Proposición 3.10. *Sea $I \subseteq K[x_1, \ldots, x_n]$ un ideal distinto de $\{0\}$.*

1. *$\langle LT(I) \rangle$ es un ideal monomial.*
2. *Existen $g_1, \ldots, g_t \in I$ tales que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.*

Demostración.

1. Los monomios líderes $LM(g)$ de los elementos $g \in I \setminus \{0\}$ generan el ideal monomial $\langle LM(g) \mid g \in I \setminus \{0\} \rangle$. Dado que $LM(g)$ y $LT(g)$ difieren por una constante no nula, este ideal es igual a $\langle LT(g) \mid g \in I \setminus \{0\} \rangle = \langle LT(I) \rangle$. Por lo tanto, $\langle LT(I) \rangle$ es un ideal monomial.
2. Dado que $\langle LT(I) \rangle$ es generado por los monomios $LM(g)$ para $g \in I \setminus \{0\}$, el Lema de Dickson nos dice que $\langle LT(I) \rangle = \langle LM(g_1), \ldots, LM(g_t) \rangle$ para un número finito de elementos $g_1, \ldots, g_t \in I$. Dado que $LM(g_i)$ difiere de $LT(g_i)$ por una constante no nula, se deduce que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

□

Ahora podemos usar la Proposición 3.10 y el algoritmo de división para demostrar la existencia de un conjunto finito de generadores para todo ideal de polinomios.

Teorema 3.11 (Teorema de la Base de Hilbert)**.** *Todo ideal $I \subseteq K[x_1, \ldots, x_n]$ tiene un conjunto finito de generadores. En otras palabras, $I = \langle g_1, \ldots, g_t \rangle$ para algunos $g_1, \ldots, g_t \in I$.*

Demostración.

Si $I = \{0\}$, tomamos nuestro conjunto generador como $\{0\}$, lo cual es ciertamente finito. Si I contiene algún polinomio no nulo, entonces se puede construir un conjunto generador $g_1, \ldots, g_t$ para I de la siguiente manera: primero seleccionamos un orden monomial

particular para usar en el algoritmo de división y en el cálculo de los términos líderes. Entonces I tiene un ideal de términos líderes $\langle \mathrm{LT}(I)\rangle$. Por la Proposición 3.10, existen $g_1, \ldots, g_t \in I$ tales que $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$. Veamos que $I = \langle g_1, \ldots, g_t\rangle$.

Es claro que $\langle g_1, \ldots, g_t\rangle \subseteq I$ ya que cada $g_i \in I$. Por otro lado, sea $f \in I$ cualquier polinomio. Si aplicamos el algoritmo de división para dividir f por $\{g_1, \ldots, g_t\}$, obtenemos una expresión de la forma

$$f = q_1 g_1 + \cdots + q_t g_t + r$$

donde ningún término de r es divisible por ninguno de $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Afirmamos que $r = 0$. Para ver esto, notemos que

$$r = f - q_1 g_1 - \cdots - q_t g_t \in I.$$

Si $r \neq 0$, entonces $\mathrm{LT}(r) \in \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$, y por el Lema 3.5, se deduce que $\mathrm{LT}(r)$ debe ser divisible por alguno de los $\mathrm{LT}(g_i)$. Esto contradice lo que significa ser un residuo, y, en consecuencia, r debe ser cero. Por lo tanto,

$$f = q_1 g_1 + \cdots + q_t g_t + 0 \in \langle g_1, \ldots, g_t\rangle,$$

lo que demuestra que $I \subseteq \langle g_1, \ldots, g_t\rangle$.

□

Observación 3.7. La base $\{g_1, \ldots, g_t\}$ utilizada en el Teorema 3.11 tiene la propiedad especial de que $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$. Estas bases especiales son las bases de Groebner, que motivan el desarrollo de este capítulo, y ayudan a construir los algoritmos de triangulación que veremos más adelante. A continuación, su definición formal:

Definición 3.11. Fijado un orden monomial en el anillo de polinomios $K[x_1, \ldots, x_n]$, sea un subconjunto finito $G = \{g_1, \ldots, g_t\}$ de un ideal $I \subseteq K[x_1, \ldots, x_n]$ distinto de $\{0\}$. Se dice que G es una **base de Groebner** de I si

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle.$$

Observación 3.8. Equivalentemente, aunque de manera más informal, un conjunto $\{g_1, \ldots, g_t\} \subseteq I$ es una base de Groebner de I si y sólo si el término líder de cualquier elemento de I es divisible por uno de los $\mathrm{LT}(g_i)$ (esto se deduce del Lema 3.5, del algoritmo de división en varias variables, y en particular del hecho de que el resto al dividir un elemento de I entre una base de Gröbner es cero).

La demostración del Teorema 3.11 también establece el siguiente resultado.

Corolario 3.12. *Fijado un orden monomial. Entonces todo ideal $I \subseteq K[x_1, \ldots, x_n]$ tiene una base de Groebner. Además, cualquier base de Groebner de un ideal I es una base de I.*

Demostración.

Dado un ideal no nulo, el conjunto $G = \{g_1, \ldots, g_t\}$ construido en la demostración del Teorema 3.11 es una base de Groebner por definición. Para la segunda afirmación, observemos que si $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, entonces el argumento dado en el Teorema 3.11 muestra que $I = \langle g_1, \ldots, g_t \rangle$, por lo que G es una base de I. □

Concluimos esta sección con una aplicación del Teorema de la Base de Hilbert.

Definición 3.12. Sean $I_1, I_2, I_3, \ldots$ ideales. Una **cadena ascendente** de ideales es una secuencia anidada e incremental:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

El próximo resultado muestra un fenómeno que ocurre en toda cadena ascendente de ideales en $K[x_1, \ldots, x_n]$.

Teorema 3.13 (Condición de Cadena Ascendente)**.** *Sea*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

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

$$I_N = I_{N+1} = I_{N+2} = \cdots .$$

Demostración.

Dada la cadena ascendente $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$, consideremos el ideal $I = \bigcup_{i=1}^{\infty} I_i$. Comenzamos mostrando que I también es un ideal en $K[x_1, \ldots, x_n]$. Primero, $0 \in I$ ya que $0 \in I_i$ para cada i. Ahora, si $f, g \in I$, entonces por definición, $f \in I_i$ y $g \in I_j$ para algún i y j (posiblemente diferentes). Sin pérdida de generalidad, reetiquetamos para que $i \leq j$, entonces tanto f como g están en I_j. Dado que I_j es un ideal, la suma $f + g \in I_j$, por lo tanto, $f + g \in I$. De manera similar, si $f \in I$ y $r \in K[x_1, \ldots, x_n]$, entonces $f \in I_i$ para algún i, y $r \cdot f \in I_i \subseteq I$. Por lo tanto, I es un ideal.

Por el Teorema de la Base de Hilbert, el ideal I debe tener un conjunto generador finito: $I = \langle f_1, \ldots, f_s \rangle$. Sin embargo, cada uno de los generadores está contenido en alguno de los I_j, digamos $f_i \in I_{j_i}$ para algún j_i, $i = 1, \ldots, s$. Tomamos N como el máximo de los j_i. Entonces por la definición de una cadena ascendente, $f_i \in I_N$ para todos los i. Por lo tanto, tenemos

$$I = \langle f_1, \ldots, f_s \rangle \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I.$$

Como resultado, la cadena ascendente se estabiliza con I_N. Todos los ideales subsecuentes en la cadena son iguales. □

Definición 3.13. Sea $I \subseteq K[x_1, \ldots, x_n]$ un ideal. Denotaremos por $\mathcal{V}(I)$ el conjunto

$$\mathcal{V}(I) = \{(a_1, \ldots, a_n) \in K^n \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } f \in I\}.$$

Proposición 3.14. *$\mathcal{V}(I)$ es una variedad afín. En particular, si $I = \langle f_1, \ldots, f_s \rangle$, entonces $\mathcal{V}(I) = \mathcal{V}(f_1, \ldots, f_s)$.*

Demostración.

Por el Teorema de la Base de Hilbert, $I = \langle f_1, \ldots, f_s \rangle$ para algún conjunto finito de generadores. Veamos que $\mathcal{V}(I) = \mathcal{V}(f_1, \ldots, f_s)$. Primero, dado que $f_i \in I$, si $f(a_1, \ldots, a_n) = 0$ para todo $f \in I$, entonces $f_i(a_1, \ldots, a_n) = 0$ para todo i. Por lo tanto, $\mathcal{V}(I) \subseteq \mathcal{V}(f_1, \ldots, f_s)$.

Por otro lado, sea $(a_1, \ldots, a_n) \in \mathcal{V}(f_1, \ldots, f_s)$ y sea $f \in I$. Dado que $I = \langle f_1, \ldots, f_s \rangle$,

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

para algunos $h_i \in K[x_1, \ldots, x_n]$. Entonces

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

Como $(a_1, \ldots, a_n) \in \mathcal{V}(f_1, \ldots, f_s)$, se tiene que $f_i(a_1, \ldots, a_n) = 0$ para todo i. Por lo tanto,

$$f(a_1, \ldots, a_n) = 0.$$

Así, $\mathcal{V}(f_1, \ldots, f_s) \subseteq \mathcal{V}(I)$ y, por lo tanto, son iguales. □

Nota 3.5. Lo interesante de esta proposición es que muestra que las variedades están determinadas por los ideales: con unos generadores adecuados del ideal I, podemos entender la variedad $\mathcal{V}(I)$.

3.5. Propiedades de las Bases de Groebner

Como vimos en la Sección 3.4, todo ideal no nulo $I \subseteq K[x_1, \ldots, x_n]$ tiene una base de Groebner. En esta sección, estudiaremos las propiedades de las bases de Groebner y aprenderemos cómo detectar cuándo una base dada es una base de Groebner. Empezaremos mostrando qué comportamiento tiene el algoritmo de división cuando dividimos entre los elementos de una base de Groebner.

Proposición 3.15. *Sea $I \subseteq K[x_1, \ldots, x_n]$ un ideal y sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner de I. Entonces dado $f \in K[x_1, \ldots, x_n]$, existe un único $r \in K[x_1, \ldots, x_n]$ con las siguientes dos propiedades:*

(i) Ningún término de r es divisible por ninguno de los $LT(g_1), \ldots, LT(g_t)$.

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

En particular, r es el residuo al dividir f por G, sin importar el orden en que los elementos de G son listados al usar el algoritmo de división.

Demostración.

El algoritmo de división da $f = q_1 g_1 + \cdots + q_t g_t + r$, donde r satisface (i). También podemos satisfacer (ii) al tomar $g = q_1 g_1 + \cdots + q_t g_t \in I$. Esto prueba la existencia de r.

Para demostrar la unicidad, supongamos que $f = g + r = g' + r'$ también satisface (i) y (ii). Entonces $r - r' = g' - g \in I$, por lo que si $r \neq r'$, entonces $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Por el Lema 3.5, esto implica que $\mathrm{LT}(r - r')$ es divisible por algún $\mathrm{LT}(g_i)$. Esto es imposible porque ningún término de r o r' es divisible por ninguno de $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Por lo tanto, $r - r'$ debe ser cero, y se prueba la unicidad.

El resultado final de la proposición se deduce de la unicidad de r. □

Corolario 3.16. *Sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner para un ideal $I \subseteq K[x_1, \ldots, x_n]$ y sea $f \in K[x_1, \ldots, x_n]$. Entonces $f \in I$ si y solo si el residuo de la división de f por G es cero.*

Demostración.

$\boxed{\Leftarrow}$ Si el residuo es cero, entonces ya hemos observado que $f \in I$.
$\boxed{\Rightarrow}$ De manera inversa, si $f \in I$, entonces $f = f + 0$ satisface las dos condiciones de la Proposición 3.15. De esto se sigue que 0 es el residuo de f al dividirlo por G. □

Usando el Corolario 3.16, obtenemos un algoritmo para resolver el problema de pertenencia al ideal, dado que conocemos una base de Groebner G para el ideal en cuestión. Solo necesitamos calcular un residuo con respecto a G para determinar si $f \in I$.

Definición 3.14. Dado $F = (f_1, \ldots, f_s)$, escribiremos $\overline{f}^F$ para el residuo de la división de f por F, es decir, el polinomio h en la descomposición:

$$f = \sum_{k=1}^{s} g_k f_k + h,$$

donde ningún término de h es divisible por ningún término líder de los f_k.

Observación 3.9. Realicemos una observación que se utilizará más adelante, en la Sección 3.7. Cuando F es una base de Groebner de un ideal I, el residuo h de la Definición 3.14 es único y se denomina la **forma normal** de f módulo I.

Ejemplo 3.6. Por ejemplo, si $F = \langle x^2y - y^2, x^4y^2 - y^2 \rangle \subseteq K[x, y]$, usando el orden lexicográfico, tenemos que

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

ya que el algoritmo de división produce

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

A continuación, veremos cómo determinar si un conjunto generador dado de un ideal es una base de Groebner. Como hemos indicado, el obstáculo para que $\{f_1, \ldots, f_s\}$ sea una base de Groebner es la posible aparición de combinaciones de los f_j cuyos términos líderes no están en el ideal generado por $\mathrm{LT}(f_j)$. Una forma en la que esto puede ocurrir es si los términos líderes en una combinación adecuada

$$x^\alpha f_i - bx^\beta f_j$$

se cancelan, dejando solo términos más pequeños. Por otro lado, $x^\alpha f_i - bx^\beta f_j \in I$, por lo que su término líder está en $\langle \mathrm{LT}(I) \rangle$.

Definición 3.15. Sean $f, g \in K[x_1, \ldots, x_n]$ polinomios no nulos.

(I) Si multideg$(f) = \alpha$ y multideg$(g) = \beta$, definimos $\gamma = (\gamma_1, \ldots, \gamma_n)$, donde $\gamma_i = \text{máx}(\alpha_i, \beta_i)$ para cada i. Llamamos x^γ al **mínimo común múltiplo** de LM(f) y LM(g), denotado por $x^\gamma = \text{mcm}(\text{LM}(f), \text{LM}(g))$.

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

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

Ejemplo 3.7. Sean los polinomios $f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2$ en $\mathbb{R}[x, y]$ con el orden grlex. Entonces $\gamma = (4, 2)$, y $x^\gamma = x^4y^2$

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

Observación 3.10. Un S-polinomio $S(f, g)$ está *diseñado* para cancelar los términos líderes. El siguiente lema muestra que toda cancelación de términos líderes entre polinomios con el mismo multigrado proviene de la cancelación que ocurre con los S-polinomios.

Lema 3.17. *Supongamos que tenemos una suma* $\sum_{i=1}^s p_i$, *donde* multideg$(p_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ *para todo* i. *Si* multideg $(\sum_{i=1}^s p_i) < \delta$, *entonces* $\sum_{i=1}^s p_i$ *es una combinación lineal, con coeficientes en* K, *de los S-polinomios* $S(p_j, p_l)$ *para* $1 \leq j, l \leq s$. *Además, cada* $S(p_j, p_l)$ *tiene multigrado* $< \delta$.

La demostración puede consultarse en [1]

Observación 3.11. Cuando $p_1, \ldots, p_s$ satisfacen la hipótesis del Lema 3.17, obtenemos una ecuación de la forma

$$\sum_{i=1}^{s} p_i = \sum_{j,l} c_{jl} S(p_j, p_l).$$

Consideremos dónde ocurre la cancelación. En la suma del lado izquierdo, cada sumando p_i tiene multigrado δ, por lo que la cancelación ocurre solo después de sumarlos. Sin embargo, en la suma del lado derecho, cada sumando $c_{jl}S(p_j, p_l)$ tiene multigrado $< \delta$, por lo que la cancelación ya ha ocurrido. Intuitivamente, esto significa que toda cancelación puede explicarse mediante S-polinomios.

Usando S-polinomios, podemos ahora demostrar el criterio de Buchberger para determinar cuando una base de un ideal es una base de Groebner.

Teorema 3.18 (Criterio de Buchberger)**.** *Sea I un ideal de polinomios. Entonces una base $G = \{g_1, \ldots, g_s\}$ de I es una base de Groebner de I si y solo si para todos los pares $i \neq j$, el residuo de la división de $S(g_i, g_j)$ por G (enumerado en algún orden) es cero.*

Demostración.

$\boxed{\Rightarrow}$ Si G es una base de Groebner, entonces dado que $S(g_i, g_j) \in I$, el residuo de la división de $S(g_i, g_j)$ por G es cero por el Corolario 3.16.

$\boxed{\Leftarrow}$ Sea $f \in I$ no nulo. Mostraremos que $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$ como sigue. Escribimos

$$f = \sum_{i=1}^{t} h_i g_i, \quad h_i \in K[x_1, \ldots, x_n].$$

Por el Lema 3.3, se sigue que

$$\mathrm{multideg}(f) \leq \mathrm{máx}\{\mathrm{multideg}(h_i g_i) \mid h_i \neq 0\}. \tag{3.1}$$

La estrategia de la demostración es elegir la representación más eficiente de f, lo que significa que entre todas las expresiones $f = \sum_{i=1}^{t} h_i g_i$, elegimos una para la cual

$$\delta = \mathrm{máx}\{\mathrm{multideg}(h_i g_i) \mid h_i \neq 0\}.$$

es mínimo. El δ mínimo existe por la propiedad de buen orden de nuestro orden monomial. Por (3.1), se deduce que $\mathrm{multideg}(f) \leq \delta$.

Si ocurre la igualdad, entonces $\mathrm{multideg}(f) = \mathrm{multideg}(h_i g_i)$ para algún i. Esto implica fácilmente que $\mathrm{LT}(f)$ es divisible por $\mathrm{LT}(g_i)$. Entonces $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$, que es lo que queremos probar.

Queda por considerar el caso en el que el δ mínimo satisface $\mathrm{multideg}(f) < \delta$. Usaremos $\overline{S(g_i, g_j)}^{G} = 0$ para $i \neq j$ para encontrar una nueva expresión para f que disminuya δ. Esto contradecirá la minimalidad de δ y completará la demostración.

Dada una expresión

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

con δ mínimo, comenzamos aislando la parte de la suma donde ocurre la multigrado δ:

$$\begin{aligned} f &= \sum_{\text{multideg}(h_i g_i)=\delta} h_i g_i + \sum_{\text{multideg}(h_i g_i)<\delta} h_i g_i \\ &= \sum_{\text{multideg}(h_i g_i)=\delta} \text{LT}(h_i) g_i + \sum_{\text{multideg}(h_i g_i)=\delta} (h_i - \text{LT}(h_i)) g_i + \sum_{\text{multideg}(h_i g_i)<\delta} h_i g_i. \end{aligned} \tag{3.2}$$

Los monomios que aparecen en la segunda y tercera sumas en la segunda línea tienen todos multigrado $< \delta$. Entonces $\text{multideg}(f) < \delta$ significa que la primera suma en la segunda línea también tiene multigrado $< \delta$.

La clave para disminuir δ es reescribir la primera suma en términos de S-polinomios y luego usar $S(g_i, g_j)^G = 0$ para reescribir los S-polinomios sin cancelación.

Para expresar la primera suma en la segunda línea de la ecuación (3.2) usando S-polinomios, observemos que:

$$\sum_{\text{multideg}(h_i g_i)=\delta} \text{LT}(h_i) g_i \tag{3.3}$$

satisface la hipótesis del Lema 3.17 ya que cada $p_i = \text{LT}(h_i) g_i$ tiene multigrado δ y la suma tiene multigrado $< \delta$. Por lo tanto, la primera suma es una combinación lineal con coeficientes en K de los S-polinomios $S(p_i, p_j)$.

$$S(p_i, p_j) = x^{\delta - \gamma_{ij}} \, S(g_i, g_j) \tag{3.4}$$

donde $x^{\gamma_{ij}} = \text{mcm}(\text{LM}(g_i), \text{LM}(g_j))$.

Por lo tanto, la suma (3.3) es una combinación lineal de $x^{\delta - \gamma_{ij}} S(g_i, g_j)$ para ciertos pares (i, j). Consideremos uno de estos S-polinomios $S(g_i, g_j)$. Dado que $S(g_i, g_j)^G = 0$, el algoritmo de división da una expresión

$$S(g_i, g_j) = \sum_{l=1}^{t} A_l g_l, \tag{3.5}$$

donde $A_l \in K[x_1, \ldots, x_n]$ y

$$\text{multideg}(A_l g_l) \leq \text{multideg}(S(g_i, g_j)), \tag{3.6}$$

cuando $A_l g_l \neq 0$. Multiplicando ambos lados de (3.5) por $x^{\delta-\gamma_{ij}}$, obtenemos

$$x^{\delta-\gamma_{ij}} S(g_i, g_j) = \sum_{l=1}^{t} B_l g_l, \tag{3.7}$$

donde $B_l = x^{\delta-\gamma_{ij}} A_l$. Luego, (3.6) implica que cuando $B_l g_l \neq 0$, tenemos

$$\text{multideg}(B_l g_l) \leq \text{multideg}(x^{\delta-\gamma_{ij}} S(g_i, g_j)) < \delta, \tag{3.8}$$

ya que $\text{LT}(S(g_i, g_j)) < \text{mcm}(\text{LM}(g_i), \text{LM}(g_j)) = x^{\gamma_{ij}}$.

$$\sum_{\text{multideg}(h_i g_i)=\delta} \text{LT}(h_i) g_i = \sum_{l=1}^{r} \tilde{B}_l g_l \tag{3.9}$$

con la propiedad de que cuando $\tilde{B}_l g_l \neq 0$, tenemos

$$\text{multideg}(\tilde{B}_l g_l) < \delta. \tag{3.10}$$

Sustituyendo (3.9) en la segunda línea de (3.3), obtenemos una expresión para f como una combinación polinómica de los g_i, donde todos los términos tienen multigrado $< \delta$. Esto contradice la minimalidad de δ y completa la demostración del teorema.

□

Nota 3.6. El criterio de Buchberger dado en el Teorema 3.18 es uno de los resultados clave sobre bases de Groebner. Hemos visto que las bases de Groebner tienen propiedades interesantes, pero hasta ahora ha sido difícil determinar si una base de un ideal es una base de Groebner. Usando el criterio de Buchberger, es fácil mostrar si una base dada es una base de Groebner. Además, en la Sección 3.6 veremos que el criterio del par-S también conduce a un algoritmo para calcular bases de Groebner.

Ejemplo 3.8. Como ejemplo de cómo usar el Teorema 3.18, consideremos el ideal $I = \langle y - x^2, z - x^3 \rangle$ en $\mathbb{R}^3$. Afirmamos que $G = \{y - x^2, z - x^3\}$ es una base de Groebner para el orden lexicográfico. Para probar 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 división, encontramos que

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

por lo que $\overline{S(y - x^2, z - x^3)}^G = 0$. Así, por el Teorema 3.18, G es una base de Groebner para I.

3.6. Algoritmo de Buchberger

En el Corolario 3.12, vimos que todo ideal en $K[x_1, \ldots, x_n]$ tiene una base de Groebner. Sin embargo, la demostración no era constructiva en el sentido de que no nos indicaba cómo producir la base de Groebner. Por lo tanto, dado un ideal $I \subseteq K[x_1, \ldots, x_n]$, ahora vamos a tratar la cuestión de construir una base de Groebner para I.

Ejemplo 3.9. Consideremos el anillo $\mathbb{Q}[x, y]$ con orden lexicográfico graduado (*grlex order*), y sea $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. En el Ejemplo 3.5 vimos que $\{f_1, f_2\}$ no es una base de Groebner para I ya que $\mathrm{LT}(S(f_1, f_2)) = -x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$.

Para construir una base de Groebner, una idea natural es intentar extender el conjunto generador original añadiendo más polinomios en I. Por lo visto en la Sección 3.5, podemos añadir S-polinomios. Tenemos $S(f_1, f_2) = -x^2 \in I$, y su residuo al dividir por $F = (f_1, f_2)$ es $-x^2$, que no es cero. Por lo tanto, debemos incluir ese residuo en nuestro conjunto generador como un nuevo generador $f_3 = -x^2$. Si definimos $F = (f_1, f_2, f_3)$, podemos usar el Criterio de Buchberger para comprobar si este nuevo conjunto es una base de Groebner para I. Calculamos:

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

Por lo tanto, debemos añadir $f_4 = -2xy$ a nuestro conjunto generador. Si definimos $F = (f_1, f_2, f_3, f_4)$, entonces:

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

Por lo tanto, también añadimos $f_5 = -2y^2 + x$ a nuestro conjunto generador. Al establecer $F = (f_1, f_2, f_3, f_4, f_5)$, se puede comprobar que

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

Por el Criterio de Buchberger, se deduce que una base de Groebner en orden lexicográfico graduado (*grlex order*) para I está dada por:

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

Observación 3.12. El ejemplo anterior sugiere que, en general, se debe intentar extender una base F a una base de Groebner añadiendo sucesivamente los residuos no nulos $\overline{S(f_i, f_j)}^F$ a F. Esta idea conduce al siguiente algoritmo, debido al criterio de Buchberger, para calcular una base de Groebner.

Teorema 3.19 (Algoritmo de Buchberger)**.** *Sea $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ un ideal de polinomios. Entonces una base de Groebner para I puede construirse en un número finito de pasos utilizando el siguiente algoritmo:*

Algoritmo 3 Algoritmo de Buchberger

- **Entrada:** $F = \{f_1, \ldots, f_s\}$
- **Salida:** Una base de Groebner $G = \{g_1, \ldots, g_t\}$ para I, con $F \subseteq G$

```
1: G := F;
2: repeat
3:    G' := G;
4:    for cada par {p, q}, p ≠ q en G' do
5:       r := S(p, q)^G;
6:       if r ≠ 0 then
7:          G := G ∪ {r};
8:       end if
9:    end for
10: until G = G'
11: return G;
12: end
```

Demostración.

Comenzamos con algunas notaciones. Si $G = \{g_1, \ldots, g_t\}$, entonces $\langle G \rangle$ y $\langle \mathrm{LT}(G) \rangle$ denotarán los siguientes ideales:

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle, \quad \langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle.$$

Pasando a la demostración del teorema, primero veamos que $G \subseteq I$ se cumple en cada etapa del algoritmo. Esto es cierto inicialmente, y cada vez que ampliamos G, lo hacemos añadiendo el residuo $r = \overline{S(p,q)}^{G'}$ para $p, q \in G' \subseteq G$. Así, si $G \subseteq I$, entonces $p, q \in I$ y, por lo tanto, $S(p,q) \in I$. Además, como estamos dividiendo por $G' \subseteq I$, obtenemos que $G \cup \{r\} \subseteq I$. También notamos que G contiene la base inicial F de I, por lo que G es efectivamente una base de I.

El algoritmo termina cuando $G = G'$, lo que significa que $r = \overline{S(p,q)}^{G'} = 0$ para todos $p, q \in G$. Por lo tanto, G es una base de Groebner de $\langle G \rangle = I$ por el Criterio de Buchberger.

Queda por demostrar que el algoritmo termina. Necesitamos considerar lo que ocurre después de cada iteración del bucle principal. El conjunto G consiste en G' (el G antiguo) junto con los residuos no nulos de los S-polinomios de los elementos de G'. Entonces:

$$\langle \mathrm{LT}(G') \rangle \subseteq \langle \mathrm{LT}(G) \rangle, \tag{3.11}$$

ya que $G' \subseteq G$. Además, si $G' \neq G$, afirmamos que $\langle \mathrm{LT}(G') \rangle$ es estrictamente menor que $\langle \mathrm{LT}(G) \rangle$. Para ver esto, supongamos que un residuo no nulo r de un S-polinomio ha sido añadido a G. Como r es un residuo tras dividir por G', $\mathrm{LT}(r)$ no es divisible por los términos líderes de los elementos de G', y por lo tanto $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$ por el Lema 3.5. Sin embargo, $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$, lo que prueba nuestra afirmación.

Por (3.11), los ideales $\langle \mathrm{LT}(G') \rangle$ de iteraciones sucesivas del bucle forman una cadena ascendente de ideales en $K[x_1, \ldots, x_n]$. Así, el Teorema 3.13 (Condición de Cadena Ascendente) implica que, tras un número finito de iteraciones, la cadena se estabiliza, de modo que $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$, lo cual debe ocurrir eventualmente. Por el párrafo anterior, esto implica que $G' = G$, de modo que el algoritmo debe terminar después de un número finito de pasos.

□

Observación 3.13. Tomados en conjunto, el Criterio de Buchberger (Teorema 3.18) y el algoritmo de Buchberger (Teorema 3.19) proporcionan una base algorítmica para la teoría de las bases de Groebner.

Observación 3.14. Notemos (como una mejora) que una vez que un residuo $\overline{S(p,q)}^{G'} = 0$, este residuo permanecerá cero incluso si añadimos más elementos al conjunto generador G'. Por lo tanto, no hay razón para volver a calcular esos residuos en iteraciones posteriores del bucle principal. De hecho, si añadimos nuestros nuevos generadores f_j uno a la vez, los únicos residuos que necesitan ser comprobados son $\overline{S(f_i, f_j)}^{G'}$, donde $i < j - 1$. Las

bases de Groebner calculadas utilizando el algoritmo del Teorema 3.19 a menudo son más grandes de lo necesario. Podemos entonces eliminar algunos generadores innecesarios utilizando el siguiente resultado.

Lema 3.20. *Sea G una base de Groebner de $I \subseteq K[x_1, \ldots, x_n]$. Sea $p \in G$ un polinomio tal que $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$. Entonces $G \setminus \{p\}$ también es una base de Groebner para I.*

Demostración.

Sabemos que $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. Si $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$, entonces tenemos $\langle \mathrm{LT}(G \setminus \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle$. Por definición, se deduce que $G \setminus \{p\}$ también es una base de Groebner para I. □

Observación 3.15. Podemos construir una base de Groebner mínima para un ideal no nulo dado aplicando el algoritmo del Teorema 3.19 y luego utilizando el Lema 3.20 para eliminar cualquier generador innecesario que haya podido ser incluido.

Ejemplo 3.10. Para ilustrar este procedimiento, retomamos el ideal $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Usando el orden *grlex*, encontramos la base de Groebner

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

Dado que algunos de los coeficientes principales son distintos de 1, el primer paso es multiplicar los generadores por constantes adecuadas para que esto sea cierto. Entonces observamos que

$$\mathrm{LT}(f_1) = x^3 = -x \cdot \mathrm{LT}(f_3).$$

Por el Lema 3.20, podemos prescindir de f_1 en la base de Groebner mínima. De manera similar, dado que

$$\mathrm{LT}(f_2) = x^2y = -(1/2)x \cdot \mathrm{LT}(f_4),$$

también podemos eliminar f_2. No hay más casos donde el término líder de un generador divida el término líder de otro generador.

Por lo tanto:

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

es una base de Groebner mínima para I.

Cuando G es una base de Groebner mínima, los términos líderes $\mathrm{LT}(p)$, $p \in G$, forman la única base mínima de $\langle \mathrm{LT}(I) \rangle$ por la Proposición 3.9. Sin embargo, el ideal original I

puede tener muchas bases de Groebner mínimas. Por ejemplo, en el ideal que consideramos arriba,

$$\tilde{f}_3 = x^2 + axy, \quad \tilde{f}_4 = xy, \quad \tilde{f}_5 = y^2 - (1/2)x$$

es una base de Groebner mínima para I, donde $a \in \mathbb{Q}$ es una constante. Esto ilustra que las bases de Groebner mínimas no son necesariamente únicas. Afortunadamente, podemos identificar una base mínima que es mejor que las demás.

Definición 3.16. Una **base de Groebner reducida** para un ideal de polinomios I es una base de Groebner G para I tal que:

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

(ii) Para todo $p \in G$, ningún monomio de p pertenece a $\langle \mathrm{LT}(G \setminus \{p\}) \rangle$.

En general, las bases de Groebner reducidas tienen la siguiente propiedad interesante.

Teorema 3.21. *Sea $I \neq \{0\}$ un ideal de polinomios. Entonces para un orden monomial dado, I tiene una base de Groebner reducida, y dicha base de Groebner reducida es única.*

Observación 3.16. Antes de comenzar la demostración realicemos una observación. Como mencionamos anteriormente, todas las bases de Groebner mínimas de I tienen los mismos términos líderes. Sea G una base de Groebner mínima para I. Decimos que $g \in G$ está **totalmente reducido** en G si ningún monomio de g pertenece a $\mathrm{LT}(G \setminus \{g\})$. Observemos que g está *totalmente reducido* para cualquier otra base de Groebner mínima G' de I que contenga g, ya que G' y G tienen los mismos términos líderes.

Demostración.

Ahora, dado $g \in G$, definamos $g' = \overline{g}^{G \setminus \{g\}}$ y sea $G' = (G \setminus \{g\}) \cup \{g'\}$. Afirmamos que G' es una base de Groebner mínima de I. Para demostrar esto, primero observemos que $\mathrm{LT}(g') = \mathrm{LT}(g)$, ya que al dividir g por $G \setminus \{g\}$, $\mathrm{LT}(g)$ pasa al término restante, pues no es divisible por ningún elemento de $\mathrm{LT}(G \setminus \{g\})$. Esto implica que $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$. Como G' está claramente contenido en I, concluimos que G' es una base de Groebner y que es mínima, por construcción. Finalmente, notemos que g' está *totalmente reducido* en G' por construcción.

Ahora, tomemos los elementos de G y apliquemos el proceso anterior hasta que todos estén *totalmente reducidos*. La base de Groebner puede cambiar durante el proceso, pero

la Observación 3.16 muestra que una vez que un elemento está *totalmente reducido*, permanece *totalmente reducido* porque nunca cambiamos los términos líderes. De este modo, obtenemos una base de Groebner *reducida*.

Para demostrar la unicidad, supongamos que G y $\tilde{G}$ son bases de Groebner *reducidas* para I. En particular, G y $\tilde{G}$ son bases de Groebner mínimas y, por lo tanto, tienen los mismos términos líderes, es decir, $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$. Así, dado $g \in G$, existe $\tilde{g} \in \tilde{G}$ tal que $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. Si podemos demostrar que $g = \tilde{g}$, se sigue que $G = \tilde{G}$ y la unicidad queda demostrada.

Para probar que $g = \tilde{g}$, consideremos $g - \tilde{g}$. Este elemento pertenece a I y, como G es una base de Groebner, se sigue que $\overline{g - \tilde{g}}^{G} = 0$. Pero también sabemos que $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. En consecuencia, estos términos se cancelan en $g - \tilde{g}$ y los términos restantes no son divisibles por ningún elemento de $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$, ya que G y $\tilde{G}$ son *reducidas*. Esto muestra que $\overline{g - \tilde{g}}^{G} = \tilde{g} - g$, y por lo tanto $g - \tilde{g} = 0$, lo que completa la demostración. □

Para concluir esta sección, indicaremos brevemente algunas de las conexiones entre el algoritmo de Buchberger y la reducción por filas (eliminación Gaussiana) para sistemas de ecuaciones lineales. El hecho interesante aquí es que, como advertíamos en la introducción, el algoritmo de reducción por filas es esencialmente un caso particular de triangulación de sistemas de ecuaciones.

Ejemplo 3.11. Consideremos el sistema de ecuaciones lineales siguiente:

$$\begin{cases} 3x - 6y - 2z = 0, \\ 2x - 4y + 4w = 0, \\ x - 2y - z - w = 0. \end{cases} \tag{3.12}$$

La matriz de coeficientes del sistema es

$$\begin{pmatrix} 3 & -6 & -2 & 0 \\ 2 & -4 & 0 & 4 \\ 1 & -2 & -1 & -1 \end{pmatrix} \tag{3.13}$$

Si usamos operaciones por filas en la matriz de coeficientes para ponerla en forma escalonada, obtenemos la matriz:

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{3.14}$$

Para obtener una matriz escalonada reducida por filas necesitamos asegurarnos de que cada 1 principal sea la única entrada no nula en su columna. Esto conduce a la matriz:

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{3.15}$$

Para traducir estos cálculos al álgebra, sea I el ideal

$$I = \langle 3x - 6y - 2z,\ 2x - 4y + 4w,\ x - 2y - z - w \rangle \subseteq K[x, y, z, w]$$

correspondiente al sistema de ecuaciones original. Usaremos el orden lexicográfico con $x > y > z > w$. Las formas lineales determinadas por la matriz escalonada por filas (3.14) dan una base de Groebner mínima

$$I = \langle x - 2y - z - w,\ z + 3w \rangle,$$

y la matriz escalonada reducida por filas (3.15) da la base de Groebner reducida

$$I = \langle x - 2y + 2w,\ z + 3w \rangle.$$

Observación 3.17. Recordemos de álgebra lineal que toda matriz puede ponerse en forma escalonada reducida por filas de manera única. Esto puede considerarse como un caso particular de la unicidad de las bases de Groebner reducidas.

3.7. Cambio de Orden

Como se mencionó tras la Definición 3.7, de orden lexicográfico graduado inverso, se ha demostrado que, para algunas operaciones, este orden es el más eficiente para realizar cálculos. Dado que, como veremos más adelante, los dos algoritmos de triangulación estudiados parten de una base de Groebner con el orden lexicográfico, una idea interesante sería realizar los cálculos con la base del orden lexicográfico graduado inverso, y a continuación cambiar a la base del orden lexicográfico para poder aplicar dichos algoritmos. Esta sección tiene como objetivo estudiar este cambio de orden, presentando un algoritmo eficiente para la transformación de una base de Groebner de un ideal con respecto a un orden dado en una base de Groebner con respecto a otro orden cualquiera.

Definición 3.17. Consideraremos un ideal I en $K[x_1, \ldots, x_n]$ dado por su base de Groebner G con respecto a algún orden admisible. Diremos que $f \in K[x_1, \ldots, x_n]$ está **reducido por G** o en **forma normal con respecto a G** si ningún elemento $g \in G$ tiene un término líder que divida cualquier término de f

Definición 3.18. Llamamos **algoritmo de reducción** al algoritmo que calcula la forma normal de un polinomio dado f, definida en la Observación 3.9.

Consideraremos un ideal de dimensión cero, es decir, un ideal I tal que el conjunto de ceros comunes de los polinomios en I es finito (consultar la Observación 2.5)

Definición 3.19. Dado un ideal de dimensión cero I en $K[x_1, \ldots, x_n]$ y $(G, <)$ una base de Groebner reducida para I, llamaremos **base natural** determinada por G del espacio vectorial cociente $K[x_1, \ldots, x_n]/I$, a la base $B(G)$ cuyos elementos son los monomios reducidos con respecto a G. Denotaremos por $D(I)$ la dimensión del espacio vectorial cociente $K[x_1, \ldots, x_n]/I$.

Definición 3.20. Sea $B(G)$ la base natural para $K[x_1, \ldots, x_n]/I$, definimos

$$M(G) = \{x_i b \mid b \in B(G),\ 1 \leq i \leq n,\ x_i b \notin B(G)\}$$

como el **borde de** G.

La siguiente proposición caracteriza los elementos de $M(G)$.

Proposición 3.22. *Sea I un ideal de dimensión cero, $(G, <)$ la base de Groebner reducida con respecto a un orden admisible $<$, y $B(G)$ la base natural de $K[x_1, \ldots, x_n]/I$. Entonces para cada elemento $m \in M(G)$, se cumple exactamente una de las siguientes condiciones:*

(i) Para cada x_i que divide a m, tenemos $m/x_i \in B(G)$.

(ii) $m = x_j m_k$ para algún j y algún $m_k \in M(G)$.

Demostración.

(i) Esto se deduce inmediatamente de las definiciones de base de Gröbner reducida y de B(G).

(ii) Sea x_j tal que x_j divide a m y $m/x_j \notin$ B(G). Entonces $m_k = m/x_j \in$ M(G). De hecho, como $m = x_j m_k = x_i b$ tenemos que $i \neq j$ y $m_k/x_i = b/x_j \in$ B(G), porque B(G) es cerrada bajo división, por definición. Por tanto, $m_k = x_i(b/x_j) \in$ M(G). □

Definición 3.21. Sea I, $(G, <)$ y $\mathrm{B}(G)$ como en la Proposición 3.22.
Definimos $\mathrm{T}(G) = (t_{ijk})$ como el tensor de dimensión $n \times D(I) \times D(I)$ donde cada t_{ijk} es la j-ésima coordenada con respecto a $\mathrm{B}(G)$ de la reducción por G del elemento $x_i b_k$ ($b_k \in \mathrm{B}(G)$):

Proposición 3.23. *Para calcular* $\mathrm{T}(G)$*, son suficientes* $O(nD(I)^3)$ *operaciones aritméticas.*

La demostración puede consultarse en [9].

3.7.1. Algoritmo de Cambio de Orden

Presentamos en esta subsección el algoritmo para el cambio de orden.

Proposición 3.24. *Sea* I *un ideal de dimensión cero y* $(G_1, <_1)$ *la base de Groebner reducida con respecto a un orden admisible* $<_1$*. Dado un orden diferente* $<_2$*, es posible construir la base de Groebner* $(G_2, <_2)$ *con respecto al orden* $<_2$ *utilizando* $O(nD(I)^3)$ *operaciones aritméticas.*

Demostración.

A partir de $(G_1, <_1)$, podemos construir $B(G_1) = \{a_1, \ldots, a_{D(I)}\}$, $M(G_1)$ y $T(G_1)$ como en la sección anterior. Queremos encontrar los elementos de $B(G_2)$ y $(G_2, <_2)$. Por esta razón, construiremos una matriz C que contendrá en la columna i-ésima las coordenadas de cada elemento $b_i \in B(G_2)$ con respecto a $B(G_1)$.

Comenzamos con $B(G_2) := \{1\}$ y $M(G_2) := \emptyset$ para construir iterativamente la nueva base (el polinomio 1 pertenece a $B(G_2)$). Consideramos $m = \mín_{<_2}\{x_j b_i \mid 1 \leq j \leq n,\ b_i \in B(G_2),\ x_j b_i \notin B(G_2) \cup M(G_2)\}$. Pueden surgir tres casos:

1. m es el término líder de algún g, para algún g que debe ser insertado en G_2.
2. m debe ser insertado en $B(G_2)$.
3. m debe ser insertado en $M(G_2)$, pero m es un múltiplo del término líder de algún g en G_2.

Podemos verificar fácilmente si se cumple el tercer caso: el término líder de g es estrictamente menor que m para cualquier orden admisible y ya ha sido insertado en $M(G_2)$.

Por lo tanto, nos queda considerar los casos 1 o 2. Dado que, por construcción, $m = x_j b_i$, podemos calcular sus coordenadas $c(m)_h$ con respecto a $B(G_1)$ utilizando la matriz C y $T(G_1) = (t_{ijk})$:

$$m = x_j b_i = x_j \sum_k c_{ki} a_k = \sum_k c_{ki}(x_j a_k) = \sum_k c_{ki} \sum_h t_{jhk} a_h$$
$$= \sum_h \left(\sum_k t_{jhk} c_{ki} \right) a_h = \sum_h c(m)_h a_h.$$

En este punto, si el vector $c(m)$ es linealmente independiente de los vectores en C, estamos en el caso 2 y hemos encontrado un nuevo monomio $m \in B(G_2)$; de lo contrario, la relación de dependencia proporciona un nuevo elemento $g \in G_2$.

Apoyándonos en la Proposición 3.23 es sencillo ver que toda la construcción requiere $O(nD(I)^3)$ operaciones. Y de hecho, el cálculo de $c(m)$ implica solo el producto de una matriz por un vector de tamaño $D(I)$. Si se mantiene una forma escalonada de la matriz C, para probar independencia lineal e incrementar C, solo se necesitan $O(D(I)^2)$ operaciones.

□

Describimos ahora un algoritmo que implementa la construcción de la proposición anterior (ver Algoritmo 4). La subfunción FormaNormal es el algoritmo de reducción definido previamente. En [9] se puede consultar la demostración la corrección del Algoritmo 4 (finitud y resultado esperado).

Algoritmo 4 Algoritmo de Cambio de Orden

- **Entrada**: $<$ un nuevo orden admisible.
  baseAntigua, una base de Groebner de un ideal de dimensión cero con respecto a un orden dado.
- **Salida**: *baseNueva*, la base de Groebner reducida del ideal generado por *baseAntigua* con respecto al orden $<$.
- **Subfunciones**:
  - *FormaNormal*(*polinomio*): Devuelve la forma reducida de *polinomio* con respecto a *baseAntigua*.
  - *SiguienteMonomio*: Elimina el primer elemento de *listaSiguientes* y lo devuelve; devuelve *nil* si la lista está vacía.
  - *InsertarSiguientes(monomio)*: Agrega a *listaSiguientes* los productos de *monomio* con todas las variables, ordena esta lista en orden creciente según $<$, y elimina duplicados.
  - *cons(elemento, conjunto)*: Inserta el *elemento* dentro del *conjunto*.
- **Variables locales**:
  - *escalera* := []: Lista de monomios principales de los elementos de *baseNueva*.
  - *baseMonomios* := []: Lista de pares $[a_i, b_i]$, donde a_i son monomios en forma normal respecto a *baseNueva* y $b_i = FormaNormal(a_i)$. Elegimos elementos de cada par con los selectores *first* y *second*.
  - *listaSiguientes* := []: Lista de "siguientes" monomios a considerar, ordenados crecientemente según $<$.

1: *baseMonomios* := []; *baseNueva* := []; *escalera* := [];
2: *listaSiguientes* := []; *monomio* := 1;
3: **while** *monomio* $\neq$ *nil* **do**
4: **if** *monomio* no es un múltiplo de algún elemento de *escalera* **then**
5: *vector* := *FormaNormal*(*monomio*);
6: **if** existe una relación lineal $vector + \sum_{v \in baseMonomios} \lambda_v \cdot second(v) = 0$ **then**
7: $pol := monomio + \sum_{v \in baseMonomios} \lambda_v \cdot first(v)$;
8: *baseNueva* := *cons*(*pol*, *baseNueva*);
9: *escalera* := *cons*(*monomio*, *escalera*);
10: **else**
11: *baseMonomios* := *cons*([*monomio*, *vector*], *baseMonomios*);
12: *InsertarSiguientes*(*monomio*);
13: **end if**
14: **end if**
15: *monomio* := *SiguienteMonomio*();
16: **end while**
17: **return** *baseNueva*;
18: **end**

Capítulo 4
Algoritmo de Lazard

4.1. Introducción

En este capítulo se estudiará el algoritmo de Lazard en el contexto de Triangulación de Sistemas de Ecuaciones Algebraicas, propuesto por Daniel Lazard en [13]. El algoritmo de Lazard parte de una base de Groebner con el orden lexicográfico (en el Capítulo 3 se estudió cómo obtenerla), y transforma el sistema de ecuaciones en un número finito de sistemas triangulares. La solución del sistema original será la unión de las soluciones de todos estos sistemas triangulares. En este capítulo nos enfocaremos en sistemas de dimensión cero, representando sus soluciones mediante una forma triangular de polinomios. Además, demostraremos que las bases triangulares son útiles para representar estas soluciones, conectándolas con las bases de Groebner estudiadas en el Capítulo 3.

A continuación, mostraremos cómo los resultados de los algoritmos clásicos no son del todo satisfactorios. Primero compararemos los resultados de un cálculo de base de Groebner (para dos órdenes diferentes) y del algoritmo de Wu Wen-Tsün (consultar [16]) con el resultado simple que sería la solución natural de un *solver* (programa o algoritmo que resuelve sistemas de ecuaciones y devuelve sus soluciones).

Ejemplo 4.1. Consideremos el siguiente conjunto de polinomios (que se convierte en un sistema de ecuaciones al igualarlos a cero):

$$\begin{cases} x+y+z+w, \\ xy+yz+zw+wx, \\ xyz+yzw+zwx+wxy, \\ xyzw-1. \end{cases} \tag{4.1}$$

Para el orden lexicográfico, su base de Groebner es

$$\begin{cases} x+y+z+w, \\ y^2+2yw+w^2, \\ yz-yw+z^2w^4+zw-2w^2, \\ yw^4-y+w^5-w, \\ z^3w^2+z^2w^3-z-w, \\ z^2w^6-z^2w^2-w^4+1. \end{cases} \tag{4.2}$$

Para el orden lexicográfico graduado, la base es

$$\begin{cases} x+y+z+w, \\ y^2+2yw+w^2, \\ y^2z^2+z^2w-yw^2-w^3, \\ yzw^2+z^2w^2-yw^3+zw^3-w^4-1, \\ yw^4+w^5-y-w, \\ z^2w^4+yz-yw+zw-2w^2, \\ z^3w^2+z^2w^3-z-w. \end{cases} \tag{4.3}$$

El resultado del algoritmo de Wu Wen-Tsün es:

$$\begin{aligned}
&\text{if } x^2(y^2-x^2)\neq 0 \quad \text{then}\\
&\quad (w+z+y+x,\ (y^2-x^2)z+xy^2-x^3,\ -x^2y^4+(x^4-1)y^2-x^2),\\
&\text{else if } -x^2y+x^3\neq 0 \quad \text{then}\\
&\quad (w+z+y+x,\ (-xy^2+x^3)z-x^3y+1,\ y^2-x^2,\ -x^8+2x^4-1),\\
&\text{else if } -x^2\neq 0 \quad \text{then}\\
&\quad (w+z+y+x,\ -z^2-2xz-x^2,\ -x^2y+x^3,\ -x^8+x^4),\\
&\text{else } 1.
\end{aligned} \tag{4.4}$$

Las soluciones (4.2) y (4.4) son suficientemente triangulares y permiten obtener soluciones numéricas asignando sucesivamente valores a las variables. Pero el resultado podría obtenerse de manera más simple: no es difícil demostrar que el ideal generado por los polinomios de (4.1) es la intersección de los tres ideales

$$\begin{aligned}
&(x+z,y+w,z^2w^2-1),\\
&(x+y+2w,(y+w)^2,z-w,w^4-1),\\
&(x-w,y+z+2w,(z+w)^2,w^4-1).
\end{aligned} \tag{4.5}$$

Aún más simple, podemos observar que el segundo polinomio de (4.2) es un cuadrado; añadiendo su raíz cuadrada $y+w$, obtenemos como nueva base de Groebner

$$(x+z,y+w,z^2w^2-1) \tag{4.6}$$

la cual genera el radical del ideal definido por (4.1) (consultar Definición 5.1).

Observación 4.1. Los elementos de (4.5) y (4.6) son ideales triangulares en el sentido de que la i-ésima variable solo puede aparecer en los primeros i polinomios. Como se comentó en la introducción del capítulo, mostraremos que cada sistema de dimensión cero puede resolverse como una unión finita de tales ideales triangulares y detallaremos cómo encontrar dichas descomposiciones.

Ejemplo 4.2. Demos ahora un ejemplo algo más complejo, el mismo que antes pero con una variable adicional:

$$\begin{cases} x+y+z+w+v, \\ xy+yz+zw+wv+vx, \\ xyz+yzw+zwv+vxy+wxv, \\ xyzw+yzwv+zwvx+wvxy+vxyz, \\ xyzvw-1. \end{cases} \tag{4.7}$$

Este sistema tiene 70 soluciones que no son inmediatas de calcular. En forma triangular, las soluciones son

$$\begin{aligned} &(x^5-1,\ y^4+xy^3+x^2y^2+x^3y+x^4,\ z-x^4y^2,\ w-x^3y^3, \\ &\quad v+x^3y^3+x^4y^2+y+x) && \text{(20 soluciones)} \\ &(x^5-1,\ y-x,\ z-x,\ w^2+3xw+x^2,\ v+w+3x) && \text{(10 soluciones)} \\ &(x^5-1,\ y-x,\ z^2+3xz+x^2,\ w+z+3x,\ v-x) && \text{(10 soluciones)} \\ &(x^5-1,\ y^2+3xy+x^2,\ z+y+3x,\ w-x,\ v-x) && \text{(10 soluciones)} \\ &(x^{10}+123x^5+1,\ 55y+x^6+144x,\ 55z+x^6+144x, \\ &\quad 55w+x^6+144x,\ 55v+x^6+144x) && \text{(10 soluciones)} \\ &(x^{10}+123x^5+1,\ 55y-3x^6-377x,\ 55z+x^6+144x, \\ &\quad 55w+x^6+144x,\ 55v+x^6+144x) && \text{(10 soluciones)} \end{aligned} \tag{4.8}$$

Observación 4.2. Los cinco grupos de 10 soluciones son las cinco permutaciones circulares de soluciones de la forma

$$(x,x,x,xr,-x(r+3)) \quad \text{donde} \quad x^5=1 \text{ y } r^2+3r+1=0. \tag{4.9}$$

4.2. Ideales Triangulares

Se acaba de mostrar que las soluciones simples y útiles son *triangulares*. Daremos un significado preciso a esto. Consideramos sistemas con un número finito de soluciones en n variables $x_1, \ldots, x_n$ y las ordenamos de tal manera que

$$x_1 < x_2 < \cdots < x_n.$$

Definición 4.1. La *variable principal* de un polinomio es la mayor variable (según el orden anterior) que aparece en él.

Definición 4.2. Un conjunto de n polinomios es *triangular* si la variable principal del i-ésimo polinomio es x_i para $i = 1, \ldots, n$ y si dicho polinomio es mónico como polinomio en x_i.

Definición 4.3. El *grado* de un conjunto triangular es el producto de los grados (en sus variables principales) de sus polinomios.

Proposición 4.1. *Si K es un cuerpo, cualquier ideal maximal en $K[X_1, \ldots, X_n]$ tiene un sistema de generadores triangular.*

Demostración.

Sea I un ideal maximal y A el cuerpo $K[X_1, \ldots, X_n]/I$. Denotemos por x_i la imagen de X_i en A y por $A_i = K(x_1, \ldots, x_i)$ el subcuerpo de A generado por $(x_1, \ldots, x_i)$. Entonces $A_i = A_{i-1}(x_i)$ es una extensión algebraica simple (como A, al ser un anillo finitamente generado, es una extensión algebraica de K). Sea P_i el polinomio mínimo mónico de x_i, con coeficientes en A_{i-1}, entonces tenemos $A_i = A_{i-1}[x_i]/P_i$ y los elementos de A_i son polinomios en X_i de grado menor que el grado de P_i. Razonando de manera recursiva, $A = K[x_1, \ldots, x_n]/(P_1, \ldots, P_n)$ y que P_i es un polinomio en $x_1, \ldots, x_i$ que es mónico en X_i. □

Proposición 4.2. *Todo sistema con un número finito de soluciones (en un cierre algebraico de K) es equivalente a la unión de un número finito de sistemas triangulares.*

Demostración.

Sea I el ideal generado por los polinomios del sistema. La hipótesis implica que I es de dimensión cero y, por el Teorema de los Ceros de Hilbert, que su radical es una intersección de ideales maximales (consultar la sección "*Nullstellensatz*" en [8]). Por lo tanto, los ceros del sistema son ceros de uno de estos ideales maximales, y la conclusión se deduce de la Proposición 4.1. □

Proposición 4.3. *Sea $(P_1, \ldots, P_n)$ un conjunto triangular de polinomios. Sea Q_1 un factor irreducible de P_1, A_1 el cuerpo $K[x_1]/Q_1$; sea Q_2 un factor irreducible de P_2 en $A_1[x_2]$ y A_2 el cuerpo $A_1[x_2]/Q_2$, y así sucesivamente. El conjunto $(Q_1, \ldots, Q_n)$ genera un ideal maximal que contiene $(P_1, \ldots, P_n)$, y el conjunto de ceros comunes de los P_i es la unión de los conjuntos de ceros comunes de todos los $(Q_1, \ldots, Q_n)$.*

Demostración.

Dado que P_1 es mónico en x_1, se puede factorizar en $K[x_1]$ como producto de factores irreducibles $P_1 = Q_1 Q_1' \cdots Q_1^{(m)}$. Cada factor irreducible Q_1 define un ideal primo en $K[x_1]$, y el cuerpo cociente correspondiente es $A_1 = K[x_1]/Q_1$.

De forma similar, P_2 es mónico en x_2 y puede escribirse en $A_1[x_2]$ como $P_2 = Q_2 Q_2' \cdots Q_2^{(k)}$, donde cada Q_2 es irreducible. El cuerpo cociente $A_2 = A_1[x_2]/Q_2$ está bien definido, y el proceso continúa para cada $i = 1, \ldots, n$, generando Q_i y A_i.

El conjunto $(Q_1, \ldots, Q_n)$ genera un ideal maximal en $K[x_1, \ldots, x_n]$, ya que cada Q_i es irreducible y mónico en x_i, y cada A_i es una extensión algebraica de A_{i-1}. Además, $(Q_1, \ldots, Q_n)$ contiene $(P_1, \ldots, P_n)$ porque los Q_i son factores de los P_i.

El conjunto de ceros comunes de los P_i es la unión de los conjuntos de ceros comunes de los $(Q_1, \ldots, Q_n)$, ya que las soluciones de $P_i = 0$ se distribuyen entre las soluciones de sus factores irreducibles. Esto se sigue de la estructura triangular del sistema, que asegura que las variables se puedan resolver sucesivamente, primero para x_1, luego para x_2 en función de x_1, y así sucesivamente hasta x_n. □

Así, dado un conjunto triangular de polinomios, encontrar los ideales maximales que lo contienen equivale a la factorización en extensiones algebraicas.

4.3. Cálculo Módulo Ideales Triangulares

Calcular numéricamente los ceros comunes de un conjunto triangular consiste en resolver polinomios mónicos obtenidos sucesivamente al sustituir las variables por las raíces de los polinomios precedentes. Esta resolución es un ejemplo de cálculo con conjuntos triangulares de polinomios. Mostraremos a continuación otros cálculos con una observación realizada por Dominique Duval y Claire Dicrescenzo en diferentes contribuciones académicas ([4], [5], [6], [7]).

Observación 4.3. Sea $P = \{P_1, \ldots, P_n\}$ un conjunto triangular en $K[x_1, \ldots, x_n]$. Notemos que para cada $1 \leq k \leq n$, $P_1, \ldots, P_k$ es un conjunto triangular en $K[x_1, \ldots, x_k]$.

Sea $A_k := K[x_1, \ldots, x_k]/(P_k, \ldots, P_k)$. P_{k+1} puede considerarse como un polinomio en $A_k[x_{k+1}]$, y A_{k+1} es isomorfo a $A_k[x_{k+1}]/P_{k+1}$. Como vimos en la Proposición 4.3, A_n es un cuerpo si P_{k+1} es irreducible en $A_k[x_{k+1}]$.

El cálculo en A_k es sencillo y está implementado en la mayoría de los sistemas algebraicos computacionales: los elementos de A_k se representan como polinomios en $x_1, \ldots, x_n$ de grado en x_k menor que el grado de P_k (en x_k), para $k = 1, \ldots, n$. Dividir por P_k no presenta problema, y la multiplicación en A_n es un producto de polinomios seguido de divisiones por $P_n, P_{n-1}, \ldots, P_1$.

La inversión en A_n (cuando es un cuerpo) se realiza del siguiente modo: si Q, elemento de A_n, es un polinomio con x_k como variable principal, se calcula el máximo común divisor extendido de Q y P_k en $A_{k-1}[x_k]$ (esto necesita inversiones en A_{k-1}). El resultado es:

$$D = QR + PS,$$

donde si $D = 1$, entonces R es el inverso de Q; si $D = P_k$, entonces P_k divide a Q y $Q = 0$ no es invertible en A_k. No hay otras posibilidades si A_n es un cuerpo, porque P_k es irreducible.

Si A_k no es un cuerpo y $D \neq 1$, $D \neq P_k$, entonces P_k es un producto, y hemos encontrado factores sin necesidad de un algoritmo de factorización. Si reemplazamos P_k por cada uno de sus factores (D y P_k/D), obtenemos dos conjuntos triangulares; módulo el primer caso, $Q = 0$ no es invertible; módulo el segundo caso, el inverso de Q es RD^{-1} (esto necesita inversión de D módulo P_k/D).

4.4. División y Combinación de Ideales Triangulares

Definición 4.4. Dos conjuntos de polinomios (y los ideales que generan) son *equivalentes* si tienen los mismos ceros. Dos familias de conjuntos de polinomios son equivalentes si la unión de sus ceros comunes es la misma.

Definición 4.5. Un conjunto triangular $(P_1, \ldots, P_n)$ de polinomios en $K[x_1, \ldots, x_n]$ es *reducido* si P_k es libre de cuadrados módulo $P_1, \ldots, P_{k-1}$ para cada $k = 1, \cdots, n$. Esto es, si existen polinomios R y S tales que $RP_k + SP'_k = 1$ módulo $P_1, \ldots, P_{k-1}$, donde P'_k es la derivada de P_k con respecto a x_k para $k = 1, \ldots, n$.

Calcular la descomposición libre de cuadrados de P_k puede conducir a separar por casos para P_i, con $i < k$, como se muestra en el siguiente ejemplo:

Ejemplo 4.3. Consideremos el conjunto triangular de polinomios

$$P_1 := x^2 - x, \quad P_2 := y^2 + x.$$

El primer polinomio $P_1 = x^2 - x$ es *libre de cuadrados* en el sentido usual, porque no tiene factores repetidos. Sin embargo, queremos analizar si el segundo polinomio $P_2 = y^2 + x$ es libre de cuadrados módulo P_1. Según la definición, esto se verifica si $mcd(P_2, P_2') = 1$ en el anillo cociente $K[x, y]/\langle P_1 \rangle$. Para comprobarlo, se calcula el resultante (ver Definición 1.1) de P_2 como polinomio en y y su derivada respecto a y:

$$\mathrm{Res}(P_2, P_2') = \mathrm{Res}(y^2 + x, 2y) = x.$$

Este resultante se anula cuando $x = 0$, lo que indica que en ese caso, P_2 y su derivada tienen raíces comunes, y por tanto P_2 no es libre de cuadrados módulo P_1.

Por lo tanto, distinguimos dos casos:

- Si $x = 0$, entonces $P_2 = y^2$, que *sí* tiene un factor cuadrado ($y^2 = (y)^2$), por lo que no es libre de cuadrados.
- Si $x = 1$, entonces $P_2 = y^2 + 1$, que es irreducible en $\mathbb{Q}$, y por tanto libre de cuadrados.

Como advertíamos antes de comenzar este ejemplo, esto nos permite separar por casos para dividir el sistema inicial en dos subsistemas triangulares reducidos, según los valores posibles de x. La familia equivalente de conjuntos triangulares reducidos es:

$$\Big((x, y), \quad (x - 1, y^2 + 1)\Big).$$

Proposición 4.4. *(i) Si $(P_1, \ldots, P_n)$ es un sistema triangular tal que $P_k = P_k' P_k''$ módulo $(P_1, \ldots, P_{k-1})$ (esto significa factorización, no derivadas), entonces $(P_1, \ldots, P_n)$ es equivalente a*

$$((P_1, \ldots, P_{k-1}, P_k', P_{k+1}', \ldots, P_n'), \quad (P_1, \ldots, P_{k-1}, P_k'', P_{k+1}'', \ldots, P_n'')),$$

donde P_i' y P_i'' $(i > k)$ se obtienen reduciendo P_i por $P_1, \ldots, P_{k-1}$, y P_k' o P_k'', respectivamente.

(ii) Si $(P_1, \ldots, P_n)$ y $(Q_1, \ldots, Q_n)$ son dos sistemas triangulares tales que $P_i = Q_i$ para $i < k$, que los grados de P_i y Q_i son iguales para $i > k$, y que $\mathrm{mcd}(P_k, Q_k) = 1$

módulo $(P_1, \ldots, P_{k-1})$*, entonces*

$$((P_1, \ldots, P_n), (Q_1, \ldots, Q_n))$$

es equivalente a

$$(P_1, \ldots, P_{k-1}, P_k Q_k, R_{k+1}, \ldots, R_n),$$

donde los R_i *se calculan utilizando el Teorema Chino del Resto.*

Demostración.

(i) Supongamos que tenemos un sistema triangular $(P_1, \ldots, P_n)$, y que existe una factorización

$$P_k = P'_k \cdot P''_k \mod (P_1, \ldots, P_{k-1}).$$

Esto quiere decir que en el anillo cociente $A_{k-1} = K[x_1, \ldots, x_n]/(P_1, \ldots, P_{k-1})$, el polinomio P_k se descompone como producto de dos polinomios no constantes P'_k, P''_k.

Entonces los ceros de P_k en $A_{k-1}[x_k]$ se dividen en dos subconjuntos: los ceros de P'_k y los ceros de P''_k. Como $P_{k+1}, \ldots, P_n$ están definidos módulo $(P_1, \ldots, P_k)$, podemos reducirlos módulo $(P_1, \ldots, P_{k-1}, P'_k)$ y $(P_1, \ldots, P_{k-1}, P''_k)$, obteniendo así dos sistemas triangulares completos:

$$(P_1, \ldots, P_{k-1}, P'_k, P'_{k+1}, \ldots, P'_n), \quad (P_1, \ldots, P_{k-1}, P''_k, P''_{k+1}, \ldots, P''_n),$$

cuyas soluciones cubren exactamente todas las soluciones del sistema original. Por lo tanto, el sistema original es equivalente a la unión de estos dos sistemas triangulares.

(ii) Supongamos ahora que tenemos dos sistemas triangulares $(P_1, \ldots, P_n)$ y $(Q_1, \ldots, Q_n)$ que coinciden en sus primeros $k-1$ polinomios: $P_i = Q_i$ para $i < k$. Además, supongamos que los grados de P_i y Q_i coinciden para $i > k$ y que $\mathrm{mcd}(P_k, Q_k) = 1$ mód $(P_1, \ldots, P_{k-1})$. Entonces en el anillo cociente $A_{k-1} = K[x_1, \ldots, x_n]/(P_1, \ldots, P_{k-1})$, los polinomios P_k y Q_k son coprimos. Como consecuencia, el producto $P_k Q_k$ se anula si y solo si se anula al menos uno de los dos factores. Por el Teorema Chino del Resto, dado que $mcd(P_k, Q_k) = 1$, existe un isomorfismo de anillos:

$$A_{k-1}[x_k]/(P_k Q_k) \cong A_{k-1}[x_k]/(P_k) \times A_{k-1}[x_k]/(Q_k).$$

Por lo tanto, el sistema con $P_k Q_k$ como polinomio en x_k, y los polinomios $R_{k+1}, \ldots, R_n$, obtenidos usando el Teorema Chino del Resto en cada caso, representa el mismo

conjunto de soluciones que la unión de los dos sistemas originales. Así,

$$((P_1,\dots,P_n),(Q_1,\dots,Q_n)) \text{ es equivalente a } (P_1,\dots,P_{k-1},P_kQ_k,R_{k+1},\dots,R_n).$$

□

La parte (i) puede aplicarse a cada conjunto triangular que aparece en (4.8), observando que la factorización completa de x^5-1 es $(x-1)(x^4+x^3+x^2+x+1)$ y de $x^{10}+123x^5+1$ es $(x^2+3x+1)\times(x^5-3x^7+8x^6-21x^5+55x^4-21x^3+8x^2-3x+1)$. Por el contrario, la parte (ii) puede usarse para combinar el primer y cuarto conjunto triangular, o el quinto y sexto conjunto triangular en (4.8), para obtener:

$$\begin{aligned}
&(x^5-1,\ y^6+4xy^5+5x^2y^4+5x^3y^3+5x^4y^2+4x^5y+x^6,\\
&\quad 5z+8xy^5+30x^2y^4+30x^3y^3+25x^4y^2+30y+22x,\\
&\quad 5w-2xy^5-10x^2y^4-15x^3y^3-10x^4y^2-10y-8x,\\
&\quad 5v-6xy^5-20x^2y^4-15x^3y^3-15x^4y^2-15y-9x)\\
&(x^5-1,\ y-x,\ z-x,\ w^2+3xw+x^2,\ v+w+3x)\\
&(x^5-1,\ y-x,\ z^2+3xz+x^2,\ w+z+3x,\ v-x)\\
&(x^{10}+123x^5+1,\ 55y^2-2x^6y-233xy-8x^7-987x^2,\\
&\quad 55z+x^6+144x,\ 55w+x^6+144x,\ 55v+55y-2x^6-233x)
\end{aligned}$$

Podemos también combinar el quinto y sexto conjunto triangular en (4.8) con el resultado del cuarto conjunto de (4.8). Obtenemos otra familia equivalente que consiste en los tres primeros conjuntos triangulares de (4.8) y:

$$\begin{aligned}
&(x^{15}+122x^{10}-122x^5-1,\\
&275y^2+(16x^{11}+1958x^6-1149x)y+42x^{12}+5126x^7-4893x^2,\\
&1375z+(11x^{10}+1353x^3+11)y+4x^{11}+517x^6+3604x,\\
&275w-8x^{11}-979x^6+712x,\\
&1375v+(-11x^{10}-1353x^3+1364)y+36x^{11}+4378x^6-5789x),
\end{aligned}$$

Observación 4.4. La no unicidad de la familia de conjuntos triangulares reducidos equivalente a un sistema dado no es un inconveniente, debido a que pasar de una familia a otra es relativamente sencillo. Sin embargo, no siempre existe una familia reducida mínima equivalente única. Por ejemplo,

$$((x, y), (x, y + 1), (x + 1, y))$$

puede combinarse mediante la parte (ii) de la última proposición en

$$((x, y^2 + y), (x + 1, y))$$

o

$$((x^2 + x, y), (x, y + 1))$$

o

$$((x, y), (x^2 + x, y + x + 1)),$$

pero no hay un conjunto triangular reducido equivalente a estas familias.

Teorema 4.5. *Sea G una base de Groebner de un ideal de dimensión cero en $K[x_1, \ldots, x_n]$, respecto al orden lexicográfico tal que $x_1 < x_2 < \cdots < x_n$, y supongamos que G está ordenada de manera creciente. Sea f un homomorfismo de anillos de $K[x_1, \ldots, x_k]$ en un cuerpo, tal que f anula los elementos de G que dependen únicamente de $x_1, \ldots, x_k$. Entonces el primer elemento de G que no es enviado a cero por f es aquel que depende solo de $x_1, \ldots, x_{k+1}$, y que tiene un término líder (como polinomio en x_{k+1}) que no se anula por f. Además, la imagen por f de este polinomio es el máximo común divisor de las imágenes por f de todos los elementos de G que dependen únicamente de $x_1, \ldots, x_{k+1}$.*

La demostración fue propuesta por Gianni (1987) y Kalkbrenner (1987) (consultar [12]).

4.5. Algoritmo

En esta sección se implementa el algoritmo de Lazard. Como se comentó en la introducción, dado un sistema de ecuaciones polinómicas, este algoritmo parte de una base de Groebner respecto al orden lexicográfico del ideal asociado a dicho sistema y calcula una colección de sistemas triangulares cuya unión de soluciones forma el conjunto de soluciones del sistema original.

Algoritmo 5 Algoritmo de Triangulación de Lazard

- **Entrada**: G, base de Groebner de un ideal de dimensión cero en $K[x_1, \ldots, x_n]$, ordenada lexicográficamente con $x_1 < \cdots < x_n$.
- **Salida**: T, lista de sistemas triangulares equivalentes a G.
- **Subfunciones**:
  - **Reducir**(p, mod): Reduce el polinomio p módulo el polinomio mod si mod solo es un polinomio, o módulo el ideal generado por los polinomios de mod si mod es un conjunto de varios polinomios.
  - **Inverso**(p, mod): Devuelve el inverso de p módulo las ecuaciones de mod, si existe. Si no existe, devuelve 0.
  - **Lider**(p, x): Devuelve el coeficiente líder del polinomio p, interpretado como un polinomio univariante en la variable x.
  - **Factor**(p): Devuelve la lista de factores mónicos e irreducibles del polinomio p.
  - **Primero**(L): Devuelve el primer elemento de la lista L.
  - **Cola**(L): Devuelve la lista que resulta de eliminar el primer elemento de L.

```
1: T := [[ ]];
2: for i = 1 to n do
3:    H := subconjunto de elementos de G que dependen de x_i pero no de x_{i+1}, ..., x_n;
4:    U := T;
5:    T := [ ];
6:    for all mod ∈ U do
7:       repeat
8:          p := Primero(H);
9:          H := Cola(H);
10:         q := Lider(p, x_i);
11:         q := Inverso(q, mod);
12:      until q ≠ 0 ;
13:      p := Reducir(p, mod);
14:      for all f ∈ Factor(p) do
15:         nuevo := mod ∪ {f};
16:         Añadir nuevo a T;
17:      end for
18:   end for
19: end for
20: return T
```

Observación 4.5. El Teorema 4.5 garantiza que sea suficiente con tomar el primer polinomio que depende de x_i pero no depende de $x_1, ..., x_{i-1}$, es decir, del conjunto H. Esto es porque los demás son múltiplos (módulo las anteriores ecuaciones) y al reducirlos después por los factores del primero, se anulan automáticamente. En otras palabras, garantiza que no se pierde ninguna información ni solución al usar solamente el primer polinomio de cada paso.

4.6. Ejemplo del Algoritmo de Lazard

Ejemplo 4.4. Consideremos el sistema siguiente:

$$\begin{cases} x^2 + y^2 - 1 = 0, \\ (x + y + z - 1)(x + y) = 0, \\ xyz = 0. \end{cases}$$

Sea I el ideal generado por los polinomios:

$$\begin{aligned} f_1 &:= x^2 + y^2 - 1, \\ f_2 &:= (x + y + z - 1)(x + y), \\ f_3 &:= xyz. \end{aligned}$$

Como ya sabemos, el algoritmo de Lazard parte de una base de Groebner para el orden lexicográfico. Llamemos G a la base de Groebner de I con ese orden (calculada como se mostró en el Capítulo 3) dada por:

$$\begin{aligned} g_1 &:= z^3 - 2z^2, \\ g_2 &:= y^2z + yz^2 - yz, \\ g_3 &:= 4y^4 - 4y^3 - 2y^2 + 2yz^2 - 2yz + 2y - z^2 + 2z, \\ g_4 &:= x - 4y^3 + 2y^2 + 2yz^2 - 2yz + 3y - z^2 + 3z - 1. \end{aligned}$$

Paso 1: Factorizamos el polinomio g_1, que solo depende de una variable. Obtenemos los factores z y $z - 2$.

Paso 2: (Bucle). Para cada uno de los factores que acabamos de obtener, reducimos el resto de ecuaciones (g_2, g_3, g_4) módulo ese factor. Por lo tanto, cada factor representa una rama en el Diagrama de Árbol 4.4. En este ejemplo vamos a realizar los cálculos para la

rama del factor $z-2$, aunque para el factor z se sigue un proceso análogo.

Tras reducir g_2, g_3, g_4 módulo $z-2$ en el **Paso 2**, obtenemos los polinomios:

$$\begin{aligned} g_{21} &:= 2y^2 + 2y, \\ g_{31} &:= 4y^4 - 4y^3 - 2y^2 + 6y, \\ g_{41} &:= x - 4y^3 + 2y^2 + 7y + 1. \end{aligned}$$

Paso 3: Volvemos a repetir el procedimiento del **Paso 1** y factorizamos el polinomio g_{21}, que depende solo de una variable. Obtenemos los factores y y $y+1$.

Paso 4: (Bucle) Para cada uno de los factores que acabamos de obtener, reducimos el resto de ecuaciones (g_{31}, g_{41}) módulo ese factor. Por lo tanto, cada factor representa una subrama dentro de la rama del factor $z-2$.

Tras reducir g_2, g_3, g_4 módulo y en el **Paso 4**, obtenemos los polinomios:

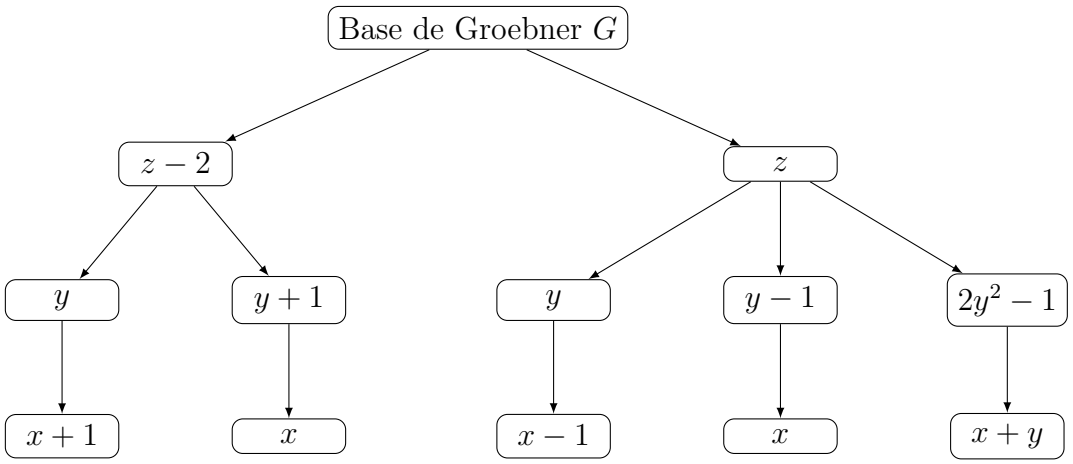
$$\begin{aligned} g_{312} &:= 0 \\ g_{412} &:= x + 1. \end{aligned}$$

Tras reducir g_2, g_3, g_4 módulo $y+1$ en el **Paso 4**, obtenemos los polinomios:

$$\begin{aligned} g_{311} &:= 0 \\ g_{411} &:= x. \end{aligned}$$

Tanto para y como para $y+1$ tenemos ya sistemas triangulares, llegando así al final de esas subramas. Y, por lo tanto, al final de la rama $z-2$. Repitiendo este proceso para la rama z, obtenemos los factores $x-1$ para la rama y, x para la rama $y+1$, y $x+y$ para la rama $2y^2-1$. Llegamos al final de la rama z, y con ello al final del algoritmo.

El siguiente diagrama recopila la información que hemos ido calculando paso a paso en el algoritmo:



Uniendo la información recogida en el árbol, tenemos los 5 sistemas triangulares que representan la salida del algoritmo de Lazard cuando le introducimos como *input* la base de Groebner G:

$$\left\{\begin{array}{rl} z & =2 \\ y & =0 \\ x & =-1 \end{array}\right. , \quad \left\{\begin{array}{rl} z & =2 \\ y & =-1 \\ x & =0 \end{array}\right. , \quad \left\{\begin{array}{rl} z & =0 \\ y & =0 \\ x & =1 \end{array}\right. ,$$

$$\left\{\begin{array}{rl} z & =0 \\ y & =1 \\ x & =0 \end{array}\right. , \quad \left\{\begin{array}{rl} z & =0 \\ 2y^2 & =1 \\ x+y & =0 \end{array}\right.$$

Nota 4.1. La resolución de estos 5 sistemas es inmediata. La unión de las soluciones de estos 5 sistemas representa el conjunto de soluciones del sistema 4.4, el cuál es más complicado de resolver directamente. En el Apéndice A se mostrará cómo utilizar el algoritmo de Lazard en el software `SINGULAR`.

Capítulo 5
Algoritmo de Möller

Este capítulo estudiará el segundo de los algoritmos de triangulación: el algoritmo de Möller [14]. Al igual que en el Capítulo 4, nos enfrentamos al problema de resolver un sistema de m ecuaciones

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0, \tag{5.1}$$

donde $f_1, \ldots, f_m$ son polinomios en n variables con coeficientes en un cuerpo K.

Este algoritmo, al igual que el de Lazard, trata sistemas de m ecuaciones polinómicas en n incógnitas que tienen un número finito de soluciones. Presenta un método que descompone el conjunto de soluciones en un número finito de subconjuntos, cada uno de ellos asociado a un sistema del tipo

$$f_1(x_1) = 0, \quad f_2(x_1, x_2) = 0, \ldots, f_n(x_1, \ldots, x_n) = 0. \tag{5.2}$$

Las principales herramientas para la descomposición provienen de la teoría de ideales que ya se ha estudiado en el trabajo. Además, para el ideal generado por los polinomios que describen el conjunto de soluciones, se requiere, al igual que en el algoritmo de Lazard, una base de Groebner con el orden lexicográfico.

5.1. Ideales y Descomposiciones

En primer lugar, algunas definiciones necesarias para este capítulo:

Definición 5.1. Sean $A, B \subseteq K[x_1, \ldots, x_n]$ ideales.

- Se define la **suma** de los ideales A y B como:

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

- Se define el **cociente** de los ideales A, B como:

$$A : B := \{p \in K[x_1, \ldots, x_n] \mid p \cdot b \in A \text{ para todo } b \in B\}.$$

  Por comodidad, denotaremos $A : b$ en lugar de $A : \langle b \rangle$ para $b \in K[x_1, \ldots, x_n]$.

- Se define el **producto** de los ideales A,B como:

$$A \cdot B := \langle a \cdot b \mid a \in A, b \in B \rangle .$$

  Además, definimos recursivamente $A^1 := A$ y $A^m := A^{m-1} \cdot A$ para $m > 1$.

- Se define el **radical de un ideal** como:

$$\sqrt{A} := \{f \in K[x_1, \ldots, x_n] \mid \exists \sigma \in \mathbb{N} \text{ tal que } f^\sigma \in A\} .$$

Observación 5.1. Como vimos en el Capítulo 2, el conjunto de todos los puntos que son ceros comunes de polinomios dados $f_1, \ldots, f_r$ es su *variedad algebraica*, $\mathcal{V}(f_1, \ldots, f_r)$. Algebraicamente, el conjunto

$$\{(x_1, \ldots, x_n) \in \overline{K}^n \mid f_i(x_1, \ldots, x_n) = 0,\ i = 1, \ldots, m\},$$

es una variedad algebraica que representa los ceros de los polinomios en el ideal $A = \langle f_1, \ldots, f_m \rangle$. Como vimos en la Observación 2.5, si el número de ceros es finito se dice que A es de dimensión cero o *cero-dimensional* y se denota dim(A) = 0.

Observación 5.2. Por el Teorema de los Ceros de Hilbert se cumple:

$$\sqrt{A} = \{f \in K[x_1, \ldots, x_n] \mid f(y) = 0 \text{ para todo } y \in \mathcal{V}(A)\} .$$

Por lo tanto, $\mathcal{V}(A) = \mathcal{V}(\sqrt{A})$.

Definición 5.2. Un ideal P se llama un *ideal primo cero-dimensional* si existe un punto $y \in \overline{K}^n$ tal que

$$f(y) = 0 \Rightarrow f \in P \quad \forall f \in K[x_1, \ldots, x_n]$$

Definición 5.3. Un ideal Q se llama *primario* (o P-primario) si, para todo $f, g \in K[x_1, \ldots, x_n]$, se cumple que:

$$f \cdot g \in Q \text{ y } g \notin Q \Rightarrow f^k \in Q \text{ para algún } k > 0.$$

Nota 5.1. Esta definición es la misma que se dio en la Subsección 1.4.4

Observación 5.3. Si Q es un ideal cero-dimensional, entonces es primario si y solo si existe $\sigma \in \mathbb{N}$ y un ideal primo cero-dimensional P tal que :

$$P^\sigma \subseteq Q \subseteq P.$$

En tal caso, se cumple $P = \sqrt{Q}$ (consultar [14]), y en particular:

$$\mathcal{V}(Q) = \mathcal{V}(P).$$

Observación 5.4. Todo ideal cero-dimensional A admite una llamada *descomposición primaria* [2], lo cual significa que existen solamente una cantidad finita de ideales primos cero-dimensionales P_i distintos, y correspondientes ideales P_i-primarios Q_i, tales que:

$$A = \bigcap Q_i.$$

Estos P_i y Q_i están determinados de manera única por A. En consecuencia:

$$\mathcal{V}(A) = \bigcup \mathcal{V}(P_i).$$

Lema 5.1. *Sean A y B ideales tales que $A \subseteq B$. Entonces para todo $m \in \mathbb{N}$ se cumple:*

$$A \subseteq B \cap (A : B^m) \subseteq \sqrt{A}. \tag{5.3}$$

Observación 5.5. Si $A = \sqrt{A}$ y $A \subseteq B$, entonces

$$A = B \cap (A : B) \quad \text{y} \quad A : B = A : B^m \quad \text{para todo entero } m > 1.$$

Demostración.

Como $A \subseteq A : B^m$ por definición del cociente de ideales, y dado que $A \subseteq B$, obtenemos la primera inclusión en (5.3).

Sea $g \in B \cap (A : B^m)$. Entonces $g \in B$ y $g \in A : B^m$. Por lo tanto, $g^m \in B^m$ y entonces $g^{m+1} \in A$, lo que implica $g \in \sqrt{A}$. Esto prueba (5.3).

Si $A = \sqrt{A}$, entonces por (5.3) se tiene:

$$A = B \cap A : B^m.$$

Si $g \in A : B^m$, entonces $g \cdot b^m \in A$ para todo $b \in B$. Por lo tanto, $g^m b^m \in A$, y como $g \cdot b \in \sqrt{A} = A$, se deduce que $g \in A : B$. Por otro lado, $A : B \subseteq A : B^m$. Así se concluye que:

$$A : B = A : B^m.$$

□

Observación 5.6. Si $\mathcal{V}(A) = \mathcal{V}(\sqrt{A})$, entonces el Lema 5.1 implica la descomposición a nivel de variedades

$$\mathcal{V}(A) = \mathcal{V}(B) \cup \mathcal{V}(A : B^m),$$

Bajo las condiciones adicionales $\dim(A) = 0$ y m suficientemente grande, mostraremos que la descomposición

$$\mathcal{V}(A) = \mathcal{V}(B) \cup \mathcal{V}(A : B^m)$$

es disjunta, es decir,

$$\mathcal{V}(B) \cap \mathcal{V}(A : B^m) = \emptyset,$$

y, además, se cumple lo siguiente.

Lema 5.2. *Sean A y B como en el Lema 5.1 y supongamos además que* $\dim(A) = 0$. *Entonces para $m \in \mathbb{N}$ suficientemente grande, se verifica*

$$\mathcal{V}(A) = \mathcal{V}(B) \cup \mathcal{V}(A : B^m)$$

y además, se cumple

$$\begin{aligned} \mathcal{V}(B) &= \{y \in \mathcal{V}(A) \mid \forall b \in B : b(y) = 0\}, \\ \mathcal{V}(A : B^m) &= \{y \in \mathcal{V}(A) \mid \exists b \in B : b(y) \neq 0\}. \end{aligned} \tag{5.4}$$

La demostración puede consultarse en [14]

Lema 5.3. *Sea* $\dim(A) = 0$ *y* $A \subseteq B = (g_1, \ldots, g_s)$. *Definimos inductivamente:*

$$A_0 := A, \quad A_i := A_{i-1} + \langle g_i \rangle, \quad i = 1, \ldots, s.$$

Entonces para enteros suficientemente grandes $m, m_1, \ldots, m_s \in \mathbb{N}$, *se cumple:*

$$\mathcal{V}(A : B^m) = \bigcup_{i=1}^{s} \mathcal{V}(A_{i-1} : g_i^{m_i}), \tag{5.5}$$

donde

$$\mathcal{V}((A_{i-1}) : g_i^{m_i}) = \{y \in \mathcal{V}(A) \mid g_1(y) = \cdots = g_{i-1}(y) = 0,\ g_i(y) \neq 0\}.$$

Si además A *es radical, entonces* (5.5) *se cumple para todos los enteros positivos* $m, m_1, \ldots, m_s$.

La demostración puede consultarse en [14]

5.2. Cocientes de ideales y Bases de Groebner

Observación 5.7. En la Sección 5.1 se ha descrito la descomposición de una variedad en variedades de ideales del tipo $A : g^m$, con m suficientemente grande. En esta sección lo relacionaremos con las bases de Groebner. Dado que $K[x_1, \ldots, x_n]$ es Noetheriano, es decir, toda cadena ascendente de ideales se estabiliza, la cadena ascendente

$$A \subseteq A : g \subseteq A : g^2 \subseteq \cdots$$

se estabiliza. Es decir, existe un entero k tal que

$$A : g^{k-1} \subseteq A : g^k = A : g^{k+1}.$$

Esto implica que $A : g^k = A : g^\ell$ para todo $\ell > k$.

Definición 5.4. Diremos que $A : g^k$ es la **saturación** de A respecto a g, y llamaremos a k su **índice de saturación**.

Queremos aplicar la descomposición dada por los Lemas 5.2 y 5.3. Por lo tanto, necesitamos calcular bases de Groebner para las saturaciones de los ideales $A_{i-1} : g_i$, donde

definimos recursivamente

$$A_i := A_{i-1} + \langle g_i \rangle, \quad \text{para } i = 1, \ldots, s.$$

Este cálculo es más sencillo si ya se conoce una base de Groebner para A_{i-1}. Por ello, preferimos contar con un algoritmo que, dada una base de Groebner para un ideal A_{i-1}, compute simultáneamente una base de Groebner para el siguiente ideal A_i y una base de Groebner para la saturación de $A_{i-1} : g_i$. Examinando con detalle un método propuesto por Gianni et al. [10], veremos que una pequeña modificación de dicho método cumple con nuestros requisitos.

Definición 5.5. Sea K un cuerpo y $K[x_1, \ldots, x_n]$ el anillo de polinomios en n variables. Para un entero $s \geq 1$, el **módulo** $K[x_1, \ldots, x_n]^s$ se define como el conjunto de s-tuplas:

$$K[x_1, \ldots, x_n]^s := \{(f_1, \ldots, f_s) \mid f_i \in K[x_1, \ldots, x_n] \text{ para todo } i = 1, \ldots, s\}$$

Observación 5.8. Dado un orden admisible $<_\tau$ sobre el conjunto de términos

$$T := \{x_1^{i_1} \cdots x_n^{i_n} \mid i_1, \ldots, i_n \geq 0\},$$

este puede extenderse al conjunto de términos de módulo

$$T^{(s)} := \{te_i \mid t \in T,\ 1 \leq i \leq s\},$$

donde $e_1, \ldots, e_s$ denotan los vectores canónicos de la base estándar.

Entonces todo $0 \neq u \in K[x_1, \ldots, x_n]^s$ tiene un término máximo $\mathrm{lt}(u) \in T^{(s)}$, y el coeficiente correspondiente se denota por $\mathrm{lc}(u)$.

Definición 5.6. Una **base de Groebner** de un submódulo $U \subseteq K[x_1, \ldots, x_n]^s$ es un subconjunto finito $G \subseteq U$ tal que, para todo $0 \neq f \in U$, el término líder $\mathrm{lt}(f)$ es un múltiplo de algún $\mathrm{lt}(g_i)$, con $g_i \in G$.

Observación 5.9. Recordemos que una base de Groebner G es *reducida* si ningún $\mathrm{lt}(g_i)$ divide al término líder de otro $g_j \in G$, con $g_i \neq g_j$.

Definición 5.7. La **forma normal** de un $f \in K[x_1, \ldots, x_n]^s$ con respecto a una base de Groebner G de U es un elemento $f' \in K[x_1, \ldots, x_n]^s$ tal que

$$f - f' \in U,$$

y f' es combinación lineal solo de términos que no son múltiplos de los $\mathrm{lt}(g_i)$, $g_i \in G$.

Lema 5.4. *Sea $A = (a_1, \ldots, a_r)$ un ideal y $0 \neq g \in K[x_1, \ldots, x_n]$. Definimos el submódulo*

$$M := \left\{(u, v) \in K[x_1, \ldots, x_n]^2 \mid u + g \cdot v \in A\right\},$$

el cual es un módulo con base

$$\{(a_1, 0), \ldots, (a_r, 0), (g, -1)\}.$$

Si $\pi_i : M \to K[x_1, \ldots, x_n]$ denota la proyección canónica sobre la i-ésima componente, para $i = 1, 2$, entonces se cumple:

$$\pi_1(M) = A + \langle g \rangle, \qquad \pi_2(\ker \pi_1) = A : g. \tag{5.6}$$

Demostración.

Observemos que $(a_i, 0) \in M$ y $(g, -1) \in M$. Sea $(u, v) \in M$. Entonces existen $h_1, \ldots, h_r \in K[x_1, \ldots, x_n]$ tales que

$$u + gv = \sum_{i=1}^{r} h_i a_i.$$

Por lo tanto,

$$(u, v) = \sum h_i \cdot (a_i, 0) + (-v) \cdot (g, -1),$$

lo que muestra que los generadores dados forman una base del módulo M.

Considerando ahora la proyección π_1 de estos elementos base, se tiene:

$$\pi_1(M) = A + \langle g \rangle.$$

Además, si $(0, v) \in M$, entonces $gv \in A$, es decir, $v \in A : g$, por lo que:

$$\pi_2(\ker \pi_1) = A : g.$$

□

5.3. Descomposición en Sistemas Triangulares

Definición 5.8. Sean $\{y_1, \ldots, y_r\}$ y $\{z_1, \ldots, z_s\}$ subconjuntos disjuntos de $\{x_1, \ldots, x_n\}$. Diremos que $\{y_1, \ldots, y_r\}$ está **lexicográficamente delante de** $\{z_1, \ldots, z_s\}$ con respecto al orden $<_\tau$ si, para todos los términos, se cumple la siguiente implicación:

$$y_1^{i_1} \cdots y_r^{i_r} <_\tau y_1^{j_1} \cdots y_r^{j_r} \;\Rightarrow\; y_1^{i_1} \cdots y_r^{i_r} z_1^{k_1} \cdots z_s^{k_s} <_\tau y_1^{j_1} \cdots y_r^{j_r} z_1^{l_1} \cdots z_s^{l_s}. \tag{5.7}$$

Lema 5.5. *Sea x_n lexicográficamente delante de $\{x_1, \ldots, x_{n-1}\}$ con respecto al orden $<_\tau$, y sea $\deg_{x_n}(f)$ el grado de f en la variable x_n. Entonces se cumplen las siguientes afirmaciones:*

(I) Si $f_1, \ldots, f_r$ son polinomios con $\deg_{x_n}(f_i) \leq d$ para $i = 1, \ldots, r$, entonces $\langle f_1, \ldots, f_r \rangle$ tiene una base de Groebner respecto a $<_\tau$, donde cada elemento f satisface $\deg_{x_n}(f) \leq d$.

(II) Si $F := \{f_1, \ldots, f_r\}$ es una base de Groebner respecto a $<_\tau$, entonces

$$F_k := \{f \in K[x_1, \ldots, x_n] \mid f \in F,\ \deg_{x_n}(f) < k\}$$

es también una base de Groebner (respecto a $<_\tau$) para todo entero positivo k.

(III) Sean $f_i = \sum_{j=0}^{d_i} \tilde{g}_{ij}(x_1, \ldots, x_{n-1}) x_n^{d_i - j}$ con $\tilde{g}_{i0} \neq 0$, para $i = 1, \ldots, r$. Si $F := \{f_1, \ldots, f_r\}$ es una base de Groebner respecto a $<_\tau$, entonces

$$G := \{\tilde{g}_{10}, \ldots, \tilde{g}_{r0}\}$$

es una base de Groebner (respecto a $<_\tau$).

Demostración.

Usando F como entrada para el algoritmo de Buchberger, observamos que, si ningún polinomio en la entrada tiene grado en x_n mayor que d, entonces esto sigue siendo cierto para todos los polinomios generados durante el algoritmo.

Esto se deduce de que $\deg_{x_n}(f) = \deg_{x_n}(\mathrm{lt}(f))$, y por lo tanto:

$$\deg_{x_n}(S(f,g)) \leq \text{máx}\left\{\deg_{x_n}(f), \deg_{x_n}(g)\right\},$$

donde $S(f,g)$ es el S-polinomio definido en la Definición 3.15. Además, en la reducción

$f \to_F g$:

$$f - \frac{\mathrm{lt}(f)}{\mathrm{lc}(f_i)\,\mathrm{lt}(f_i)} f_i,$$

también se cumple que $\deg_{x_n}(g) \leq \deg_{x_n}(f)$, ya que $g = \mathrm{lc}(f) \cdot \mathrm{S}(f, f_i)$ y $\mathrm{lt}(f_i)$ divide a $\mathrm{lt}(f)$. Esto demuestra la afirmación *(I)*.

Si F es una base de Groebner, entonces $S(f, g) \to_F^* 0$ (es decir, El S-polinomio de f y g se reduce a cero) para todos $f, g \in F_k$. Pero todo f_i que interviene en la reducción de $S(f, g)$ a cero satisface $\deg_{x_n}(f_i) < k$, por el mismo argumento anterior. Entonces $S(f, g) \to_{F_k}^* 0$, es decir, F_k ya es una base de Groebner. Esto demuestra *(II)*.

Si F es una base de Groebner, entonces observando solo la reducción de los términos de mayor grado en x_n en $S(f_i, f_j) \to^* 0$, obtenemos:

$$S(\tilde{g}_{i0}, \tilde{g}_{j0}) \to_G^* 0.$$

Esto demuestra *(III)*. □

Observación 5.10. Este lema muestra que, al disponer de una base de Groebner lexicográfica $F := \{f_1, \ldots, f_r\}$, se pueden deducir muchas otras bases de Groebner lexicográficas a partir de F. Por ejemplo, cuando los f_i están ordenados de modo que $\mathrm{lt}(f_j) < \mathrm{lt}(f_i)$ si $i > j$, y cuando, para un cierto s, el polinomio f_i es el único en $F \cap K[x_1, \ldots, x_k]$ con $\deg_{x_k}(f_i) = s$, entonces los conjuntos

$$\{f_i, f_{i+1}, \ldots, f_r\} \quad \text{y} \quad \{f_1, \ldots, f_i\}$$

son ambos bases de Groebner lexicográficas.

Ejemplo 5.1. Sea $\mathbb{Q}$ el cuerpo de los racionales, y consideremos en $\mathbb{Q}[x, y, z, w]$, $<_\tau$, el orden lexicográfico con

$$x <_\tau y <_\tau z <_\tau w.$$

Una base de Groebner lexicográfica es $\{f_1, \ldots, f_6\}$ [14], donde:

$$
\begin{aligned}
f_1 &:= w + z + y + x,\\
f_2 &:= z^2 + 2zx + x^2,\\
f_3 &:= zy - zx + y^2x^4 + yx - 2x^2,\\
f_4 &:= zx^4 - z + x^5 - x,\\
f_5 &:= y^3x^2 + y^2x^3 - y - x,\\
f_6 &:= y^2x^6 - y^2x^2 - x^4 + 1.
\end{aligned}
$$

Entonces los subconjuntos $\{f_2, f_3, f_4, f_5, f_6\}$, $\{f_3, f_4, f_5, f_6\}$, $\{f_5, f_6\}$, y $\{f_6\}$ también son bases de Groebner por el Lema 5.5 (parte III).

Aplicando dicho lema a estas cinco bases se obtienen, además, bases de Groebner lexicográficas (no reducidas), que tras reducción corresponden a:

- $\{1\}$ (a partir de $\{f_1, \ldots, f_6\}$),
- $\{f_2, \ldots, f_6\}$,
- $\{y - x, x^4 - 1\}$ (a partir de $\{f_3, f_4, f_5, f_6\}$),
- $\{x^2\}$,
- $\{x^6 - x^2\}$.

Ejemplo 5.2. Consideremos en $\mathbb{Q}[x, y, z]$, $<_\tau$, el orden lexicográfico con

$$x <_\tau y <_\tau z.$$

El conjunto $\{f_1, f_2, f_3, f_4\}$, donde :

$$
\begin{aligned}
f_1 &:= z^3 + z + y - 1,\\
f_2 &:= zy + zx + z + yx + x + 2,\\
f_3 &:= y^2 + 2y - 1,\\
f_4 &:= x^2 - 2,
\end{aligned}
$$

es una base de Groebner lexicográfica [14].

Entonces por el Lema 5.5 (II), los subconjuntos

$$\{f_2, f_3, f_4\}, \quad \{f_3, f_4\}, \quad \text{y} \quad \{f_4\}$$

también son bases de Groebner lexicográficas. Además, por la parte (III) del mismo lema, después de aplicar reducción se obtienen también como bases:

- $\{1\}$,
- $\{y + x + 1,\ x^2 - 2\}$ (a partir de $\{f_2, f_3, f_4\}$).

Lema 5.6. *Sea A un ideal cero-dimensional y G una base de Groebner de A. Entonces para cada $i = 1, \ldots, n$, existe $f_i \in G$ y un entero $k_i > 0$ tal que*

$$\mathrm{lt}(f_i) = x_i^{k_i}.$$

Demostración.

Como A es un ideal cero-dimensional, contiene para cada x_i un polinomio univariado en x_i. Su término líder, que es una potencia pura de x_i, debe ser múltiplo del término líder de algún $f_i \in G$, por definición de base de Groebner. □

Lema 5.7. *Sea $G = \{f_1, \ldots, f_r\}$ una base de Groebner reducida respecto a un orden $<_\tau$, donde x_n está lexicográficamente delante de $\{x_1, \ldots, x_{n-1}\}$. Supongamos que cada f_i tiene la forma:*

$$f_i := \sum_{j=0}^{d_i} \tilde{g}_{ij}(x_1, \ldots, x_{n-1}) x_n^{d_i - j},$$

con $\tilde{g}_{i0} \neq 0$, para $i = 1, \ldots, r$, y que $\mathrm{lt}(f_i) <_\tau \mathrm{lt}(f_j)$ para $i < j$. Si g_{10} es constante, entonces $\langle f_2, \ldots, f_r \rangle : f_1$ tiene como base de Groebner (respecto a $<_\tau$) al conjunto $\{\tilde{g}_{20}, \ldots, \tilde{g}_{r0}\}$, y $f_1 \notin \langle f_2, \ldots, f_r \rangle$.

La demostración puede consultarse en [14].

Observación 5.11. Si $\{f_1, \ldots, f_r\}$ genera un ideal cero-dimensional, entonces $\tilde{g}_{10}$ es constante. Esto se debe a que, por el Lema 5.6, existe un f_i tal que $\mathrm{lt}(f_i) = x_n^{k_n}$, y ese debe ser f_1, por la forma en que están ordenados los polinomios.

Nota 5.2. Para formular el algoritmo, necesitamos dos definiciones técnicas. Denotaremos por $<_k$ el orden lexicográfico de términos en $x_1, \ldots, x_k$, con

$$x_1 <_k \cdots <_k x_k.$$

Además, $\mathrm{SAT}(G, g, <_k)$ denota la saturación $A : g$, donde:

- G es una base de Groebner respecto al orden $<_k$,
- y A es el ideal generado por G.

Algoritmo 6 Algoritmo de Triangulación de Möller

- **Entrada:** $(\{f_1, \ldots, f_r\}; <_n)$, donde $\{f_1, \ldots, f_r\}$ es una base de Groebner reducida de un ideal cero-dimensional A respecto a $<_n$
- **Salida:** Un conjunto Z de subconjuntos $\{g_1, \ldots, g_n\}$ de tipo triangular tal que

$$\mathcal{V}(A) = \bigcup_{\{g_1,\ldots,g_n\}\in Z} \mathcal{V}(g_1, \ldots, g_n)$$

1: **Paso 1:** Sean $f_1, \ldots, f_r$ tales que $\mathrm{lt}(f_j) <_n \mathrm{lt}(f_i)$ para $i > j$. Para cada $i > 1$, sea $\tilde{f}_i := \mathrm{lc}_{x_n}(f_i) \in K[x_1, \ldots, x_{n-1}]$ el coeficiente líder de f_i considerado como polinomio en x_n. Sea $G_1 := \{f_1, \ldots, f_r\}$. Reducir la base de Groebner lexicográfica $\{\tilde{f}_2, \ldots, \tilde{f}_r\}$ a una base de Groebner reducida G.

2: **Paso 2:** Llamar al algoritmo con entrada $(G; <_{n-1})$, obteniendo un conjunto Z' formado por un número finito de conjuntos de polinomios $\{\tilde{g}_1, \ldots, \tilde{g}_{n-1}\}$. Entonces definir Z como el conjunto de todos los conjuntos de la forma

$$\left\{-\frac{1}{\mathrm{lc}(f_1)} f_1, \tilde{g}_1, \ldots, \tilde{g}_{n-1}\right\}, \quad \text{con } \{\tilde{g}_1, \ldots, \tilde{g}_{n-1}\} \in Z'.$$

3: **Paso 3: for** $i = 2, \ldots, r$, **do while** $\tilde{f}_i \notin A$:
calcular una base de Groebner G_i' de $\mathrm{SAT}(G_{i-1}, \tilde{f}_i, <_n)$, y una base de Groebner G_i del ideal $\langle f_1, \ldots, f_r, \tilde{f}_2, \ldots, \tilde{f}_i\rangle$, ambas respecto al orden $<_n$. Luego, llamar recursivamente al algoritmo con entrada $(G_i'; <_n)$ y ampliar el conjunto Z con los conjuntos triangulares obtenidos.

4: **return** Z;

A continuación demostraremos la correción y terminación de este algoritmo:

Demostración.

Para demostrarlo, sea $B := \langle f_2, \ldots, f_r\rangle : f_1 + (f_1)$. Como $f_i \in \langle f_2, \ldots, f_r\rangle \subseteq \langle f_2, \ldots, f_r\rangle : f_1$, para $i = 2, \ldots, r$, se tiene que $A \subseteq B$. Por el Lema 5.7, el conjunto $\{f_1, \tilde{f}_2, \ldots, \tilde{f}_r\}$ genera B y los $\tilde{f}_i$, para $i > 1$, dependen solo de $x_1, \ldots, x_{n-1}$ y constituyen una base de Groebner lexicográfica. Usando que

$$\mathcal{V}(B) = \mathcal{V}(f_1) \cap \mathcal{V}(\tilde{f}_2, \ldots, \tilde{f}_r) = \mathcal{V}(f_1) \cap \mathcal{V}(G),$$

donde G es una base de Groebner reducida de $\{\tilde{f}_2, \ldots, \tilde{f}_r\}$, y asumiendo que la corrección

y terminación ya están probadas para el algoritmo en $n-1$ variables, se deduce que en el Paso 2 se realiza la descomposición requerida de $\mathcal{V}(B)$.

Por el Lema 5.3, la variedad de la saturación $A : B$ es la unión disjunta de las variedades

$$\mathcal{V}(A : f_1^{m_1}), \quad \mathcal{V}((A + (f_1)) : \tilde{f}_2^{m_2}), \quad \ldots, \quad \mathcal{V}((A + \langle f_1, \ldots, \tilde{f}_{r-1}\rangle) : \tilde{f}_r^{m_r}),$$

para enteros suficientemente grandes m_i, $i = 1, \ldots, r$. Dado que $f_1 \in A$, la primera variedad es vacía, y $A + (f_1) = A$. Por lo tanto, $\mathcal{V}(A : B^m)$ es la unión disjunta de

$$\mathcal{V}(A : \tilde{f}_2^{m_2}), \quad \mathcal{V}((A + (\tilde{f}_2)) : \tilde{f}_3^{m_3}), \quad \ldots, \quad \mathcal{V}((A + \langle \tilde{f}_2, \ldots, \tilde{f}_{r-1}\rangle) : \tilde{f}_r^{m_r}),$$

donde se pueden omitir las variedades vacías. Por ejemplo, $(A + \langle \tilde{f}_2, \ldots, \tilde{f}_{i-1}\rangle) : \tilde{f}_i^{m_i}$ tiene variedad vacía si $\tilde{f}_i \in A$. Por construcción, $\tilde{f}_i \in A$ si y solo si $\deg_{x_n}(f_i) = 0$. El ordenamiento en el Paso 1 implica entonces que existe un índice k tal que $\tilde{f}_i \notin A$ si y solo si $i \leq k$. Por tanto, en el Paso 3 se computan todas las variedades no triviales, cuya unión es $\mathcal{V}(A : B^m)$.

Para la terminación, notamos que A es un subconjunto propio de la saturación $A : B$. Esto se sigue de la descomposición disjunta $\mathcal{V}(A) = \mathcal{V}(B) \cup \mathcal{V}(A : B^m)$ y del hecho de que $\mathcal{V}(B) \neq \emptyset$, ya que de lo contrario $1 \in \langle f_2, \ldots, f_r\rangle : f_1$, en contradicción con que $f_i \notin \langle f_2, \ldots, f_r\rangle$ por el Lema 5.7. Por lo tanto, $A \subsetneq \mathrm{SAT}(G_{i-1}, \tilde{f}_i, <_n) \supseteq A : B^m$. Si sabemos que el algoritmo termina al aplicarse a ideales en $K[x_1, \ldots, x_{n-1}]$ y a ideales que contienen adecuadamente a A, entonces un argumento inductivo prueba la terminación del algoritmo aplicado a A, ya que $K[x_1, \ldots, x_n]$ es noetheriano.

□

Teorema 5.8. *Sean $f_1, \ldots, f_r$ polinomios en $K[x_1, \ldots, x_n]$ con solamente un número finito de ceros comunes. Entonces el conjunto $\mathcal{V}(f_1, \ldots, f_r)$ de estos ceros es la unión disjunta de un número finito de conjuntos $\mathcal{V}(g_1, \ldots, g_n)$, obtenidos mediante el algoritmo de descomposición, donde:*

$$\begin{aligned}
g_1 &= x_1^{d_1} + \sum_{j=0}^{d_1-1} a_j x_1^j && \in K[x_1], \\
g_2 &= x_2^{d_2} + \sum_{j=0}^{d_2-1} g_{2,j}(x_1) x_2^j && \in K[x_1, x_2], \\
&\vdots \\
g_n &= x_n^{d_n} + \sum_{j=0}^{d_n-1} g_{n,j}(x_1, \ldots, x_{n-1}) x_n^j && \in K[x_1, \ldots, x_n].
\end{aligned} \tag{5.8}$$

5.4. Ejemplos del Algoritmo de Möller

Finalmente, veamos cómo funciona el algoritmo de descomposición cuando se aplica a las bases consideradas en los Ejemplos 5.1 y 5.2.

Ejemplo 5.3. Como vimos en el Ejemplo 5.1, tenemos que

$$\begin{aligned} f_1 &:= w + z + y + x, \\ f_2 &:= z^2 + 2zx + x^2, \\ f_3 &:= zy - zx + y^2x^4 + yx - 2x^2, \\ f_4 &:= zx^4 - z + x^5 - x, \\ f_5 &:= y^3x^2 + y^2x^3 - y - x, \\ f_6 &:= y^2x^6 - y^2x^2 - x^4 + 1. \end{aligned}$$

es una base de Groebner lexicográfica. La primera llamada al algoritmo es con entrada $(\{f_1, \ldots, f_6\}, <_4)$:

Paso 1: (Sin cálculo, solo aplicación del Lema 5.7): $\tilde{f}_i = f_i$, $i = 2, \ldots, 6$.

Paso 2: Llamamos al algoritmo con entrada $(\{f_2, \ldots, f_6\}, <_3)$, y añadimos f_1 a todos los conjuntos triangulares resultantes.

Paso 3: Bucle vacío.

La llamada con entrada $(\{f_2, \ldots, f_6\}, <_3)$ da:

Paso 1: (Sin cálculo, solo aplicación del Lema 5.7): $\{\tilde{f}_3, \ldots, \tilde{f}_6\} = \{y - x, x^4 - 1, f_5, f_6\}$. La reducción de esta base de Groebner (es decir, cancelación de polinomios redundantes) da $\{y - x, x^4 - 1\}$.

Paso 2: Llamamos al algoritmo con entrada $(\{y - x, x^4 - 1\}, <_2)$, lo que resulta en $\{\{x^4 - 1, y - x\}\}$. Se añade f_2, lo que da:

$$\left\{x^4 - 1, y - x, z^2 + 2zx + x^2\right\}.$$

Paso 3: Como $\langle f_2, \ldots, f_6\rangle : (y - x) = \langle 2z - yx^3 + 3x, f_5, f_6\rangle$, se llama al algoritmo con entrada $(\{2z - yx^3 + 3x, f_5, f_6\}, <_3)$. Entonces $\langle f_2, \ldots, f_6, y - x\rangle : (x^4 - 1) = \langle 1\rangle$, sin más llamadas (variedad vacía).

La llamada con entrada $(\{2z - y^2x^3 + 3x, f_5, f_6\}, <_3)$ da, de forma análoga a la primera llamada, una llamada con entrada $(\{f_5, f_6\}, <_2)$, donde $2z - y^2x^3 + 3x$ se añade a todos

los conjuntos triangulares resultantes.

La llamada con entrada $(\{f_5, f_6\}, <_2)$ se traduce en:

Paso 1: El Lema 5.7 no es aplicable ya que $\mathrm{lt}_y(f_5) = x^3$. Este paso computa B. Obtenemos $B = \langle f_5, x^4 - 1\rangle$ porque $\langle f_6\rangle : f_5 = \langle x^4 - 1\rangle$.

Paso 2: Como $\{x^4 - 1\}$ ya es "triangular", este paso devuelve $\{x^4 - 1, f_5\}$.

Paso 3: $\langle f_5, f_6\rangle : \langle x^4 - 1\rangle = \langle y^2x^2 - 1\rangle$. No es posible más descomposición. Por tanto, $\{y^2x^2 - 1\}$ se devuelve sin cambios.

Finalmente, el algoritmo devuelve $\{S_1, S_2, S_3\}$, donde:

$$
\begin{aligned}
S_1 &:= \{x^4 - 1,\ y - x,\ z^2 + 2zx + x^2,\ w + z + y + x\},\\
S_2 &:= \{x^4 - 1,\ y^3x^2 + 2y^2x^3 - y - x,\ 2z - y^2x^3 + 3x,\ w + z + y + x\},\\
S_3 &:= \{yx^2 - 1,\ 2z - y^2x^3 + 3x,\ w + z + y + x\}.
\end{aligned}
$$

Ejemplo 5.4. Como vimos en el Ejemplo 5.2, tenemos que

$$
\begin{aligned}
f_1 &:= z^2 + z + y - 1,\\
f_2 &:= zy + zx + z + yx + x + 2,\\
f_3 &:= y^2 + 2y - 1,\\
f_4 &:= x^2 - 2.
\end{aligned}
$$

es una base de Groebner lexicográfica.

La primera llamada al algoritmo es con entrada $(\{f_1, f_2, f_3, f_4\}, <_3)$:

Paso 1: (Sin cálculos, solo aplicación del Lema 5.7) $\tilde{f}_2 = y + x + 1$, $\tilde{f}_3 = f_3$, $\tilde{f}_4 = f_4$. La cancelación de elementos redundantes de la base de Groebner da el conjunto $\{y + x + 1, x^2 - 2\}$.

Paso 2: Como la entrada $\{y + x + 1, x^2 - 2\}$ ya es triangular, el algoritmo con entrada $(\{y + x + 1, x^2 - 2\}, <_2)$ devuelve este conjunto sin cambios. Añadiendo f_1, obtenemos el primer conjunto triangular para el ideal $\langle f_1, f_2, f_3, f_4\rangle$.

Paso 3: El bucle solo se usa una vez, ya que $x^2 - 2 = f_4 \in \langle f_1, f_2, f_3, f_4\rangle$. Entonces $\langle f_1, f_2, f_3, f_4\rangle : (y + x + 1) = \langle z + x, y - x + 1, f_4\rangle$, que ya es un conjunto triangular. Por tanto, el algoritmo devuelve el conjunto $\{f_4, y - x + 1, z + x\}$.

En total, el algoritmo devuelve el conjunto $\{S_1, S_2\}$, donde:

$$S_1 := \{x^2 - 2, y + x + 1, z^2 + z + y - 1\},$$
$$S_2 := \{x^2 - 2, y - x + 1, z + x\}.$$

Capítulo 6
Conclusiones

Un aporte significativo de este trabajo ha sido evidenciar cómo los algoritmos de triangulación permiten no solo simplificar el análisis algebraico de los sistemas, sino también mejorar la eficiencia computacional en la obtención de sus soluciones. Al descomponer los sistemas originales en familias triangulares, es posible reducir el problema a una sucesión de ecuaciones de complejidad controlada, lo que constituye una ventaja muy relevante, especialmente en contextos simbólicos o cuando se requiere una descripción completa de todas las soluciones. Un aspecto central ha sido el uso de bases de Groebner como etapa intermedia. Como se ha mostrado en los Capítulos 4 y 5, ambos algoritmos de triangulación parten de una base de Gröbner con orden lexicográfico, que actúa como una herramienta de reordenamiento y preparación del sistema para su posterior descomposición. Esto pone de manifiesto el valor de las bases de Groebner no solo como técnica de simplificación de ideales, sino también como paso previo para la obtención de formas trianguladas y, por tanto, para la resolución efectiva de sistemas.

Asimismo, se han mencionado otras técnicas algebraicas complementarias, como la teoría de eliminación, los resultantes o la descomposición primaria, que aunque no son el foco principal del presente trabajo, enriquecen el abanico de herramientas disponibles y ayudan a contextualizar los métodos utilizados.

De este trabajo podemos extraer la conclusión de que la triangulación es una herramienta poderosa en la práctica. Todos los sistemas tratados en este trabajo presentaban una complejidad significativa si se abordaban directamente, tanto desde el punto de vista algebraico como computacional. Sin embargo, una vez aplicados los algoritmos de triangulación, los sistemas resultantes adquirieron una estructura jerárquica que permitió resolverlos de forma secuencial, con métodos directos y sencillos.

Apéndice A
Ejemplos en SINGULAR

En este apéndice se expondrán ejemplos de los dos algoritmos de triangulación estudiados en este trabajo implementados con el software de álgebra computacional SINGULAR [3].

A.1. Algoritmo de Lazard

El software SINGULAR implementa el algoritmo de triangulación de Lazard mediante el procedimiento `triangL`. Además, se dispone de una variante denominada `triangLfak`, que realiza una factorización explícita de los polinomios en cada sistema triangular. Esta factorización puede resultar útil para un análisis más detallado de las raíces. Ambos procedimientos están disponibles en la librería `triang.lib` de SINGULAR [11].

A.1.1. Descripción de los procedimientos `triangL` y `triangLfak`

Ambos procedimientos están diseñados para aplicarse sobre ideales de dimensión cero. Requieren como entrada una base de Gröbner reducida, calculada con orden lexicográfico y ordenada por términos líderes crecientes.

Sintaxis general:

```
triangL(G);
triangLfak(G);
```

donde:

- `G` es un `ideal` que representa la base de Gröbner reducida del sistema original.

Salida: Ambos procedimientos devuelven una lista finita de sistemas triangulares, con la siguiente diferencia:

- `triangL`: devuelve sistemas triangulares cuya unión de variedades coincide con la variedad del ideal original.
- `triangLfak`: hace lo mismo que `triangL`, pero además factoriza cada polinomio de los sistemas triangulares resultantes.

A.1.2. Ejemplo

Consideremos el sistema del Ejemplo 4.4, dado por los siguientes polinomios:

$$\begin{aligned} f_1 &:= x^2 + y^2 - 1, \\ f_2 &:= (x + y + z - 1)(x + y), \\ f_3 &:= xyz. \end{aligned}$$

A continuación, utilizamos en SINGULAR el procedimiento `triangL` para obtener la descomposición del sistema $f_i = 0 \quad i = 1 \dots 3$ en sistemas triangulares con el algoritmo de Lazard:

```
LIB "triang.lib";

ring r = 0,(x,y,z),lp;

ideal F = x^2+y^2-1,(x+y+z-1)*(x+y),x*y*z;

ideal G = stdfglm(F);
list S = triangL(G);
list Sfak = triangLfak(G);

S;
Sfak;
```

Listing A.1: Implementación en SINGULAR de triangL

Nota 1. *Como hemos comentado,* ***triangL*** *y* ***triangLfak*** *reciben una base de Groebner calculada con el orden lexicográfico. El comando* ***stdfglm(F)*** *calcula primero la base de Gröbner de F en orden* ***degrevlex*** *por ser el más rápido, comprueba que el ideal sea*

de dimensión cero y aplica el algoritmo FGLM para transformar dicha base al orden lexicográfico, guardando el resultado en la variable `G`.

El resultado que nos devuelve `SINGULAR` es que S es el conjunto de los tres sistemas triangulares S_1, S_2, S_3 siguientes:

```
[1]:
   _[1]=z-2
   _[2]=y2+y
   _[3]=x+y+1
[2]:
   _[1]=z
   _[2]=2y4-2y3-y2+y
   _[3]=x-4y3+2y2+3y-1
[3]:
   _[1]=z
   _[2]=2y4-2y3-y2+y
   _[3]=x-4y3+2y2+3y-1
```

Figura 1.1: *Salida del procedimiento* `triangL`

Nota 2. *Cabe destacar que el segundo y tercer sistema devueltos por* `SINGULAR` *son idénticos. Se detectó y comunicó esta errata a su autor para su posterior corrección en el programa.*

$$S_1 = \Big\{ z-2,\ y^2+y,\ x+y+1 \Big\},$$
$$S_2 = \Big\{ z,\ 2y^4-2y^3-y^2+y,\ x-4y^3+2y^2+3y-1 \Big\}.$$

Las soluciones de estos 2 sistemas triangulares son:

$$T_1 = \Big\{ (0,\ -1,\ 2),\ (-1,\ 0,\ 2) \Big\},$$
$$T_2 = \Big\{ \Big(\tfrac{\sqrt{2}}{2},\ -\tfrac{\sqrt{2}}{2},\ 0\Big),\ (1,\ 0,\ 0),\ \Big(-\tfrac{\sqrt{2}}{2},\ \tfrac{\sqrt{2}}{2},\ 0\Big),\ (0,\ 1,\ 0) \Big\}.$$

Y el resultado que nos devuelve `SINGULAR` es que Sfak (salida de triangLfak, es decir, misma salida que triangL pero con los polinomios ya factorizados) es el conjunto de los cinco sistemas triangulares S_1^{fak},S_2^{fak},S_3^{fak},S_4^{fak},S_5^{fak} siguientes:

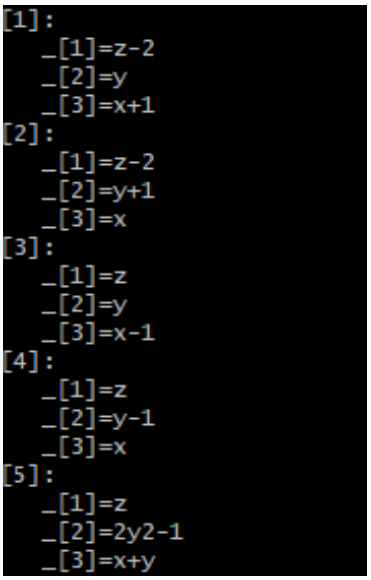


Figura 1.2: *Salida del procedimiento* ***triangLfak***

$$S_1^{\text{fak}} := \left\{ z-2,\ y,\ x+1 \right\}, \quad S_2^{\text{fak}} := \left\{ z-2,\ y+1,\ x \right\}, \quad S_3^{\text{fak}} := \left\{ z,\ y,\ x-1 \right\},$$
$$S_4^{\text{fak}} := \left\{ z,\ y-1,\ x \right\}, \quad S_5^{\text{fak}} := \left\{ z,\ 2y^2-1,\ x+y \right\}.$$

Las soluciones de estos 5 sistemas triangulares son:

$$T_1^{\text{fak}} = \{\,(-1,\ 0,\ 2)\,\}, T_2^{\text{fak}} = \{\,(0,\ -1,\ 2)\,\}, T_3^{\text{fak}} = \{\,(1,\ 0,\ 0)\,\},$$
$$T_4^{\text{fak}} = \{\,(0,\ 1,\ 0)\,\}, T_5^{\text{fak}} = \left\{ \left(\tfrac{\sqrt{2}}{2},\ -\tfrac{\sqrt{2}}{2},\ 0\right),\ \left(-\tfrac{\sqrt{2}}{2},\ \tfrac{\sqrt{2}}{2},\ 0\right) \right\}.$$

Observación 1. *La primera observación es que*

$$\bigcup_{i=1}^{3} T_i = \bigcup_{i=1}^{5} T_i^{\text{fak}}$$

La segunda observación es que, como es de esperar, el conjunto de soluciones del sistema original $f_i = 0 \quad i = 1 \ldots 3$ *es el conjunto*

$$\bigcup_{i=1}^{5} T_i^{\text{fak}}$$

Es decir, los procedimientos ***triangL*** *y* ***triangLfak*** *han devuelto una descomposición del sistema original en sistemas triangulares cuya unión de soluciones conforma el conjunto de soluciones del sistema original.*

A.2. Algoritmo de Möller

El software `SINGULAR` implementa el algoritmo de triangulación de Möller a través del procedimiento `triangM`. Como mejora, `SINGULAR` incluye también el procedimiento `triangMH`, que incorpora una etapa de factorización intermedia. Esta versión puede reducir la complejidad de los sistemas generados y mejorar el rendimiento computacional. Ambos procedimientos están disponibles en la librería `triang.lib` de `SINGULAR` [11].

A.2.1. Descripción de los procedimientos `triangM` y `triangMH`

Ambos procedimientos están diseñados para aplicarse sobre ideales de dimensión cero. Requieren como entrada una base de Gröbner reducida, calculada con orden lexicográfico y ordenada por términos líderes crecientes.

Sintaxis general:

```
triangM(G[,i]);
triangMH(G[,i]);
```

donde:

- `G` es un `ideal` que representa la base de Gröbner reducida del sistema original.
- `i` es un parámetro opcional. Si se indica `i = 2`, los polinomios en los sistemas triangulares serán factorizados.

Salida: Ambos procedimientos devuelven una lista de sistemas triangulares. La diferencia entre ellos es:

- `triangM`: la unión de variedades de los sistemas generados es igual a la variedad del ideal original.
- `triangMH`: la unión disjunta de variedades coincide con la del ideal original, evitando solapamientos entre los sistemas obtenidos.

A.2.2. Ejemplo

Retomando el Ejemplo 5.4, consideremos el sistema dado por los siguientes polinomios:

$$\begin{aligned} f_1 &:= z^2 + z + y - 1, \\ f_2 &:= zy + zx + z + yx + x + 2, \\ f_3 &:= y^2 + 2y - 1, \\ f_4 &:= x^2 - 2. \end{aligned}$$

A continuación, utilizamos en SINGULAR el procedimiento `triangM` para obtener la descomposición del sistema $f_i = 0 \quad i = 1 \dots 4$ en sistemas triangulares con el algoritmo de Möller:

```
LIB "triang.lib";

ring r = 0,(x,y,z),lp;

ideal F = z^2 + z + y - 1,
          z*y + z*x + z + y*x + x + 2,
          y^2 + 2*y - 1,
          x^2 - 2;
ideal G = stdfglm(F);
list S = triangM(G);
S;
```

Listing A.2: Implementación en SINGULAR del Ejemplo 5.4

Nota 3. *Como hemos comentado,* ***`triangM`*** *recibe una base de Groebner calculada con el orden lexicográfico. El comando* ***`stdfglm(F)`*** *calcula primero la base de Gröbner de F en orden* ***`degrevlex`*** *por ser el más rápido, comprueba que el ideal sea de dimensión cero y aplica el algoritmo FGLM para transformar dicha base al orden lexicográfico, guardando el resultado en la variable* ***`G`****. En este caso, utilizar* ***`stdfglm`*** *es redundante dado que, como vimos en el Ejemplo 5.4, F ya es una base de Groebner con el orden lexicográfico. Pero se ha incluido en el código para que el lector comprenda que, en caso de no ser así, sí sería necesario. Por otro lado, en este caso triangM y triangMH devuelven el mismo resultado, por lo que solo se ha incluido el primero.*

El resultado que nos devuelve SINGULAR es que S es el conjunto de los dos sistemas triangulares S_1' y S_2' siguientes:

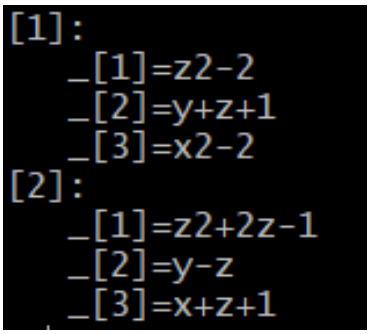


Figura 1.3: *Salida del procedimiento* ***triangM***

$$S_1' := \left\{ z^2 - 2,\ y + z + 1,\ x^2 - 2 \right\},$$
$$S_2' := \left\{ z^2 + 2z - 1,\ y - z,\ x + z + 1 \right\}.$$

Las soluciones de estos sistemas triangulares son:

$$\begin{aligned} T_1' = \{ & (\sqrt{2},\ -1 - \sqrt{2},\ \sqrt{2}), (\sqrt{2},\ -1 + \sqrt{2},\ -\sqrt{2}), \\ & (-\sqrt{2},\ -1 - \sqrt{2},\ \sqrt{2}), (-\sqrt{2},\ -1 + \sqrt{2},\ -\sqrt{2})\}, \\ T_2' = \{ & (-\sqrt{2},\ \sqrt{2} - 1,\ \sqrt{2} - 1),\ (\sqrt{2},\ -1 - \sqrt{2},\ -1 - \sqrt{2})\}. \end{aligned}$$

Como era de esperar, el sistema original, dado por $f_i = 0 \quad i = 1 \ldots 4$, tiene 6 soluciones y son los 6 elementos del conjunto $T_1' \cup\ T_2'$.

Observación 2. *Para finalizar, cabe hacer una importante observación. En el Capítulo 5, el algoritmo de Möller, ejecutado para este mismo sistema inicial paso a paso, nos devolvía los conjuntos S_1 y S_2 siguientes:*

$$S_1 := \{x^2 - 2, y + x + 1, z^2 + z + y - 1\},$$
$$S_2 := \{x^2 - 2, y - x + 1, z + x\}.$$

Cabe destacar que estos conjuntos no son idénticos a los conjuntos S_1' y S_2' devueltos por la implementación del algoritmo de Möller en ***SINGULAR****. Sin embargo, el sistema asociado a S_1 tiene 4 soluciones y el de S_2 tiene 2 soluciones, y esas 6 soluciones son:*

$$\begin{aligned} T = \{ & (\sqrt{2},\ -1 - \sqrt{2},\ \sqrt{2}), (\sqrt{2},\ -1 + \sqrt{2},\ -\sqrt{2}), \\ & (-\sqrt{2},\ -1 - \sqrt{2},\ \sqrt{2}), (-\sqrt{2},\ -1 + \sqrt{2},\ -\sqrt{2})\}, \\ & (-\sqrt{2},\ \sqrt{2} - 1,\ \sqrt{2} - 1),\ (\sqrt{2},\ -1 - \sqrt{2},\ -1 - \sqrt{2})\} \end{aligned}$$

Las 6 soluciones coinciden en ambos casos y, por tanto, ambas descomposiciones son válidas, y sus soluciones conforman las soluciones del sistema original. Esto sucede porque la descomposición en sistemas triangulares no es única, y factores como cambios en la implementación del algoritmo en ***SINGULAR*** *por parte del autor, puede llevar a diferentes descomposiciones, aunque todas ellas con las mismas soluciones.*

Bibliografía

[1] D. A. Cox, J. Little y D. O'Shea. *«Ideals, Varieties, and Algorithms»*. 4th. Springer, 2015. ISBN: 978-3-319-16720-6.

[2] W. Decker y C. Lossen. *«Computing in Algebraic Geometry: A Quick Start Using SINGULAR»*. Vol. 16. Algorithms and Computation in Mathematics. Springer, 2006. ISBN: 978-3-540-28992-8.

[3] W. Decker et al. *«SINGULAR 4-4-0 — A Computer Algebra System for Polynomial Computations»*. 2024. URL: http://www.singular.uni-kl.de.

[4] C. Dicrescenzo y D. Duval. «Algebraic computations on algebraic numbers». En: *Computers and Computing*. Ed. por P. Chenin et al. Conference volume. Paris, France: Masson y Wiley, 1985, págs. 54-61.

[5] C. Dicrescenzo y D. Duval. «Algebraic Extensions and Algebraic Closure in SCRATCHPAD II». En: *Proceedings of ISSAC '88: International Symposium on Symbolic and Algebraic Computation*. Ed. por P. Gianni. Vol. 358. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1988, págs. 440-446.

[6] J. Della Dora, C. Dicrescenzo y D. Duval. «About a New Method for Computing in Algebraic Number Fields». En: *Proc. EUROCAL '85, Vol. 2*. Vol. 204. Lecture Notes in Computer Science. Springer, 1985, págs. 289-290.

[7] D. Duval. «Diverses questions relatives au calcul formel avec des nombres algébriques». Thèse d'État. Université de Grenoble, 1987.

[8] D. Eisenbud. *«Commutative Algebra with a View Toward Algebraic Geometry»*. Vol. 150. Graduate Texts in Mathematics. Springer, 1995. ISBN: 978-0-387-94268-1.

[9] J. C. Faugère et al. «Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering». En: *Journal of Symbolic Computation* 16.4 (1993). Received 27 June 1989, págs. 329-344.

[10] P. Gianni, B. M. Trager y G. Zacharias. «Gröbner Bases and Primary Decomposition of Polynomial Ideals». En: *Journal of Symbolic Computation* 6 (1988), págs. 149-167.

[11] G.-M. Greuel, G. Pfister y H. Schönemann. *«*`triang.lib`. *A* SINGULAR *4-4-0 Library for Triangular Decomposition and Related Methods»*. 2023. URL: https://www.singular.uni-kl.de/Manual/4-4/sing_2193.htm#SEC2274.

[12] M. Kalkbrenner. «Solving Systems of Algebraic Equations by Using Gröbner Bases». En: *European Conference on Computer Algebra*. Ed. por J. H. Davenport. Lecture Notes in Computer Science. Springer, 1987.

[13] D. Lazard. «Solving Zero-dimensional Algebraic Systems». En: *Journal of Symbolic Computation* 13.2 (1992). Received 27 June 1989, págs. 117-131.

[14] H. M. Möller. «On Decomposing Systems of Polynomial Equations With Finitely Many Solutions». En: *Applicable Algebra in Engineering, Communication and Computing* 4 (1993). Received June 15, 1992; revised version March 2, 1993, págs. 217-230.

[15] G. Strang. *«Introduction to Linear Algebra»*. 5th. Wellesley-Cambridge Press, 2016.

[16] W. Wen-Tsün. «A Zero Structure Theorem for Polynomial Equation Solving». En: *Math. Mechanization Research Preprints* 1 (1987).