USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Bases de Gröbner

Xabier García Martínez

2011/2012

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Bases de Gröbner

Xabier García Martínez

Xullo, 2012

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: Bases de Gröbner
Director/a: Manuel Ladra González
Breve descrición do contido
Algoritmo da división. Algoritmo de Buchberger. Bases de Gröbner reducidas. Problema de pertencer a un ideal. Relación cos algoritmos de Euclides e de Gauss. Algunhas aplicacións: Demostracións automáticas en xeometría euclidiana do plano. Cálculo de polinomios mínimos de elementos en extensións de corpos.
Recomendacións
É recomendable cursar a materia "Álxebra, Números e Xeometría".
Outras observacións
Bibliografía: W.W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Mathematics 3, American Mathematical Society, Providence, RI, 1994. S.C. Coutinho, Polinômios e Computação Algébrica, Universidade Federal do Rio de Janeiro, 2009. `http://www.dcc.ufrj.br/~collier/e-books/Compalg.pdf` D. Cox, J. Little, D.O. O'Shea, Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra, Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

Índice general

Resumen

En este trabajo se presentarán los órdenes monomiales y el algoritmo de la división. Se definirán y se caracterizarán las bases de Gröbner, y se dará un algoritmo para calcularlas, el algoritmo de Buchberger, viendo su relación con los algoritmos de Gauss y de Euclides. Se resolverán varios problemas usando bases de Gröbner como el de pertenecer a un ideal, dar las ecuaciones implícitas de una variedad dada en forma paramétrica, dar algoritmos para realizar operaciones básicas con ideales, dar una K-base de $\frac{K[x_1,\ldots,x_n]}{I}$ o hallar el núcleo y la imagen de un homomorfismo de anillos de polinomios. Se darán aplicaciones de las bases de Gröbner externas al álgebra conmutativa tales como el cálculo de polinomios mínimos en extensiones de cuerpos, demostraciones automáticas en geometría euclidiana en el plano y una aproximación a un algoritmo para colorear grafos con k colores y en particular para resolver Sudokus.

Abstract

In this paper, we present monomial orders and division algorithm. We define and characterize Gröbner bases, and we provide a method to calculate them, the Buchberger's algorithm, relating this algorithm to Gaussian elimination and the Euclidean algorithm. Several problems will be solved using Gröbner bases, such as the ideal membership problem, the implicitization problem, obtaining algorithms to do algebraic operations with ideals, finding a K-basis of $\frac{K[x_1,\ldots,x_n]}{I}$ or finding the kernel and the image of a polynomial map. We also present some Gröbner bases applications outside commutative algebra, such as finding minimal polynomials in field extensions, automatic geometric theorem proving and an approximation to an algorithm to k-color a graph, and in particular to solve Sudokus.

Introducción

La construcción de algoritmos en el campo del álgebra conmutativa y geometría algebraica es relativamente reciente. El avance más significativo en la construcción de algoritmos para álgebra conmutativa y geometría algebraica, surge de la teoría y técnicas que desarrolló Bruno Buchberger en su tesis doctoral [2]. La teoría de Buchberger o bases de Gröbner, permite manipular polinomios en varias variables casi de la misma forma, que uno manipula polinomios en una variable. El algoritmo de Buchberger, piedra angular de la teoría de las bases de Gröbner, es una generalización del Algoritmo de Euclides al caso multivariable, si se ve desde el punto de vista de la teoría de ideales sobre $K[x_1, \ldots, x_n]$ (K cuerpo), debido a la unicidad del resto de la división de un polinomio por una base de Gröbner. También se puede considerar como una generalización del algoritmo de eliminación de Gauss al caso no lineal, si se ve desde el punto de vista de la teoría de variedades, pues, en el caso lineal, los polinomios que definen una variedad lineal en el sistema final, tras haber aplicado Gauss, forman una base de Gröbner respecto al orden monomial lexicográfico.

En 1964, Gröbner propuso a su estudiante Bruno Buchberger resolver el problema del cálculo de una K-base de $\dfrac{K[x_1, \ldots, x_n]}{I}$ siendo I un ideal de dimensión cero. Para su sorpresa, consiguieron desarrollar un algoritmo que era válido para cualquier ideal I. Incomprensiblemente los resultados obtenidos por Buchberger recibieron escasa atención hasta principios de los años setenta, fue entonces cuando Buchberger acuñó el término base de Gröbner.

A la vez que se desarrollaba la teoría de las bases de Gröbner, Hironaka (1964) [8] introduce, aunque de modo no constructivo, las bases estándar ("standard bases") para ideales en el anillo de series de potencias; estas bases han resultado ser análogas de las bases de Gröbner. El trabajo de Hironaka fue independiente del de Buchberger, y no fue hasta los años setenta cuando la analogía fue sacada a la luz. Knuth y Bendix (1970) [9] desarrollaron la idea de la compleción del par crítico, estructura que recuerda al algoritmo de Buchberger, para la completa reescritura de sistemas de ecuaciones ("term-rewriting systems"). Incluso antes que el correspondiente concepto en álgebras asociativas conmutativas libres, las bases de Gröbner para ideales en álgebras de Lie libres fueron introducidas por Shirshov [12].

Desde su creación, la teoría de las bases de Gröbner ha experimentado un notable crecimiento. Si se restringe a sus aplicaciones, se ve que estas aparecen por doquier, en áreas tan diversas de las matemáticas como la integración indefinida de funciones racionales, la teoría de códigos, la estadística, las ecuaciones en derivadas parciales, la teoría de grafos, programación entera, funciones hipergeométricas, análisis numérico, diseño geométrico asistido por ordenador, teoría de homotopía combinatoria, etc. En el caso particular del álgebra conmutativa y geometría algebraica, proporciona métodos para el cálculo de inversas de aplicaciones racionales, la resolución de sistemas de ecuaciones polinómicas, la inversión de matrices, el cálculo del máximo común divisor de varios polinomios, la pertenencia de un polinomio a un ideal del anillo de polinomios en n variables, el cálculo de las ecuaciones implícitas de una variedad a partir de sus ecuaciones paramétricas, etc.

Este trabajo está dividido en 5 capítulos. En el primero se introducirán los órdenes monomiales, para escribir de manera única los polinomios y definir el término principal. Una vez hecho esto, se obtendrá el algoritmo de la división y se demostrará el Lema de Dickson. En el segundo capítulo, se dará una prueba del Teorema de la Base de Hilbert distinta de la clásica, y se definirán y se caracterizarán las bases de Gröbner. Luego se dará el criterio de Buchberger para detectar bases de Gröbner y se construirá el algoritmo de Buchberger, y se resolverá el problema de pertenecer a un ideal. Por último, se introducirán los conceptos de base de Gröbner minimal y reducida, demostrando la unicidad de la última, y se verá que el algoritmo de Buchberger generaliza los algoritmos de Gauss y Euclides. En el tercer capítulo, se relacionarán las bases de Gröbner directamente con la geometría algebraica, dándose demostraciones del Teorema de Eliminación, del Teorema de Extensión y del Teorema de Clausura, y dando métodos para calcular las ecuaciones implícitas de una variedad a partir de sus ecuaciones paramétricas. En el capítulo 4, se verán aplicaciones directas de las bases de Gröbner a los anillos de polinomios. Se verán algoritmos para operar con ideales de $K[x_1, \ldots, x_n]$, para calcular una K-base de $\dfrac{K[x_1, \ldots, x_n]}{I}$ y para calcular el núcleo y la imagen de homomorfismos de anillos. Por último, en el capítulo 5, se darán aplicaciones más generales de las bases de Gröbner. Se empezará por el cálculo de polinomios mínimos en extensiones de cuerpos, luego se darán métodos de demostraciones automáticas en geometría euclidiana, y por último se tratará el problema de colorear grafos con k colores y se relacionará con la resolución de Sudokus.

Capítulo 1

Monomios y algoritmo de la división

1.1. Órdenes

Siempre que K es un cuerpo, al observar el algoritmo de la división en una variable, o el método de eliminación de Gauss, vemos que es necesario mantener ordenados los términos de los polinomios. Cuando dividimos polinomios en el anillo $K[x]$, el orden que usamos habitualmente es :

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

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

$$x_1 > x_2 > \cdots > x_n.$$

En ambos algoritmos, el éxito se basa en no eliminar términos de manera aleatoria, sino en seguir un orden. Para lograr nuestro primer objetivo, que es conseguir un algoritmo de la división en el caso de varias variables, tenemos que introducir el concepto de orden monomial. Dado un monomio $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, los exponentes $\alpha = (\alpha_1, \ldots, \alpha_n)$ son elementos de $\mathbb{N}^n$, lo que nos permite establecer una correspondencia biunívoca entre el conjunto de monomios y $\mathbb{N}^n$. Entonces, cualquier orden que establezcamos en $\mathbb{N}^n$ nos dará un orden en los monomios, ya que si $\alpha > \beta$, podremos decir que $x^\alpha > x^\beta$.

Definición 1.1. Un orden monomial en $K[x_1, \ldots, x_n]$ es una relación $>$ en $\mathbb{N}^n$, equivalentemente una relación en el conjunto de los monomios, que satisface las siguientes propiedades:

1. $>$ es un orden total.

2. Si $\alpha > \beta$ y $\gamma \in \mathbb{N}^n$, se tiene que $\alpha + \gamma > \beta + \gamma$.

3. $>$ es un buen orden.

La razón de incluir la segunda propiedad, es que si x^α divide a x^β, tendremos que $x^\alpha \leq x^\beta$. Que $>$ sea un buen orden, es equivalente a que $\alpha \geq 0$ para todo $\alpha \in \mathbb{N}^n$. Si tomamos el orden usual en $K[x]$, que también es el orden usual en $\mathbb{N}$, está claro que es un orden monomial, y de hecho, es el único que se puede dar. Ahora veamos ejemplos en $K[x_1, \ldots, x_n]$.

Definición 1.2 (Orden Lexicográfico)**.** Sean $\alpha, \beta \in \mathbb{N}^n$. Decimos que $\alpha >_{lex} \beta$ si la primera componente distinta de cero del vector $\alpha - \beta \in \mathbb{Z}^n$ es positiva.

Definición 1.3 (Orden Graduado Lexicográfico)**.** Sean $\alpha, \beta \in \mathbb{N}^n$. Decimos que $\alpha >_{grlex} \beta$ si

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

Definición 1.4 (Orden Graduado Lexicográfico Inverso)**.** Sean $\alpha, \beta \in \mathbb{N}^n$. Decimos que

$$\alpha >_{grevlex} \beta \Leftrightarrow \begin{cases} |\alpha| > |\beta| \\ |\alpha| = |\beta| \text{ y la primera componente distinta de cero empezando por la} \\ \text{derecha del vector } \alpha - \beta \in \mathbb{Z}^n \text{ es negativa.} \end{cases}$$

Los órdenes definidos anteriormente satisfacen las propiedades de órdenes monomiales, y al estar definidos en $\mathbb{N}^n$, definen órdenes en el conjunto de los monomios.

Una vez escogido un orden, dado un polinomio $f \in K[x_1, \ldots, x_n]$, podemos ordenar los monomios de una manera única. Veamos un ejemplo.

Ejemplo 1.5. Sea $f = 2xyz^2 + 3z^3 + 5x^3 - y^3z$. Si escogemos el orden lexicográfico, escribiremos el polinomio del siguiente modo:

$$f = 5x^3 + 2xyz^2 - y^3z + 3z^3.$$

Por otra parte, si escogemos el orden graduado lexicográfico,

$$f = 2xyz^2 - y^3z + 5x^3 + 3z^3.$$

Y si escogemos el orden graduado lexicográfico inverso,

$$f = -y^3z + 2xyz^2 + 5x^3 + 3z^3.$$

Definición 1.6. Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio distinto de cero en el anillo $K[x_1, \ldots, x_n]$ y sea $>$ un orden monomial. Definimos:

- El multigrado de f:

$$\text{multideg}(f) = \text{máx}\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}.$$

- El coeficiente principal de f:

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

- El monomio principal de f:

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

- El término principal de f:

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

Lema 1.7. *Sean $f, g \in K[x_1, \ldots, x_n]$ polinomios distintos de cero. Entonces:*

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

(i) *Si $f + g \neq 0$,* $\text{multideg}(f + g) \leq \text{máx}\{\text{multideg}(f), \text{multideg}(g)\}$. *Además, se cumple la igualdad si* $\text{multideg}(f) \neq \text{multideg}(g)$.

La demostración de este resultado es inmediata.

1.2. Algoritmo de la división

Nuestro objetivo en esta sección, es conseguir un algoritmo para dividir $f \in K[x_1, \ldots, x_n]$ entre $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$. Esto es, conseguir una expresión de la forma

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

donde los "cocientes" $a_1, \ldots, a_s$ y el resto r pertenecen a $K[x_1, \ldots, x_n]$. La idea básica del algoritmo es cancelar el término principal de f usando el término principal de algún f_i, y repetir este proceso hasta que no se pueda hacer. Veamos un ejemplo.

Ejemplo 1.8. Queremos dividir $f = x^2y + xy^2 + y^2$ entre $f_1 = xy - 1$ y $f_2 = y^2 - 1$. Usaremos el orden lexicográfico con $x > y$. Como $\text{LT}(f)$ es múltiplo de $\text{LT}(f_1)$, primero dividimos entre f_1.

$$\begin{array}{rl|l|l} x^2y + xy^2 + y^2 & & xy - 1 & y^2 - 1 \\ \cline{3-4} xy^2 + x + y^2 & x & & \end{array}$$

Como xy^2 es divisible por $\mathrm{LT}(f_1)$, continuamos dividiendo entre f_1.

$$\begin{array}{rl|l|l} x^2y+xy^2+y^2 & xy-1 & y^2-1 \\ \cline{1-3} xy^2+x+y^2 & x+y & \\ x+y^2+y & & \end{array}$$

Como x no es divisible ni por $\mathrm{LT}(f_1)$, ni por $\mathrm{LT}(f_2)$, lo pasamos al resto. Ahora, y^2 no es divisible por $\mathrm{LT}(f_1)$, pero si lo es por $\mathrm{LT}(f_2)$, entonces

$$\begin{array}{rl|l|l} x^2y+xy^2+y^2 & xy-1 & y^2-1 \\ \cline{1-3} xy^2+x+y^2 & x+y & 1 \\ x+y^2+y & & \\ x+y+1 & & \end{array}$$

Ahora, vemos que ni y, ni 1 son divisibles por $\mathrm{LT}(f_1)$ ni por $\mathrm{LT}(f_2)$, entonces pasan los dos al resto, y terminamos la división.

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

Teorema 1.9 (Algoritmo de la división en $K[x_1,\ldots,x_n]$)**.** *Fijado un orden monomial $>$ en $\mathbb{N}^n$ y sea $F=(f_1,\ldots,f_s)$ una s-tupla ordenada de polinomios de $K[x_1,\ldots,x_n]$. Cada $f\in K[x_1,\ldots,x_n]$ se puede escribir como:*

$$f = a_1f_1+\cdots+a_sf_s+r,$$

con $a_i, r\in K[x_1,\ldots,x_n]$, y o bien $r=0$ o bien r es una combinación lineal de monomios con coeficientes en K, de los cuales ninguno es divisible por ningún LT(f_i). Además, si $a_if_i\neq 0$, tenemos que

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

El algoritmo de la división tiene la siguiente estructura:

$a_1 := 0; \ldots; a_s := 0; r := 0$
$p := f$
while $p \neq 0$ **do**
  $i := 1$
  ocurriodivision := falso

while $i \leq s$ & ocurriodivision = falso **do**
  if $\mathrm{LT}(f_i)$ divide a $\mathrm{LT}(p)$ **then**
    $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
    $p := p - \big(\mathrm{LT}(p)/\mathrm{LT}(f_i)\big) f_i$
    ocurriodivision := verdadero
  else
    $i := i + 1$
  end if
end while
if ocurriodivision = falso **then**
  $r := r + \mathrm{LT}(p)$
  $p := p - \mathrm{LT}(p)$
end if
end while

El algoritmo recorre los polinomios f_i ordenadamente, para ver si algún $\mathrm{LT}(f_i)$ divide a $\mathrm{LT}(f)$. Cuando encuentra un i que cumple la condición, al cociente i-ésimo a_i se le añade $\mathrm{LT}(f)/\mathrm{LT}(f_i)$, y a f, se le resta $\big(\mathrm{LT}(f)/\mathrm{LT}(f_i)\big) f_i$. Si ningún $\mathrm{LT}(f_i)$ divide a $\mathrm{LT}(f)$, entonces $\mathrm{LT}(f)$ se mueve al resto, y se quita de f. Estamos viendo, que en cada iteración, el término $\mathrm{LT}(f)$ se elimina o pasa al resto, y además el nuevo término principal, será menor que el anterior (usando el orden monomial previamente fijado).

Este algoritmo nos da una manera de descomponer un polinomio, pero uno de los mayores problemas de éste, es que si cambiamos el orden en el que los elementos aparecen en la base, nos pueden dar resultados distintos.

Ejemplo 1.10. Sean $f = xy^2 - x$ y $f_1 = xy + 1$, $f_2 = y^2 - 1 \in K[x, y]$ con el orden lexicográfico. Si dividimos f por $F = (f_1, f_2)$

$$\begin{array}{l|l|l} xy^2 - x & xy + 1 & y^2 - 1 \\ \cline{2-3} -x - y & y & \end{array}$$

Como ni $-x$ y $-y$ son múltiplos de $\mathrm{LT}(f_1)$ ni de $\mathrm{LT}(f_2)$, terminamos la división obteniendo $xy^2 - x = (xy + 1)y + (-x - y)$.

Si ahora dividimos f por $F = (f_2, f_1)$

$$\begin{array}{r|c|c} xy^2 - x & xy+1 & y^2-1 \\ \hline 0 & & x \end{array}$$

Con la segunda división vemos que f pertenece al ideal generado por F, ya que $xy^2 - x = (y^2 - 1)x$, pero en la primera división vemos que el resto es distinto de cero. Entonces, la condición que tenemos en el caso de una variable de que f pertenece al ideal si y solo si el resto es cero, no es aplicable al caso de varias variables.

1.3. Ideales monomiales

Definición 1.11. Un ideal $I \subset K[x_1, \ldots, x_n]$ es un ideal monomial si existe un subconjunto $A \subset \mathbb{N}^n$ tal que I está formado por todos los polinomios que son sumas finitas de la forma $\sum_{\alpha \in A} h_\alpha x^\alpha$, donde $h_\alpha \in K[x_1, \ldots, x_n]$.

Lema 1.12. *Sea $I = \langle x^\alpha : \alpha \in A \rangle$ 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. Si x^β es múltiplo de x^α para algún $\alpha \in A$, entonces $x^\beta \in I$ por la definición de ideal. Por otra parte, si $x^\beta \in I$, tenemos que $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, donde $h_i \in K[x_1, \ldots, x_n]$ y $\alpha(i) \in A$. Si expandimos cada h_i como una combinación lineal de monomios, vemos que todo término del lado derecho de la ecuación es divisible por algún $x^{\alpha(i)}$, entonces el lado izquierdo de la ecuación, x^β, tiene que tener la misma propiedad. □

Lema 1.13. *Sea I un ideal monomial y $f \in K[x_1, \ldots, x_n]$. Son equivalentes:*

(i) *$f \in I$.*

(ii) *Todo término de f pertenece I.*

(iii) *f es una combinación K-lineal de monomios en I.*

Demostración. Las implicaciones (iii) $\implies$ (ii) $\implies$ (i) son triviales. La implicación (i) $\implies$ (iii) es igual a la demostración del Lema 1.12. □

Teorema 1.14 (Lema de Dickson)**.** *Un ideal monomial $I = \langle x^\alpha : \alpha \in A \rangle \subset K[x_1, \ldots, x_n]$ se puede escribir de la forma $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, donde los enteros $\alpha(1), \ldots, \alpha(s) \in A$. En particular, I tiene una base finita.*

Demostración. La prueba la haremos por inducción en n, el número de variables.

Si $n = 1$, I está generado por los monomios x_1^α, con $\alpha \in A \subset \mathbb{N}$. Sea β el menor elemento de $A \subset \mathbb{N}$. Como $\beta \leq \alpha$ para todo $\alpha \in A$, tenemos que x_1^β divide a todos los generadores x_1^α. Por lo tanto, $I = \langle x_1^\beta \rangle$.

Supongamos ahora que $n > 1$ y es cierto para $n - 1$. Escribiremos las variables como $x_1, \ldots, x_{n-1}, y$, y los monomios de $K[x_1, \ldots, x_{n-1}, y]$ se pueden escribir como $x^\alpha y^m$, donde $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}^{n-1}$ y $m \in \mathbb{N}$.

Sea $I \subset K[x_1, \ldots, x_{n-1}, y]$ un ideal monomial. Para encontrar generadores de I, tomamos el ideal $J \subset K[x_1, \ldots, x_{n-1}]$ generado por los monomios x^α para los que existe $m \geq 0$, tal que $x^\alpha y^m \in I$. Por la hipótesis de inducción, J está generado por un número finito de elementos, $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Para cada i entre 1 y s, por definición, existe un $m_i \geq 0$ tal que $x^{\alpha(i)} y^{m_i} \in I$. Sea m el máximo de los m_i. Para cada k entre 0 y $m-1$, consideramos el ideal $J_k \subset K[x_1, \ldots, x_{n-1}]$ generado por los monomios x^β tales que $x^\beta y^k \in I$. Usando la hipótesis de inducción, J_k está generado por un número finito de elementos, $J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s)} \rangle$.

Veamos que I está generado por los siguientes monomios:

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

Primero veamos que todo monomio de I es divisible por alguno de los anteriores. Sea $x^\alpha y^p \in I$. Si $p \geq m$, entonces $x^\alpha y^p$ es divisible por algún $x^{\alpha(i)} y^m$ por construcción de J. Si $p \leq m - 1$, entonces $x^\alpha y^p$ es divisible por algún $x^{\alpha_p(j)} y^p$ por construcción de J_p. Por el Lema 1.12, los monomios anteriores, generan un ideal que tiene los mismos monomios que I, así que tienen que ser iguales.

Para terminar la demostración, tenemos que demostrar que el conjunto finito de generadores, se puede escoger de entre un conjunto de generadores dados del ideal. Si volvemos a escribir las variables como $x_1, \ldots, x_n$, nuestro ideal monomial es $I = \langle x^\alpha : \alpha \in A \rangle \subset K[x_1, \ldots, x_n]$. Como $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$, para ciertos monomios $x^{\beta(i)} \in I$, por el Lema 1.12, cada $x^{\beta(i)}$ es divisible por $x^{\alpha(i)}$ para algún $\alpha(i) \in A$. De este modo, $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. □

Capítulo 2

Bases de Gröbner

2.1. Definición y Propiedades

Definición 2.1. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal distinto del $\{0\}$. Definimos $\mathrm{LT}(I)$ como:

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

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

Si I es el ideal generado por $\{f_1, \ldots f_s\}$ está claro que $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ está contenido en $\langle \mathrm{LT}(I) \rangle$, pero pueden ser distintos, como veremos en el siguiente ejemplo:

Ejemplo 2.2. Sea I el ideal generado por $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$. Si tomamos el orden graduado lexicográfico, el polinomio x^2 pertenece a I, ya que $x^2 = yf_1 - xf_2$. entonces $x^2 \in \mathrm{LT}(I)$, pero $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$. De este modo, vemos que $\mathrm{LT}(I) \neq \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$.

Proposición 2.3. *Sea $I \subset K[x_1, \ldots, x_n]$ un ideal*

(i) $\langle \mathrm{LT}(I) \rangle$ *es un ideal monomial.*

(ii) *Existen $g_1, \ldots, g_s \in I$ tales que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$.*

Demostración. Es consecuencia del Lema de Dickson y de que $\mathrm{LM}(g)$ y $\mathrm{LT}(g)$ difieren solamente en una constante. □

Ahora estamos en condiciones de enunciar el teorema de la base de Hilbert.

Teorema 2.4 (Teorema de la Base de Hilbert)**.** *Todo ideal $I \subset K[x_1, \ldots, x_n]$ tiene un conjunto finito de generadores.*

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

Por una parte está claro que $\langle g_1, \ldots, g_s \rangle \subset I$. Para ver la otra inclusión, tomemos un polinomio cualquiera $f \in I$. Aplicando el algoritmo de la división para dividir f entre $\langle g_1, \ldots, g_s \rangle$, obtenemos una expresión de la forma

$$f = a_1 g_1 + \cdots + a_s g_s + r,$$

donde ningún término de r es divisible por ningún $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. Por otra parte,

$$r = f - a_1 g_1 - \cdots - a_s g_s \in I.$$

ya que tanto f como $g_1, \ldots, g_s$ pertenecen a I. Entonces, $\mathrm{LT}(r) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Así que no queda más remedio que $r = 0$. De este modo,

$$f = a_1 g_1 + \cdots + a_s g_s + 0 \in \langle g_1, \ldots, g_s \rangle$$

por lo que $I \subset \langle g_1, \ldots, g_s \rangle$. □

Con este resultado, no solo tenemos que todo ideal tiene una base finita, sino que la base usada en la prueba, cumple una propiedad muy especial, que es que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Esto nos motiva a dar la siguiente definición.

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

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

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

En el Ejemplo 2.2, la base $\{f_1, f_2\}$ no es una base de Gröbner ya que $x^2 \in \langle \mathrm{LT}(I) \rangle$, pero $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$. Más adelante, veremos que estas bases cumplen unas propiedades "buenas", y daremos algoritmos para computarlas. Antes de eso, necesitaremos probar el siguiente teorema.

Teorema 2.7 (Condición de Cadena Ascendente)**.** *Sea*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

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

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

Demostración. Consideremos $I = \cup_{i=1}^{\infty} I_i$. Veamos que I es un ideal.

- $0 \in I$ ya que $0 \in I_i$ para todo i.
- Sean $f, g \in I$. Por definición, $f \in I_i$ y $g \in I_j$ para algunos i, j. Supongamos $j \geq i$. Como los ideales forman una cadena ascendente, $I_i \subset I_j$, así que $f \in I_j$, por lo tanto $f + g \in I_j$.
- Sean $f \in I$ y $r \in K[x_1, \ldots, x_n]$, $f \in I_i$ para algún i, y como I_i, $rf \in I_i$, por lo tanto $rf \in I$.

Una vez tenemos que I es un ideal, por el Teorema de la Base de Hilbert, el ideal I tiene un conjunto finito de generadores $I = \langle f_1, \ldots, f_s \rangle$. Cada uno de estos generadores, pertenece a un I_j, es decir $f_k \in I_{j_k}$. Tomamos como N el máximo de los j_k. Entonces

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

□

Veamos ahora algunas propiedades básicas de las bases de Gröbner.

Proposición 2.8. *Sea $G = \{g_1, \ldots, g_s\}$ una base de Gröbner de un ideal $I \subset K[x_1, \ldots, x_n]$ y sea $f \in K[x_1, \ldots, x_n]$. Existe un único $r \in K[x_1, \ldots, x_n]$ que cumple las siguientes condiciones:*

(i) *Ningún término de r es divisible por ningún* $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$.

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

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

Demostración. La existencia nos la da el algoritmo de la división. Para probar la unicidad, supongamos que $f = g_1 + r_1 = g_2 + r_2$, satisfaciendo las propiedades (i) y (ii). Entonces $r_2 - r_1 = g_1 - g_2 \in I$, así que si $r_2 \neq r_1$, tenemos que $\mathrm{LT}(r_2 - r_1) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Pero por el Lema 1.12 se sigue que $\mathrm{LT}(r_2 - r_1)$ es divisible por algún $\mathrm{LT}(g_i)$. Pero esto es imposible ya que ningún término de r_1 ni de r_2 es divisible por ningún $\mathrm{LT}(g_j)$, así que $r_2 - r_1$ tiene que ser 0, probando así la unicidad. □

A pesar de que el resto siempre es igual, los "cocientes" pueden variar si ordenamos los elementos de la base de maneras distintas.

Ejemplo 2.9. Sea $G = \{x + z, y - z\}$ una base de Gröbner con el orden lexicográfico. Si dividimos el polinomio xy entre $\{x+z, y-z\}$, obtenemos que $xy = y(x+z)-z(y-z)-z^2$, y si dividimos el mismo polinomio entre $\{y-z, x+z\}$, resulta que $xy = x(y-z)+z(x+z)-z^2$. Es decir, el resto permanece igual, ya que G es una base de Gröbner, pero los "cocientes" varían.

Corolario 2.10. *Sea $G = \{g_1, \ldots, g_s\}$ una base de Gröbner para un ideal $I \subset K[x_1, \ldots, x_n]$ y sea $f \in K[x_1, \ldots, x_n]$, $f \in I$ si y solo si el resto de dividir f entre G es* 0.

Este corolario, nos da una solución al problema de pertenecer a un ideal, siempre que tengamos una base de Gröbner de dicho ideal. Para resolver el problema completamente, tendremos que dar un algoritmo para encontrar bases de Gröbner.

Una propiedad a tener en cuenta, es que dada una base de Gröbner, si cambiamos el orden del anillo de polinomios, puede dejar de ser base de Gröbner. Usaremos `Singular` para ver esta propiedad en el siguiente ejemplo.

Ejemplo 2.11. Sea $I = \langle x^3 - 2xy, x^2y + x - 2y^2 \rangle$ el ideal descrito en el Ejemplo 2.2, pero tomando ahora el orden lexicográfico. Con el siguiente código de `Singular`, obtenemos una base de Gröbner para este ideal

```
> ring R = 0,(x,y),lp;      //definimos cuerpo, variables y orden
> poly f1 = x^3 - 2xy;      //definimos polinomios generadores
> poly f2 = x^2*y - 2*y^2 + x;
> ideal I = f1, f2;         //definimos ideal
> std(I);                   //hallamos base de Gröbner
_[1]=y3
_[2]=x-2y2
```

Vemos que la base de Gröbner es $G = \{y^3, x - 2y^2\}$. Si ahora cambiamos al orden graduado lexicográfico, vemos que G no es base de Gröbner. Si lo fuese, el resto de dividir x^2 entre G tendría que ser cero por el Corolario 2.10, ya que $x^2 \in I$ (por del Ejemplo 2.2).

```
> ring R = 0,(x,y),Dp;
> poly f1 = y^3;
> poly f2 = -2*y^2 + x;
> ideal I = f1,f2;
> reduce(x^2,I);                  //resto de la división entre I
// ** I is no standard basis
x2
```

Nos da como resultado que el resto es distinto de cero, por lo que G no es base de Gröbner. Además, el programa ya nos avisa de que el ideal que generamos no es base de Gröbner.

Definición 2.12. Dado $f \in K[x_1, \ldots, x_n]$, denotamos por $\overline{f}^F$ al resto de la división de f por la s-tupla ordenada $F = (f_1, \ldots, f_s)$. Si F es una base de Gröbner, podemos ver F como un conjunto (sin ningún orden en particular), por la Proposición 2.8.

Definición 2.13. Sean $f, g \in K[x_1, \ldots, x_n]$ polinomios distintos de cero.

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

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

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

Ejemplo 2.14. Sean $f = x^3y^2 - x^2y^3 + x$ y $g = 3x^4 + y^2$ en $\mathbb{R}[x, y]$ con el orden graduado lexicográfico. El S-polinomio de f y g será:

$$\text{S}(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = x \cdot f - \frac{1}{3} \cdot y \cdot g = -x^3 + x^2 - \frac{1}{3}y^3$$

Cabe mencionar, que la "S" del nombre de S-polinomio, viene de la palabra Sizigia que en astronomía denota el momento en el que un astro está alineado con la Tierra y el Sol. Estos polinomios están "diseñados" para producir cancelación de los coeficientes principales, y con ellos seremos capaces de caracterizar mejor las bases de Gröbner. Para este resultado, necesitamos un lema preliminar.

Lema 2.15. *Supongamos que tenemos una suma* $\sum_{i=1}^s c_i f_i$*, donde* $c_i \in K$ *y* multideg$(f_i) = \delta \in \mathbb{N}^n$ *para todo* i*. Si* multideg$(\sum_{i=1}^s c_i f_i) < \delta$*, entonces* $\sum_{i=1}^s c_i f_i$ *es una combinación lineal con coeficientes en* K*, de los S-polinomios* $\text{S}(f_j, f_k)$ *para* $1 \leq j, k \leq s$*. Además, cada* $\text{S}(f_i, f_k)$ *tiene multigrado menor que* δ*.*

Demostración. Escribimos $f_i = a_i x^\delta +$términos menores, $a_i \in K$. Por hipótesis, $\sum_{i=1}^s c_i a_i = 0$. Por definición, $\text{S}(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j$. Entonces,

$$
\begin{aligned}
f &= c_1 f_1 + \cdots + c_s f_s \\
&= c_1 a_1 (\frac{1}{a_1} f_1) + \cdots + c_s a_s (\frac{1}{a_s} f_s) \\
&= c_1 a_1 (\frac{1}{a_1} f_1 - \frac{1}{a_2} f_2) + (c_1 a_1 + c_2 a_2)(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3) + \cdots \\
&\quad + (c_1 a_1 + \cdots + c_{s-1} a_{s-1})(\frac{1}{a_{s-1}} f_{s-1} + \frac{1}{a_s} f_{s-1}) + (c_1 a_1 + \cdots + c_s a_s) \frac{1}{a_s} f_s \\
&= c_1 a_1 \mathrm{S}(f_1, f_2) + (c_1 a_1 + c_2 a_2) \mathrm{S}(f_2, f_3) + \cdots \\
&\quad + (c_1 a_1 + \cdots + c_{s-1} a_{s-1}) \mathrm{S}(f_{s-1}, f_s).
\end{aligned}
$$

□

Ahora estamos en condiciones de probar el criterio de Buchberger para saber si una base de un ideal es o no una base de Gröbner.

Teorema 2.16 (Criterio de Buchberger)**.** *Sea I un ideal de $K[x_1, \ldots, x_n]$. Una base $G = \{g_1, \ldots, g_s\}$ de I es una base de Gröbner de I si y solo si para todos los pares $i \neq j$, el resto de dividir $\mathrm{S}(g_i, g_j)$ por G (listados en cualquier orden) es cero.*

Demostración. Como G es base de Gröbner y $S(g_i, g_j) \in I$, el resto es cero por el Corolario 2.10.

Recíprocamente, sea $f \in I$ un polinomio distinto de cero. Tenemos que demostrar que si los restos de dividir los S-polinomios entre G son cero, $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Sea f de la forma

$$f = \sum_{i=1}^{t} h_i g_i. \tag{2.1}$$

con $h_i \in K[x_1, \ldots, x_n]$.

Sea $m(i) = \mathrm{multideg}(h_i g_i)$, definimos $\delta = \mathrm{máx}\{m(1), \ldots, m(t)\}$. Por el Lema 1.7 tenemos que

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

Consideremos ahora todos los posibles modos en los que f puede ser escrito de la forma (2.1). Para cada expresión, es posible que obtengamos un δ distinto. Como un orden monomial es un buen orden, podemos escoger una expresión del tipo (2.1) tal que δ sea minimal.

Veamos por contradicción que $\mathrm{multideg}(f) = \delta$, así que supongamos que $\mathrm{multideg}(f) < \delta$. Escribiremos f de la siguiente forma, para aislar los términos de grado δ.

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

Los monomios de la segunda y tercera suma, tienen multideg $< \delta$. Como supusimos que multideg$(f) < \delta$, los de la primera suma, también tienen multideg $<\delta$.

Sea $\mathrm{LT}(h_i) = c_i x^{\alpha(i)}$. El sumando $\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ tiene la forma descrita en el Lema 2.15 con $f_i = x^{\alpha(i)} g_i$. Entonces, por el Lema 2.15, esta suma es una combinación lineal de los S-polinomios $\mathrm{S}(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)$. Además, los S-polinomios tienen la forma

$$\begin{aligned}\mathrm{S}(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k) &= \frac{x^\delta}{x^{\alpha(j)}\mathrm{LT}(g_j)} x^{\alpha(j)g_j} - \frac{x^\delta}{x^{\alpha(k)}\mathrm{LT}(g_k)} x^{\alpha(k)g_k} \\ &= x^{\delta-\gamma_{jk}}\mathrm{S}(g_j, g_k),\end{aligned}$$

donde $x^{\gamma_{jk}} = \mathrm{LCM}(\mathrm{LM}\big(g_j\big), \mathrm{LM}(g_k)\big)$. Entonces, existen constantes $c_{jk} \in K$ tal que

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} \mathrm{S}(g_j, g_k). \tag{2.2}$$

Por hipótesis, el resto de dividir $\mathrm{S}(g_j, g_k)$ entre G es cero, entonces podemos escribir

$$\mathrm{S}(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{2.3}$$

donde $a_{ijk} \in K[x_1, \ldots, x_n]$. Además, el algoritmo de la división nos dice que

$$\mathrm{multideg}(a_{ijk}g_i) \leq \mathrm{multideg}\big(\mathrm{S}(g_j, g_k)\big),$$

para todo i, j, k.

Si multiplicamos la expresión (2.3) por $x^{\delta-\gamma_{jk}}$, obtenemos

$$x^{\delta-\gamma_{jk}}\mathrm{S}(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i,$$

donde $b_{ijk} = x^{\delta-\gamma_{jk}} a_{ijk}$. De este modo, por el Lema 2.15,

$$\mathrm{multideg}(b_{ijk}g_i) \leq \mathrm{multideg}\big(x^{\delta-\gamma_{jk}}\mathrm{S}(g_j, g_k)\big) < \delta. \tag{2.4}$$

Si sustituimos la expresión anterior en (2.2), tenemos la siguiente ecuación

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} \mathrm{S}(g_j, g_k) = \sum_{j,k} c_{jk} \left(\sum_i b_{ijk} g_i \right) = \sum_i \tilde{h}_i g_i,$$

que por (2.4) tiene la propiedad de que para todo i,

$$\mathrm{multideg}(\tilde{h}_i g_i) < \delta.$$

De este modo, si sustituimos $\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i = \sum_i \tilde{h}_i g_i$ en la primera ecuación, tenemos una expresión de f como combinación de los polinomios de la base en los que todos los términos tienen multideg $< \delta$, lo que contradice la minimalidad de δ.

Una vez obtenemos que multideg(f) = multideg$(h_i g_i)$ para algún i, tenemos que LT(f) es divisible por algún LT(g_i), así que LT$(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, demostrando así que G es una base de Gröbner. □

Este es un resultado muy importante, ya que nos permite conocer cuando un conjunto de generadores es una base de Gröbner, y además nos lleva de manera natural a un algoritmo para construirlas, el algoritmo de Buchberger.

Ejemplo 2.17. Sea el anillo $K[x, y, z]$ con el orden lexicográfico con $y > z > x$ y sea $I = \langle y - x^2, z - x^3 \rangle$. Veamos si $G = \{y - x^2, z - x^3\}$ es una base de Gröbner. Para ello, consideramos el S-polinomio

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

Usando el algoritmo de la división, obtenemos

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

De este modo, por el Criterio de Buchberger, como el resto de dividir S(f_1, f_2) por G es cero, G es base de Gröbner.

2.2. Algoritmo de Buchberger

Por el Corolario 2.6 sabemos que todo ideal en $K[x_1, \ldots, x_n]$ tiene una base de Gröbner, aunque la prueba no es constructiva. Para obtener una base de Gröbner, dado cualquier ideal $I \subset K[x_1, \ldots, x_n]$, describiremos el algoritmo de Buchberger, pero antes de dar la definición, veamos un ejemplo.

Ejemplo 2.18. Sea el anillo $K[x, y]$ con el orden graduado lexicográfico, y sea $I = \langle f_1, f_2 \rangle$, siendo $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$. El conjunto $\{f_1, f_2\}$ no es base de Gröbner, ya que $\text{S}(f_1, f_2) = -x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$. Para intentar construir una a partir de f_1 y f_2, deberíamos añadir más generadores a la base. La idea natural, es añadir $f_3 = -x^2$, el resto de dividir S(f_1, f_2) entre (f_1, f_2). Sea $F = (f_1, f_2, f_3)$, comprobamos los S-polinomios de nuestra nueva base de I.

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

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

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

Por lo tanto, tendremos que añadir $f_5 = -2y^2 + x$ al conjunto generador. Estableciendo $F = (f_1, f_2, f_3, f_4, f_5)$, si computamos para todo $1 \leq i \leq j \leq 5$ obtenemos que

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

Entonces, por el Teorema 2.16, $\{f_1, f_2, f_3, f_4, f_5\}$ es una base de Gröbner para I con el orden graduado lexicográfico.

Este ejemplo nos sugiere una idea para obtener una base de Gröbner a partir de un conjunto de generadores, añadiendo los restos distintos de cero de los S-polinomios. Esto es lo que hace el algoritmo de Buchberger.

Teorema 2.19. *Sea $I = \langle f_1, \ldots, f_s\rangle \neq \{0\}$ un ideal de $K[x_1, \ldots, x_n]$. Entonces, el siguiente algoritmo nos construye una base de Gröbner tras un número finito de pasos.*

$a_1 := 0; \ldots; a_s := 0; r := 0$
repeat
  $G' := G$
  for *cada par* $\{p, q\}$, $p \neq q$ *en* G' ***do***
    $S := \overline{\mathrm{S}(p, q)}^{G'}$
    if $S \neq 0$ ***then***
      $G := G \cup \{S\}$.
    end if
  end for
until $G = G'$

Demostración. Veamos primero que $G \subset I$ en todos los momentos del algoritmo. Inicialmente es cierto, y lo único que hacemos es añadir el $S = \overline{\mathrm{S}(p, q)}^{G'}$ para $p, q \in G$, y como dividimos entre $G' \subset I$, $G \cup \{S\} \subset I$. Además, notemos que como G contiene a la base dada inicialmente, G es una base de I.

El algoritmo termina cuando $G = G'$, lo que quiere decir que $S = \overline{\mathrm{S}(p, q)}^{G'} = 0$ para todo $p, q \in G$. Es decir, por el Teorema 2.16 el algoritmo termina cuando G es una base de Gröbner.

Falta probar que el algoritmo termina en tras un número finito de pasos. Para ver esto, tenemos que considerar que pasa después de cada iteración. El conjunto G está formado por G' (el antiguo G) y los restos distintos de cero de los S-polinomios de los elementos de G'. Entonces

$$\langle \mathrm{LT}(G') \rangle \subset \langle \mathrm{LT}(G) \rangle \tag{2.5}$$

ya que $G' \subset G$. Si $G' \neq G$, podemos afirmar que $\langle \mathrm{LT}(G') \rangle \subsetneq \langle \mathrm{LT}(G) \rangle$. Para ver esto, suponemos un resto distinto de cero r de un S-polinomio que fue adjuntado a G. Como r es resto de la división entre G', $\mathrm{LT}(r)$ no es divisible por los LT de los elementos de G', así que $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$, pero $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$.

De este modo, por (2.5), los ideales $\langle \mathrm{LT}(G') \rangle$ de las sucesivas iteraciones, forman una cadena ascendente de ideales en $K[x_1, \ldots, x_n]$, y por la Condición de Cadena Ascendente (Teorema 2.7) la cadena se estabilizará, por lo tanto $G' = G$ para algún N, así que el algoritmo termina después de un número finito de pasos. □

Lema 2.20. *Sea G una base de Gröbner para un ideal de polinomios I. Sea $p \in G$ un polinomio tal que $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$. Entonces $G - \{p\}$ también es una base de Gröbner de I.*

Demostración. Como $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$, tenemos que $\langle \mathrm{LT}(G - \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$, así que por definición, $G - \{p\}$ es una base de Gröbner. □

Usando el algoritmo de Buchberger, es posible que obtengamos polinomios cuyos términos principales no aportan nada al ideal generado por los LT, así que por el lema anterior, podemos suprimirlos y seguir teniendo aún una base de Gröbner pero con menos elementos. Esto motiva la siguiente definición.

Definición 2.21. Una base de Gröbner minimal para un ideal $I \subset K[x_1, \ldots, x_n]$ es una base de Gröbner G de I tal que

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

(ii) Para todo $p \in G$, $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\}) \rangle$

Podemos construir bases de Gröbner minimales para un ideal distinto de cero a partir de un conjunto finito de generadores, aplicando el Teorema 2.19 y después usando el Lema 2.20 para eliminar generadores innecesarios.

Ejemplo 2.22. Sea I el ideal estudiado en el Ejemplo 2.18 con el orden graduado lexicográfico. Encontramos la base de Gröbner $F = \{f_1, f_2, f_3, f_4, f_5\}$, siendo

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

Para construir una base minimal a partir de F, el primer paso es que tengan todos los polinomios 1 como coeficiente principal.

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

Después, vemos que $\mathrm{LT}(\tilde{f}_1) = x^3 = x \cdot \mathrm{LT}(\tilde{f}_3)$ y $\mathrm{LT}(\tilde{f}_2) = x^2y = x \cdot \mathrm{LT}(\tilde{f}_4)$. De este modo, por el Lema 2.20, $\{\tilde{f}_3, \tilde{f}_4, \tilde{f}_5\}$ es una base de Gröbner. Además, como no hay más casos en los que un término principal divide a otro distinto, $\{\tilde{f}_3, \tilde{f}_4, \tilde{f}_5\}$ es una base de Gröbner minimal.

Si observamos la base minimal que construimos en este ejemplo, podemos ver que dado cualquier $a \in K$, el conjunto

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

es una base de Gröbner minimal. Suponiendo que el cuerpo es infinito, tenemos infinitas bases de Gröbner minimales para el mismo ideal, así que escogeremos una entre todas ellas, que consideramos según la siguiente definición.

Definición 2.23. Una base de Gröbner reducida para un ideal $I \subset K[x_1, \ldots, x_n]$ es una base de Gröbner G de I tal que

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

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

Proposición 2.24. *Sea $I \neq \{0\}$ un ideal del anillo de polinomios. Dado un orden monomial, I tiene una única base de Gröbner reducida.*

Demostración. Sea G una base de Gröbner minimal de I. Decimos que $g \in G$ es reducido para G si ningún monomio de g está en $\langle \mathrm{LT}(G - \{g\})\rangle$. Si g es reducido para G, lo es para cualquier otra base de Gröbner minimal de I que contiene a g y tiene los mismos términos principales. Esto es así porque la definición de reducida, solo involucra a los términos principales.

Dado $g \in G$, sea $g' = \overline{g}^{G-\{g\}}$ y sea $G' = (G - \{g\}) \cup \{g'\}$. Sabemos que $\mathrm{LT}(g') = \mathrm{LT}(g)$, ya que G es minimal, entonces $\langle \mathrm{LT}(G')\rangle = \langle \mathrm{LT}(G)\rangle$, por lo que es inmediato ver que G' es minimal, y que g' es reducido para G' por construcción.

Tomamos ahora los elementos de G y aplicamos el proceso definido en el párrafo anterior hasta que todos sean reducidos. La base de Gröbner puede cambiar cada vez que realizamos el proceso, pero por nuestra observación previa, cuando un elemento es reducido, siempre es reducido ya que no cambiamos los términos principales. De este modo, nuestra base final es reducida.

Para probar la unicidad, supongamos que G y $\tilde{G}$ son bases de Gröbner reducidas de I. Como son minimales, $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$. Como consecuencia, dado $g \in G$ existe $\tilde{g} \in \tilde{G}$ tal que $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. El elemento $g - \tilde{g}$ pertenece a I y como G es base de Gröbner, $\overline{g - \tilde{g}}^{G} = 0$. Como $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$, los términos principales se cancelan en $g - \tilde{g}$ y ninguno de los términos que queda son divisibles por ningún $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$ ya que G y $\tilde{G}$ son reducidas. De este modo, $\overline{g - \tilde{g}}^{G} = g - \tilde{g} = 0$, demostrando así que $g = \tilde{g}$. □

Ejemplo 2.25. Sea el ideal $I = \langle 22x+77y+z-3, x+y+z-77, x-y-z+11\rangle \subset K[x_1, \ldots, x_n]$. Usando `Singular`, podemos calcular una base de Gröbner y una base de Gröbner reducida.

```
> ring r = 0, (x,y,z), lp;
> poly f=22x+77y+z-3;
> poly g=x+y+z-77;
> poly h=x-y-z+11;
> ideal I=f,g,h;
> std(I);
_[1]=76z-4111
_[2]=y+z-44
_[3]=x-y-z+11
> option(redSB);           //opción para calcular bases reducidas
> std(I);
_[1]=76z-4111
```

```
_[2]=76y+767
_[3]=x-33
```

Vemos que la salida de `Singular` nos da una base de Gröbner reducida, salvo los coeficientes.

Una consecuencia inmediata de la Proposición 2.24 es el algoritmo de igualdad de ideales. Si queremos ver si dos ideales son iguales, basta con hallar la base de Gröbner reducida de cada uno. Si coinciden las bases, los ideales serán iguales, y si son distintas, los ideales serán distintos.

Observación 2.26. El algoritmo de eliminación Gaussiana, no es más que un caso particular del algoritmo de Buchberger. Cuando hallamos la matriz escalonada, estamos hallando una base de Gröbner minimal, respecto al orden lexicográfico. Además, cuando hallamos la matriz escalonada reducida, estamos calculando la única base de Gröbner reducida. En el Ejemplo 2.25 vemos esta propiedad. En el capítulo 3, veremos que la propiedad de eliminar variables, se puede extender al caso no lineal.

Observación 2.27. El algoritmo de Euclides para el cálculo del máximo común divisor de dos polinomios en una variable, también es un caso particular del algoritmo de Buchberger. El polinomio que obtenemos al final, no es más que la base de Gröbner reducida del ideal generado por los dos polinomios iniciales.

Capítulo 3

Teoría de la eliminación

3.1. Teoremas de eliminación y extensión

Para ver como funciona la teoría de la eliminación, comenzaremos con un ejemplo.

Ejemplo 3.1. Nuestro objetivo es resolver el sistema de ecuaciones

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

Sea $I \subset K[x, y, z]$ el ideal

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

Los polinomios

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^4 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2. \end{aligned}$$

nos dan una base de Gröbner de I respecto al orden lexicográfico. Además, las soluciones del sistema de ecuaciones son las mismas que los ceros de los polinomios de la base de Gröbner formada por $\{g_1, g_2, g_3, g_4\}$. Si nos fijamos, vemos que g_4 solo involucra a la variable z, así que los posibles valores de z son $0, 1$ y $-1 \pm \sqrt{2}$. Si sustituimos en g_2 y g_3, determinamos los posibles valores de y, y por último, sustituyendo en g_1, los de x. De este modo, encontramos

las siguientes cinco soluciones:

$$(1,0,0),(0,1,0),(0,0,1),$$
$$(-1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2}),$$
$$(-1-\sqrt{2},-1-\sqrt{2},-1-\sqrt{2}).$$

Para encontrar estas soluciones, hemos seguido dos pasos. El primero es el paso de eliminación, en el cual eliminamos las variables x e y del sistema de ecuaciones. El segundo, es el paso de extensión, en el cual una vez determinados los valores de z, los extendimos a las soluciones de las ecuaciones originales.

Definición 3.2. Sean $\mathbf{x} = \{x_1, \ldots, x_l\}$, $\mathbf{y} = \{x_{l+1}, \ldots, x_n\}$. Un orden monomial $>$ en $K[\mathbf{x}, \mathbf{y}]$ se dice que elimina a $\mathbf{x}$ si para todo $\mathbf{y}^\gamma, \mathbf{y}^\delta$

$$\mathbf{x}^\alpha > \mathbf{x}^\beta \implies \mathbf{x}^\alpha \mathbf{y}^\gamma > \mathbf{x}^\beta \mathbf{y}^\delta.$$

El orden lexicográfico con $x_1 > \cdots > x_n$, elimina las variables $\{x_1, \ldots, x_s\}$ para todo s.

Definición 3.3. Dado $I = \langle f_1, \ldots, f_s \rangle \subset K[x_1, \ldots, x_n]$, el l-ésimo ideal de eliminación I_l es el ideal de $K[x_{l+1}, \ldots, x_n]$ definido por

$$I_l = I \cap K[x_{l+1}, \ldots, x_n]$$

Teorema 3.4 (Teorema de Eliminación)**.** *Sea $I \subset K[x_1, \ldots, x_n]$ un ideal y sea G una base de Gröbner de I respecto un orden que elimina a $\{x_1, \ldots, x_l\}$. Entonces para cada $0 \leq l \leq n$, el conjunto*

$$G_l = G \cap K[x_{l+1}, \ldots, x_n]$$

es una base de Gröbner del l-ésimo ideal de eliminación I_l.

Demostración. Sea l entre 0 y n. Por construcción, $G_l \subset I_l$, entonces, tenemos que ver que

$$\langle \mathrm{LT}(I_l) \rangle = \langle \mathrm{LT}(G_l) \rangle.$$

Una inclusión es trivial, así que llega con probar que $\langle \mathrm{LT}(I_l) \rangle \subset \langle \mathrm{LT}(G_l) \rangle$. Sea $f \in I_l$, tenemos que ver que $\mathrm{LT}(f)$ es divisible por $\mathrm{LT}(g)$ para algún $g \in G_l$. $\mathrm{LT}(f)$ es divisible por $\mathrm{LT}(g)$ para algún $g \in G$, ya que G es base de Gröbner. Además, como $f \in I_l$, f solo involucra a las variables $\{x_{l+1}, \ldots, x_l\}$. Pero como el orden que estamos usando, elimina $\{x_1, \ldots, x_l\}$, cualquier monomio que tenga algún elemento de $\{x_1, \ldots, x_l\}$ es mayor que todos los monomios de $K[x_{l+1}, \ldots, x_n]$, entonces $\mathrm{LT}(g) \in K[x_{l+1}, \ldots, x_n]$ implica que $g \in K[x_{l+1}, \ldots, x_n]$. De esta forma, $g \in G_l$, y queda probado el teorema.

□

Teorema 3.5 (Teorema de Extensión)**.** *Sea $I \subset K[x_1, \ldots, x_n]$ un ideal con K algebraicamente cerrado y sea I_1 el primer ideal de eliminación de I. Supongamos que tenemos una solución parcial $b = (a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. Si el ideal I contiene a un polinomio f tal que*

$$f = c(x_2, \ldots, x_n)x_1^N + \text{ términos de grado } < N \text{ en } x_1$$

con $c(b) \neq 0$, entonces existe un $a \in K$ tal que $(a, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Para ver la demostración de este teorema, necesitamos información auxiliar.

Definición 3.6. Definimos

$$\mathrm{LC}_{x_1}(f) = c(x_2, \ldots, x_n)$$

$$\deg_{x_1}(f) = N$$

siendo $c(x_2, \ldots, x_n)$ el polinomio y el N el entero que resultan al escribir f de la forma

$$f = c(x_2, \ldots, x_n)x_1^N + \text{ términos de grado } < N \text{ en } x_1.$$

Definición 3.7. Sea $f \in K[x_1, \ldots, x_n]$ y sea $b = (a_2, \ldots, a_n)$, definimos

$$\overline{f} = f(x, b) \in K[x_1].$$

Lema 3.8. *Dadas las condiciones del Teorema de Extensión y sea G una base de Gröbner de I con respecto a un orden que elimina a x_1. Entonces, existe $g \in G$ tal que $\overline{LC_{x_1}(g)} \neq 0$.*

Demostración. Sea $f \in I$ tal que $\overline{LC_{x_1}(f)} \neq 0$. Tomamos $f = \sum_{g \in G} h_g g$. Entonces,

$$\mathrm{LT}(f) = \text{máx}\{\mathrm{LC}(h_g g) : h_g \neq 0\}.$$

Como $>$ elimina x_1, tenemos que

$$\deg_{x_1}(f) = \text{máx}\{\deg_{x_1}(h_g g) : h_g \neq 0\}$$

y entonces,

$$\mathrm{LC}_{x_1}(f) = \sum_{\deg_{x_1}(h_g g) = \deg_{x_1}(f)} \mathrm{LC}_{x_1}(h_g)\mathrm{LC}_{x_1}(g).$$

Quedando probado el lema. □

Estamos ahora en condiciones de demostrar el Teorema de Extensión.

Demostración (Teorema de Extensión). Por el lema anterior, podemos escoger $g \in G$ con $\overline{\mathrm{LC}_{x_1}(g)} \neq 0$, y $M = \deg_{x_1}(g)$ mínimo. Sabemos que $M = \deg_{x_1}(\overline{g}) > 0$.

Afirmamos que

$$\{\overline{f} : f \in I\} = \langle \overline{g} \rangle \subseteq K[x_1]. \tag{3.1}$$

Si esto es cierto, como el grado de $\overline{g}$ es mayor que cero y K es algebraicamente cerrado, existirá algún $a \in K$ tal que

$$\overline{g}(a) = 0 \implies \overline{f}(a) = f(a, b) = 0$$

lo que probaría el teorema.

Para probar la afirmación (3.1), veremos que $\overline{h} \in \langle \overline{g} \rangle$ para todo $h \in G$. Veamos primero que si dado $h \in G$ tal que $\deg_{x_1}(h) < M = \deg_{x_1}(g)$, implica que $\overline{h} = 0$. Sea $m = \deg_{x_1}(h)$. Como M es mínimo, $\overline{\mathrm{LC}_{x_1}(h)} = 0$, así que $\deg_{x_1}(\overline{h}) < \deg_{x_1}(h)$. Definimos

$$S = \mathrm{LC}_{x_1}(g) x_1^{M-m} h - \mathrm{LC}_{x_1}(h) g \in I.$$

Como $S \in I$, lo expresamos como combinación lineal de elementos de la base. $S = \sum_{\ell \in G} A_\ell \ell$. Vemos que

(i) $\overline{\mathrm{LC}_{x_1}(g)} x_1^{M-m} \overline{h} = \overline{S} = \sum_{\ell \in G} \overline{A_\ell} \ell$.

(ii) $\max\{\deg_{x_1}(A_\ell) + \deg_{x_1}(\ell) : A_\ell \neq 0\} = \deg_{x_1}(S) < M$.

Por (i), como $\overline{\mathrm{LC}_{x_1}(g)} \neq 0$ y $m = \deg_{x_1}(h)$,

$$M - \deg_{x_1}(h) + \deg_{x_1}(\overline{h}) \leq \max\{\deg_{x_1}(\overline{A_\ell}) + \deg_{x_1}(\overline{\ell})\},$$

así que

$$\deg_{x_1}(h) - \deg_{x_1}(\overline{h}) \geq \min\{M - \big(\deg_{x_1}(\overline{A_\ell}) + \deg_{x_1}(\overline{\ell})\big)\}. \tag{3.2}$$

Por otra parte, para todo $\ell \in G$ en S tiene $\deg_{x_1}(\ell) < M$, así que $\deg_{x_1}(\overline{\ell}) < \deg_{x_1}(\ell)$. Entonces,

$$\deg_{x_1}(\overline{A_\ell}) + \deg_{x_1}(\overline{\ell}) < \deg_{x_1}(\overline{A_\ell}) + \deg_{x_1}(\ell) < M. \tag{3.3}$$

Uniendo las desigualdades (3.2) y (3.3), obtenemos que

$$\deg_{x_1}(h) - \deg_{x_1}(\overline{h}) \geq 2. \tag{3.4}$$

La desigualdad, se aplica a todos los $h \in G$ con $\deg_{x_1}(h) < M$ y por lo tanto, se aplica a todos los $\ell \in G$ de $\sum_{\ell \in G} A_\ell \ell$. Si argumentamos como antes,

$$\deg_{x_1}(\overline{A_\ell}) + \deg_{x_1}(\overline{\ell}) < \deg_{x_1}(\overline{A_\ell}) + \deg_{x_1}(\ell) < M.$$

Pero por (3.4) en la primera desigualdad estricta, la diferencia es de al menos 2, así que

$$\deg_{x_1}(h) - \deg_{x_1}(\overline{h}) \geq \min\{M - \big(\deg_{x_1}(\overline{A_\ell}) + \deg_{x_1}(\overline{\ell})\big)\} \geq 3.$$

Si seguimos argumentando de esta manera, vemos que $\overline{h} = 0$ para todo $h \in G$ con $\deg_{x_1}(h)$. Una vez probado esto, vamos a demostrar que $\overline{h} \in \langle \overline{g} \rangle$ para todo $h \in G$.

Seguiremos inducción en $\deg_{x_1}(h)$. Si $\deg_{x_1}(h) < M$ implica que $\overline{h} = 0 \in \langle \overline{g} \rangle$ por lo demostrado anteriormente.

Supongamos que $\overline{h} \in \langle \overline{g} \rangle$ para todo $h \in G$ con $\deg_{x_1}(h) < m$, siendo $m \geq M$. Sea $h \in G$ con $\deg_{x_1}(h) = m$. Entonces

$$S = \mathrm{LC}_{x_1}(g)h - \mathrm{LC}_{x_1}(h)x^{m-M}g \in I.$$

representado como combinación lineal de elementos de la base $S = \sum_{\ell \in G} A_\ell \ell$. Así que

$$\deg_{x_1}(S) < m \implies \deg_{x_1}(\ell) < m \text{ para todo } \ell \text{ en } S.$$

Por la hipótesis de inducción, $\overline{\ell} \in \langle \overline{g} \rangle$. De este modo,

$$\overline{\mathrm{LC}_{x_1}(g)}\overline{h} - \overline{\mathrm{LC}_{x_1}(h)}x^{m-M}\overline{g} = \overline{S} = \sum_{\ell \in G} \overline{A_\ell}\overline{\ell}.$$

Entonces, $\overline{\mathrm{LC}_{x_1}(g)} \neq 0$ implica que $\overline{h} \in \langle \overline{g} \rangle$, quedando así probado el teorema. □

La demostración tradicional de este teorema, que podemos encontrar en [4] usa las llamadas Resultantes, o métodos mas abstractos de la geometría algebraica. La demostración que hacemos está basada en [11].

Corolario 3.9. *Sea $I = \langle f_1, \ldots, f_s \rangle \subset K[x_1, \ldots, x_n]$, y supongamos que para algún i, f_i es de la forma*

$$f_i = cx_1^N + \text{ términos de grado } < N \text{ en } x_1,$$

donde $c \in K$ distinto de cero y $N > 0$. Si I_1 es el primer ideal de eliminación de I, y $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$, entonces existe $a_1 \in K$ tal que $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Ejemplo 3.10. Consideremos las siguientes ecuaciones en $\mathbb{C}$

$$xy = 1,$$
$$xz = 1.$$

Consideramos el ideal $I = \langle xy - 1, xz - 1 \rangle$ y hallamos una base de Gröbner respecto el orden lexicográfico. El código en `Singular` para esto es:

```
> ring r=0,(x,y,z), lp;
> poly f=xy - 1;
> poly g=xz - 1;
> ideal I = f, g;
> std(I);
_[1]=y-z
_[2]=xz-1
```

Vemos que $G = \langle xz - 1, y - z\rangle$ y que el primer ideal de eliminación es $I_1 = \langle y - z\rangle$. Las soluciones parciales son de la forma (a, a), y para poder extenderlas a soluciones completas, usando el teorema de extensión, reescribimos el polinomio de la base que no está en I_1

$$xz - 1 = c(y, z)x - 1,$$

con $c(y, z) = z$. Entonces, podremos extender la solución, siempre que $a \neq 0$. Así, las soluciones del sistema de ecuaciones serán de la forma $(1/a, a, a)$ para todo $a \in \mathbb{C}$, con $a \neq 0$, lo que es lo mismo,

$$\mathbf{V}(I) = \{(1/a, a, a) \in \mathbb{C}^3 : a \in \mathbb{C}, a \neq 0\}.$$

3.2. Geometría de la Eliminación

En esta sección veremos una interpretación geométrica de los teoremas probados en la sección anterior, y hablaremos del Teorema de Clausura, que describe la relación entre soluciones parciales e ideales de eliminación.

Definición 3.11. Para eliminar las l primeras variables, definimos la función proyección

$$\pi_l : K \longrightarrow K^{n-l},$$

que lleva $(a_1, \ldots, a_n)$ a $(a_{l+1}, \ldots, a_n)$. Si aplicamos π_l a una variedad $V \subset K^n$, obtenemos $\pi_l(V) \subset K^{n-l}$.

Lema 3.12. *Sea $V = \mathbf{V}(f_1, \ldots, f_s) \subset K$ una variedad y $I_l = \langle f_1, \ldots, f_s\rangle \cap K[x_{l+1}, \ldots, x_n]$ el l-ésimo ideal de eliminación. Entonces, en K^{n-l} tenemos que*

$$\pi_l(V) \subset \mathbf{V}(I_l).$$

Demostración. Dado un polinomio $f \in I_l$, si $(a_1, \ldots, a_n) \in V$, como $f \in \langle f_1, \ldots, f_s\rangle$, tenemos que $f(a_1, \ldots, a_n) = 0$. Pero como f solo involucra a las variables $x_{l+1}, \ldots, x_n$, podemos escribir

$$f(a_{l+1}, \ldots, a_n) = f\big(\pi_l(a_1, \ldots, a_n)\big) = 0.$$

□

Como en la sección anterior, llamaremos a los puntos de $\mathbf{V}(I_l)$ soluciones parciales, y usando el lema anterior, podemos escribir $\pi_l(V)$ de la manera siguiente:

$$\pi_l(V) = \{(a_{l+1}, \ldots, a_n) \in \mathbf{V}(I_l) : \exists a_1, \ldots, a_l \in K \text{ tal que } (a_1, \ldots, a_l, a_{l+1}, \ldots, a_n) \in V\}.$$

Si volvemos al Ejemplo 3.10, la variedad $\mathbf{V}(I_1)$ era la recta $y = z$, y podíamos extender soluciones siempre que $z \neq 0$. Es decir

$$\mathbf{V}(I_1) = \{(a, a) \in \mathbb{C}^2\}.$$
$$\pi_1(V) = \{(a, a) \in \mathbb{C}^2 : a \neq 0\}.$$

En particular, $\pi_1(V)$ no es una variedad afín, ya que le falta el punto $(0, 0)$.

Teorema 3.13. *Sea K un cuerpo algebraicamente cerrado. Sea una variedad de la forma $V = \mathbf{V}(f_1, \ldots, f_s) \subset K^n$, y sean g_i los polinomios que acompañan al monomio x_1^N al expresar f_i de la forma descrita en el Teorema de Extensión (Teorema 3.5). Si I_1 es el primer ideal de eliminación de $\langle f_1, \ldots, f_s\rangle$, entonces tenemos la siguiente igualdad en K^{n-1}*

$$\mathbf{V}(I_1) = \pi_1(V) \cup \big(\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)\big).$$

donde $\pi_1 : K^n \longrightarrow K^{n-1}$ es la proyección en las últimas $n - 1$ componentes.

Demostración. Por el Lema 3.12, está claro que $\mathbf{V}(I_1) \supset \pi_1(V) \cup \big(\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)\big)$. Para ver la otra inclusión, tomamos un punto $a = (a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. Si $a \notin V(g_1, \ldots, g_s)$ entonces por el Teorema de Extensión $a \in \pi_1(V)$. Entonces, a pertenece a $\big(\mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)\big)$ o pertenece a $\pi_1(V)$. □

Este teorema nos dice que si al conjunto $\pi_1(V)$ le añadimos la variedad $\mathbf{V}(g_1, \ldots, g_s)$, obtenemos la variedad $\mathbf{V}(I_1)$. El problema, es que no sabemos como de grande puede llegar a ser $\mathbf{V}(g_1, \ldots, g_s)$, entonces el teorema anterior, no nos dice nada sobre el tamaño de $\pi_1(V)$. Para conseguir una relación más fuerte entre $\pi_l(V)$ y $\mathbf{V}(I_1)$, demostraremos el Teorema de Clausura, pero para ello necesitamos algunos resultados previos.

Definición 3.14. Sea un conjunto $S \subset K^n$ definimos el ideal de S como

$$\mathbf{I}(S) = \{f \in K[x_1, \ldots, x_n] : f(a) = 0 \text{ para todo } a \in S\}.$$

Definición 3.15. Llamaremos clausura de Zariski de $S \subset K^n$ a la menor variedad afín que contiene a S.

Proposición 3.16. *Sea $S \subset K^n$, la clausura de Zariski de S es igual a $\mathbf{V}\big(\mathbf{I}(S)\big)$.*

La demostración de este resultado la podemos encontrar en [4].

Definición 3.17. Sea $I \subset K[x_1, \ldots, x_n]$ un ideal. El radical de I es el siguiente ideal

$$\sqrt{I} = \{f : f^N \in I \text{ para algún } N \geq 1\}.$$

Teorema 3.18 (Teorema débil de los Ceros de Hilbert)**.** *Sea K un cuerpo algebraicamente cerrado y sea $I \subset K[x_1, \ldots, x_n]$ un ideal. Entonces $\mathbf{V}(I) = \emptyset$ si y solo si $I = K[x_1, \ldots, x_n]$.*

Corolario 3.19. *Sea K un cuerpo algebraicamente cerrado. Dado un ideal $I \subset K[x_1, \ldots, x_n]$ y G la base de Gröbner reducida de I, $\mathbf{V}(I) = \emptyset$ si y solo si $G = \{1\}$.*

Teorema 3.20 (Teorema de los Ceros de Hilbert)**.** *Sea K un cuerpo algebraicamente cerrado. Sean $f, f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ tales que $f \in \mathbf{I}\big(\mathbf{V}(f_1, \ldots, f_s)\big)$, entonces existe un entero $N \geq 1$ tal que*

$$f^N \in \langle f_1, \ldots, f_s \rangle.$$

Teorema 3.21 (Teorema fuerte de los Ceros de Hilbert)**.** *Sea $I \subset K[x_1, \ldots, x_n]$ es un ideal, y $\overline{K}$ la clausura algebraica de K, entonces*

$$\mathbf{I}\big(\mathbf{V}_{\overline{K}}(I)\big) = \sqrt{I}.$$

La prueba de estos resultados la podemos encontrar en [1] y [4].

Teorema 3.22 (Teorema de Clausura)**.** *Sea K un cuerpo algebraicamente cerrado. Sea $V = \mathbf{V}(f_1, \ldots, f_s) \subset K^n$ y sea I_1 el primer ideal de eliminación de $\langle f_1, \ldots, f_s \rangle$. Entonces*

(i) *$\mathbf{V}(I_1)$ es la variedad afín más pequeña que contiene a $\pi_1(V) \subset K^{n-1}$.*

(ii) *Si $V \neq \emptyset$, existe una variedad afín $W \subsetneq \mathbf{V}(I_1)$ tal que $\mathbf{V}(I_1) - W \subset \pi_1(V)$.*

Demostración. Como consecuencia de la Proposición 3.16 para demostrar (i), tenemos que demostrar que $\mathbf{V}(I_1) = \mathbf{V}\big(\mathbf{I}\big(\pi_1(V)\big)\big)$. Por el Lema 3.12, $\pi_1(V) \subset \mathbf{V}(I_1)$. Como $\mathbf{V}\big(\mathbf{I}\big(\pi_1(V)\big)\big)$ es la variedad afín más pequeña que contiene a $\pi_1(V)$, es inmediato que $\mathbf{V}\big(\mathbf{I}\big(\pi_1(V)\big)\big) \subset \mathbf{V}(I_1)$.

Para ver la otra inclusión, sea $f \in \mathbf{I}\big(\pi_1(V)\big)$, es decir, $f(a_2, \ldots, a_n) = 0$ para todo $(a_2, \ldots, a_n) \in \pi_1(V)$. Si consideramos f como un elemento de $K[x_1, \ldots, x_n]$, está claro que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in V$. Por el Teorema de los Ceros de Hilbert, existe un entero N para el que $f^N \in \langle f_1, \ldots, f_s \rangle$. Sabemos que f^N no depende de x_1, ya que f tampoco depende de x_1, así que $f^N \in \langle f_1, \ldots, f_s \rangle \cap K[x_2, \ldots, x_n] = I_1$. Entonces $f \in \sqrt{I_1}$, lo que implica que $\mathbf{I}\big(\pi_1(V)\big) \subset \sqrt{I_1}$. Entonces $\mathbf{V}(I_1) = \mathbf{V}(\sqrt{I_1}) \subset \mathbf{V}\big(\mathbf{I}\big(\pi_1(V)\big)\big) \subset \mathbf{V}(I_1)$.

Veamos ahora el apartado (ii) del teorema. Sea $W = \mathbf{V}(g_1, \ldots, g_s) \cap \mathbf{V}(I_1)$. W es una variedad afín por ser intersección de variedades. La descomposición del Teorema 3.13, nos dice que $\mathbf{V}(I_1) - W \subset \pi_1(V)$. Si $W \neq \mathbf{V}(I_1)$, habríamos terminado, pero puede pasar que $W = \mathbf{V}(I_1)$.

En este caso, tenemos que cambiar las ecuaciones que definen V para que W se vuelva más pequeño. Primero tenemos que

$$\text{si } W = \mathbf{V}(I_1), \text{ entonces } V = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_s).$$

Veamos la demostración de esto. Una inclusión es obvia, ya que solamente estamos añadiendo ecuaciones $\mathbf{V}(f_1,\ldots,f_s,g_1,\ldots,g_s) \subset \mathbf{V}(f_1,\ldots,f_s) = V$. Para ver la otra inclusión, sea $a = (a_1,\ldots,a_n) \in V$. Está claro que cada $f_i(a) = 0$ para todo i, y como $(a_2,\ldots,a_n) \in \pi_1(V) \subset \mathbf{V}(I_1) = W$, tenemos que para cada i, $g_i(a) = 0$. Entonces $(a_1,\ldots,a_n) \in \mathbf{V}(f_1,\ldots,f_s,g_1,\ldots,g_s)$.

Sea ahora $I = \langle f_1,\ldots,f_s\rangle$ el ideal original, y sea $\tilde{I} = \langle f_1,\ldots,f_s,g_1,\ldots,g_s\rangle$. Por el apartado (i) del teorema, que ya esta probado, sabemos que $\mathbf{V}(I_1)$ y $\mathbf{V}(\tilde{I}_1)$ son ambos la variedad mas pequeña que contiene a $\pi(V)$, tenemos que $\mathbf{V}(I_1) = \mathbf{V}(\tilde{I}_1)$.

El siguiente paso, es encontrar una base mejor para $\tilde{I}$. Recordamos que los g_i están definidos al escribir

$$f_i = g_i(x_2,\ldots,x_n)x_1^{N_i} + \text{ términos de grado } < N_i \text{ en } x_1,$$

donde $N_i > 0$ y $g_i \in K[x_2,\ldots,x_n]$ es distinto de cero. Definimos ahora los siguientes polinomios

$$\tilde{f}_i = f_i - g_i x_1^{N_i}.$$

Para cada i, o $\tilde{f}_i$ es cero, o tiene grado estrictamente menor en x_1 que f_i. Además, está claro que

$$\tilde{I} = \langle \tilde{f}_1,\ldots,\tilde{f}_s,g_1,\ldots,g_s\rangle.$$

Si aplicamos el Teorema 3.13 a $V = \mathbf{V}(\tilde{f}_1,\ldots,\tilde{f}_s,g_1,\ldots,g_s)$, como los coeficientes principales de los generadores son diferentes, tendremos una descomposición diferente

$$\mathbf{V}(I_1) = \mathbf{V}(\tilde{I}_1) = \pi_1(V) \cup \tilde{W}.$$

En general, no podemos asegurar que $\tilde{W}$ sea estrictamente menor, es decir, puede darse que $\tilde{W} = \mathbf{V}(I_1)$. Si esto pasa, repetimos el proceso una y otra vez hasta que consigamos que sea estrictamente menor. Supongamos ahora que cada vez que realizamos el proceso obtenemos $\mathbf{V}(I_1)$. Los grados en x_1 cada vez son menores, hasta que llega un punto en el que son 0. Esto quiere decir que V puede ser definida buscando soluciones de polinomios en $K[x_2,\ldots,x_n]$. Entonces, si $(a_2,\ldots,a_n)$ es una solución parcial, $(a_1,a_2,\ldots,a_n) \in V$ para todo $a_1 \in K$ ya que x_1 no aparece en las ecuaciones que definen V. Entonces, como toda solución parcial se extiende, $\pi_1(V) = \mathbf{V}(I_1)$, entonces tenemos que $W = \emptyset$. □

Este teorema se puede probar cambiando en el enunciado el primer ideal de eliminación por el l-ésimo ideal de eliminación. La prueba clásica usa resultantes y otros métodos de álgebra abstracta y se puede encontrar en [4]. En [11] se da una demostración alternativa, que no usa las herramientas de la prueba clásica.

Corolario 3.23. *Sea $V = \mathbf{V}(f_1, \ldots, f_s) \subset$ con K algebraicamente cerrado, y supongamos que para algún i, f_i es de la forma*

$$f_i = cx_1^N + \text{ términos de grado } < N \text{ en } x_1,$$

donde $c \in K$ distinto de cero y $N > 0$. Si I_1 es el primer ideal de eliminación, entonces en K^{n-1}

$$\pi(V) = \mathbf{V}(I_1).$$

3.3. Implicitación

En esta sección, trataremos el problema de implicitación. El principal objetivo es que dada una variedad V descrita usando ecuaciones paramétricas, convertir la parametrización en ecuaciones que definan V. Nos pueden surgir diferentes problemas, como que la parametrización no cubre todos los puntos de la variedad V. Entonces, el problema que vamos a tratar, es el de buscar las ecuaciones que definen la variedad V más pequeña que contiene a la parametrización. Además, trataremos el caso en que la parametrización está dada por funciones racionales en vez de polinomios.

Ejemplo 3.24. Sea la superficie dada paramétricamente por

$$\begin{aligned} x &= uv, \\ y &= v, \\ z &= u^2. \end{aligned}$$

Si despejamos los parámetros, obtenemos la ecuación implícita $f = x^2 - y^2 z$, que nos define una variedad $V = \mathbf{V}(f)$. Como veremos más adelante, V es la menor variedad que contiene a la parametrización. El problema que nos encontramos es que si nuestro cuerpo es $\mathbb{R}$, los puntos (x, y, z) que obtenemos al variar u y v, no llenan la variedad V. Por ejemplo, los puntos de la forma $(0, 0, t)$ con $t < 0$, somos incapaces de obtenerlos con la parametrización, en cambio pertenecen a la variedad.

Examinaremos primero el caso de una parametrización polinómica de la forma

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m). \end{aligned}$$

donde $f_1, \ldots, f_n$ son polinomios de $K[t_1, \ldots, t_m]$. Podremos verlo geométricamente como la función

$$F : K^m \longrightarrow K^n,$$

definida por

$$F(t_1, \ldots, t_m) = \big(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)\big).$$

Entonces, $F(K^m) \subset K^n$ es el subconjunto de K^n parametrizado. Como ya vimos, puede darse que $F(K^m)$ no sea una variedad afín, entonces nuestro objetivo es encontrar la menor variedad afín que contiene a $F(K^m)$.

Definimos la variedad $V = \mathbf{V}(x_1 - f_1, \ldots, x_n - f_n) \subset K^{n+m}$. Los puntos de V se pueden escribir de la forma

$$\big(t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)\big),$$

lo que muestra que V se puede escribir como grafo de una función. Consideramos además la función

$$i : K^m \longrightarrow K^{n+m},$$

definida por

$$i(t_1, \ldots, t_m) = \big(t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)\big),$$

y la función proyección

$$\pi_m : K^{n+m} \longrightarrow K^n,$$

definida por

$$\pi_m(t_1, \ldots, t_m, x_1, \ldots, x_n) = (x_1, \ldots, x_n).$$

Vemos que $F = \pi_m \circ i$ y que $i(K^m) = V$. Entonces obtenemos

$$F(K^m) = \pi_m\big(i(K^m)\big) = \pi_m(V), \tag{3.5}$$

es decir, la imagen de la parametrización es la proyección del grafo. Podemos aplicar ahora la teoría de la eliminación desarrollada en el capítulo 3 para encontrar la menor variedad que contiene a $F(K^m)$.

Teorema 3.25. *Sea K un cuerpo infinito y sea $F : K^m \longrightarrow K^n$ la función determinada por la parametrización polinómica. Sea $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subset K[t_1, \ldots, t_m, x_1, \ldots, x_n]$ y sea $I_m = I \cap K[x_1, \ldots, x_n]$ el m-ésimo ideal de eliminación. Entonces $\mathbf{V}(I_m)$ es la variedad afín más pequeña de K^n que contiene a $F(K^m)$.*

Demostración. Sea $V = \mathbf{V}(I) \subset K^{n+m}$. Por lo desarrollado antes del enunciado del teorema, V es el grafo de F. Si suponemos que K es algebraicamente cerrado, $F(K^m) = \pi_m(V)$, y por el Teorema de Clausura (Teorema 3.22), sabemos que $\mathbf{V}(I_m)$ es la menor variedad que contiene a $\pi_m(V)$, por lo que queda probado.

Supongamos ahora que K no es algebraicamente cerrado. Llamaremos $\overline{K}$ a su clausura algebraica y $\mathbf{V}_K(I_m)$ será la variedad en K^n mientras que $\mathbf{V}_{\overline{K}}(I_m)$ será la variedad en $\overline{K}$.

Por la ecuación (3.5) y el Lema 3.12 sabemos que $F(K^m) = \pi_m(V) \subset \mathbf{V}_K(I_m)$. Sea $Z_K = \mathbf{V}_K(g_1, \ldots, g_s) \subset K^n$ una variedad de K^n tal que $F(K^m) \subset Z_K$. Tenemos que demostrar que $\mathbf{V}_K(I_m) \subset Z_K$. Como $F(K^m) \subset Z_K$, para todo i, $g_i \circ F$ es cero en todo punto de K^m. Como $g_i \in K[x_1, \ldots, x_n]$, y $F = (f_1, \ldots, f_n)$ está construido por polinomios en $K[t_1, \ldots, t_m]$ tenemos que $g_i \circ F \in K[t_1, \ldots, t_m]$.

Entonces, los polinomios $g_i \circ F$ son cero en todo punto de K^m, así que como K es infinito, $g_i \circ F$ es el polinomio cero. En particular, esto significa que $g_i \circ F$ también es cero en $\overline{K}^m$, y que los g_i son cero en todo punto de $F(\overline{K}^m)$. De hecho, $Z_{\overline{K}} = \mathbf{V}_{\overline{K}}(g_1, \ldots, g_s)$ es una variedad de $\overline{K}^n$ que contiene a $F(\overline{K}^m)$. Como el teorema es cierto para $\overline{K}$ ya que es algebraicamente cerrado, tenemos que $\mathbf{V}_{\overline{K}}(I_m) \subset Z_{\overline{K}}$ en $\overline{K}^n$. Si solo tomamos las soluciones que están en K^n, es inmediato que $\mathbf{V}_K(I_m) \subset Z_K$, quedando probado el teorema. □

Este teorema, nos da un algoritmo para obtener las ecuaciones implícitas de una parametrización polinómica. Basta con computar una base de Gröbner con respecto un orden que elimine las variables t del ideal $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$. Por el Teorema de Eliminación, las ecuaciones que no tengan a las variables t forman una base de I_m, y este ideal definirá la menor variedad de K^n que contiene a la parametrización.

Ejemplo 3.26. Si volvemos al problema del Ejemplo 3.24, tomando $\mathbb{C}$ como cuerpo, una base de Gröbner respecto del orden lexicográfico con $u > v > x > y > z$ del ideal $I = \langle x - uv, y - v, z - u^2 \rangle$ está formada por los polinomios

$$\begin{aligned} g_1 &= x^2 - y^2 z, \\ g_2 &= v - y, \\ g_3 &= uy - x, \\ g_4 &= ux - yz, \\ g_5 &= u^2 - z. \end{aligned}$$

Vemos que $I_2 = \langle g_1 \rangle$, la ecuación que obteníamos al despejar u y v, que por el Teorema 3.25 sabemos que $\mathbf{V}(I_2)$ es la menor variedad que contiene a la parametrización. Ahora queremos saber si los puntos de la parametrización llenan toda la variedad $\mathbf{V}(g_1) \subset \mathbb{C}^3$. El

Teorema de Eliminación nos dice que $I_1 = \langle g_1, g_2 \rangle$. Sea $(x, y, z) \in \mathbf{V}(I_2)$, como g_2 está en la forma del Corolario 3.9, se puede extender a una solución de la forma $(v, x, y, z) \in \mathbf{V}(I_1)$. Del mismo modo, si tomamos un punto $(v, x, y, z) \in \mathbf{V}(I_1)$, como g_5 vuelve a estar en la forma del Corolario 3.9, podemos extender la solución a $(u, v, x, y, z) \in \mathbf{V}(I)$. Entonces, demostramos que la parametrización es igual a $\mathbf{V}(I_2) = \mathbf{V}(g_1)$.

Veamos ahora que pasa si consideramos una parametrización formada por funciones racionales.

Ejemplo 3.27. Sea la parametrización

$$\begin{aligned} x &= \frac{u^2}{v}, \\ y &= \frac{v^2}{u}, \\ z &= u. \end{aligned}$$

Es inmediato comprobar que todo punto siempre pertenece a la superficie $x^2y = z^3$.

Nuestro primer instinto para hallar la variedad más pequeña que contiene a la parametrización, puede ser quitar denominadores y utilizar el proceso descrito para parametrizaciones polinómicas. Si hacemos esto, obtenemos el ideal

$$I = \langle vx - u^2, uy - v^2, z - u \rangle \subset K[u, v, x, y, z],$$

y si usamos el Teorema de Eliminación para eliminar las variables u y v, obtenemos que $I_2 = \langle z(x^2y - z^3) \rangle$, por lo que

$$\mathbf{V}(I_2) = \mathbf{V}(x^2y - z^3) \cup \mathbf{V}(z),$$

en particular, $\mathbf{V}(I_2)$ no es la variedad más pequeña que contiene a la parametrización.

En general, para que el truco descrito antes funcione, tenemos que hacer algunos cambios. La situación que tenemos es la siguiente:

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}, \end{aligned}$$

donde $f_1, \ldots, f_n, g_1, \ldots, g_n \in K[t_1, \ldots, t_m]$. La función F definida de K^m a K^n dada por la parametrización puede no estar definida en todo K^m por los denominadores. Si tomamos $W = \mathbf{V}(g_1 \cdot g_2 \cdots g_n) \subset K^m$, está claro que

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right),$$

define una función

$$F : K^m - W \longrightarrow K^n.$$

Entonces, para resolver el problema de implicitación, tenemos que encontrar la menor variedad de K^n que contiene a $F(K^m - W)$. Si consideramos las aplicaciones i y π_m como en el apartado anterior, es fácil comprobar que $i(K^m - W) \subset \mathbf{V}(I)$, donde $I = \langle (g_1x_1 - f_1, \ldots, g_nx_n - f_n)\rangle$ es el ideal obtenido al quitar denominadores.

Pero este ideal no nos es suficiente, como vimos en el ejemplo anterior. Lo que vamos a hacer, es usar una dimensión extra para controlar a los denominadores. Sea $g = g_1 \cdot g_2 \cdots g_n$, tenemos que $W = \mathbf{V}(g)$. Consideramos el ideal

$$J = \langle (g_1x_1 - f_1, \ldots, g_nx_n - f_n), 1 - gy\rangle \subset K[y, t_1, \ldots, t_m, x_1, \ldots, x_n].$$

La ecuación $1 - gy = 0$ significa que los denominadores $g_1, \ldots, g_n$ nunca son cero en $\mathbf{V}(J)$. Consideramos ahora las siguientes funciones

$$j : K^m - W \longrightarrow K^{n+m+1},$$
$$\pi_{m+1} : K^{n+m+1} \longrightarrow K^n,$$

definidas por

$$j(t_1, \ldots, t_m) = \left(\frac{1}{g(t_1, \ldots, t_m)}, t_1, \ldots, t_m, \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}\right),$$

$$\pi_{m+1}(y, t_1, \ldots, t_m, x_1, \ldots, x_n) = (x_1, \ldots, x_n).$$

Como antes, tenemos que $F = \pi_{m+1} \circ j$.

Lema 3.28. *En las condiciones anteriores, $j(K^m - W) = \mathbf{V}(J)$ en K^{n+m+1}.*

Demostración. De las definiciones de j y J, es inmediato que $j(K^m - W) \subset \mathbf{V}(J)$.

Para ver la otra inclusión, tomamos un punto $(y, t_1, \ldots, t_m, x_1, \ldots, x_n) \in \mathbf{V}(J)$. Como $g(t_1, \ldots, t_m)y = 1$, implica que ninguno de los g_i es cero en $(t_1, \ldots, t_m)$ y por lo tanto, $g_i(t_1, \ldots, t_m)x_i = f_i(t_1, \ldots, t_m)$ puede ser resuelta por $x_i = f_i(t_1, \ldots, t_m)/g_i(t_1, \ldots, t_m)$. Como $y = 1/g(t_1, \ldots, t_m)$, está claro que el punto pertenece a $j(K^m - W)$. □

Entonces, como consecuencia de que $F = \pi_{m+1} \circ j$ y de este lema, obtenemos que

$$F(K^m - W) = \pi_{m+1}\big(j(K^m - W)\big) = \pi_{m+1}\big(\mathbf{V}(J)\big). \tag{3.6}$$

De este modo, como en el Teorema 3.25 podemos usar la Teoría de la Eliminación para resolver el problema.

Teorema 3.29. *Sea K un cuerpo infinito y sea $F : K^m - W \longrightarrow K^n$ la función determinada por la parametrización racional. Sea $J = \langle x_1 g_1 - f_1, \ldots, x_n g_n - f_n, 1 - gy \rangle \subset K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$ donde $g = g_1 \cdot g_2 \cdots g_n$ y sea $J_{m+1} = J \cap K[x_1, \ldots, x_n]$ el (m+1)-ésimo ideal de eliminación. Entonces $\mathbf{V}(J_{m+1})$ es la variedad afín más pequeña de K^n que contiene a $F(K^m - W)$.*

Demostración. Como en la demostración del Teorema 3.25, si K es algebraicamente cerrado, es consecuencia inmediata del Teorema de Clausura (Teorema 3.22).

Suponemos ahora que K no es algebraicamente cerrado y continuamos con la notación del Teorema 3.25. Sea $V = \mathbf{V}(J) \subset K^{n+m+1}$, por la ecuación (3.6) y el Lema 3.12 sabemos que $F(K^m - W) = \pi_{m+1}(V) \subset \mathbf{V}_K(I_m)$. Sea $Z_K = \mathbf{V}_K(g_1, \ldots, g_s) \subset K^n$ una variedad de K^n tal que $F(K^m - W) \subset Z_K$. Tenemos que demostrar que $\mathbf{V}_K(I_m) \subset Z_K$. Como $F(K^m - W) \subset Z_K$ para todo i, $g_i \circ F$ es cero en todo punto de $K^m - W$. Como $g_i \in K[x_1, \ldots, x_n]$, y $F = (f_1, \ldots, f_n)$ está construido por polinomios en $K[t_1, \ldots, t_m]$, tenemos que $g_i \circ F \in K[t_1, \ldots, t_m]$.

Si demostramos que cada polinomio $g_i \circ F$ es el polinomio cero, proseguiríamos el razonamiento como en el Teorema 3.25 y quedaría probado el enunciado. Entonces si consideramos el polinomio $(g_i \circ F) \cdot g$, es cero para todo punto $a \in K^n$, ya que si $a \in W$, tenemos que $g(a) = 0$, y si $a \in K^n - W$, tenemos que $(g_i \circ F)(a) = 0$. Entonces $(g_i \circ F) \cdot g$ es el polinomio cero, y como sabemos que $g \neq 0$, no queda mas remedio que $g_i \circ F$ lo sea. □

Ejemplo 3.30. Si usamos el algoritmo descrito en el teorema anterior para el Ejemplo 3.27

```
> ring R = 0, (t,u,v,x,y,z), lp;
> ideal I = v*x - u^2, u*y - v^2, z - u, 1 - v*u*t;
> std(I);
_[1]=x2y-z3
_[2]=vz-xy
_[3]=vx-z2
_[4]=v2-yz
_[5]=u-z
_[6]=tz3-x
_[7]=tyz2-v
_[8]=txy-1
```

Es decir, la menor variedad que contiene a la parametrización es $\mathbf{V}(I_2) = \mathbf{V}(x^2y - z^3)$. Además, observando los 3 últimos polinomios y aplicando el Teorema de Extensión, comprobamos que el punto $(0, 0, 0) \in \mathbb{C}^3$ pertenece a la variedad, pero no se puede alcanzar con la parametrización.

Ejemplo 3.31. Podemos expresar la circunferencia de radio unidad con las siguientes ecuaciones paramétricas.

$$x = \frac{1-t^2}{1+t^2},$$
$$y = \frac{2t}{1+t^2}.$$

Hallamos una base de Gröbner del ideal descrito en el enunciado del Teorema 3.29, $G = \{x^2+y^2-1, ty+x-1, tx+t-y, 4u-2x+y^2-2\}$. Vemos que efectivamente la menor variedad que contiene a la parametrización es $\mathbf{V}(x^2+y^2-1)$, la circunferencia de radio unidad. Si trabajamos sobre $\mathbb{C}$, podemos extender las soluciones, ya que el único punto de $\mathbb{C}^2$ donde no podemos aplicar el Teorema de Extensión, es el $(0,0)$, pero este punto no pertenece a $\mathbf{V}(I_2)$.

Por otra parte, si trabajamos en $\mathbb{R}$, vemos que el punto $(-1,0)$ no se alcanza nunca.

Ejemplo 3.32. Consideramos la curva en $\mathbb{C}^n$ parametrizada por $x_i = f_i(t)$, donde $f_1, \ldots, f_n$ son polinomios en $\mathbb{C}[t]$. Obtenemos el ideal

$$I = \langle x_1 - f_1(t), \ldots, x_n - f_n(t)\rangle \subset \mathbb{C}[t, x_1, \ldots, x_n].$$

Como la variable t, nunca aparece multiplicada por x_i, aplicando el Corolario 3.9 del Teorema de Extensión, podremos extender siempre la solución, es decir, la parametrización llena la variedad $\mathbf{V}(I_1)$.

Esto no es cierto si trabajamos en $\mathbb{R}$, ya que si tomamos la parametrización

$$x = t^2,$$
$$y = t^2,$$

una base de Gröbner respecto del orden lexicográfico con $t > x > y$ del ideal I descrito en el Teorema 3.25 es $G = \{x-y, t-x\}$, y los puntos de la forma (a,a) con $a < 0$, pertenecen a la variedad $\mathbf{V}(I_1) = \mathbf{V}(x-y)$ y no se pueden alcanzar con la parametrización.

Si volvemos a $\mathbb{C}$, pero los $f_i(t)$ permitimos que sean funciones racionales en vez de polinomios, tampoco podemos asegurar que la parametrización llene la variedad. Por ejemplo, considerando la parametrización

$$x = \frac{t-1}{t^2+1},$$
$$y = \frac{1}{t}.$$

Una base de Gröbner respecto del orden lexicográfico del ideal $J = \langle (t^2+1)x - (t-1), ty - 1, (1-ut)(t^2+1)\rangle$ es $G = \{xy^2 + x + y^2 - y, ty - 1, tx - ty + xy + y, 2u - xy^3 - xy^2 - y^3\}$.

Vemos que el punto $(0,0) \in \mathbb{C}^2$ pertenece a la variedad $\mathbf{V}(I_2) = \mathbf{V}(xy^2 + x + y^2 - y)$ pero no podemos obtenerlo con la parametrización.

Ejemplo 3.33. Dada una parametrización racional, existe un caso donde el ideal $I = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n \rangle$ obtenido quitando denominadores, nos da la solución al problema, sin tener que añadir la ecuación $1 - gy$. Supongamos que $x_i = f_i(t)/g_i(t)$, donde solamente tenemos un parámetro t. Podemos suponer que para cada i, los polinomios $f_i(t)$ y $g_i(t)$ son relativamente primos en $K[t]$, en particular no tienen raíces comunes. Si $I \subset K[t, x_1, \ldots, x_n]$, tenemos que $\mathbf{V}(I_1)$ es la menor variedad afín conteniendo a $F(K - W)$, donde $W = \mathbf{V}(g) \subset K$ con $g = g_1 \cdots g_n \in K[t]$.

Si pasa esto, no solo $i(K - W) \subset \mathbf{V}(I)$ sino que tenemos la igualdad. Esto es por que si un punto $a = (\tilde{t}, a_1, \ldots, a_n) \in K^{n+1}$ está en $\mathbf{V}(I)$, $g_i(\tilde{t})$ tiene que ser distinto de cero para todo i, ya que se cumple que $g_i(\tilde{t})a_i = f_i(\tilde{t})$, y que g_i y f_i tienen raíces distintas. Al tener que $i(K - W) = \mathbf{V}(I)$ podemos adaptar la demostración del Teorema 3.25 para obtener el resultado.

Capítulo 4

Aplicaciones

Con la teoría desarrollada hasta aquí, somos capaces de dar aplicaciones muy variadas de las bases de Gröbner. En este capítulo veremos algunas aplicaciones directamente relacionadas con el álgebra conmutativa.

4.1. Operaciones con ideales

Definición 4.1. Si I y J son ideales del anillo $K[x_1, \ldots, x_n]$, definimos la suma de I y J como

$$I + J = \{f + g : g \in I \text{ y } g \in J\}.$$

Proposición 4.2. *Si I y J son ideales en $K[x_1, \ldots, x_n]$, entonces $I + J$ también lo es. Además, $I + J$ es el ideal más pequeño que contiene a I y a J. Si $I = \langle f_1, \ldots, f_r \rangle$ y $J = \langle g_1, \ldots, g_s \rangle$, entonces $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$.*

Demostración. Primero es inmediato que $0 = 0 + 0 \in I + J$. Sean $h_1, h_2 \in I + J$. Por definición, existen $f_1, f_2 \in I$ y $g_1, g_2 \in J$ tal que $h_1 = f_1 + g_1$, $h_2 = f_2 + g_2$. Entonces, $h_1 + h_2 = (f_1 + f_2) + (g_1 + g_2)$, y como I y J son ideales, $h_1 + h_2 \in I + J$. Sea $h \in I + J$ y $l \in K[x_1, \ldots, x_n]$. Existen $f \in I$ y $g \in J$ tales que $h = f + g$. Entonces, $l \cdot h = l \cdot (f + g) = l \cdot f + l \cdot g$. Otra vez, como I y J son ideales, $l \cdot h \in I + J$, demostrando así que es ideal.

Si H es un ideal que contiene a I y a J, entonces H debe contener a todos los elementos $f \in I$ y $g \in J$. Como H es ideal, tiene que contener a $f + g$, así que $I + J \subset H$. Es decir, si un ideal contiene a I y a J, contiene a $I + J$.

Sean $I = \langle f_1, \ldots, f_r \rangle$ y $J = \langle g_1, \ldots, g_s \rangle$, tenemos que $\langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle \subset I + J$ por construcción. Por el párrafo anterior, como contiene a I y a J, $I + J \subset \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. □

Definición 4.3. Sean I y J ideales en $K[x_1, \ldots, x_n]$, definimos su producto como el ideal generado por todos los productos $f \cdot g$, donde $f \in I$ y $g \in J$.

Proposición 4.4. *Sean $I = \langle f_1, \ldots, f_r \rangle$ y $J = \langle g_1, \ldots, g_s \rangle$, entonces*

$$I \cdot J = \langle f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s \rangle.$$

Demostración. Está claro que $I \cdot J \supset \langle f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s \rangle$. Para demostrar la otra inclusión, tomamos un polinomio en $I \cdot J$ de la forma fg con $f \in I$ y $g \in J$. Escribimos f y g en términos de los generadores

$$f = a_1 f_1 + \cdots a_r f_r, \qquad g = b_1 g_1 + \cdots + b_s g_s.$$

Entonces fg, se puede escribir de la forma $\sum c_{ij} f_i g_j$, donde $c_{ij} \in K[x_1, \ldots, x_n]$. □

Si queremos tratar el caso de hallar la intersección de ideales, se complica un poco. Es claro que dados los ideales I y J de $K[x_1, \ldots, x_n]$, $I \cap J$ es un ideal, y que $I \cdot J \subset I \cap J$. Con el siguiente ejemplo, vemos que la otra inclusión no es cierta.

Ejemplo 4.5. Sean $I = J = \langle x, y \rangle$. Por una parte tenemos que $I \cdot J = \langle x^2, xy, y^2 \rangle$ y $I \cap J = \langle x, y \rangle$. Y estos ideales son distintos, ya que $x \notin I \cdot J$.

Teorema 4.6. *Sean I, J ideales en $K[x_1, \ldots, x_n]$. Entonces*

$$I \cap J = \big(tI + (1-t)J\big) \cap K[x_1, \ldots, x_n].$$

Demostración. Sea $f \in I \cap J$. Entonces $f = tf + (1-t)f \in tI + (1-t)J$.

Recíprocamente, sea $f \in \big(tI + (1-t)J\big) \cap K[x_1, \ldots, x_n]$. Entonces

$$f(x) = t \cdot \sum_{i=1}^{r} a_i(t, x) f_i(x) + (1-t) \sum_{j=1}^{s} b_j(t, x) g_j(x).$$

Ya que el polinomio f es independiente de t, tenemos $f = \sum_{i=1}^{r} a_i(1, x) f_i \in I$ y $f = \sum_{j=1}^{s} b_j(0, x) g_j \in J$ y por lo tanto $f \in I \cap J$. □

Este resultado nos da un algoritmo para calcular la intersección de ideales. Si $I = \langle f_1, \ldots, f_r \rangle$ y $J = \langle g_1, \ldots, g_s \rangle$, consideramos el ideal

$$\langle tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s \rangle \subset K[t, x_1, \ldots, x_n].$$

y calculamos una base de Gröbner respecto de un orden que elimina a t, y después calculamos el primer ideal de eliminación y por el Teorema de Eliminación (Teorema 3.4) tendremos una base de Gröbner de $I \cap J$. Veamos un ejemplo en `Singular`.

Ejemplo 4.7. Sean los ideales $I = \langle x, y \rangle$, $J = \langle y^2, z \rangle$. Primero calcularemos la intersección con la función propia de `Singular`, y después el método descrito anteriormente.

```
> ring R = 0,(x,y,z),lp;
> ideal I = x,y;
> ideal J = y^2,z;
> intersect(I, J);                    //función propia de Singular
_[1]=yz
_[2]=xz
_[3]=y2
```

```
> ring S = 0,(t,x,y,z),lp;
> ideal I = imap(R, I);
> ideal J = imap(R, J);
> ideal H = t*I + (1-t)*J;
> std(H);                        //base de Gröbner de t*I + (1-t)*J
_[1]=yz
_[2]=y2
_[3]=xz
_[4]=tz-z
_[5]=ty
_[6]=tx
```

Vemos que la base de Gröbner que nos da con el comando `std`, tiene tres polinomios que no incluyen a la variable t. Otra forma de eliminar la variable t directamente es con el comando `eliminate`.

```
> eliminate(H, t);               /Otra forma de eliminar variables
_[1]=yz
_[2]=y2
_[3]=xz
```

Como era de esperar, usando los tres métodos distintos nos da el mismo resultado.

Otra aplicación de conocer un algoritmo para la intersección de dos ideales, es que de manera inmediata tenemos un algoritmo para calcular el mínimo común múltiplo y máximo común divisor de dos polinomios, porque sabemos que

$$\langle f \rangle \cap \langle g \rangle = \langle \mathrm{LCM}(f, g) \rangle.$$

$$\mathrm{GCD}(f,g) = \frac{f \cdot g}{\mathrm{LCM}(f,g)}.$$

Definición 4.8. Sean I y J ideales en $K[x_1,\ldots,x_n]$. Llamamos ideal cociente al siguiente ideal

$$J : I = \{g \in K[x_1,\ldots,x_n] : gI \subset J\}.$$

Lema 4.9. *Sea J un ideal y $f \neq 0$ un polinomio de $K[x_1,\ldots,x_n]$. Entonces*

$$J : \langle f\rangle = \frac{1}{f}(J \cap \langle f\rangle).$$

Demostración. Si $g \in \frac{1}{f}(J\cap\langle f\rangle)$, entonces $gf \in J$, por lo tanto $g \in J : \langle f\rangle$. Por otra parte, si $g \in J : \langle f\rangle$, entonces $gf \in J$, lo que implica que $gf \in J\cap\langle f\rangle$, por lo tanto $g \in \frac{1}{f}(J\cap\langle f\rangle)$. □

Proposición 4.10. *Sea $I = \langle f_1,\ldots,f_s\rangle$ y J ideales en $K[x_1,\ldots,x_n]$. Entonces*

$$J : I = \bigcap_{i=1}^{s} J : \langle f_i\rangle.$$

Demostración. Si $g \in J : I$, entonces $gI \subset J$, así que en particular $gf_i \in J$ para $1 \leq i \leq s$, entonces $g \in \bigcap_{i=1}^{s} J : \langle f_i\rangle$. Por otra parte, si $g \in \bigcap_{i=1}^{s} J : \langle f_i\rangle$, entonces $g\langle f_i\rangle \subset J$ para todo $1 \leq i \leq s$, y por lo tanto $gI \subset J$, obteniendo que $g \in J : I$. □

Como sabemos calcular intersecciones de ideales, esta proposición y el Lema 4.9 nos dan un algoritmo para calcular ideales cocientes.

Ejemplo 4.11. Sean $I = \langle x, y\rangle$ y $J = \langle y^2, z\rangle$, calcularemos $J : I$ con `Singular` de dos maneras. La primera con un comando incorporado dentro del propio programa, y la segunda usando el algoritmo definido arriba.

```
> ring R = 0, (x,y), dp;                          //primer método
> ideal I = x^2, x+y;
> ideal J = x*(x+y)^2, y;
> quotient(J, I);
_[1]=y
_[2]=x2
```

```
ideal H1 = intersect(J, x^2)/x^2;                 //segundo método
> ideal H2 = intersect(J, x+y)/(x+y);
> intersect(H1, H2);
```

```
_[1]=y
_[2]=x2
```

Vemos que por ambos métodos, obtenemos que $J : I = \langle y, x^2 \rangle$.

Por último, intentaremos obtener información del radical de un ideal. En general, calcularlo es un problema complicado, pero podemos dar un criterio fácil de pertenencia a un radical.

Teorema 4.12. *Sea $I = \langle f_1, \ldots, f_s \rangle$ un ideal en $K[x_1, \ldots, x_n]$. Entonces $f \in \sqrt{I}$ si y solo si $1 \in \langle f_1, \ldots, f_s, 1 - yf \rangle \subset K[x_1, \ldots, x_n, y]$, donde y es una nueva variable.*

Demostración. Sea $\overline{K}$ la clausura algebraica de K, por el Teorema fuerte de los Ceros de Hilbert (Teorema 3.21) tenemos que $\sqrt{I} = \mathbf{I}\big(\mathbf{V}_{\overline{K}}(I)\big)$, y por lo tanto $f \in \sqrt{I}$ si y solo si $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in \mathbf{V}_{\overline{K}}(I)$. Sea $f \in \sqrt{I}$. Si $(a_1, \ldots, a_n, b) \in \mathbf{V}(\langle f_1, \ldots, f_s, 1 - yf \rangle)$, entonces

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

Pero como $(a_1, \ldots, a_n) \in \mathbf{V}_{\overline{K}}(I)$, tenemos que $f(a_1, \ldots, a_n) = 0$ lo que es una contradicción ya que $1 - bf(a_1, \ldots, a_n) = 1 \neq 0$. Entonces no hay puntos en $\mathbf{V}_{\overline{K}}$, así que $1 \in \langle f_1, \ldots, f_s, 1 - yf \rangle$.

Recíprocamente, sea $1 \in \langle f_1, \ldots, f_s, 1 - yf \rangle$. Entonces

$$1 = \sum_{i=1}^{s} h_i f_i + h(1 - yf),$$

con $h_i, h \in K[x_1, \ldots, x_n, y]$. Entonces para todo $(a_1, \ldots, a_n) \in \mathbf{V}_{\overline{K}}(I)$, tenemos que

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

Si $f(a_1, \ldots, a_n) \neq 0$, tomando $y = \dfrac{1}{f(a_1, \ldots, a_n)}$ obtenemos una contradicción. Entonces, $f(a_1, \ldots, a_n) = 0$, y por lo tanto $f \in \sqrt{I}$. □

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

Ejemplo 4.13. Sea $f = x + y + z$, y sea $I = \langle x^5, xy^2, y^7, z^3 + xyz \rangle \subset K[x, y, z]$ un ideal. Queremos ver usando `Singular` si $f \in \sqrt{I}$.

```
> ring R = 0,(x,y,z,t), dp;
> poly f = x + y + z;
> ideal I = x^5, x*y^3, y^7, z^3 + x*y*z, 1 - t*f;
> std(I);
_[1]=1
```

Por lo tanto, vemos que $f \in \sqrt{I}$.

4.2. Anillos cociente

En esta sección, vamos a obtener información del anillo cociente $K[x_1, \ldots, x_n]/I$, siendo $I \subset K[x_1, \ldots, x_n]$ un ideal.

Proposición 4.14. *Sean $f, g \in K[x_1, \ldots, x_n]$ y G una base de Gröbner del ideal $I \subset K[x_1, \ldots, x_n]$. Entonces*

$$f \equiv g \pmod{I} \text{ si y solo si } \overline{f}^G = \overline{g}^G.$$

Además, $\{\overline{f}^G : f \in K[x_1, \ldots, x_n]\}$ es el conjunto de clases de equivalencia del anillo cociente $K[x_1, \ldots, x_n]/I$. La aplicación $N_G : K[x_1, \ldots, x_n] \longrightarrow K[x_1, \ldots, x_n]$ que lleva a cada f a $\overline{f}^G$ es K-lineal.

Demostración. Por el Algoritmo de la División, existe $q \in I$ tal que $f = q + \overline{f}^G$, así que $f - \overline{f}^G \in I$. De este modo, $f + I = \overline{f}^G + I$ en $K[x_1, \ldots, x_n]/I$.

Veamos que la aplicación descrita es K-lineal. Sean $c_1, c_2 \in K$, y $f_1, f_2 \in K[x_1, \ldots, x_n]$, tenemos que $c_1 f_1 + c_2 f_2 - (c_1 \overline{f_1}^G + c_2 \overline{f_2}^G) \in I$ entonces por la unicidad del resto, $\overline{c_1 f + c_2 g}^G = \overline{c_1 \overline{f}^G + c_2 \overline{g}^G}^G = c_1 \overline{f}^G + c_2 \overline{g}^G$, quedando demostrado que es K-lineal.

Entonces, $f \equiv g \pmod{I}$ si y solo si existe $q \in I$ tal que $f = q + g$. Como la aplicación anterior es lineal, $\overline{f}^G = \overline{q}^G + \overline{g}^G$. Pero $\overline{q}^G = 0$ ya que $q \in I$, entonces $\overline{f}^G = \overline{g}^G$. Por otra parte si $\overline{f}^G = \overline{g}^G$, tenemos que $f - g = (f - \overline{f}^G) - (g - \overline{g}^G) \in I$, así que $f \equiv g \pmod{I}$. □

Proposición 4.15. *Una base del K-espacio vectorial $K[x_1, \ldots, x_n]/I$ está formada por el* 1 *unido a las clases de equivalencia de los monomios que no son múltiplos de ningún* $\mathrm{LT}(g_i)$ *para todo $g_i \in G$.*

Demostración. En la proposición anterior, vimos que para cualquier $f \in K[x_1, \ldots, x_n]$, $f + I = \overline{f}^G + I$ en $K[x_1, \ldots, x_n]/I$. Como $\overline{f}^G$ es resto de dividir entre G, es una combinación lineal de monomios tales que $\mathrm{LT}(g_i)$ no divide a ninguno para todo $g_i \in G$. Además, estos monomios son linealmente independientes por la unicidad del resto. □

Ejemplo 4.16. Sea $I \subset \mathbb{Q}[x, y]$ el ideal generado por $f_1 = x^2 y - y + x$ y $f_2 = xy^2 - x$. Una base de Gröbner con respecto al orden graduado lexicográfico con $y > x$, es $G = \{x^y - y + x, -y^2 + xy + x^2, x^3 + y - 2x\}$. Entonces, una base de $\mathbb{Q}[x, y]/I$ está formada por las clases de equivalencia de $1, x, y, x^2, xy$, y $\dim_{\mathbb{Q}}(\mathbb{Q}[x, y]/I) = 5$. También podemos construir fácilmente una tabla de multiplicar en $\mathbb{Q}[x, y]/I$. Por ejemplo, si queremos multiplicar $y + I$ por $xy + I$, basta con hallar $\overline{xy^2}^G = x$.

$\cdot$	1	x	y	x^2	xy
1	1	x	y	x^2	xy
x	x	x^2	xy	$-y+2x$	$y-x$
y	y	xy	$xy+x^2$	$y-x$	x
x^2	x^2	$-y+2x$	$y-x$	$-xy+2x^2$	$xy-x^2$
xy	xy	$y-x$	x	$xy-x^2$	x^2

Entonces, si por ejemplo queremos multiplicar $(2x^2+y)+I$ por $(3xy-5)+I$, $(2x^2+y)(3xy-5) = (6x^3y-10x^2+3xy^y-5y) \equiv 6(xy-x^2)-10x^2+3x-5y = 6xy-16x^2-5y+3x$ (mód I). De este modo, $\big((2x^2+y)+I\big)\big((3xy-5)+I\big) = (6xy-16x^2-5y+3x)+I$.

Teorema 4.17. *Sea K un cuerpo algebraicamente cerrado y sea el ideal $I \subset K[x_1,\ldots,x_n]$, con $G=\{g_1,\ldots,g_t\}$ su base de Gröbner reducida. Son equivalentes:*

(i) *La variedad $\mathbf{V}(I)$ es finita.*

(ii) *Para cada $i=1,\ldots,n$, existe $j\in\{1,\ldots,t\}$ tal que $\mathrm{LM}(g_j)=x_i^{\nu}$ para algún $\nu\in\mathbb{N}$.*

(iii) *La dimensión del K-espacio vectorial $K[x_1,\ldots,x_n]/I$ es finita.*

Demostración. (i) $\implies$ (ii). Sea $V=\mathbf{V}(I)$ finita. Si V es vacía, entonces por el Teorema débil de los Ceros de Hilbert (Teorema 3.18) $I=K[x_1,\ldots,x_n]$ y por lo tanto $G=\{1\}$, así que (ii) se satisface trivialmente. Supongamos que $V\neq\emptyset$. Sea $i\in\{1,\ldots,n\}$. Tomamos a_{ij}, $j=1,\ldots,\ell$ las distintas coordenadas i-ésimas de los puntos en V. Para cada $1\leq j\leq\ell$, sea $0\neq f_j\in K[x_i]$ tal que $f_j(a_{ij})=0$. Sea $f=f_1,\ldots,f_\ell\in K[x_i]\subset K[x_1,\ldots,x_n]$, $f\in\mathbf{I}(V)$, y por el Teorema fuerte de los Ceros de Hilbert (Teorema 3.21), existe un e tal que $f^e\in I$. Como $\mathrm{LM}(f^e)=x_i^{em}$ para algún $m\in\mathbb{N}$, y como G es base de Gröbner, existe un g_j tal que g_j divide a x_i^{em}. Esto es cierto para todo $i=1,\ldots,n$.

(ii) $\implies$ (iii). Es consecuencia inmediata de la Proposición 4.15.

(iii) $\implies$ (i). Sea $i\in\{1,\ldots,n\}$. Como $K[x_1,\ldots,x_n]/I$ tiene dimensión finita, las potencias $1,x_i,x_i^2,\ldots$ de x_i son linealmente dependientes módulo I. Entonces existe un

entero m y constantes $c_j \in K$, $0 \leq j \leq m$, alguna distinta de cero tales que

$$\sum_{j=0}^{m} c_j x_i^j \in I.$$

Como este polinomio tiene un número finito de raíces en K, solo hay un número finito de valores para la coordenada i-ésima de los puntos de V. Si hacemos esto para todas las coordenadas, obtenemos que solo hay un número finito de puntos en V. □

4.3. Funciones polinómicas

Otra aplicación directa de las bases de Gröbner, es que podemos conseguir información sobre el núcleo y la imagen de un homomorfismo de anillos de polinomios dado. Una transformación de este estilo

$$\phi : K[y_1, \ldots, y_m] \longrightarrow K[x_1, \ldots, x_n],$$

está únicamente determinada por

$$\phi : y_i \mapsto f_i,$$

donde $f_i \in K[x_1, \ldots, x_n]$, $1 \leq i \leq m$. Sea $h \in K[y_1, \ldots, y_m]$, si escribimos el polinomio del siguiente modo $h = \sum_\nu c_\nu y_1^{\nu_1} \cdots y_m^{\nu_m}$, donde $c_\nu \in K$, $\nu = (\nu_1, \ldots, \nu_m) \in \mathbb{N}^m$, y solo un número finito de c_ν son distintos de cero, tenemos

$$\phi(h) = \sum_\nu c_\nu f_1^{\nu_1} \cdots f_m^{\nu_m} = h(f_1, \ldots, f_m) \in K[x_1, \ldots, x_n].$$

Para dar una caracterización del núcleo, necesitamos un lema auxiliar previo.

Lema 4.18. *Sean $a_1, \ldots, a_n, b_1, \ldots, b_n$ elementos de un anillo conmutativo R. El elemento $a_1 \cdots a_n - b_1 \cdots b_n$ está en el ideal $\langle a_1 - b_1, \ldots, a_n - b_n \rangle$.*

Demostración. Usando el hecho de que

$$a_1 a_2 \cdots a_n - b_1 b_2 \cdots b_n = a_1(a_2 \cdots a_n - b_2 \cdots b_n) + b_2 \cdots b_n(a_1 - b_1),$$

podemos aplicar inducción y es inmediato. □

Teorema 4.19. *Sea $\phi : K[y_1, \ldots, y_m] \longrightarrow K[x_1, \ldots, x_n]$ un homomorfismo de anillos y sea el ideal $I = \langle y_1 - f_1, \ldots, y_m - f_m \rangle \subset K[y_1, \ldots, y_m, x_1, \ldots, x_n]$, siendo $f_i = \phi(y_i)$. Entonces,* $\ker(\phi) = I \cap K[y_1, \ldots, y_m]$.

Demostración. Veamos primero que $\ker(\phi) \supset I \cap K[y_1, \ldots, y_m]$. Sea $g \in I \cap K[y_1, \ldots, y_m]$. Entonces

$$g(y_1, \ldots, y_m) = \sum_{i=1}^{m} \big(y_i - f_i(x_1, \ldots, x_n)\big) h_i(y_1, \ldots, y_m, x_1, \ldots, x_n),$$

donde $h_i \in K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Entonces g es cero si la evaluamos en $(y_1, \ldots, y_m) = (f_1, \ldots, f_m)$, por lo tanto $g \in \ker(\phi)$.

Para ver la otra inclusión, sea $g \in \ker(\phi)$, lo podemos escribir como

$$g = \sum_{\nu} c_\nu y_1^{\nu_1} \cdots y_m^{\nu_m},$$

donde $c_\nu \in K$, $\nu = (\nu_1, \ldots, \nu_m) \in \mathbb{N}^m$ y solo un número finito de c_ν son distintos de cero. Como $g(f_1, \ldots, f_m) = 0$, tenemos que

$$g = g - g(f_1, \ldots, f_m) = \sum_{\nu} c_\nu (y_1^{\nu_1} \cdots y_m^{\nu_m} - f_1^{\nu_1} \cdots f_m^{\nu_m}).$$

Por el Lema 4.18, cada término de la suma anterior, está en el ideal I, por lo tanto $g \in I \cap K[y_1, \ldots, y_m]$. □

Con este teorema, obtenemos un método para computar una base de Gröbner del núcleo de un homomorfismo. Este algoritmo no es mas que calcular una base de Gröbner del ideal $I = \langle y_1 - f_1, \ldots, y_m - f_m \rangle$ usando un orden que elimine a las variables x. Los polinomios de la base en los que no intervengan las variables x, formaran una base de Gröbner del núcleo del homomorfismo.

Ejemplo 4.20. Sea $\phi : K[x, y, z] \longrightarrow K[a, b]$ un homomorfismo de anillos determinado por $\phi(x) = a^2$, $\phi(y) = ab$, $\phi(z) = b^2$. Calcularemos $\ker(\phi)$ usando `Singular` de dos maneras. La primera usando un comando incorporado dentro del propio programa, y la segunda usando el algoritmo definido arriba.

```
> ring R = 0, (x,y,z), lp;
> ring S = 0, (a,b), lp;
> map phi = R, a^2, ab, b^2;
> ideal zero;                                  //preimagen de cero
> setring R;
> preimage(S, phi, zero);            //función propia de Singular
_[1]=-xz+y2
```

```
> ring T = 0, (a,b,x,y,z), lp;
> ideal I = x-a^2, y-ab, z-b^2;
> std(I);
_[1]=xz-y2                                  //único polinomio en x,y,z
_[2]=b2-z
_[3]=az-by
_[4]=ay-bx
_[5]=ab-y
_[6]=a2-x
```

Vemos que por ambos métodos $\ker(\phi) = \langle xz - y^2 \rangle$.

Teorema 4.21. *Sea $I = \langle y_1 - f_1, \ldots, y_m - f_m \rangle \subset K[y_z, \ldots, y_m, x_1, \ldots x_n]$ el ideal considerado en el Teorema 4.19 y sea G una base de Gröbner reducida de I respecto un orden que elimina a las variables x. Entonces $f \in K[x_1, \ldots, x_n]$ está en la imagen de ϕ si y solo si existe $h \in K[y_1, \ldots, y_m]$ tal que $\overline{f}^G = h$. En este caso, $f = \phi(h) = h(f_1, \ldots, f_m)$.*

Demostración. Sea $f \in K[x_1, \ldots, x_n]$ un elemento de $\mathrm{im}(\phi)$. Entonces $f = g(f_1, \ldots, f_m)$ para algún $g \in K[y_1, \ldots, y_m]$. Consideramos el polinomio

$$f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) \in K[y_1, \ldots, y_m, x_1, \ldots, x_n].$$

Como $f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) = g(f_1, \ldots, f_m) - g(y_1, \ldots, y_m)$, usando el Lema 4.18 vemos que $f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) \in I$. Por la Proposición 4.14, $\overline{g}^G = \overline{f}^G = h$. Como $g \in K[y_1, \ldots, y_m]$ y las variables x son siempre mayores que las variables y, obtenemos que $h \in K[y_1, \ldots, y_m]$.

Por otra parte, sea f tal que $\overline{f}^G = h$, donde $h \in K[y_1, \ldots, y_m]$. Entonces $f - h \in I$, así que

$$f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) = \sum_{i=1}^{m} g_i(y_1, \ldots, y_m, x_1, \ldots, x_n)\big(y_i - f_i(x_1, \ldots, x_n)\big).$$

Si sustituimos los y_i por f_i, vemos que $f = h(f_1, \ldots, f_m) = \phi(h)$, así que f está en la imagen de ϕ. □

Corolario 4.22. *En las condiciones del teorema anterior, $f \in K[x_1, \ldots, x_n]$ está en la imagen de ϕ si y solo si $\overline{f}^G \in K[y_1, \ldots, y_m]$.*

Demostración. Es consecuencia inmediata del teorema anterior y de la Proposición 4.14. □

De este modo, tenemos un algoritmo para saber si un polinomio pertenece a la imagen de un homomorfismo o no.

Ejemplo 4.23. Volviendo al Ejemplo 4.20, queremos saber si los polinomios $a+b^2$ y a^2+ab^3 pertenecen a la imagen de ϕ. Usamos el algoritmo estudiado, ayudados por `Singular` y obtenemos

```
> ring T = 0,(a,b,x,y,z), lp;
> ideal I = x-a^2,y-ab,z-b^2;
> option(redSB);
> ideal G = std(I);
> reduce(a+b^2, G);
a+z                                    //no pertenece a la imagen
> reduce(a^2+a*b^3, G);
x+yz                                      //pertenece a la imagen
```

Una vez conocido el algoritmo anterior, podemos dar una condición para saber si un homomorfismo es sobreyectivo. Basta con comprobar si $x_1, \ldots, x_n$ pertenecen a la imagen. Con el siguiente resultado podemos averiguarlo simplemente inspeccionando la base de Gröbner.

Teorema 4.24. *Sea $I = \langle y_1 - f_1, \ldots, y_m - f_m \rangle \subset K[y_1, \ldots, y_m, x_1, \ldots, x_n]$ el ideal considerado en el Teorema 4.19, y sea G la base de Gröbner reducida de I respecto un orden que elimina las variables x. Entonces ϕ es sobreyectiva si y solo si para cada $1 \leq i \leq n$, existe $g_i \in G$ de la forma $g_i = x_i - h_i$, con $h_i \in K[y_1, \ldots, y_m]$. En este caso, $x_i = h_i(f_1, \ldots, f_m)$.*

Demostración. Supongamos primero que ϕ es sobreyectiva. Sin pérdida de generalidad, podemos suponer que el orden es tal que $x_n > \cdots > x_1$. Por el Teorema 4.21, como $x_1 \in \mathrm{im}(\phi)$, existe $\tilde{h}_1 \in K[y_1, \ldots, y_m]$ tal que $\overline{x_1}^G = \tilde{h}_1$. De este modo, $x_1 - \tilde{h}_1 \in I$, y por lo tanto existe $g_1 \in G$ tal que $\mathrm{LT}(g_1)$ divide a $\mathrm{LT}(x_1 - \tilde{h}_1) = x_1$. Además, como todos los términos estrictamente menores que x_1 son términos en variables y, $g_1 = x_1 - h_1$ para algún $h_1 \in K[y_1, \ldots, y_m]$. De modo similar, como x_2 está en la imagen, existe $\tilde{h}_2 \in K[y_1, \ldots, y_m]$ tal que $\overline{x_2}^G = \tilde{h}_2$, así que existe $g_2 \in G$ tal que $\mathrm{LT}(g_2)$ divide a $\mathrm{LT}(x_2 - \tilde{h}_2) = x_2$. Como los únicos términos estrictamente menores que x_2 son términos en variables x_1 y en variables y, como G es reducida, cualquier término que tenga a x_1 podría ser reducido usando $g_1 = x_1 - h_1$, entonces tenemos que $g_2 = x_2 - h_2$ para algún $h_2 \in K[y_1, \ldots, y_m]$. Aplicando esto para todos los x_i que existen $g_i \in G$ de la forma del enunciado.

Para ver la otra implicación, tenemos que ver que $x_i \in \mathrm{im}(\phi)$ para todo $1 \leq i \leq n$. Como $x_i - h_i \in G$, tenemos que $\overline{x_i}^G = h_i$. Como h_i es un polinomio que solo contiene a las variables y, tenemos que ese x_i está en la imagen de ϕ por el Teorema 4.21, y por lo tanto ϕ es sobreyectiva. Obtenemos también por el Teorema 4.21 que $x_i = h_i(f_1, \ldots, f_m)$. □

Ejemplo 4.25. Sea el homomorfismo $\phi : \mathbb{Q}[x, y, z] \longrightarrow \mathbb{Q}[a]$ definido por $\phi(x) = a^4 + a$,

$\phi(y) = a^3$, $\phi(z) = a^5$. Veamos si ϕ es sobreyectiva. Una base de Gröbner del ideal $I = x - a^4 - a, y - a^3, z - a^5$ con el orden lexicográfico $a > x > y > z$ es

$$G = \{y^5 - z^3, xz - y^3 - y^2, xy^3 - yz^2 - z^2, x^2y - y^2z - 2yz - z,$$

$$x^3 - y^4 - 3y^3 - 3y^2 - y, a - xy^2 + xy - x + z^2\}.$$

Como $a - xy^2 + xy - z + z^2 \in G$, por el Teorema 4.24 el homomorfismo ϕ es sobreyectivo. De hecho, tenemos que $a = \phi(xy^2 + xy - x + z^2) = (a^4 + a)(a^3)^2 - (a^4 + a)a^3 + a^4 + a - (a^5)^2$.

Ahora extenderemos los resultados obtenidos a homomorfismos entre anillos cociente. Sean $J \subset K[y_1, \ldots, y_m]$, $I \subset K[x_1, \ldots, x_n]$ ideales y un homomorfismo de anillos

$$\phi : K[y_1, \ldots, y_m]/J \longrightarrow K[x_1, \ldots, x_n]/I.$$

Este homomorfismo está definido por los valores $\phi(y_i + J) = f_i + I$, estará bien definido si se satisface la siguiente condición:

$$\text{si } J = \langle g_1, \ldots g_t \rangle, \text{ para cada } 1 \leq i \leq t, \ g_i(f_1, \ldots f_m) \in I.$$

Veamos las generalizaciones del Teorema 4.19 y del Teorema 4.21.

Teorema 4.26. *Sea* $H = \langle I, y_1 - f_1, \ldots, y_m - f_m \rangle \subset K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. *Entonces,* $\ker(\phi) = H \cap K[y_1, \ldots, y_m]$ (mód J). *Es decir, si* $H \cap K[y_1, \ldots, y_m] = \langle \tilde{f}_1, \ldots, \tilde{f}_p \rangle$, *entonces* $\ker(\phi) = \langle \tilde{f}_1 + J, \ldots, \tilde{f}_p + J \rangle$.

Demostración. Sea $\tilde{f} \in H \cap K[y_1, \ldots, y_m]$. Podemos escribirlo de forma

$$\begin{aligned} \tilde{f}(y_1, \ldots, y_m) = &\sum_{i=1}^{m} \big(y_i - f_i(x_1, \ldots, x_n)\big) h_i(y_1, \ldots, y_m, x_1, \ldots, x_n) \\ &+ w(y_1, \ldots, y_m, x_1, \ldots, x_n), \end{aligned}$$

donde

$$w(y_1, \ldots, y_m, x_1, \ldots, x_n) = \sum_{\nu} u_\nu(y_1, \ldots, y_m, x_1, \ldots, x_n) v_\nu(x_1, \ldots, x_n),$$

con $v_\nu \in I$ y $h_i, u_\nu \in K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Entonces

$$\phi(\tilde{f} + J) = \tilde{f}(f_1, \ldots, f_m) + I = w(f_1, \ldots, f_m, x_1, \ldots, x_n) + I = 0,$$

ya que $v_\nu \in I$ y

$$w(f_1, \ldots, f_m, x_1, \ldots, x_n) = \sum_{\nu} u_\nu(f_1, \ldots, f_m, x_1, \ldots, x_n) v_\nu(x_1, \ldots, x_n) \in I.$$

Para ver la otra implicación, tomamos $\tilde{f} \in K[y_1, \ldots, y_m]$ con $\phi(\tilde{f} + J) = 0$. Entonces $\tilde{f}(f_1, \ldots, f_m) \in I$. Sea $\tilde{f}(y_1, \ldots, y_m) = \sum_\nu c_\nu y_1^{\nu_1} \cdots y_m^{\nu_m}$, donde $\nu = (\nu_1, \ldots, \nu_m) \in \mathbb{N}^m$, $c_\nu \in K$, y solo un número finito de c_ν son distintos de cero. Entonces,

$$\begin{aligned}\tilde{f}(y_1, \ldots, y_m) =& \big(\tilde{f}(y_1, \ldots, y_m) - \tilde{f}(f_1, \ldots, f_m)\big) + \tilde{f}(f_1, \ldots, f_m) \\ =& \sum_\nu c_\nu (y_1^{\nu_1} \cdots y_m^{\nu_m} - f_1^{\nu_1} \cdots f_m^{\nu_m}) + \tilde{f}(f_1, \ldots, f_m).\end{aligned}$$

Por el Lema 4.18

$$\sum_\nu c_\nu (y_1^{\nu_1} \cdots y_m^{\nu_m} - f_1^{\nu_1} \cdots f_m^{\nu_m}),$$

está en el ideal $\langle y_1 - f_1, \ldots, y_m - f_m \rangle$ y por lo tanto

$$\tilde{f}(y_1, \ldots, y_m) \in \langle I, y_1 - f_1, \ldots, y_m - f_m \rangle = H,$$

ya que $\tilde{f}(f_1, \ldots, f_m) \in I$. De este modo, $\tilde{f}(y_1, \ldots, y_m) \in H \cap K[y_1, \ldots, y_m]$. □

Teorema 4.27. *Sea $H = \langle I, y_1 - f_1, \ldots, y_m - f_m \rangle$ el mismo ideal que en el teorema anterior, y sea G una base de Gröbner de H respecto un orden que elimina las variables x. Entonces $f + I \in K[x_1, \ldots, x_n]/I$ está en la imagen de ϕ si y solo si existe $h \in K[y_1, \ldots, y_m]$ tal que $\overline{f}^G = h$. En este caso $f + I = \phi(h + J) = h(f_1, \ldots, f_m) + I$.*

Demostración. Sea $f + I \in \mathrm{im}(\phi)$. Existe un polinomio $g \in K[y_1, \ldots, y_m]$ tal que $f - g(f_1, \ldots, f_m) \in I$. Sea el polinomio $f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) \in K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Como se cumple que

$$f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) = g(f_1, \ldots, f_m) - g(y_1, \ldots, y_m) + \big(f(x_1, \ldots, x_n) - g(f_1, \ldots, f_m)\big)$$

usando el Lema 4.18, tenemos que $f(x_1, \ldots, x_n) - g(y_1, \ldots, y_m) \in H$. Por la Proposición 4.14, $\overline{g}^G = \overline{f}^G = h$. Como $g \in K[y_1, \ldots, y_m]$ y las variables x son siempre mayores que las variables y, obtenemos que $h \in K[y_1, \ldots, y_m]$.

Por otra parte, sea f tal que $\overline{f}^G = h$, donde $h \in K[y_1, \ldots, y_m]$. Entonces $f - h \in H$, y

$$f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) =$$

$$\sum_{i=1}^{m} g_i(y_1, \ldots, y_m, x_1, \ldots, x_n)\big(y_i - f_i(x_1, \ldots, x_n)\big) + w(y_1, \ldots, y_m, x_1, \ldots, x_n),$$

donde

$$w(y_1, \ldots, y_m, x_1, \ldots, x_n) = \sum_\nu u_\nu(y_1, \ldots, y_m, x_1, \ldots, x_n) v_\nu(x_1, \ldots, x_n),$$

con $v_\nu \in I$ y $g_i, u_\nu \in K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Si sustituimos los y_i por f_i, vemos que $f - h(f_1, \ldots, f_m) \in I$, y por lo tanto $f + I = \phi(h + J)$. □

Corolario 4.28. *Continuando con la notación del teorema anterior, tenemos que* $f + I \in K[x_1, \ldots, x_n]/I$ *está en la imagen del homomorfismo* ϕ *si y solo si* $\overline{f}^G \in K[y_1, \ldots, y_m]$.

Teorema 4.29. *Sea* $H = \langle I, y_1 - f_1, \ldots, y_m - f_m \rangle \subset K[y_1, \ldots, y_m, x_1, \ldots, x_n]$ *el ideal del Teorema 4.26, y sea* G *la base de Gröbner reducida de* H *respecto de un orden que elimina las variables* x. *Entonces* ϕ *es sobreyectiva si y solo si para cada* $1 \leq i \leq n$, *existe* $g_i \in G$ *de la forma* $g_i = x_i - h_i$, *con* $h_i \in K[y_1, \ldots, y_m]$.

Demostración. La prueba es análoga a la del Teorema 4.24. □

Capítulo 5

Otras aplicaciones

En este capítulo, trataremos otro tipo de aplicaciones, que salen de los anillos de polinomios. Primero trataremos de calcular el polinomio mínimo en extensiones de cuerpos. Después expondremos el tema de las demostraciones automáticas en geometría euclidiana, que es un modo de demostrar teoremas usando directamente ideales, y por último aplicaremos las bases de Gröbner a la teoría de grafos, y en particular a los conocidos Sudokus.

5.1. Polinomio mínimo en extensiones de cuerpos

Nuestro objetivo en esta sección es calcular el polinomio mínimo de un elemento algebraico sobre un cuerpo k. Sea $k \subset K$ una extensión de cuerpos.

Definición 5.1. Sea $\alpha \in K$ algebraico sobre k. El polinomio mínimo de α sobre k es el polinomio mónico p en una variable, con coeficientes en k, de menor grado tal que $p(\alpha) = 0$.

Si consideramos el homomorfismo $\phi : k[x] \longrightarrow k(\alpha)$ definido por $\phi(x) = \alpha$, tenemos que $\ker(\phi) = \langle p \rangle$. Además, como α es algebraico,

$$k[x]/\langle p \rangle \cong k(\alpha),$$

con la función que lleva a $x + \langle p \rangle$ a α.

Consideraremos primero el caso en el que $K = k(\alpha)$, con α algebraico sobre k, y nuestro objetivo es calcular el polinomio mínimo de cualquier $\beta \in K$, suponiendo que conocemos el polinomio mínimo p de α.

Teorema 5.2. *Sea $k \subset K$ una extensión de cuerpos, y sea $\alpha \in k$ algebraico sobre k. Sea $p \in k[x]$ el polinomio mínimo de α sobre k. Sea $0 \neq \beta \in k(\alpha)$ de la forma,*

$$\beta = \frac{a_0 + a_1\alpha + \cdots + a_n\alpha^n}{b_0 + b_1\alpha + \cdots + b_m\alpha^m},$$

donde $a_i, b_j \in k$ *para todo* $0 \leq i \leq n$, $0 \leq j \leq m$. *Sea* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *y* $g(x) = b_0 + b_1x + \cdots + b_mx^m$ *los polinomios correspondientes en* $k[x]$. *Consideramos el ideal* $J = \langle p, gy - f\rangle$ *de* $k[x, y]$. *Entonces el polinomio mínimo de* β *sobre* k *es el polinomio mónico que genera el ideal* $J \cap k[y]$.

Demostración. Como p es irreducible, $k[x]/\langle p\rangle$ es un cuerpo, y como $g(\alpha) \neq 0$, existe un polinomio $\ell \in k[x]$ tal que $g\ell \equiv 1 \pmod{\langle p\rangle}$, es decir $g\ell - 1 \in \langle p\rangle$. Sea $h = f\ell$, vemos que $h(\alpha) = \beta$. Consideramos ahora ϕ, la composición de los homomorfismos:

$$\begin{array}{rccccc} \phi: & k[y] & \longrightarrow & k[x]/\langle p\rangle & \longrightarrow & k(\alpha) \\ & y & \longmapsto & h + \langle p\rangle & \longmapsto & \beta. \end{array}$$

Nuestro objetivo, es calcular el núcleo de esta aplicación ϕ, ya que $q \in \ker(\phi)$ si y solo si $q(\beta) = 0$. Además, el núcleo es un ideal generado por un solo elemento, ya que $k[y]$ es un dominio de ideales principales al ser k cuerpo. Entonces, si hallamos el núcleo, tenemos resuelto el problema. Además, por el Teorema 4.26, el núcleo de ϕ es $\langle p, y - h\rangle \cap k[y]$, así que basta con demostrar que $\langle p, y - h\rangle = \langle p, gy - f\rangle$.

Por un lado $y - h = y - f\ell \equiv \ell(gy - f) \pmod{\langle p\rangle}$, así que $y - h \in \langle p, gy - f\rangle$. Por otra parte, $gy - f \equiv g(y - f\ell) = g(y - h) \pmod{\langle p\rangle}$. Entonces $gy - f \in \langle p, y - h\rangle$. □

Este resultado, nos da un algoritmo para encontrar el polinomio mínimo de β en $k(\alpha)$. Dados α y β como en el teorema, calculamos la base de Gröbner reducida G del ideal $\langle p, gy - f\rangle \subset k[x, y]$ respecto el orden lexicográfico con $x > y$. El polinomio de G en el que no interviene la variable x es el polinomio mínimo de β.

Ejemplo 5.3. Sea la extensión de cuerpos $\mathbb{Q} : \mathbb{Q}(\alpha)$, donde α es una raíz del polinomio irreducible $x^5 - x - 2$. Consideramos el elemento $\beta = \dfrac{x - \alpha - 2\alpha^3}{\alpha} \in \mathbb{Q}(\alpha)$. Queremos encontrar el polinomio mínimo de β. Sea el ideal $J = \langle x^5 - x - 2, xy + 2x^3 + x - 1\rangle \subset \mathbb{Q}[x, y]$. Calculamos la base de Gröbner reducida de J respecto el orden lexicográfico con $x > y$

```
> ring R = 0,(x,y), lp;
> ideal I = x^5 - x - 2, x*y + 2*x^3 + x - 1;
> option(redSB);
> std(I);
_[1]=2y5+11y4+8y3-10y2+190y+518
_[2]=45887x-1438y4-2183y3+10599y2-8465y-101499
> _[1]/2;
y5+11/2y4+4y3-5y2+95y+259
```

Entonces el polinomio mínimo de β es $y^5 + \frac{11}{2}y^4 + 4y^3 - 5y^2 + 95y + 259$.

Esta técnica se puede extender al caso general de extensiones de cuerpos de la forma $K = k(\alpha_1, \ldots, \alpha_n)$. Usaremos la siguiente notación en esta sección. Para cada $i = 2, \ldots, n$ y $p \in k(\alpha_1, \ldots, \alpha_{i-1})[x_i]$, llamamos $\overline{p}$ a un polinomio de $k[x_1, \ldots, x_i]$ tal que $\overline{p}(\alpha_1, \ldots, \alpha_{i-1}, x_i) = p$. Cabe notar que $\overline{p}$ no tiene por que ser único. Veamos ahora un resultado similar al Teorema 5.2.

Teorema 5.4. *Sea $K = k(\alpha_1, \ldots, \alpha_n)$ una extensión algebraica de k. Para cada $i = 1, \ldots, n$, sea $p_i \in k(\alpha_1, \ldots, \alpha_{i-1})[x_i]$ el polinomio mínimo de α_i sobre $k(\alpha_1, \ldots, \alpha_{i-1})$. Sea $\beta \in k(\alpha_1, \ldots, \alpha_n)$, de la forma*

$$\beta = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)},$$

donde $f, g \in k[x_1, \ldots, x_n]$. Consideramos el ideal $J = \langle \overline{p}_1, \ldots, \overline{p}_n, gy - f \rangle \subset k[x_1, \ldots, x_n, y]$. Entonces el polinomio mínimo de β sobre k es el polinomio mónico que genera el ideal $J \cap k[y]$.

Demostración. Primero demostraremos que

$$k[x_1, \ldots, x_n]/\langle \overline{p}_1, \ldots, \overline{p}_n \rangle \cong k(\alpha_1, \ldots, \alpha_n),$$

usando el homomorfismo

$$\phi_n : k[x_1, \ldots, x_n] \longrightarrow k(\alpha_1, \ldots, \alpha_n),$$

que lleva cada x_i a α_i. Como los $\alpha_1, \ldots, \alpha_n$ son algebraicos sobre k, ϕ_n es sobreyectiva.

Veamos ahora por inducción que $\ker(\phi_n) = \langle \overline{p}_1, \ldots, \overline{p}_n \rangle$. Es inmediato que los $\overline{p}_1, \ldots, \overline{p}_n$ pertenecen al núcleo de la función por construcción. Sea ahora $f \in k[x_1, \ldots, x_n]$ tal que $f(\alpha_1, \ldots, \alpha_n) = 0$. Sea

$$h(x_n) = f(\alpha_1, \ldots, \alpha_{n-1}, x_n) \in k(\alpha_1, \ldots, \alpha_{n-1})[x_n].$$

Como $h(\alpha_n) = 0$, tenemos que p_n divide a h. Sea $h = p_n \ell_n$, para algún elemento $\ell \in k(\alpha_1, \ldots, \alpha_{n-1})[x_n]$. Consideramos $f - \overline{p}_n \ell_n \in k[x_1, \ldots, x_n]$ y escribimos

$$f - \overline{p}\overline{\ell}_n = \sum_{\nu} g_\nu(x_1, \ldots, x_{n-1}) x_n^\nu.$$

Entonces

$$(f - \overline{p}_n \overline{\ell}_n)(\alpha_1, \ldots, \alpha_{n-1}, x_n) = h - p_n \ell_n = 0,$$

y vemos que para todo ν, $g_\nu(\alpha_1, \ldots, \alpha_{n-1}) = 0$. Además, $g_\nu(x_1, \ldots, x_{n-1})$ está en el núcleo

$$\phi_{n-1} : k[x_1, \ldots, x_{n-1}] \longrightarrow k(\alpha_1, \ldots, \alpha_{n,1}),$$

y por inducción

$$g_\nu(x_1,\ldots,x_{n-1}) \in \langle \overline{p}_1,\ldots,\overline{p}_{n-1}\rangle.$$

Entonces, $f - \overline{p}_n\overline{\ell}_n \in \langle \overline{p}_1,\ldots,\overline{p}_{n-1}\rangle$, y $f \in \langle \overline{p}_1,\ldots,\overline{p}_n\rangle$.

Una vez llegados a este punto, la demostración continúa como en el Teorema 5.2. □

Ejemplo 5.5. Sea la extensión de cuerpos $\mathbb{Q} : \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. El polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es $p_1 = x_1^2 - 2 \in \mathbb{Q}[x_1]$, y el polinomio mínimo de $\sqrt[3]{5}$ sobre $\mathbb{Q}(\sqrt{2})$ es $p_2 = x_2^3 - 5 \in \mathbb{Q}(\sqrt{2})[x_2]$. Queremos encontrar el polinomio mínimo de $\sqrt{2} + \sqrt[3]{5}$. Calculamos la base de Gröbner del ideal

$$J = \langle \overline{p}_1, \overline{p}_2, y - (x_1 + x_2)\rangle = \langle x_1^2 - 2, x_2^3 - 5, y - (x_1 + x_2)\rangle \subset \mathbb{Q}[x_1, x_2, y],$$

respecto el orden lexicográfico con $x_1 > x_2 > y$

```
> ring R = 0,(x1, x2, y), lp;
> ideal I = x1^2 - 2, x2^3 - 5, y - (x1 + x2);
> option(redSB);
> std(I);
_[1]=y^6-6*y^4-10*y^3+12*y^2-60*y+17
_[2]=1187*x2+48*y^5+45*y^4-320*y^3-780*y^2-452*y-1820
_[3]=1187*x1-48*y^5-45*y^4+320*y^3+780*y^2-735*y+1820
```

Entonces vemos que el polinomio mínimo de $\sqrt{2} + \sqrt[3]{5}$ sobre $\mathbb{Q}$ es $y^6 - 6y^4 - 10y^3 + 12y^2 + 60y + 17$.

Por último, daremos un teorema que nos dejará un algoritmo para saber si dos extensiones $k(\beta)$ y $k(\alpha_1,\ldots,\alpha_n)$ son iguales.

Teorema 5.6. *Sean $\alpha_1,\ldots,\alpha_n$ y sean $\overline{p}_1,\ldots,\overline{p}_n$ de la forma del Teorema 5.4. Sea $\beta \in k(\alpha_1,\ldots,\alpha_n)$, con $\beta = \dfrac{f(\alpha_1,\ldots,\alpha_n)}{g(\alpha_1,\ldots,\alpha_n)}$, siendo $f, g \in k[x_1,\ldots,x_n]$. Sea $J = \langle \overline{p}_1,\ldots,\overline{p}_n, gy - f\rangle \subset k[x_1,\ldots,x_n,y]$ respecto un orden que elimina las variables x. Entonces $k(\alpha_1,\ldots,\alpha_n) = k(\beta)$ si y solo si para cada $i = 1,\ldots,n$, existe un polinomio $g_i \in G$ tal que $g_i = x_i - h_i$, para algún $h_i \in k[y]$. En este caso, $\alpha_i = h_i(\beta)$.*

Demostración. Sea $I = \langle \overline{p}_1,\ldots,\overline{p}_n\rangle$ y sea $\ell \in k[x_1,\ldots,x_n]$ tal que $g\ell - 1 \in I$. Sea $h = f\ell$, y sabiendo que $h(\alpha_1,\ldots,\alpha_n) = \beta$, consideramos

$$\begin{array}{rccccc} \phi: & k[y] & \longrightarrow & k[x]/I & \longrightarrow & k(\alpha) \\ & y & \longmapsto & h + I & \longmapsto & \beta. \end{array}$$

Entonces $k(\alpha_1, \ldots, \alpha_n) = k(\beta)$ si y solo si ϕ es sobreyectiva. Así, $J = \langle I, y - h \rangle$ y por el Teorema 4.29 queda demostrado el enunciado. □

Ejemplo 5.7. Siguiendo el Ejemplo 5.5, vemos que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{5})$, ya que la base de Gröbner calculada, nos queda de la forma del teorema anterior. Además, nos da una forma de calcular los elementos en función de la base

$$\sqrt{2} = \frac{1}{1187}\Big(48(\sqrt{2}+\sqrt[3]{5})^5 + 45(\sqrt{2}+\sqrt[3]{5})^4 - 320(\sqrt{2}+\sqrt[3]{5})^3$$
$$-780(\sqrt{2}+\sqrt[3]{5})^2 + 735(\sqrt{2}+\sqrt[3]{5}) - 1820\Big),$$

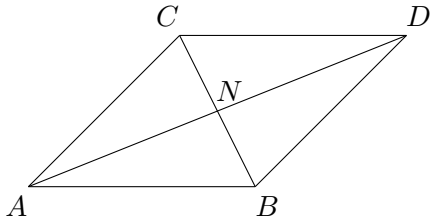
y

$$\sqrt[3]{5} = \frac{1}{1187}\Big(- 48(\sqrt{2}+\sqrt[3]{5})^5 - 45(\sqrt{2}+\sqrt[3]{5})^4 + 320(\sqrt{2}+\sqrt[3]{5})^3$$
$$+780(\sqrt{2}+\sqrt[3]{5})^2 + 452(\sqrt{2}+\sqrt[3]{5}) + 1820\Big).$$

5.2. Demostraciones automáticas en Geometría Euclidiana

En esta sección, trataremos dos métodos algorítmicos que nos determinarán la veracidad o falsedad de diferentes afirmaciones en geometría euclidiana. En los últimos años, varios problemas han sido resueltos gracias a "demostradores de teoremas" y estos métodos tienen el potencial de resolver muchos problemas geométricos. La idea básica es que una vez introducimos coordenadas cartesianas en el plano, expresar las hipótesis y las conclusiones como ecuaciones polinómicas. Veamos un ejemplo introductorio.

Ejemplo 5.8. Sean A, B, C, D los vértices de un paralelogramo, y N el punto de corte de sus diagonales.



Un teorema clásico, es que las diagonales $\overline{AD}$ y $\overline{BC}$ de cualquier paralelogramo, se cortan en un punto N que es el punto medio de ambas diagonales. Es decir, $AN = DN$ y $BN = CN$, donde XY denota la longitud del segmento $\overline{XY}$. La prueba geométrica de este teorema, esta basada en demostrar que los triángulos $\triangle ANC$ y $\triangle BND$ son congruentes.

Las propiedades de los paralelogramos son invariantes por traslaciones y rotaciones en el plano, así que haremos transformaciones de este estilo. Situamos el vértice A en el origen, y el segmento $\overline{AB}$ en el eje x. Es decir, $A = (0, 0)$ y $B = (u_1, 0)$ para algún $u_1 \in \mathbb{R} - \{0\}$. Esto quiere decir, que u_1 es una variable indeterminada que podemos escoger en todo $\mathbb{R} - \{0\}$. El vértice C puede ser cualquier punto $C = (u_2, u_3)$ con $u_3 \neq 0$. El vértice D está completamente determinado por las elecciones de A, B y C.

Para las coordenadas que sean arbitrarias, usaremos las variables u_i, y las coordenadas que estén estrictamente determinadas, las nombraremos con las variables x_i. Como D está completamente determinado, escribiremos $D = (x_1, x_2)$. Una hipótesis de nuestro teorema, es que el cuadrilátero $ABCD$ es un paralelogramo, es decir, que los lados opuestos son paralelos. Usando la fórmula de la tangente, vemos que podemos traducir del siguiente modo:

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

Sacando denominadores, obtenemos

$$\begin{aligned} h_1 &= x_2 - u_3 = 0, \\ h_2 &= (x_1 - u_1)u_3 - x_2 u_2 = 0. \end{aligned}$$

El punto N también está completamente determinado por los datos que ya tenemos, así que escribiremos $N = (x_3, x_4)$. Como N es la intersección de las diagonales, N está en los segmentos $\overline{AD}$ y $\overline{BC}$, es decir, las ternas de puntos A, N, D y B, N, C son colineales. Usando otra vez la fórmula de la tangente

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

Sacando denominadores, obtenemos

$$\begin{aligned} h_3 &= x_4 x_1 - x_3 u_3 = 0, \\ h_4 &= x_4(u_2 - u_1) - (x_3 - u_1)u_3 = 0. \end{aligned}$$

El sistema de cuatro ecuaciones formado por h_1, h_2, h_3 y h_4 nos da las hipótesis de nuestro teorema. Las conclusiones pueden ser escritas en forma polinómica usando el Teorema de

Pitágoras y elevando al cuadrado

$$AN = ND : x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2,$$
$$BN = NC : (x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2.$$

Operando, obtenemos las ecuaciones

$$g_1 = x_1^2 - 2x_1x_3 - 2x_4x_2 + x_2^2 = 0,$$
$$g_2 = 2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2 = 0.$$

Entonces, nuestro teorema dice que cuando se cumplen las ecuaciones h_1, h_2, h_3 y h_4, se cumplen las ecuaciones g_1 y g_2. Cabe considerar que las traducciones de las hipótesis o a conclusiones, no son únicas. Por ejemplo, la hipótesis de $\overline{AB} \parallel \overline{CD}$, podemos expresarla simplemente diciendo que D es la suma de los vectores $B = (u_1, 0)$ y $C = (u_2, u_3)$. Si $D = (x_1, x_2)$ la traducción alternativa sería

$$h_1' = x_1 - u_1 - u_2 = 0,$$
$$h_2' = x_2 - u_3 = 0.$$

Ejemplo 5.9. Sean $A = (a_1, a_2)$, $B = (b_1, b_2)$, $C = (c_1, c_2)$, $D = (d_1, d_2)$ puntos en el plano. Vamos a expresar las siguientes propiedades geométricas usando ecuaciones polinómicas.

(i) $\overline{AB}$ es paralelo a $\overline{CD}$:

$$(b_2 - a_2)(d_1 - c_1) = (b_1 - a_1)(d_2 - c_2)$$

(ii) $\overline{AB}$ es perpendicular a $\overline{CD}$:

$$(b_1 - a_1)(d_1 - c_1) + (b_2 - a_2)(d_2 - c_2) = 0$$

(iii) A, B, y C son colineales:

$$(c_2 - a_2)(b_1 - a_1) = (b_2 - a_2)(c_1 - a_1)$$

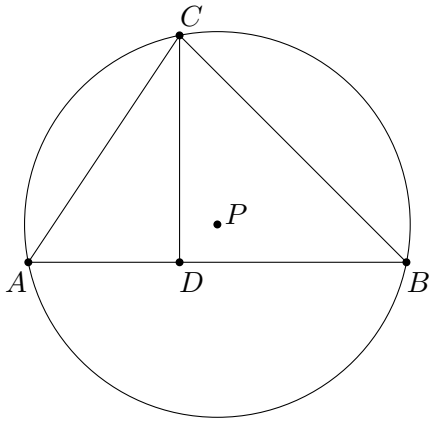
(iv) La distancia de A a B es igual a la distancia de C a D ($AB = CD$):

$$(b_1 - a_1)^2 + (b_2 - a_2)^2 = (d_1 - c_1)^2 + (d_2 - c_2)^2$$

(v) C es el punto medio de $\overline{AB}$:

Se cumple si se da que A, B y C son colineales y $AC = BC$.

Ejemplo 5.10. El producto de dos lados de un triángulo es igual al producto de la altura sobre el tercero por el diámetro de la circunferencia circunscrita.



Supondremos que el triángulo tiene vértices

$$A = (0, 0), \quad B = (1, 0), \quad C = (u_1, u_2).$$

Sea $P = (x_1, x_2)$ el centro de la circunferencia circunscrita. Plantearemos las ecuaciones correspondientes, es decir que $AP = BP$ y que $AP = CP$:

$$\begin{aligned} h_1 &= (x_1 - 1)^2 + x_2^2 - (x_1^2 + x_2^2), \\ h_2 &= (x_1 - u_1)^2 + (x_2 - u_2)^2 - (x_1^2 + x_2^2), \end{aligned}$$

y queremos demostrar que $AC \cdot BC = 2 \cdot AP \cdot CD$:

$$\sqrt{u_1^2 + u_2^2}\sqrt{(u_1 - 1)^2 + u_2^2} = 2y\sqrt{x_1^2 + x_2^2}.$$

entonces nuestra conclusión viene dada por el polinomio

$$g = (u_1^2 + u_2^2)\big((u_1 - 1)^2 + u_2^2\big) - 4y^2(x_1^2 + x_2^2).$$

Una base de Gröbner respecto al orden lexicográfico con $u_1 > u_2 > x_1 > x_2$ del ideal generado por $\{h_1, h_2\}$ es

$$G = \{u_1^2 - u_1 + u_2^2 - 2u_2x_2, x_1 - 1/2\},$$

y con un simple cálculo vemos que $\overline{g}^G = 0$. Como g pertenece al ideal generado por h_1 y h_2, podemos asegurar que el teorema es cierto. Aún así, veremos más adelante que el teorema puede ser cierto, y g no pertenecer al ideal.

Tanto en el ejemplo anterior como en el Ejemplo 5.8 el número de hipótesis y el número de variables dependientes x_j es el mismo. Esta es una propiedad típica de las hipótesis geométricas. Consideraremos ahora la forma habitual de presentar un teorema geométrico. Tendremos m variables arbitrarias, que denotaremos por $u_1, \ldots, u_m$, y una colección de n variables dependientes $x_1, \ldots, x_n$. Entonces, las hipótesis del teorema serán representadas por una colección de ecuaciones polinómicas en u_i, x_j, y habrá n hipótesis que escribiremos

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

Las conclusiones del teorema, las expresaremos también como polinomios en u_i y x_j. Es suficiente considerar el caso en el que hay una sola conclusión, ya que si hay más de una, podemos tratar el problema una por una. Escribimos la conclusión como

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

La pregunta es, como podemos deducir g de $h_1, \ldots, h_n$ algebraicamente. La idea básica es que queremos que g sea cero siempre que $h_1, \ldots, h_n$ sean cero. Las hipótesis nos definen una variedad

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

que motiva la siguiente definición.

Definición 5.11. Decimos que la conclusión g se deduce estrictamente de las hipótesis $h_1, \ldots, h_n$ si $g \in \mathbf{I}(V) \subset \mathbb{R}^{m+n}$, donde $V = \mathbf{V}(h_1, \ldots, h_n)$.

Aunque esta definición parece razonable, veremos que es demasiado estricta debido a los casos "degenerados". Además, trabajando en $\mathbb{R}$, no tenemos un método efectivo para calcular $\mathbf{I}(V)$.

Proposición 5.12. *Si $g \in \sqrt{\langle h_1, \ldots, h_n \rangle}$, entonces g se deduce estrictamente de $h_1, \ldots, h_n$.*

Demostración. Si $g \in \sqrt{\langle h_1, \ldots, h_n \rangle}$, implica que existe un s tal que $g^s \in \langle h_1, \ldots, h_n \rangle$. Entonces g^s es cero en los puntos donde $h_1, \ldots, h_n$ son cero, y por lo tanto g también es cero en dichos puntos. □

El recíproco de esta proposición falla cuando $\sqrt{\langle h_1, \ldots, h_n \rangle} \subsetneq \mathbf{I}(V)$, lo que puede pasar fácilmente si trabajamos sobre $\mathbb{R}$. Esta proposición, usando el algoritmo que obtenemos del Teorema 4.12, nos da un método para comprobar si una conclusión se deduce estrictamente.

Ejemplo 5.13. Continuamos el Ejemplo 5.8. Teníamos las hipótesis

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

y tomamos como conclusión el polinomio de los dos que tenemos que comprobar para demostrar el teorema.

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

Para aplicar la Proposición 5.12, tenemos que calcular la base de Gröbner reducida de

$$\tilde{I} = \langle h_1, h_2, h_3, h_4, 1 - yg \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4, y].$$

A pesar de saber que el teorema enunciado es cierto, ya que está demostrado de manera geométrica, la base obtenida no es $\{1\}$. Entonces, tenemos que descubrir en que falla el método. Si calculamos una base de Gröbner de $I = \langle h_1, h_2, h_3, h_4 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$, usando el orden lexicográfico con $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$ tenemos

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

La variedad $V = \mathbf{V}(h_1, h_2, h_3, h_4) = \mathbf{V}(f_1, \ldots, f_6) \subset \mathbb{R}^7$ definida por las hipótesis es reducible. El polinomio f_2 se puede factorizar como $(x_1 - u_2 - u_2)u_3$, lo que implica que

$$V = \mathbf{V}(f_1, x_1 - u_1 - u_2, f_3, f_4, f_5, f_6) \cup \mathbf{V}(f_1, u_3, f_3, f_4, f_5, f_6).$$

Del mismo modo, podemos factorizar f_5 y f_6, y continuar con el proceso de descomposición. Si proseguimos obtenemos la descomposición en variedades irreducibles

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

donde

$$V' = \mathbf{V}\left(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2}\right),$$
$$U_1 = \mathbf{V}(x_2, x_4, u_3),$$
$$U_2 = \mathbf{V}(x_1, x_2, u_1 - u_2, u_3),$$
$$U_3 = \mathbf{V}(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1).$$

Se puede comprobar que ninguna variedad está contenida en ninguna otra, así que son componentes irreducibles de V.

Si observamos cuidadosamente las variedades U_1 y U_2, tenemos que $u_3 = 0$, lo que puede dar problemas, ya que establecimos u_3 arbitrario. Además, cuando $u_3 = 0$, el vértice C está en el lado $\overline{AB}$, por lo que no tenemos paralelogramo, es decir estamos en un caso degenerado. De modo similar, $u_1 = 0$ en U_3.

Si comprobamos nuestra conclusión g en U_1, vemos que no es cero. Esto explica nuestro fallo al intentar probar el teorema. En cambio, si excluimos los casos degenerados U_1, U_2 y U_3, vemos que g es cero en todo punto de V'.

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

$$V = V_1 \cup \cdots \cup V_k. \tag{5.1}$$

Como vimos en el ejemplo anterior, puede que obtengamos alguna ecuación polinómica que solamente tenga las variables u_i. Como al definir las hipótesis, pretendíamos que u_i fuesen independientes, queremos excluir estas componentes.

Definición 5.14. Sea W una variedad irreducible en el espacio afín $\mathbb{R}^{m+n}$ con coordenadas $u_1, \ldots, u_m, x_1, \ldots, x_n$. Decimos que las funciones $u_1, \ldots, u_m$ son algebraicamente independientes en W si ningún polinomio distinto de cero que solo tenga variables u_i sea cero en W, es decir si $\mathbf{I}(W) \cap \mathbb{R}[u_1, \ldots, u_m] = \{0\}$.

Entonces, en la descomposición de la variedad V dada en (5.1), podemos reagrupar las componentes irreducibles de la forma

$$V = W_1 \cup \cdots \cup W_p \cup U_1 \cup \cdots \cup U_q,$$

donde las u_i son algebraicamente independientes en las componentes W_i, y no lo son en las componentes U_j. Como los U_j representan casos "degenerados" de las hipótesis del teorema, consideraremos solamente la subvariedad

$$V' = W_1 \cup \cdots \cup W_p \subset V.$$

Definición 5.15. Decimos que la conclusión g se deduce genéricamente de las hipótesis $h_1, \ldots, h_n$ si $g \in \mathbf{I}(V') \subset \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, donde como antes, $V' \subset \mathbb{R}^{m+n}$ es la unión de las componentes de la variedad $V = \mathbf{V}(h_1, \ldots, h_n)$ en las que u_i son algebraicamente independientes.

Decir que un teorema geométrico es cierto en el sentido usual significa que las conclusiones se deducen genéricamente de las hipótesis. Entonces, el problema se reduce a determinar cuando $g \in \mathbf{I}(V')$. Por una parte, descomponer una variedad en componentes irreducibles puede no ser una tarea fácil. Además, si conseguimos calcular V', tendremos el problema de calcular $\mathbf{I}(V')$.

Proposición 5.16. *En la situación descrita anteriormente, g se deduce genéricamente de $h_1, \ldots, h_n$ si existe un polinomio distinto de cero $c(u_1, \ldots, u_m) \in \mathbb{R}[u_1, \ldots, u_m]$ tal que*

$$c \cdot g \in \sqrt{H},$$

siendo H el ideal generado por las hipótesis $h_i \in \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$.

Demostración. Sea V_j una componente irreducible de V'. Como $c \cdot g \in \sqrt{H}$, vemos que $c \cdot g$ es cero en V y por lo tanto en V_j. Entonces, el producto $c \cdot g$ está en $\mathbf{I}(V_j)$. Pero V_j es irreducible, entonces $\mathbf{I}(V_j)$ es un ideal primo. De este modo, $c \cdot g \in \mathbf{I}(V_j)$ implica que o bien c o bien g está en $\mathbf{I}(V_j)$. Sabemos que $c \notin \mathbf{I}(V_j)$ ya que las funciones $u_1, \ldots, u_m$ son algebraicamente independientes en V_j. Entonces, $g \in \mathbf{I}(V_j)$, y como es cierto para toda componente de V', tenemos que $g \in \mathbf{I}(V')$. □

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

Proposición 5.17. *Sea $H \subset \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ el ideal generado por las hipótesis h_i, existe $c \in \mathbb{R}[u_1, \ldots, u_m]$ tal que $c \cdot g \in \sqrt{H}$ si y solo si g pertenece al radical del ideal generado por $h_1, \ldots, h_n$ en el anillo $\mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$, siendo $\mathbb{R}(u_1, \ldots, u_m)$ el cuerpo de las funciones racionales en $(u_1, \ldots, u_m)$ es decir, $\mathbb{R}(u_1, \ldots, u_m) = \{\frac{f}{g} : f, g \in \mathbb{R}[u_1, \ldots, u_m], g \neq 0\}$.*

Demostración. Por la definición de radical, sabemos que $c \cdot g \in \sqrt{H}$ si y solo si

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

con $A_j \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ y $s \geq 1$. Si dividimos entre c^s obtenemos

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

lo que demuestra que g está en el radical del ideal $\tilde{H}$ generado por $h_1, \ldots, h_n$ sobre el anillo $\mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$.

Recíprocamente, si $g \in \sqrt{\tilde{H}}$, entonces

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

donde $B_j \in \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$. Si tomamos como c el mínimo común múltiplo de los denominadores, y multiplicamos la igualdad anterior por c^s, obtenemos

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

con $B'_j \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ y c depende solamente de u_i. De este modo, $c \cdot g \in \sqrt{H}$. □

Corolario 5.18. *En las condiciones de la Proposición 5.16, son equivalentes:*

(i) *Existe un polinomio distinto de cero* $c \in \mathbb{R}[u_1, \ldots, u_m]$ *tal que* $c \cdot g \in \sqrt{H}$.

(ii) g *está en* $\sqrt{\tilde{H}}$, *donde* $\tilde{H}$ *es el ideal generado por los* h_j *en* $\mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$.

(iii) $\{1\}$ *es la base de Gröbner reducida del ideal*

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

Demostración. La prueba es combinación del Teorema 4.12 y de la Proposición 5.16. □

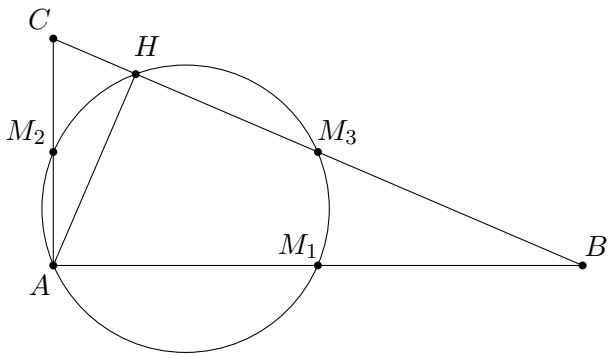
Entonces, combinando la parte (iii) de este corolario y la Proposición 5.16, obtenemos un método algorítmico para probar que una conclusión se deduce genéricamente de un conjunto de hipótesis. Lo llamaremos el método de la base de Gröbner en demostraciones de teoremas geométricos.

Este algoritmo, nos dice que si la base de Gröbner reducida del ideal

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

es $\{1\}$, la conclusión se deduce genéricamente de las hipótesis. Pero si no es $\{1\}$, no tenemos nada garantizado. En [4] podemos ver que este método solo puede probar teoremas, donde la conclusión se deduce genéricamente sobre $\mathbb{C}$ aunque solo estemos interesados en lo que pasa sobre $\mathbb{R}$. En particular, existen teoremas que son ciertos sobre $\mathbb{R}$ pero no lo son sobre $\mathbb{C}$. Un ejemplo de este hecho,que podemos encontrar en [13], es el Teorema de Sylvester–Galai. Este teorema dice que en el plano real, dados n puntos que no estén todos en una recta, existen dos de ellos tales que ningún otro punto es colineal con ellos.

Ejemplo 5.19 (Teorema del círculo de Apolonio)**.** Sea $\triangle ABC$ un triángulo rectángulo en el plano con el ángulo recto en A. Sea H el punto de corte de la altura que parte de A con el lado $\overline{BC}$. Los puntos medios de los tres lados y H están todos en una circunferencia.



Establecemos el punto A en el origen $(0,0)$, y los puntos $B = (u_1, 0)$, $C = (0, u_2)$. Los puntos medios tienen coordenadas $M_1 = (x_1, 0)$, $M_2 = (0, x_2)$, y $M_3 = (x_3, x_4)$. Obtenemos las ecuaciones

$$h_1 = 2x_1 - u_1 = 0,$$
$$h_2 = 2x_2 - u_2 = 0,$$
$$h_3 = 2x_3 - u_1 = 0,$$
$$h_4 = 2x_4 - u_2 = 0.$$

Nos interesa construir el punto $H = (x_5, x_6)$, la base de la altura que pasa por A. Tenemos dos hipótesis,

$$AH \perp BC : h_5 = x_5u_1 - x_6u_2 = 0,$$
$$B, H, C \text{ son colineales } : h_6 = x_5u_2 + x_6u_1 - u_1u_2 = 0.$$

Por último, sabemos que tres puntos no colineales determinan una circunferencia, así que plantearemos el problema del siguiente modo. Describiremos la circunferencia que pasa por los puntos medios de los lados M_1, M_2 y M_3, y nuestra conclusión será ver que el punto H está en ese círculo. Para esto necesitaremos el punto auxiliar $O = (x_7, x_8)$ que es el centro de la circunferencia, con sus dos hipótesis adicionales

$$M_1O = M_2O : h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0,$$
$$M_1O = M_3O : h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0.$$

Y nuestra conclusión $HO = M_1O$ es de la forma

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

Calculamos la base de Gröbner reducida del ideal generado por los h_i en el anillo $\mathbb{R}(u_1, u_2)[x_1, \ldots, x_8]$ usando el orden lexicográfico donde $x_1 > \cdots > x_8 > u_1 > u_2$,

```
> ring R = (0,u_1,u_2),(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,y), lp;
> poly g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2;
>  ideal I = 2*x_1 - u_1, 2*x_2 - u_2, 2*x_3 - u_1, 2*x_4 - u_2,
. x_5*u_1 - x_6*u_2, x_5*u_2 + x_6*u_1 - u_1*u_2, (x_1 - x_7)^2 +
. x_8^2 - x_7^2 - (x_8 - x_2)^2, (x_1 - x_7)^2 + x_8^2 -
. (x_3 - x_7)^2 - (x_4 - x_8)^2, 1 - g*y;
> option(redSB);
> std(I);
_[1]=1
```

Vemos que la base es $\{1\}$, por lo que queda probado el teorema.

5.3. Teoría de Grafos

En esta sección, aplicaremos las bases de Gröbner a la teoría de grafos, y veremos la relación entre los Sudokus y lo desarrollado previamente.

Sea $\mathcal{G}$ un grafo simple, no dirigido con vértices $V = \{1, \ldots, n\}$ y aristas E. Dado un entero positivo $k \leq n$, y sea $C_k = \{c_1, \ldots, c_k\}$ un conjunto de k elementos. A cada elemento de C_k le llamaremos color. Una k-coloración es una función $\gamma : V \longrightarrow C_k$. Diremos que una k-coloración es propia si dos vértices unidos por una arista tienen colores distintos. Decimos que $\mathcal{G}$ es k-coloreable, si existe una k-coloración propia de $\mathcal{G}$.

Supongamos que queremos colorear un grafo con 3 colores. Sea $\xi = e^{\frac{2\pi i}{3}} \in \mathbb{C}$ una raíz cúbica primitiva de la unidad. Sea $C_3 = \{1, \xi, \xi^2\}$, donde cada raíz cúbica de la unidad es un color. Sean $x_1, \ldots, x_n$ variables representando los vértices del grafo $\mathcal{G}$. A cada vértice le queremos asignar un color, lo que podemos representar con las siguientes n ecuaciones.

$$x_i^3 - 1 = 0,\ 1 \leq i \leq n. \tag{5.2}$$

Además, si los vértices x_i y x_j están conectados por una arista, tienen que tener colores distintos. Como $x_i^3 = x_j^3$, tenemos que $(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$.Entonces, x_i y x_j tienen colores distintos si y solo si

$$x_i^2 + x_i x_j + x_j^2 = 0. \tag{5.3}$$

Sea I el ideal de $\mathbb{C}[x_1, \ldots, x_n]$ generado por los n polinomios de la ecuación (5.2) y todos los polinomios de la forma (5.3), cuando x_i, x_j están conectados por una arista. Si ahora consideramos $\mathbf{V}(I) \subset \mathbb{C}^n$, vemos que el grafo $\mathcal{G}$ es 3-coloreable si y solo si $\mathbf{V}(I) \neq \emptyset$. Además,

por el Corolario 3.19, el grafo es 3-coloreable si y solo si $1 \notin G$, siendo G la base de Gröbner reducida de I.

Ejemplo 5.20. Consideramos el grafo $\mathcal{G}$ de la Figura 5.1.

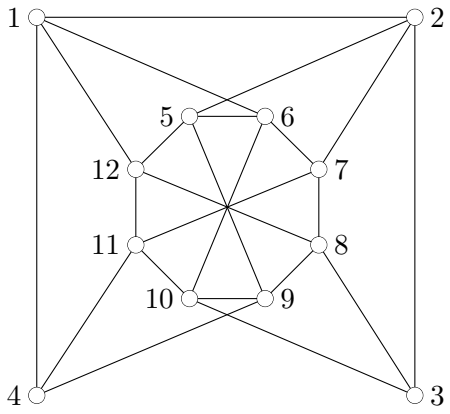


Figura 5.1: Grafo $\mathcal{G}$

Tomamos el ideal I, definido anteriormente y hallamos su base de Gröbner reducida G usando el orden lexicográfico con $x_1 > \cdots > x_{12}$.

$$G = \{x_{12}^3 - 1, x_7 - x_{12}, x_4 - x_{12}, x_3 - x_{12}, x_{11}^2 + x_{11}x_{12} + x_{12}^2, x_9 - x_{11}, x_6 - x_{11},$$

$$x_2 - x_{11}, x_{10} + x_{11} + x_{12}, x_8 + x_{11} + x_{12}, x_5 + x_{11} + x_{12}, x_1 + x_{11} + x_{12}\}.$$

Como 1 no pertenece a la base de Gröbner reducida, podemos 3-colorear el grafo. Supongamos que queremos colorear $\mathcal{G}$ con los colores blanco, negro y gris. Escogemos por ejemplo el color blanco para el vértice x_{12}. Si observamos cuidadosamente la base de Gröbner, x_7 tiene que tener también color blanco ya que $x_7 - x_{12} \in G$. Por esta misma razón, los vértices x_4 y x_3 también tendrán el color blanco. El vértice x_{11} tendrá un color distinto al blanco, ya que $x_{11}^2 + x_{11}x_{12} + x_{12}^2 \in G$. Supongamos que es el negro. Entonces, x_9, x_6 y x_2, tendrán el color negro también. Por último colorearemos con gris los vértices restantes, ya que observando los polinomios de G, vemos que su color tiene que ser distinto al de x_{12} y al de x_{11}. De este modo obtenemos una 3-coloración del grafo $\mathcal{G}$, que vemos en la Figura 5.2.

Ahora formalizaremos el caso de k colores.

Definición 5.21. Sea un grafo $\mathcal{G}$ simple y no dirigido, con vértices $V = \{1, \ldots, n\}$ y aristas

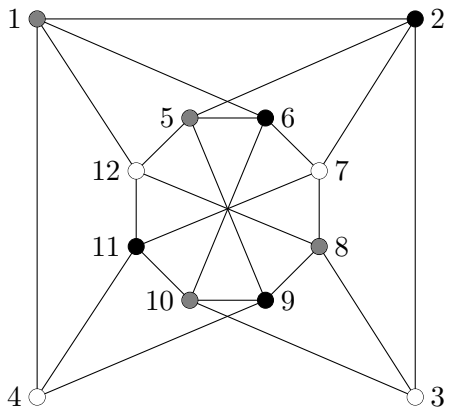


Figura 5.2: $\mathcal{G}$ 3-coloreado

E, llamaremos ideal de k-coloración del grafo $\mathcal{G}$ al ideal $I_{\mathcal{G},k} \subset \mathbb{C}[x_1, \ldots, x_n]$, generado por

$$x_i^k - 1, \text{ para todo } i \in V,$$

$$x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} \text{ para todo } (i,j) \in E.$$

Lema 5.22. $\mathbf{V}(I) \subset \mathbb{C}^n$ *está formado por todas las* k*-coloraciones de* $\mathcal{G}$*, siendo el conjunto de colores las* k*-ésimas raíces de la unidad.*

Demostración. Los polinomios $x_i^k - 1$ son cero si y solo si en cada vértice tenemos una raíz k-ésima de la unidad. Los polinomios $x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1}$ son cero si y solo si los vértices i y j tienen colores distintos, ya que

$$x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} = \frac{(x_i^k - 1) - (x_j^k - 1)}{x_i - x_j}.$$

□

Definición 5.23. Decimos que un grafo es k-coloreable de manera única si existe una única k-coloración propia salvo permutaciones de colores.

Supongamos que tenemos una k-coloración de un grafo $\mathcal{G}$, que usa los k colores, y supongamos que en los k últimos vértices tienen k colores distintos. Usaremos las variables $x_1, \ldots, x_{n-k}$ para los $n-k$ primeros vértices y las variables $y_1, \ldots, y_k$ para los k últimos, con el orden lexicográfico $x_1 > \cdots x_{n-k} > y_1 > \cdots > y_k$. Consideramos n polinomios de la forma siguiente:

(i) $y_k^k - 1$,

(ii) $h_j(y_j, \ldots, y_k) = \sum_{\alpha_j + \cdots + \alpha_k = j} y_j^{\alpha_j} \cdots y_k^{\alpha_k}$ con $j = 1, \ldots, k-1$,

(ii) $x_i + y_2 + \cdots + y_k$, si $\text{color}(x_i) = \text{color}(y_1)$.

(iv) $x_i - y_j$, si $\text{color}(x_i) = \text{color}(y_j)$, $j \geq 2$.

Llamamos $g_1, \ldots, g_n$ a los n polinomios anteriores.

Ejemplo 5.24. Los polinomios $g_1, \ldots, g_n$ del grafo de la Figura 5.2 son los siguientes:

$$G = \{y^3 - 1, h_2(y_2, y_3) = y_2^2 + y_2y_3 + y_3^2, h_1(y_1, y_2, y_3) = y_1 + y_2 + y_3, x_7 - y_3, x_4 - y_3,$$

$$x_3 - y_3, x_9 - y_2, x_6 - y_2, x_2 - y_2, x_8 + y_2 + y_3, x_5 + y_2 + y_3, x_1 + y_2 + y_3\}.$$

Teorema 5.25. *Dado un grafo $\mathcal{G}$, sea $I_{\mathcal{G},k}$ su ideal de k-coloración denotando las variables como antes y sean g_n los polinomios definidos anteriormente. Entonces los siguientes enunciados son equivalentes:*

(i) *$\mathcal{G}$ es k-coloreable de manera única.*

(ii) *$g_1, \ldots, g_n \in I_{\mathcal{G},k}$.*

(iii) *$\{g_1, \ldots, g_n\}$ es la base de Gröbner reducida de $I_{\mathcal{G},k}$ respecto al orden lexicográfico con $x_1 > \cdots > x_{n-k} > y_1 > \cdots > y_k$.*

La demostración de este resultado la podemos encontrar en [14].

Ejemplo 5.26. Si observamos los polinomios que forman la base de Gröbner del ideal I del Ejemplo 5.20, vemos que el grafo $\mathcal{G}$ solo se puede colorear de una manera (salvo permutaciones de los colores), dada en la Figura 5.2.

Este teorema lo podemos aplicar a la resolución de Sudokus. Para hacer esto, lo primero es ver el Sudoku como un grafo. Cada cuadrado, será una arista, por lo que $V = \{1, \ldots, 81\}$. Si dos cuadrados i y j están ligados, es decir, pertenecen a la misma fila, a la misma columna o al mismo cuadrado 3×3, diremos que $(i, j) \in E$, es decir, habrá una arista del grafo uniéndolos. Nuestro objetivo, es extender a una 9-coloración propia, es decir dar colores (dígitos del 1 al 9) a cada vértice y si dos cuadrados están ligados, tienen que tener colores distintos.

Entonces, dado un Sudoku, haremos lo siguiente:

- Construimos el grafo $\mathcal{G}$ como describimos antes.
- Tomamos las variables x_i, $i = 1, \ldots, 81$, y por cada dígito $j = 1, \ldots, 9$, buscamos un vértice i que lo tenga como dato inicial, y renombramos x_i por y_j.
- Consideramos el ideal de 9-coloración del grafo $I_{\mathcal{G},9}$.

- Le añadimos los 8 polinomios de la forma $h_j(y_j, \ldots, y_9) = \sum_{\alpha_j+\cdots+\alpha_9=j} y_j^{\alpha_j} \cdots y_9^{\alpha_9}$, con $j = 1, \ldots, 8$, al ideal $I_{\mathcal{G},9}$.
- Por cada dígito adicional $j \neq 1$ que tengamos como dato, que esté en un vértice i que no renombramos, le añadimos a $I_{\mathcal{G},9}$ el polinomio $x_i - y_j$.
- Por cada 1 que tengamos como dato, que esté en un vértice i que no renombramos, le añadimos a $I_{\mathcal{G},9}$ el polinomio $x_i + y_2 + \cdots + y_9$.

Si el Sudoku está bien planteado, la base de Gröbner reducida del ideal $I_{\mathcal{G},9}$, contendrá polinomios de la forma $x_i - y_j$, lo que nos dirá que el cuadrado i tiene el número j.

Ejemplo 5.27. Sea el Sudoku siguiente:

				3	5			
	1		2			9		
7		6						
6			5				3	7
				4				
2	3				1			5
								8
5		4			6		7	1
			3	1	2			

Para obtener el ideal $I_{\mathcal{G},9}$ seguiremos los pasos siguientes:

(i) Consideramos los polinomios $x_i^9 - 1$, para todo $i = 1, \ldots, 81$.

(ii) Añadimos los polinomios $x_i^8 + x_i^7 x_j + \cdots + x_i x_j^7 + x_j^8$, para todos los pares (i, j) que estén ligados.

(iii) Renombramos las casillas con dígitos más claros, $y_1 = x_{11}$, $y_2 = x_{13}$, $y_3 = x_5$, $y_4 = x_{41}$, $y_5 = x_6$, $y_6 = x_{21}$, $y_7 = x_{19}$, $y_8 = x_{63}$, $y_9 = x_{16}$, ya que son las casillas dato que tienen los dígitos del 1 al 9, y añadimos los polinomios: $y_9^9 - 1$, $h_8(y_8, y_9) = y_8^2 + y_8 y_9 + y_9^2$, $\ldots, h_1(y_1, \ldots, y_9) = y_1 + \cdots + y_9$.

(iv) Añadimos los 13 polinomios correspondientes a los cuadros, que no hemos renombrado, con datos distintos de 1: $x_{28} - y_6$, $x_{31} - y_5$, $x_{35} - y_3$, $x_{36} - y_7, \ldots$

(v) Añadimos los 3 polinomios correspondientes a los cuadros, que no hemos renombrado, con un 1 como dato: $x_{51} + y_2 + \cdots + y_9$, $x_{72} + y_2 + \cdots + y_9$ y $x_{77} + y_2 + \cdots + y_9$.

Sea G la base de Gröbner reducida de este ideal. Si el Sudoku tiene solución única, para cada casilla vacía i, habrá un polinomio en G de la forma $x_i - y_j$ o de la forma $x_i + y_2 + \cdots + y_9$. Si es de la primera forma, en la casilla i pondremos el dígito j. Si es de la segunda forma, en la casilla i pondremos el dígito 1.

Este método funciona, pero realmente es una mala solución para el problema, ya que calcular la base de Gröbner reducida de un ideal con tantos generadores (tengamos en cuenta que en un Sudoku 9×9 hay 81 vértices y 810 aristas) puede ser muy costoso. Aún así, si consideramos un Sudoku 4×4, podemos resolverlo fácilmente con `Singular`.

Ejemplo 5.28. Sea el Sudoku 4×4 (también llamado Shidoku) siguiente:

1			
		2	
	3		4

Figura 5.3: Shidoku

Para resolverlo, primero renombramos las variables $y_1 = x_1$, $y_2 = x_7$, $y_3 = x_{10}$, $y_4 = x_{12}$. Lo que tenemos que hacer, es hallar la base de Gröbner reducida, respecto el roden

lexicográfico $x_2 > \cdots > x_{16} > y_1 \cdots > y_4$, del ideal que resulta al añadirle los polinomios

$$\begin{aligned} h_4 &= y_4^4 - 1, \\ h_3 &= y_4^3 + y_4^2 y_3 + y_4 y_3^2 + y_3, \\ h_2 &= y_4^2 + y_3^2 + y_2^2 + y_4 y_3 + y_4 y_2 + y_3 y_2, \\ h_1 &= y_1 + y_2 + y_3 + y_4, \end{aligned}$$

al ideal de 4-coloración del Shidoku visto como un grafo.

Primero insertamos la posición en la que se encuentran los números 1, 2, 3 y 4.

```
list M = (1, 7, 10, 12);
```

Ahora renombramos las variables y definimos el anillo con el orden lexicográfico apropiado.

```
> int i, j;
>     list N;
>     for(i=1;i<=16;i++)
.     {
.         if(i != M[1])
.         {
.             if(i != M[2])
.             {
.                 if(i != M[3])
.                 {
.                     if(i !=M[4])
.                     {
.                         N[size(N)+1] = i;
.                      }
.                  }
.              }
.          }
.     }
>     N[13] = M[1];
>     N[14] = M[2];
>     N[15] = M[3];
>     N[16] = M[4];
>     ring R = 32003, (x(N[1]), x(N[2]), x(N[3]), x(N[4]),
x(N[5]), x(N[6]), x(N[7]), x(N[8]), x(N[9]), x(N[10]),
```

```
x(N[11]), x(N[12]),  x(N[13]), x(N[14]), x(N[15]),
 x(N[16])), lp;
```

Definimos el conjunto de aristas.

```
> list E;
> for(i=1;i<=4;i++)
. {
.       E[size(E)+1]=list(i,i+4);
.       E[size(E)+1]=list(i, i+8);
.       E[size(E)+1]=list(i, i+12);
.       E[size(E)+1]=list(i+4, i+8);
.       E[size(E)+1]=list(i+4, i+12);
.       E[size(E)+1]=list(i+8, i+12);
.       E[size(E)+1]=list(4*i-3,4*i-2);
.       E[size(E)+1]=list(4*i-3, 4*i-1);
.       E[size(E)+1]=list(4*i-3, 4*i);
.       E[size(E)+1]=list(4*i-2, 4*i-1);
.       E[size(E)+1]=list(4*i-2, 4*i);
.       E[size(E)+1]=list(4*i-1, 4*i);
. }
> for(j=1;j<=2;j++)
. {
.       E[size(E)+1]=list(2*j-1,2*j+4);
.       E[size(E)+1]=list(2*j + 7, 2*j + 12);
.       E[size(E)+1]=list(2*j, 2*j +3);
.       E[size(E)+1]=list(2*j + 8, 2*j + 11);
. }
```

Ahora definimos el ideal $I_{\mathcal{G},4}$

```
> ideal G;
> for(i=1;i<=nvars(basering);i++)
. {
.       G[i] = x(i)^4 - 1;
. }
> for(i=1;i<=size(E);i++)
. {
```

```
.       G[size(G)+1] = (G[E[i][1]] - G[E[i][2]])/(x(E[i][1]) -
x(E[i][2]));
. }
> G[size(G)+1] = var(16)^4 - 1;
> G[size(G)+1] = var(16)^3 + var(15)*var(16)^2 +
var(16)*var(15)^2 + var(15)^3;
> G[size(G)+1] = var(16)^2 + var(15)^2 + var(14)^2 +
var(16)*var(15) + var(16)*var(14) + var(15)*var(14);
> G[size(G)+1] = var(16) + var(15) + var(14) + var(13);
```

Por último, hallamos la base de Gröbner reducida

```
> option(redSB);
> std(G);
_[1]=x(12)^4-1
_[2]=x(10)^3+x(10)^2*x(12)+x(10)*x(12)^2+x(12)^3
_[3]=x(7)^2+x(7)*x(10)+x(7)*x(12)+x(10)^2+x(10)*x(12)+x(12)^2
_[4]=x(1)+x(7)+x(10)+x(12)
_[5]=x(16)-x(7)
_[6]=x(15)-x(10)
_[7]=x(14)+x(7)+x(10)+x(12)
_[8]=x(13)-x(12)
_[9]=x(11)+x(7)+x(10)+x(12)
_[10]=x(9)-x(7)
_[11]=x(8)+x(7)+x(10)+x(12)
_[12]=x(6)-x(12)
_[13]=x(5)-x(10)
_[14]=x(4)-x(10)
_[15]=x(3)-x(12)
_[16]=x(2)-x(7)
```

La base de Gröbner que obtenemos está formada por los siguientes elementos:

$$
\begin{aligned}
&y_4^4 - 1,\\
&y_3^3 + y_3^2 y_4 + y_3 y_4^2 + y_4^3,\\
&y_2^2 + y_2 y_3 + y_2 y_4 + y_3^2 + y_3 y_4 + y_4^2,\\
&y_1 + y_2 + y_3 + y_4,
\end{aligned}
$$

$$x_{16} - y_2,$$

$$x_{15} - y_3,$$

$$x_{14} + y_2 + y_3 + y_4,$$

$$x_{13} - y_4,$$

$$x_{11} + y_2 + y_3 + y_4,$$

$$x_9 - y_2,$$

$$x_8 + y_2 + y_3 + y_4,$$

$$x_6 - y_4,$$

$$x_5 - y_3,$$

$$x_4 - y_3,$$

$$x_3 - y_4,$$

$$x_2 - y_2.$$

Entonces, las casillas 12, 13, 6 y 3, tendrán el número 4. Las casillas 10, 15, 5 y 4 tendrán el número 3. Las casillas 7, 16, 9 y 2 tendrán el número 2. Las casillas 1, 14, 11 y 8 tendrán el número 1.

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

Figura 5.4: Shidoku Resuelto

Bibliografía

[1] Adams, W.W. and Loustaunau, P. *An Introduction to Gröbner Bases*. American Mathematical Society, 1994.

[2] Buchberger B. *An algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Ideal.* Ph. D. Thesis, University of Innsbruck, Math. Inst., 1965.

[3] Coutinho, S.C. *Polinômios e Computação Algébrica*. Universidade Federal de Rio de Janeiro, 2009.

[4] Cox, D. Little, J. and O'Shea, D. *Ideals, Varieties, and algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd ed. Springer–Verlag, New York, 2007.

[5] Cox, D. Little, J. and O'Shea, D. *Using Algebraic Geometry*, 3rd ed. Springer–Verlag, New York, 2005.

[6] Decker, W. and Pfister, G. *A First Course in Computational Algebraic Geometry*, 2011. `http://www.mathematik.uni-kl.de/~decker/Lehre/SS12/AlgebraicGeometry/material/BookDeckerPfister.pdf`

[7] Greuel, G.M. and Pfister, G. *A Singular Introduction to Commutative Algebra*, 2nd ed. Springer–Verlag, Berlin, 2002.

[8] Hironaka, H. *Resolution of singularities of an algebraic variety over a field of characteristic zero*. Ann. Math. **79** (1964), 109–326.

[9] Knuth, D. and Bendix, P. *Simple word problems in universal algebras*. In: Leech, J. (ed.), Computational Problems in Abstract Algebra, Pergamon Press, 1970, 263–297.

[10] Kreuzer, M. and Robbiano, L. *Computational Commutative Algebra 1*. Springer–Verlag, Berlin, 2000.

[11] Schauenburg, P. *A Gröbner–based treatment of elimination theory for affine varieties*. Journal of Symbolic Computation **42** (2007), 859–870.

[12] Shirshov, A. *Some algorithmic problems for Lie algebras*, Siberian Math. J. **3** (1962), 292–296.

[13] Sturmfels, B. *Computing Final Polynomials and Final Syzygies Using Buchberger's Gröbner Bases Method*. Results in Mathematics **15** (1989), 351–360.

[14] Windfeldt, T. *Computational Aspects of Graph Coloring and the Quillen–Suslin Theorem*. Ph. D. Thesis, University of Copenhagen, 2009.