FRANCISCO UGARTE GUERRA
editor

VI ESCUELA DOCTORAL INTERCONTINENTAL DE MATEMÁTICAS

PUCP-UVA 2013

Capítulo 4

FONDO EDITORIAL
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

VI Escuela Doctoral Intercontinental de Matemáticas
PUCP-UVA 2013
Francisco Ugarte Guerra, editor

De esta edición:

Fondo Editorial de la Pontificia Universidad Católica del Perú, 2014
Avenida Universitaria 1801, Lima 32, Perú
Teléfono (51 1) 626 2650
feditor@pucp.edu.pe
www.fondoeditorial.pucp.edu.pe

Diseño de interiores: FranciscoUgarte Guerra / Janet Yucra Núñez
Diseño de cubierta: Francisco Ugarte Guerra / DCI-PUCP
Primera edición: octubre de 2014
Tiraje: 500 ejemplares

Hecho el Depósito Legal en la Biblioteca Nacional del Perú Nº 2014-16314
ISBN: 978-612-317-056-1
Registro del Proyecto Editorial: 31501361401068

Impreso en Tarea Asociación Gráfica Educativa
Pasaje María Auxiliadora 156, Lima 5, Perú

Una introducción a las bases de Gröbner y algunas de sus aplicaciones

Philippe Gimenez

1. Introducción

Estas notas pretenden ofrecer una introducción elemental a la teoría de bases de Gröbner y presentar algunas de sus aplicaciones. Son las notas del curso impartido durante la VI Escuela Doctoral Intercontinental de Matemáticas PUPC-UVA en mayo de 2013 y quiero, antes de nada, agradecer a sus organizadores la invitación y la oportunidad de participar en un proyecto tan bonito que me permitió, sin salir de casa, interactuar con estudiantes y profesores de Valladolid pero también de Lima en Perú, de Belo Horizonte en Brasil, de México D.F. y de Cuernavaca en México. Un agradecimiento muy especial a Francisco por su paciencia en la espera de estas notas y su constante apoyo y ánimo para que lleguen a ver la luz.

En los años 60, Bruno Buchberger y Heisuke Hironaka introdujeron independientemente nuevos algoritmos para manipular sistemas de ecuaciones polinomiales que desembocaron en la creación de la teoría de bases de Gröbner, también llamadas bases estándar en un contexto local. Empezaremos ilustrando nuestro propósito con un problema.

El problema de pertenencia

Tomamos una lista de m polinomios en n indeterminadas con coeficientes en un cuerpo K arbitrario, $f_1, \dots, f_m \in A := K[x_1, \dots, x_n]$, y nos preguntamos cómo determinar de manera sistemática si otro polinomio f de A pertenece o no al ideal I de A generado por $f_1, \dots, f_m$. La pregunta es por tanto la siguiente:

$$\text{¿ Existen } q_1, \dots, q_m \in A \text{ tales que } f = q_1 f_1 + \cdots + q_m f_m? \tag{1}$$

Desde un punto de visto geométrico, esto es lo mismo que preguntarse si, dada una variedad algebraica $V(f_1, \dots, f_m) \subset \mathbb{A}^n_K$, está contenida o no en la hipersuperficie $V(f)$. Podemos además ir un poco más lejos en la pregunta anterior y pedir, si la respuesta es positiva, cómo determinar unos polinomios $q_1, \dots, q_m \in A$ que cumplan la igualdad $f = q_1 f_1 + \cdots + q_m f_m$.

Hay un contexto en el que sabemos fácilmente contestar a la pregunta (1). Es el caso de una sola variable x, es decir cuando $n = 1$. En este caso el método que todos conocemos para contestar es el siguiente:

1. Como $K[x]$ es un dominio de ideales principales, sabemos que existe $g \in I$ tal que $I = (g)$. Además, sabemos quién es g y cómo encontrarlo: g es el máximo divisor común de $f_1, \ldots, f_m$, $g = \text{mcd}(f_1, \ldots, f_m)$, y se determina usando de algoritmo de Euclides. Este primer paso del método consiste en cambiar el sistema de generadores de I por otro mejor, es decir pasar de $\{f_1, \ldots, f_m\}$ a $\{g\}$ con $I = (f_1, \ldots, f_m) = (g)$. El segundo sistema de generadores del ideal I es claramente mejor ya que pasamos de un número arbitrariamente grande de generadores a un único generador, y además éste es de grado menor que el grado de los generadores originales.

2. El segundo paso es ahora sencillo. Basta con dividir el polinomio f por g para obtener una expresión de la forma $f = qg + r$ con $q, r \in K[x]$ tales que $f \in I = (g)$ si y sólo si $r = 0$. Esto proporciona una respuesta efectiva al problema planteado en (1) en el caso $n = 1$.

Obviamente este método falla por todas partes cuando tenemos más variables. En efecto, sabemos que si $n \geq 2$, $K[x_1, \ldots, x_n]$ no es un dominio de ideales principales por lo que falla la clave del primer paso. Por otra parte, el algoritmo de división en n variables (que recordaremos en la sección 2) no goza, para $n \geq 2$, de las buenas propiedades que tiene cuando $n = 1$ (la unicidad del resto) para asegurar que un elemento pertenece a un ideal si y sólo si el resto de su división por los generadores del ideal es nulo.

Sin embargo, podremos responder a la pregunta (1) en general recuperando la esencia del método anterior usando las bases de Gröbner. Empezaremos cambiando los generadores del ideal I, sustituyendo $\{f_1, \ldots, f_m\}$ por $\mathcal{G} = \{g_1, \ldots, g_t\}$, una base de Gröbner de I, que será mejor en un sentido menos obvio que el caso de una variable. En efecto, ahora tanto el número de elementos como el grado de estos elementos pueden crecer (y lo harán en general) pero dividiendo un polinomio f arbitrario por los elementos de $\mathcal{G}$ podremos contestar a la pregunta (1) de la manera siguiente: $f \in I = (f_1, \ldots, f_m) = (g_1, \ldots, g_t)$ si y sólo si el resto de su división por los elementos de $\mathcal{G}$ es nulo.

Estructura de estas notas

Dividiremos el contenido de estas notas en 3 partes teóricas que completaremos con una sección de problemas, muchos de ellos elementales. En la primera parte introduciremos los órdenos monomiales y las bases de Gröbner y daremos sus propiedades básicas. En la segunda, desvelaremos las herramientas ligadas a las bases de Gröbner, en particular el algoritmo de Buchberger que nos permitirá construirlas. En la tercera sección, propondremos algunas aplicaciones de las bases de Gröbner. Elegí aquí entre las muchas

posibilidades simplemente siguiendo mi gusto personal y por esta razón, muchas de ellas se sitúan en el ámbito del álgebra conmutativa. Pero cabe destacar que existen hoy en día multitud de aplicaciones en otras áreas de las matemáticas.

Comentarios sobre las referencias bibliografícas

En estas notas no incluiremos todas las demostraciones, ya que existen libros que las recogen, las sustituiremos por referencias, intentando siempre que éstas sean adaptadas al nivel de este curso. Personalmente, creo que la referencia para una buena introducción a las bases de Gröbner es el libro de Cox, Little y O'Shea, [5], pues es un manual estupendo para dar clase y también un apoyo sólido para los que, como yo, usan las bases de Gröbner como una herramienta en su investigación. Lo mismo ocurre con el segundo libro de los mismos autores [6], donde se generalizan los conceptos para módulos y se presentan aplicaciones más avanzadas. Existen otros magníficos libros de texto como los ya clásicos [2] y [10] (capítulo 15), o los recientes [12] y [9]. Cabe destacar también las excelentes notas sin publicar de Monique Lejeune-Jalabert [17] que aportan un punto de vista distinto y contienen resultados que no encontraremos en las demás referencias. También quiero citar aquí el survey de Bayer y Mumford [3], una referencia clásica que ha impulsado en su momento la investigación en el campo de la geometría algebraica computacional. Y el magnífico libro de Wolmer Vasconcelos [19], que aporta la visión del prestigioso algebrista sobre aspectos computacionales en álgebra conmutativa y en geometría algebraica.

Nota sobre los programas especializados y sus manuales

Además de su interés teórico, las bases de Gröbner presentan un interés práctico. En efecto, la implementación de los algoritmos para construir bases de Gröbner las ha convertido en una herramienta muy cómoda para tratar ejemplos no triviales. Hoy en día, es difícil imaginar trabajar en álgebra conmutativa y en geometría algebraica sin usar un ordenador para tratar algún ejemplo que nos llevaría mucho trabajo a mano, o simplemente para poner a prueba una conjetura. Existen tres programas especializados en cálculos polinomiales. Todos llevan implementados muchos de los algoritmos que involucran las bases de Gröbner y comparten que son de libre distribución, que han sido creados y desarrollados por matemáticos de primer nivel, y que siguen desarrollandose e incorporando resultados nuevos: CoCoA [1], desarrollado en la universidad de Génova (Italia), Singular [7], desarrollado en la universidad de Kaiserslautern (Alemania), y Macaulay2[1]

[1]El los años 90, Dave Bayer y Mike Stillman desarrollaron el primer programa para trabajar con bases de Gröbner, Macaulay. Este programa, que ha dejado de desarrollarse y fué sustituido por Macaulay2,

[13], desarrollado en las universidades de Illinois y Cornell (USA). Para cada uno de estos programas encontraremos, aparte de su sistema de ayuda y manual online incorporados, unos libros de texto escritos por los propios creadores del programa, y que proponen una introducción al álgebra conmutativa y a la geometría algebraica haciendo uso de su programa. Todos ponen hicapié en los métodos computacionales de ambas áreas. Así tenemos [16] para CoCoA, [14] y [8] para Singular y [11] para Macaulay2. También puede resultar interesante observar cómo estos programas se usan en la actualidad en temas concretos de investigación. Por ejemplo, en el recientemente publicado [4] encontraremos las notas de tres cursos avanzados sobre temas de actualidad impartidos en una escuela doctoral y donde la parte teórica de cada curso se complementa con un tutorial con alguno de estos tres programas.

En estas notas utilizaremos Singular para resolver algunos problemas por lo que ofreceremos una pequeña introducción al manejo de este programa en la sección 3.4.

Notaciones

A lo largo de estas notas manejaremos las siguientes notaciones:

- $A = K[x_1, \ldots, x_n]$ siendo K un cuerpo a priori arbitrario;
- un monomio de A se denotará por $\mathbf{x}^\alpha$: para $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. El grado del monomio $\mathbf{x}^\alpha$ de A es $\deg \mathbf{x}^\alpha = |\alpha| = \sum_{i=1}^n \alpha_i$;
- dados dos monomios $\mathbf{x}^\alpha, \mathbf{x}^\beta \in A$, $\mathbf{x}^\alpha | \mathbf{x}^\beta$ significa que $\mathbf{x}^\alpha$ divide $\mathbf{x}^\beta$;
- dado un polinomio $f \in A$, el *soporte de* f, denotado por $\operatorname{supp}(f)$, es el conjunto de los monomios que forman el polinomio f, es decir que si $f = \sum_\alpha a_\alpha \mathbf{x}^\alpha$, $\operatorname{supp}(f) = \{\mathbf{x}^\alpha \,/\, a_\alpha \neq 0\}$. Si $f = 0$ entonces $\operatorname{supp}(f) = \emptyset$;
- dados m polinomios de A, $f_1, \ldots, f_m$, denotaremos por $(f_1, \ldots, f_m)$ al ideal de A engendrado por estos polinomios;
- dado un ideal I de A, $V(I) \subset \mathbb{A}_K^n$ es la variedad algebraica afín formada por los puntos en los que se anulan todos los polinomios de I;

todavía se puede descargar en `http://www.math.columbia.edu/~bayer/Macaulay/`. Muchos de los que aprendimos a manipular bases de Gröbner con este sencillo programa le seguimos teniendo mucho cariño. Y algunos siguen usándolo ya que, aunque haga menos que los demás, lo que hace lo hace perfectamente y de manera muy sencilla.

- dado un subconjunto V de $\mathbb{A}^n_K$, $I(V)$ es el ideal de A formado por los polinomios que se anulan en todos los puntos de V.

Prerequisitos

Este curso pretende ser elemental y autocontenido pero requiere conocimientos básicos en álgebra conmutativa y en geometría algebraica: los conceptos de ideal en un anillo de polinomios en varias variables con coeficientes en un cuerpo, de variedad algebraica afín y proyectiva y de ideal de una variedad algebraica, y los teoremas de la base y de los ceros de Hilbert que, en nuestro contexto, se pueden enunciar de la siguiente manera:

Teorema 1 (Teorema de la base de Hilbert)**.** *El anillo $A = K[x_1, \ldots, x_n]$ es noetheriano, es decir, satisface cualquiera de las dos condiciones equivalentes siguientes:*

1. *Todo ideal de A es finitamente generado.*
2. *Toda cadena ascendente de ideales de A estabiliza.*

Teorema 2 (Teorema de los ceros de Hilbert)**.** *Si K es un cuerpo algebraicamente cerrado, para todo ideal I de $K[x_1, \ldots, x_n]$, se tiene:*

- (versión débil) $\quad V(I) = \emptyset \quad \Rightarrow \quad I = (1)$;
- (versión fuerte) $\quad I(V(I)) = \sqrt{I}$.

Los teoremas 1 y 2 pueden demostrarse usando bases de Gröbner por lo que no es estrictamente necesario suponerlos conocidos (véase, por ejemplo, los capítulos 2.5 y 4.1 de [5] respectivamente). Sin embargo, preferimos suponerlos conocidos para agilizar estas notas.

También supondremos conocidos los ideales monomiales, su definición (un ideal de A es monomial si está engendrado por un conjunto, posiblemente infinito, de monomios) y sus propiedades elementales:

Proposición 3. *Sea I es un ideal monomial de A.*

1. ([5, Lemma 2, p. 67]). *Dado $\mathcal{M}$ un conjunto de monomios generadores de I, un monomio $\mathbf{x}^\alpha$ de A pertenece a I si y sólo si es múltiplo de un elemento de $\mathcal{M}$.*
2. ([5, Exercice 8, p. 71], [12, Prop. 1.11]). *I admite un único sistema minimal de generadores formado por monomios (y éste es finito).*

2. Definiciones y propiedades básicas

2.1. Órdenes monomiales

Como veremos en la sección 2.2, el principio del algoritmo de división sobre $A = K[x_1, \ldots, x_n]$ es el mismo que con una variable. Podemos resumirlo de manera grosera de la siguiente manera: restando un múltiplo del divisor, haremos bajar el término de mayor grado hasta que no podamos hacerlo más y entonces tendremos el cociente y el resto que buscamos. Por tanto lo primero que tenemos que hacer es ordenar de mayor a menor los monomios del polinomio que queremos dividir y los del divisor.

Este problema no se plantea para una variable ya que el orden es heredado del orden natural sobre los enteros (los exponentes de los monomios). Pero cuando tenemos varias variables, sabemos que no hay una manera única de ordenar los monomios. Claramente la relación de orden $>$ sobre el conjunto de los monomios de A que necesitamos para la división tiene que ser *total* para ordenar los monomios de mayor a menor sin ninguna ambiguedad. Además tiene que ser *compatible con el producto*, es decir satisfacer que dados 3 monomios $\mathbf{x}^\alpha, \mathbf{x}^\beta, \mathbf{x}^\gamma$ de A, si $\mathbf{x}^\alpha > \mathbf{x}^\beta$ entonces $\mathbf{x}^\alpha\mathbf{x}^\gamma > \mathbf{x}^\beta\mathbf{x}^\gamma$ para garantizar que al restar un múltiplo del divisor, el término mayor del resto parcial obtenido sea más pequeño que el que teníamos en el paso anterior (imaginamos facilmente el caos en la división si esta propiedad no se diera: al restar un múltiplo del divisor para cancelar el término de mayor grado, la multiplicación podría producir un monomio mayor y por tanto habriamos empeorado la situación en lugar de mejorarla). Finalmente, dadas las dos condiciones anteriores, es necesario que *toda sucesión decreciente de monomios estabilice* para garantizar que el algoritmo de división termine. Esto nos lleva a la definición siguiente:

Definición 4. Una relación de orden $>$ sobre el conjunto de los monomios de A es un **orden monomial** si es

1. total,
2. compatible con el producto, es decir: $\forall \mathbf{x}^\alpha, \mathbf{x}^\beta, \mathbf{x}^\gamma \in A$, $\mathbf{x}^\alpha > \mathbf{x}^\beta \Rightarrow \mathbf{x}^\alpha\mathbf{x}^\gamma > \mathbf{x}^\beta\mathbf{x}^\gamma$, y
3. si es un **buen orden**, es decir si todo subconjunto no vacio de monomios de A tiene mínimo.

La última condición en la definición anterior es equivalente a la que queríamos: toda sucesión decreciente de monomios de A estabiliza. Es muy facil demostrar el contrarecíproco de esta equivalencia (ver [5, Lemma 2, p.53]). Además, si suponemos que se cumplen

las dos primeras condiciones (es decir que la relación de orden es total y compatible con el producto) la tercera condición es equivalente a otras tres condiciones:

Proposición 5. *Si $>$ es una relación de orden sobre el conjunto de los monomios de A que cumple las condiciones 1 y 2 de la definición 4, entonces las siguientes propiedades son equivalentes:*

1. *$>$ es un buen orden;*
2. *$\forall\ \mathbf{x}^\alpha \in A\ /\ \mathbf{x}^\alpha \neq 1,\ \mathbf{x}^\alpha > 1$;*
3. *$\forall\ i,\ 1 \leq i \leq n,\ x_i > 1$;*
4. *$\forall\ \mathbf{x}^\alpha, \mathbf{x}^\beta \in A\ /\ \mathbf{x}^\alpha \neq \mathbf{x}^\beta,\ \mathbf{x}^\alpha | \mathbf{x}^\beta \Rightarrow \mathbf{x}^\beta > \mathbf{x}^\alpha$.*

Demostración. La demostración es sencilla. Para $1 \Rightarrow 3$ usaremos el contrarecíproco, $3 \Rightarrow 2$ se demuestra por inducción sobre $\deg \alpha$, $2 \Rightarrow 4$ es directo y facil, y $4 \Rightarrow 1$ se obtiene usando el teorema 1 (propiedad 1) y la proposición 3 (propiedad 1). □

Nota 6. Dado que aquí sólo vamos a trabajar con polinomios, hemos seguido la terminología usual en este contexto. Por ejemplo, la definición de orden monomial que damos en la definición 4 coincide con [5, Definition 1, p. 53] y [12, Definition 2.1]. Sin embargo, no coincide con [14, Definition 1.2.1] donde sólo se exigen las propiedades 1 y 2 de la definición 4 para definir un orden monomial. Cuando también se cumple la propiedad 3 de la definición 4 (es decir, por la proposición 5, cuando además para todo $\mathbf{x}^\alpha \in A$ tal que $\mathbf{x}^\alpha \neq 1$ se tiene $\mathbf{x}^\alpha > 1$), se habla en [14] de *orden monomial global*, en contraposición con la noción de *orden monomial local* que es aquel que cumple las condiciones 1 y 2 de la definición 4 y tal que, para todo $\mathbf{x}^\alpha \in A$ con $\mathbf{x}^\alpha \neq 1$, se tiene $\mathbf{x}^\alpha < 1$ (véase [14, Definition 1.2.4]). La noción de orden monomial local es necesaria para manipular series formales ya que, en lugar de trabajar mirando el término mayor de un polinomio, se trabaja mirando el término más pequeño de la serie. Allí aparece la diferencia entre las *standard bases* de Hironaka y las *Gröbner bases* de Buchberger. Como en estas notas sólo trabajaremos con polinomios, nos limitamos a los ordenes monomiales globales.

Los tres ejemplos clásicos de órdenes monomiales son los siguientes:

1. El **orden lexicográfico** (*lex*):

   $\mathbf{x}^\beta >_{lex} \mathbf{x}^\alpha \iff$ la primera componente no nula del vector $\beta - \alpha$ es positiva.

2. El **orden lexicográfico graduado** (*glex*):

   $\mathbf{x}^\beta >_{glex} \mathbf{x}^\alpha \iff [\deg \mathbf{x}^\beta > \deg \mathbf{x}^\alpha]$ ó $[\deg \mathbf{x}^\beta = \deg \mathbf{x}^\alpha$ y $\mathbf{x}^\beta >_{lex} \mathbf{x}^\alpha]$.

3. El **orden lexicográfico inverso graduado** (*grevlex*):

   $\mathbf{x}^\beta >_{grevlex} \mathbf{x}^\alpha \iff$ $[\deg \mathbf{x}^\beta > \deg \mathbf{x}^\alpha]$ ó $[\deg \mathbf{x}^\beta = \deg \mathbf{x}^\alpha$ y la última componente no nula del vector $\beta - \alpha$ es negativa].

Es un ejercicio fácil de demostrar que cada una de estas relaciones de orden cumple las 2 primeras condiciones de la definición 4 y la tercera de la proposición 5 y que por tanto son órdenes monomiales. Existen muchas otras formas de definir órdenes monomiales (véase, por ejemplo, el orden producto definido en la sección 5, ejercicio 2).

De manera general, calificaremos un orden monomial como *graduado* cuando ordena los monomios primero por su grado total (como *glex* y *grevlex*). Dado un orden monomial no graduado (por ejemplo *lex*), se le puede siempre asociar un orden monomial graduado ordenando los monomios primero por su grado total y luego con el orden monomial propuesto para desempatar los monomios de mismo grado. Otra variante sería hacer lo mismo pero dando pesos distintos a las variables, es decir sustituyendo en la definición de *glex*, de *grevlex*, o de cualquier orden graduado, el grado total de los monomios ($\deg \mathbf{x}^\alpha = \sum_{i=1}^n \alpha_i$) por un orden pesado ($\deg_{\mathbf{w}} \mathbf{x}^\alpha = \sum_{i=1}^n w_i \alpha_i$ para unos pesos w_i dados). Así se definen los llamados *órdenes pesados*.

Observamos que el orden lexicográfico inverso no graduado no es un orden monomial según nuestra definición 4. Es facil comprobar que es una relación de orden total compatible con el producto pero que no es un buen orden (sería un orden monomial local en el sentido de [14]). Con esta observación vemos claramente que la diferencia entre el orden lexicográfico y el orden lexicográfico inverso no es simplemente una reordenación de las variables (un error frecuente cuando se empieza a manejar estos conceptos). Son dos ordénes radicalmente distintos tal como observaremos más adelante.

Nota 7. Se puede usar una matriz inversible $n \times n$ con entradas enteras M para definir una relación de orden sobre el conjunto de los monomios de A de la manera siguiente: $\mathbf{x}^\beta >_M \mathbf{x}^\alpha \iff \mathbf{x}^{M.^t\beta} >_{lex} \mathbf{x}^{M.^t\alpha}$. Un resultado de Robbiano (1985) demuestra que toda relación de orden total sobre el conjunto de los monomios de A que sea compatible con el producto se puede obtener de esta manera; véase [14, Remark 1.2.7]. En particular, todo orden monomial tal como lo hemos definido en la definición 4 es de esta forma.[2]

[2]En este sentido, todos los órdenes monomiales pueden considerarse equivalentes tal como lo ob-

Definición 8. Fijado un orden monomial $>$ sobre A y dado un polinomio $f = \sum_\alpha a_\alpha \mathbf{x}^\alpha \in A$ no nulo, utilizaremos las siguientes nociones:

- el *monomio inicial* de f, denotado por $\text{in}(f)$, es el mayor de los monomios que forman el polinomio f (con respecto al orden $>$ elegido), es decir:

$$\text{in}(f) = \text{máx}\{\mathbf{x}^\alpha \,/\, a_\alpha \neq 0\} = \text{máx}\{\mathbf{x}^\alpha \,/\, \mathbf{x}^\alpha \in \text{supp}(f)\};$$

- el *coeficiente dominante* de f es el elemento de K que acompaña $\text{in}(f)$, es decir a_α si $\text{in}(f) = \mathbf{x}^\alpha$, y el *término dominante* de f, denotado por $\text{lt}(f)$, es el producto de su coeficiente dominante por su monomio inicial.

Por ejemplo, si $f = x^2yz^2 + 2xy^3 - 7y^4z \in \mathbb{Q}[x, y, z]$ y si fijamos sobre $\mathbb{Q}[x, y, z]$ el orden lexicográfico inverso graduado, entonces el monomio inicial de f es $\text{in}(f) = y^4z$. Sus coeficiente y término dominantes son -7 y $\text{lt}(f) = -7y^4z$ respectivamente.

2.2. El algoritmo de división sobre $K[x_1, \ldots, x_n]$

Una vez fijado un orden monomial sobre A, ya podemos plantear un algoritmo de división muy parecido al que conocemos con una variable. Empezamos ordenando de mayor a menor los monomios que forman los polinomios implicados y aplicamos el mismo principio que con una variable: un paso del algortimo consistirá en restar al resto parcial obtenido hasta el momento un múltiplo del divisor para que baje estrictamente el monomio inicial y así obtener el siguiente resto parcial. Y terminaremos la división cuando no podamos hacer nada más. Las diferencias principales con el caso de una variable son las siguientes:

- Si pensamos aquí en el problema de pertenencia planteado en la introducción, dado que el anillo A no es un dominio de ideales principales si $n \geq 2$, necesitaremos poder dividir un polinomio $f \in A$ no sólo por un polinomio sino por una lista (a priori ordenada) de polinomios, $[f_1, \ldots, f_m]$. Esto no es ningún problema. Primero miraremos si el resto parcial de la división se divide por $\text{in}(f_1)$. Si es el caso, restaremos el múltiplo conveniente de f_1 para que baje el monomio inicial y obtendremos el siguiente resto parcial. En caso contrario, probaremos con los siguientes elementos de la lista. Iremos contruyendo de esta manera los cocientes relativos a los distintos polinomios de la lista de divisores.

servó José Manuel Aroca durante el curso. Sin embargo veremos en la sección 4 que los órdenes monomiales se comportan de manera muy distinta y usaremos algunos, y otros no, para resolver ciertos problemas (por ejemplo el problema de eliminación de variables).

- Cuando encontramos que el monomio inicial del resto parcial no se divide por ninguno de las monomios iniciales de la lista $[f_1, \ldots, f_m]$, la división no tiene porque haber terminado. En efecto, algún monomio más pequeño que el monomio inicial podría dividirse por alguno de los términos iniciales de nuestra lista, digamos $\text{in}(f_i)$. Si eso pasa, queremos restar de nuevo un múltiplo de f_i para que baje este término. Es una situación que no podía darse con una variable (¿porque? dejo esta pregunta facil como ejercicio). De nuevo esto no es ningún problema: construiremos el resto poco a poco, almacenando el término dominante del resto parcial cuando éste no se divide por ninguno de los monomios iniciales de nuestra lista y seguiremos con nuestra división. Ésta habrá terminado cuando lleguemos a un resto parcial nulo.

Estas observaciones nos llevan de manera natural al siguiente algoritmo:

Algoritmo 9 (Algoritmo de división)**.** Para dividir el polinomio $f \in A$ por la lista ordenada de polinomios $[f_1, \ldots, f_m]$ aplicaremos el siguiente algoritmo que hemos escrito en pseudocódigo en la columna de la izquierda y comentado en la columna de la derecha:

Input: $f, f_1, \ldots, f_m$	Los datos de entrada son los polinomios $f, f_1, \ldots, f_m$.
Output: $q_1, \ldots, q_m, r$	Obtendremos como salida los cocientes $q_1, \ldots, q_m$ y el resto r.
$q_1 := 0; \ldots; q_m := 0; r := 0$	Inicializamos cocientes y resto a 0.
$p := f$	La variable p es el resto parcial que inicializamos a f.
WHILE $p \neq 0$ DO	Terminaremos la división cuando el resto parcial será nulo.
$i := 1; d := 0$	Inicializamos las 2 variables auxiliares i y d
WHILE $i \leq m$ AND $d = 0$ DO	que son las que nos permitiran salir de este bucle WHILE.
IF $\text{in}(f_i) \mid \text{in}(p)$ THEN	Si el monomio inicial de f_i divide a p, entonces
$q_i := q_i + \text{lt}(p)/\text{lt}(f_i)$	modificamos el cociente correspondiente a f_i,
$p := p - (\text{lt}(p)/\text{lt}(f_i))f_i$	restamos a p el múltiplo de f_i que elimina su monomio inicial,
$d := 1$	y salimos del bucle: hemos realizado un paso de la división.
ELSE	Si el monomio inicial de f_i no divide a p,
$i := i + 1$	probamos con el siguiente de la lista.
IF $d = 0$ THEN	Si aquí $d = 0$, entonces $\text{in}(f_1) \not\mid \text{in}(p), \ldots, \text{in}(f_m) \not\mid \text{in}(p)$.
$p := p - \text{lt}(p)$	En este caso, quitamos $\text{lt}(p)$ del resto parcial,
$r := r + \text{lt}(p)$	lo guardamos en el resto,
	y seguimos con la división volviendo al inicio del bucle.

Cuando el algoritmo acaba, las variables $q_1, \ldots, q_m, r$ contienen los cocientes y el resto de

la división.

Si p es el resto parcial en un paso dado de la división, pueden ocurrir dos cosas:

- ó bien $\text{in}(p)$ se divide por uno de los monomios iniciales de los divisores. En este caso, si f_i es el primer elemento de la lista ordenada $[f_1, \ldots, f_m]$ cuyo monomio inicial divide a $\text{in}(p)$, modificamos el cociente q_i y le restamos a p un múltiplo de f_i (precisamente el múltiplo de f_i que cancela el término dominante de p);
- ó bien $\text{in}(p)$ no se divide por ninguno de los monomios iniciales de los divisores. En este caso, le restamos a p su término dominante y se lo añadimos al resto r.

Es facil comprobar que en ambos casos, ocurre lo siguiente:

1. el monomio inicial del resto parcial baja (estrictamente) en cada paso del algoritmo de división (ó bien porque le hemos restado un múltiplo de un elemento de la lista de divisores, ó bien porque le hemos restado su término dominante), y
2. en cada paso de la división, si p es el resto parcial en este paso, se cumple la igualdad:

$$f = q_1 f_1 + \cdots + q_m f_m + r + p\,.$$

Como consecuencia de 1, y usando que nuestro orden monomial es un buen orden, obtenemos que el algoritmo de división termina, es decir que llegamos siempre en un número finito de pasos a $p = 0$. Y por 2 concluimos que cuando el algoritmo ha terminado, hemos llegado a expresar f de la manera descrita en el siguiente resultado que queda, por tanto, demostrado:

Teorema 10. *Fijado un orden monomial $>$ sobre A y dados $f, f_1, \ldots, f_m \in A$ no nulos, existen polinomios $q_1, \ldots, q_m, r \in A$ tales que*

$$f = q_1 f_1 + \cdots + q_m f_m + r$$

y satisfaciendo las dos propiedades siguientes:

1. $\forall\, \mathbf{x}^\alpha \in \text{supp}\,(r),\ \mathbf{x}^\alpha \notin (\text{in}\,(f_1), \ldots, \text{in}\,(f_m))$;
2. $\forall\, i \in \{1, \ldots, m\} \,/\, q_i \neq 0,\ \text{in}\,(f) \geq \text{in}\,(q_i f_i)$.

Ejemplo 11. En $\mathbb{Q}[x,y,z]$ con el orden lexicográfico inverso graduado, si aplicamos el algoritmo 9 a los polinomios $f = x^2y^3z^3 + x^4y + y^3z^2 + xyz^2$, $f_1 = xy - z^2$, $f_2 = x^2 - yz$, $f_3 = y^3 - xz^2$, obtenemos que

$$f = q_1f_1 + q_2f_2 + q_3f_3 + r$$

para $q_1 = xy^2z^3 + yz^5 + x^3 + z^3 + z^2$, $q_2 = xz^2$, $q_3 = z^2$, y $r = yz^7 + xz^4 + z^5 + z^4$.

Observamos que, a diferencia del caso de una variable, no hemos hablado de unicidad de los cocientes y del resto en el teorema 10. De hecho no la hay como podemos observar volviendo al ejemplo 11. Como $\mathrm{in}\,(f) = x^2y^3z^3$, vemos que $\mathrm{in}\,(f)$ no sólo se divide por $\mathrm{in}\,(f_1) = xy$ sino que también es múltiplo de $\mathrm{in}\,(f_2) = x^2$ y de $\mathrm{in}\,(f_3) = y^3$. Es por tanto facil imaginar que el resultado de la división será distinto si en el primer paso de la división, en lugar de restar a f un múltiplo de f_1, empezamos restando un múltiplo de f_2 o de f_3. Se podría por ejemplo llegar, en este ejemplo, a la expresión

$$f = q_1'f_1 + q_2'f_2 + q_3'f_3 + r'$$

para $q_1' = z^6 + z^2$, $q_2' = y^3z^3 + x^2y + y^2z$, $q_3' = yz^4 + 2z^2$, $r' = z^8 + 2xz^4 + z^4$, que también cumplen las condiciones del teorema 10.

Esto nos lleva a la siguiente definición que resultará de interés en el teorema 22.

Definición 12. Dados una lista de polinomios $\mathcal{F} = \{f_1, \ldots, f_m\}$ de A y otro polinomio f, si existe una expresión de la forma

$$f = q_1f_1 + \ldots + q_mf_m + r$$

con $q_1, \ldots, q_m, r \in A$ que cumpla las condiciones 1 y 2 del teorema 10, se dice que r *es una reducción de* f *módulo* $\mathcal{F}$ o que f *se reduce a* r *módulo* $\mathcal{F}$. Cuando esto ocurre, usaremos la notación $f \to_{\mathcal{F}} r$. Está claro que el resto de la división de f por los elementos de $\mathcal{F}$ obtenido aplicando el algoritmo 9 es una reducción de f módulo $\mathcal{F}$ pero en general no es la única.

Nota 13. La no unicidad del resto en el teorema 10 impide usar directamente el algoritmo de división para resolver el problema de pertenencia planteado en la introducción. Obviamente si encontramos un resto nulo al dividir f por $f_1, \ldots, f_m$ podemos concluir que $f \in I = (f_1, \ldots, f_m) \subset A$. Pero si $r \neq 0$, no podemos concluir nada por culpa de la no unicidad del resto. En efecto, basta con tomar un ejemplo en el que encontremos dos restos distintos r, r' cumpliendo el resultado del teorema 10 (como en el ejemplo 11). Entonces claramente tendremos que $r - r' \in I$ pero el resto de la división de $r - r'$ por $f_1, \ldots, f_m$ es $r - r' \neq 0$. Las bases de Gröbner permitirán justamente solucionar este problema.

2.3. Bases de Gröbner

Empezamos definiendo el concepto de ideal inicial de un ideal.

Definición 14. Fijamos un orden monomial $>$ sobre A. Dado un ideal I de A no nulo, el *ideal inicial de I respecto del orden monomial $>$*, denotado por $\text{in}(I)$[3], es el ideal monomial engendrado por los monomios iniciales de todos los elementos de I, es decir

$$\text{in}(I) = (\{\text{in}(f) \,/\, f \in I\}).$$

Claramente si tenemos un sistema de generadores $\{f_1, \ldots, f_m\}$ de un ideal I de A, no es cierto en general que $\text{in}(I)$ esté engendrado por los monomios iniciales de estos elementos. Basta con volver al ejemplo mencionado en la nota 13 para ver que el elemento $r - r'$ $(\neq 0)$, que pertenece al ideal $I = (f_1, \ldots, f_m)$, satisface que ninguno de sus monomios, y en particular su monomio inicial, pertenece al ideal $(\text{in}(f_1), \ldots, \text{in}(f_m))$ por lo que hemos encontrado un elemento de I cuyo monomio inicial no pertenece a $(\text{in}(f_1), \ldots, \text{in}(f_m))$.

Esto nos lleva a la siguiente definición.

Definición 15. Una *base de Gröbner* de un ideal no nulo I de A respecto de un orden monomial $>$ es un subconjunto **finito** de elementos de I, $\mathcal{G} = \{g_1, \ldots, g_t\}$, cuyos monomios iniciales generan $\text{in}(I)$, es decir tales que

$$\text{in}(I) = (\text{in}(g_1), \ldots, \text{in}(g_t)).$$

Por el Teorema de la Base de Hilbert (propiedad 1 del teorema 1), todo ideal no nulo I de A admite una base de Gröbner[4]

Observamos que en la definición 15, no pedimos que $\mathcal{G}$ sea un sistema de generadores del ideal I ya que con esta definición, aparentemente más débil, se obtiene que I está engendrado por $\mathcal{G}$:

[3]El ideal inicial depende claramente del orden monomial elegido. Cuando la notación $\text{in}(I)$ resulte confusa, usaremos la notación $\text{in}_>(I)$.

[4]Lo que necesitamos aquí es un resultado más debil, el Lema de Dickson, que viene a ser la propiedad 1 del teorema 1 para ideales monomiales y se demuestra directamente por inducción sobre el número n de variables de A; véase [5, Section 2.4]. Entonces el teorema 1 viene a ser consecuencia inmediata del teorema 16 que demostramos a continuación. Observamos por tanto que no era necesario suponer conocido el Teorema de la Base de Hilbert ya que las bases de Gröbner nos permiten deducir este resultado del Lema de Dickson. Según Eisenbud ([10, Exercice 15.15]), esta demostración del Teorema de la Base de Hilbert está inspirada en la prueba dada por Gordan en 1900 que podría considerarse como el primer uso de la noción de ideal inicial.

Teorema 16. *Toda base de Gröbner de I es un sistema de generadores de I.*

Demostración. Si $\mathcal{G} = \{g_1, \ldots, g_t\}$ es una base de Gröbner de un ideal I de A no nulo, está claro que $(\mathcal{G})$, el ideal engendrado por los elementos de $\mathcal{G}$, está contenido en I, $(\mathcal{G}) \subseteq I$. Para ver la otra inclusión, tomamos un elemento f de I arbitrario y lo dividimos por los elementos de $\mathcal{G}$. Obtenemos que $f = q_1 g_1 + \cdots + q_t g_t + r$ para unos polinomios $q_1, \ldots, q_t, r$ de A tales que, para todo monomio $\mathbf{x}^\alpha$ de $\operatorname{supp}(r)$, $\mathbf{x}^\alpha \notin (\operatorname{in}(g_1), \ldots, \operatorname{in}(g_t))$ pero este ideal monomial coincide con $\operatorname{in}(I)$ ya que $\mathcal{G}$ es una base de Gröbner de I. Esto implica que si $r \neq 0$, $\operatorname{in}(r) \notin \operatorname{in}(I)$, una contradicción ya que $r = f - (q_1 g_1 + \cdots + q_t g_t) \in I$. Por lo concluimos que $r = 0$, y por tanto $f \in (\mathcal{G})$. □

Véamos ahora que la no unicidad del resto en la división de un polinomio f de A por una lista de polinomios de A desaparece cuando esta lista es una base de Gröbner:

Proposición 17. *Supongamos que $\mathcal{G} = \{g_1, \ldots, g_t\}$ es una base de Gröbner de un ideal I de A respecto de un orden monomial fijo sobre A. Entonces, para todo polinomio f de A, existen dos polinomios q y r de A, únicos, tales que:*

- $f = q + r$,
- $q \in I$, *y*
- $\forall\, \mathbf{x}^\alpha \in \operatorname{supp}(r),\ \mathbf{x}^\alpha \notin (\operatorname{in}(g_1), \ldots, \operatorname{in}(g_t))$.

Demostración. La existencia es consecuencia directa del teorema 10: si dividimos f por los elementos de $\mathcal{G}$, obtenemos $q_1, \ldots, q_t, r \in A$ tales que $f = q_1 g_1 + \cdots + q_t g_t + r$ y si tomamos $q = q_1 g_1 + \cdots + q_t g_t$, los polinomios q y r cumplen las condiciones de la proposición.

Para la unicidad, supongamos que $f = q + r = q' + r'$ para $q, q', r, r' \in A$ con $q, q' \in I$ y r, r' cumpliendo la tercera condición de la proposición. Entonces $r - r' = q' - q \in I$ y por tanto $\operatorname{in}(r - r') \in \operatorname{in}(I)$. Si $r - r' \neq 0$, el monomio $\operatorname{in}(r - r')$ tiene que pertenecer al ideal $(\operatorname{in}(g_1), \ldots, \operatorname{in}(g_t))$ ya que $\mathcal{G}$ es una base de Gröbner de I. Pero $\operatorname{in}(r - r') \in \operatorname{supp}(r) \cup \operatorname{supp}(r')$ lo cual contradice que tanto r como r' cumplen la tercera condición de la proposición por lo $r - r' = 0$, y por tanto $r = r'$ y $q = q'$. □

Observamos que con este resultado ya tenemos resuelto el problema de pertenencia:

Corolario 18. *Si $\mathcal{G} = \{g_1, \ldots, g_t\}$ es una base de Gröbner de un ideal I de A respecto de un orden monomial fijo sobre A y f es un polinomio de A, tenemos que*

$$f \in I \iff \textit{el resto de la división de } f \textit{ por los elementos de } \mathcal{G} \textit{ es nulo.}$$

Demostración. Como $I = (\mathcal{G})$ por el teorema 16, la implicación ($\Leftarrow$) es cierta. Recíprocamente, si $f \in I$, entonces para $q = f$ y $r = 0$ tenemos dos polinomios $q, r \in A$ que cumplen las condiciones de la proposición 17. Como ya hemos observado que la división de f por los elementos de $\mathcal{G}$ proporciona también dos polinomios que cumplen las condiciones, por unicidad obtenemos el resultado. □

Para que el resultado anterior sea efectivo, nos queda determinar si un conjunto de generadores de un ideal es o no una base de Gröbner, y en caso de que no lo sea, construir una base de Gröbner a partir del sistema de generadores dado. Estos dos problemas se resuelven en el siguiente capítulo.

3. Herramientas para trabajar con bases de Gröbner

3.1. El criterio de Buchberger

Lo primero que necesitamos es un criterio para determinar si un subconjunto finito $\mathcal{G} = \{g_1, \ldots, g_t\}$ de un ideal I de A es o no una base de Gröbner de I respecto de un orden monomial $>$ dado. El criterio de Buchberger proporciona tal criterio pero antes de enunciarlo, veamos en dos ejemplos que dicho criterio surge de manera muy natural al querer comprobar si un sistema de generadores dado es o no una base de Gröbner utilizando la definición (de momento no tenemos otra herramienta entre las manos para hacerlo).

Ejemplo 19. En $\mathbb{Q}[x, y]$, fijamos el orden lexicográfico (*lex*) y consideramos dos polinomios, $f_1 = xy - 1$, $f_2 = y^2 - 1$, el ideal I que generan, $I = (f_1, f_2)$, y nos preguntamos si $\{f_1, f_2\}$ es una base de Gröbner de I para el orden *lex*, es decir si $\operatorname{in}(I) = J$ siendo J el ideal $J = (\operatorname{in}(f_1), \operatorname{in}(f_2)) = (xy, y^2)$. Si tomamos cualquier múltiplo de f_1, obtendremos un elemento de I cuyo monomio inicial pertenece a J. Lo mismo ocurre con cualquier múltiplo de f_2, o con cualquier combinación de f_1 y f_2, $q_1 f_1 + q_2 f_2$, cuyo monomio inicial sea $\operatorname{in}(q_1 f_1)$ o $\operatorname{in}(q_2 f_2)$. Por tanto la única forma en nuestro contexto de obtener un elemento de I cuyo monomio inicial no pertenezca a J es tomar una combinación $q_1 f_1 + q_2 f_2$ de f_1 y f_2 tal que $\operatorname{in}(q_1 f_1 + q_2 f_2) \neq \operatorname{in}(q_1 f_1)$ y $\operatorname{in}(q_1 f_1 + q_2 f_2) \neq \operatorname{in}(q_2 f_2)$. Para ello es necesario que los términos dominantes de $q_1 f_1$ y $q_2 f_2$ se cancelen al sumarse. La combinación más económica en este sentido consiste en elegir $q_1 = \dfrac{\mathbf{x}^\gamma}{\operatorname{lt}(f_1)}$ y $q_2 = -\dfrac{\mathbf{x}^\gamma}{\operatorname{lt}(f_2)}$ donde

$\mathbf{x}^\gamma$ es el máximo divisor común (m.c.d.) de $\mathrm{in}\,(f_1)$ e $\mathrm{in}\,(f_2)$, es decir $q_1 = y$ y $q_2 = -x$. Obtenemos de esta manera el elemento $yf_1 - xf_2 = x - y$ de I cuyo monomio inicial es x. Como $x \notin J$, se incumple la definición 15 y concluimos que $\{f_1, f_2\}$ no es una base de Gröbner de I para el orden *lex*.

Ejemplo 20. Consideramos ahora los dos polinomios $f_1 = x + z$ y $f_2 = y - z$ de $\mathbb{Q}[x, y, z]$ y de nuevo nos preguntamos si $\{f_1, f_2\}$ es una base de Gröbner de $I = (f_1, f_2)$ para el orden *lex*, es decir si $\mathrm{in}\,(I) = J$ con $J = (\mathrm{in}\,(f_1), \mathrm{in}\,(f_2)) = (x, y)$. Aplicando exactamente la misma idea que en el ejemplo anterior, obtenemos la combinación $yf_1 - xf_2 = xz + yz$ pero ahora el monomio inicial de este elemento de I es xz que si pertenece a J. Esto no demuestra que $\{f_1, f_2\}$ sea una base de Gröbner de I para el orden *lex* ya que otra combinación de f_1 y f_2 podría proporcionar un elemento cuyo monomio inicial no pertenezca a J. Por ejemplo podríamos dividir el elemento $xz + yz$ de I que hemos obtenido por $\{f_1, f_2\}$ para ver si el resto es nulo o no. Si no es nulo, ya tendríamos el elemento de I que buscamos. Al realizar la división obtenemos que $xz + yz = zf_1 + zf_2$ y el resto es nulo. De momento esto tampoco nos permite concluir que $\{f_1, f_2\}$ sea una base de Gröbner, pero ya se nos agotan las ideas para encontrar un elemento de I cuyo monomio inicial no pertenezca a J. De hecho el criterio de Buchberger nos dirá que si de esta manera no lo hemos encontrado, entonces no lo hay, y esto nos permitirá concluir que $\{f_1, f_2\}$ si es una base de Gröbner de I para el orden *lex*.

La siguiente definición intenta formalizar la idea introducida en los ejemplos anteriores.

Definición 21. Fijamos un orden monomial $>$ sobre A. Dados f, g dos polinomios no nulos de A, si $\mathbf{x}^\gamma$ es el m.c.d. de $\mathrm{in}\,(f)$ e $\mathrm{in}\,(g)$, el *S-polinomio de f y g*:

$$S(f, g) = \frac{\mathbf{x}^\gamma}{\mathrm{lt}\,(f)} \times f - \frac{\mathbf{x}^\gamma}{\mathrm{lt}\,(g)} \times g\,.$$

Las combinaciones de f_1 y f_2 construidas en los dos ejemplos anteriores son justamente los S-polinomios de f_1 y f_2. El S-polinomio de dos polinomios f y g es la combinación de estos dos polinomios que produce una cancelación de los términos dominantes, es decir:

$$\forall f, g \in A,\ \mathrm{in}\,(S(f, g)) < \mathrm{in}\,(\frac{\mathbf{x}^\gamma}{\mathrm{lt}\,(f)} \times f) = \mathrm{in}\,(\frac{\mathbf{x}^\gamma}{\mathrm{lt}\,(g)} \times g)\,.$$

Podemos ahora enunciar el criterio de Buchberger.

Teorema 22. *Fijamos sobre A un orden monomial $>$ y consideramos un ideal $I = (g_1, \ldots, g_t)$ de A. Entonces las siguientes propiedades son equivalentes:*

1. $\mathcal{G} = \{g_1, \ldots, g_t\}$ *es una base de Gröbner de* I *respecto del orden* $>$*;*
2. $\forall\, i, j,\ 1 \leq i < j \leq t$*, el resto de la división de* $S(f_i, f_j)$ *por los elementos de* $\mathcal{G}$ *es* 0*;*
3. $\forall\, i, j,\ 1 \leq i < j \leq t$*,* $S(f_i, f_j) \to_{\mathcal{G}} 0$ *(ver la definición 12).*

Demostración. La prueba es algo técnica pero facil; véase, por ejemplo, [5, Thm. 6 p. 82, Thm. 3 p. 101] o [12, Thm. 2.14]. □

Ejemplo 23. Si volvemos ahora al ejemplo 20, el teorema 22 nos permite afirmar que $\{f_1, f_2\}$ es una base de Gröbner del ideal $I = (f_1, f_2)$ para el orden *lex*.

3.2. El algoritmo de Buchberger

Usando el criterio de Buchberger, se obtiene facilmente un algoritmo para comprobar si un sistema de generadores dado es o no una base de Gröbner y, si no lo es, para construir una a partir de este sistema de generadores.

Algoritmo 24 (Algoritmo de Buchberger)**.** Dado un sistema de generadores $\{f_1, \ldots, f_m\}$ de un ideal I de A, para determinar si es una base de Gröbner de I (para un orden monomial dado) y, si no lo es, obtener a partir de él una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_t\}$ de I, aplicaremos el siguiente algoritmo que hemos escrito en pseudocódigo en la columna de la izquierda y comentado en la columna de la derecha:

Input: $f_1, \ldots, f_m$	Los datos de entrada son los polinomios que generan I.
Output: $\mathcal{G} = \{g_1, \ldots, g_t\}$	Obtendremos como salida una base de Gröbner de I.
$\mathcal{G} := \{f_1, \ldots, f_m\}$	Inicializamos la variable $\mathcal{G}$ con los generadores originales.
REPEAT	Repetimos el bucle siguiente:
$\quad \mathcal{G}' := \mathcal{G}$	- guardamos lo que tenemos en $\mathcal{G}$ en la variable auxiliar $\mathcal{G}'$,
$\quad$ FOR each pair $\{p, q\}$, $p \neq q$ in $\mathcal{G}$ DO	- para cada par de elementos distintos de $\mathcal{G}$, calculamos
$\quad\quad S := \mathrm{rem}(S(p, q), \mathcal{G})$	el resto de la división de su S-polinomio por $\mathcal{G}$, y
$\quad\quad$ IF $S \neq 0$ THEN $\mathcal{G} := \mathcal{G} \cup \{S\}$	- si es no nulo, lo añadimos a la lista $\mathcal{G}$,
UNTIL $\mathcal{G} = \mathcal{G}'$	hasta que no encontremos ningún elemento nuevo.
$\mathcal{G}$	Si $\mathcal{G}$ no crece en el bucle anterior, es una base de Gröbner (por el criterio de Buchberger).

Cada vez que encontramos un resto no nulo al dividir el S-polinomio de dos elementos distintos de $\mathcal{G}$ por los elementos de $\mathcal{G}$, lo añadimos a $\mathcal{G}$ por lo que el ideal monomial

$(\mathrm{in}\,(g),\ g \in \mathcal{G})$ crece estrictamente. Por el teorema 1 (propiedad 2), podemos afirmar que el algoritmo termina ya que esta cadena ascendente de ideales monomiales tiene que estabilizar. Y por el criterio de Buchberger (teorema 22), cuando el algoritmo ha terminado, tenemos en $\mathcal{G}$ una base de Gröbner del ideal I que contiene nuestro sistema de generadores original (sólo hemos añadido elementos, no hemos quitado ninguno).

Ejemplo 25. Podemos ahora volver al ejemplo 19 donde $\{f_1, f_2\}$ no era una base de Gröbner de I para el orden *lex*. El primer paso del algoritmo produce el elemento $f_3 = x - y \in I$ que agregamos al conjunto de generadores para obtener $\mathcal{G} = \{f_1, f_2, f_3\}$. Si seguimos aplicando el algoritmo, vemos que $S(f_1, f_3) = f_1 - yf_3 = y^2 - 1 = f_2$ por lo que el resto de su división por los elementos de $\mathcal{G}$ es cero. Finalmente, $S(f_2, f_3) = xf_2 - y^2 f_3 = -x + y^3$ y la división de este polinomio por los elementos de $\mathcal{G}$ es $-x + y^3 = -f_3 + yf_2$. De nuevo el resto es nulo por lo que concluimos, aplicando el teorema 22, que $\mathcal{G} = \{f_1, f_2, f_3\}$ es una base de Gröbner del ideal $I = (f_1, f_2)$ para el orden *lex*.

3.3. El problema de la unicidad

Observamos que en una base de Gröbner $\mathcal{G}$ de un ideal $I \subset A$ respecto de un orden monomial $>$ dado, pueden sobrar claramente algunos elementos si los monomios iniciales de los elementos de $\mathcal{G}$ no generan $\mathrm{in}\,(I)$ minimalmente, algo que no hemos pedido en la definición 15. Podemos por tanto mejorar nuestra definición pidiendo esta condición adicional.

Definición 26. Fijamos sobre A un orden monomial $>$. Una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_t\}$ de un ideal I de A es *minimal* si los monomio iniciales de los elementos de $\mathcal{G}$ generan el ideal $\mathrm{in}\,(I)$ minimalmente, es decir si, además de la condición en la definición 15 se pide que

$$\forall\ i \in \{1, \ldots, t\},\ \mathrm{in}\,(g_i) \quad \notin \quad (\mathrm{in}\,(g_1), \ldots, \widehat{\mathrm{in}\,(g_i)} \ldots, \mathrm{in}\,(g_t))\,. \tag{2}$$

Se suele pedir además que los elementos de $\mathcal{G}$ sean polinomio unitarios, es decir que su coeficiente dominante sea 1.

Es fácil ver que, en cualquier base de Gröbner, suprimiendo todos los elementos cuyos monomios iniciales sobran para generar $\mathrm{in}\,(I)$ y normalizando los elementos que nos quedan, obtendremos una base de Gröbner minimal.

Ejemplo 27. Vemos que en la base de Gröbner $\{f_1, f_2, f_3\}$ obtenida en el ejemplo 25, el elemento f_1 sobra ya que $\text{in}\,(I) = (xy, y^2, x) = (y^2, x)$ por lo podemos afirmar que $\{f_2, f_3\}$ es una base de Gröbner minimal del ideal I para el orden *lex*.

Nota 28. Por la propiedad 2 en la proposición 3, observamos que, fijado un orden monomial $>$ sobre A, todas las bases de Gröbner minimales de un ideal I respecto de $>$ tendrán el mismo número de elementos. Es más, los términos dominantes de los elementos de una base de Gröbner minimal respecto de $>$ son idénticos en todas ellas. Pero aún así, no tenemos unicidad. En el ejemplo 27, $\{f_2, f_3\}$ y $\{f_2, f_3 + f_2\}$ son dos bases de Gröbner minimales del ideal I para el orden *lex*.

Para obtener un objeto único, exigiremos una condición más fuerte.

Definición 29. Fijamos sobre A un orden monomial $>$. Una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_t\}$ de un ideal I de A es *reducida* si el coeficiente dominante de cada elemento de $\mathcal{G}$ es 1, y si además

$$\forall\, i \in \{1, \ldots, t\},\ \forall\, \mathbf{x}^\alpha \in \text{supp}\,(g_i),\ \mathbf{x}^\alpha \notin (\text{in}\,(g_1), \ldots, \widehat{\text{in}\,(g_i)}, \ldots, \text{in}\,(g_t))\,. \tag{3}$$

La diferencia entre las nociones de base de Gröbner minimal y reducida es que la condición $\mathbf{x}^\alpha \notin (\text{in}\,(g_1), \ldots, \widehat{\text{in}\,(g_i)} \ldots, \text{in}\,(g_t))$ se exige sólo para el monomio $\mathbf{x}^\alpha = \text{in}\,(g_i)$ para la primera, y para todos los monomios del soporte de g_i (en particular para su monomio inicial) para la segunda. En particular, toda base de Gröbner reducida es minimal pero la recíproca no es cierta. Volviendo de nuevo al ejemplo 27, entre las dos bases de Gröbner minimales $\{f_2, f_3\}$ y $\{f_2, f_3 + f_2\}$ de I, sólo la primera es reducida.

Con esta definición, ya obtenemos unicidad:

Teorema 30. *Todo ideal no nulo I de A admite una única base de Gröbner reducida respecto de un orden monomial $>$ fijo de A.*

Demostración. Fijamos el orden monomial $>$ sobre A. Como ya hemos observado, todo ideal I de A admite una base de Gröbner respecto de $>$, y de ésta siempre podemos extraer una base de Gröbner minimal, $\mathcal{G} = \{g_1, \ldots, g_t\}$. Entonces, por la propiedad (2), para todo $i \in \{1, \ldots, t\}$, si dividimos g_i por los elementos de $\{g_1, \ldots, \widehat{g_i}, \ldots, g_t\}$, obtendremos un resto r_i tal que $\text{in}\,(g_i) = \text{in}\,(r_i)$ y como $r_i \in I$, obtenemos que $\{r_1, \ldots, r_t\}$ también es una base de Gröbner minimal de I. Pero cumple además la propiedad (3) por lo que es reducida, y esto justifica la existencia de una base de Gröbner reducida.

Supongamos ahora que tenemos dos bases de Gröbner reducidas $\mathcal{G}$ y $\mathcal{G}'$ de I respecto del mismo orden monomial $>$. Como ambas son minimales, tienen el mismo número de elementos y además los monomios iniciales de ambas coinciden, es decir que, reordenando los elementos, podemos suponer que $\mathcal{G} = \{g_1, \ldots, g_t\}$, $\mathcal{G}' = \{g'_1, \ldots, g'_t\}$ y para todo $i \in \{1, \ldots, t\}$, $\text{in}(g_i) = \text{in}(g'_i)$. Pero g_i y g'_i son dos polinomios unitarios con el mismo monomio inicial por lo que al hacer la diferencia, se cancelan los dos términos dominantes. Esto implica que para todo monomio $\mathbf{x}^\alpha$ del soporte de $g_i - g'_i$, tenemos que $\mathbf{x}^\alpha$ es estrictamente más pequeño que $\text{in}(g_i) = \text{in}(g'_i)$ y por tanto no se divide por este monomio por la propiedad 4 de la proposición 5. Pero tampoco se divide por los demás generadores del ideal $\text{in}(I)$ por la propiedad (3) por lo que tenemos que $\mathbf{x}^\alpha \notin \text{in}(I)$ lo cual es imposible si $g_i - g'_i \in I$. Concluimos por tanto que $\text{supp}(g_i - g'_i) = \emptyset$ o, lo que es lo mismo, que $g_i = g'_i$. Esto justifica la unicidad de la base de Gröbner reducida respecto de $>$. □

La primera parte de la prueba del resultado anterior nos dice también cómo construir la base de Gröbner reducida de un ideal I dado cuando tenemos una base de Gröbner. Primero suprimimos los elementos superfluos (simplemente quitando los elementos cuyo monomio inicial no pertenece al sistema minimal de generadores monomiales de $\text{in}(I)$, es decir que es múltiplo del monomio inicial de otro elemento tal como lo hicimos en el ejemplo 27) y normalizamos los demás elementos (dividiendo por su coeficiente dominante) para obtener una base de Gröbner minimal. Luego reducimos cada elemento de la base de Gröbner minimal así obtenida por los demás elementos, por ejemplo sustituyendo cada elemento por su resto en la división por los demás elementos.

Nota 31. Observamos que la unicidad de la base de Gröbner reducida permite contestar a la siguiente pregunta: dados dos ideales I y J de A,

$$\text{¿ cómo determinar si } I = J? \tag{4}$$

Eligiendo un orden monomial $>$ sobre A, la unicidad en el teorema 30 nos permite afirmar que $I = J$ si y sólo si sus bases de Gröbner reducidas respecto de $>$ coinciden. Esto proporciona un método efectivo para contestar a la pregunta (4). También podríamos usar la solución que hemos dado al problema de pertenencia para contestar a esta pregunta pero este método sería menos eficiente. Veremos en la sección 4.3 una tercera forma de contestar a (4) que nos permitirá detectar, en caso de que los dos ideales no coincidan, si uno está contenido en el otro.

Por supuesto, si cambiamos el orden monomial sobre A, puede que la base de Gröbner reducida del I cambie. Sin embargo, se puede demostrar que el número de ideales iniciales

distintos de I es finito aunque tengamos infinitos órdenes monomiales distintos sobre A (si $n \geq 2$); véase [18, Theorem 1.2]. Esto permite garantizar que cualquier ideal I de A admite un subconjunto finito que es una base de Gröbner respecto de cualquier orden monomial. Esto lleva a la siguiente definición:

Definición 32. Una *base de Gröbner universal* de un ideal no nulo I de A es un subconjunto finito de elementos de I que es una base de Gröbner de I respecto de cualquier orden monomial sobre A.

3.4. El programa Singular

Presentamos aquí una muy breve introducción al programa Singular ([7]) ya que utilizaremos este programa en la sección 4 para resolver, en algunos ejemplos, varios de los problemas allí planteados.

Lo primero absolutamente fundamental es saber cómo pedir ayuda utilizando el manual online del programa. Éste se abre en una ventana emergente así:

```
> help;
```

Resultarán de especial utilidad el índice (*Table of contents*) y el índice alfabético (*Index*). No explicaremos en estas notas como se usan los comandos de Singular que manejaremos. Dejamos al lector usar la ayuda del programa mientras va realizando la parte práctica del curso (en particular en la sección 4).

Empezaremos definiendo el anillo de polinomios en el que estaremos trabajando. En Singular el anillo de polinomios $K[x_1, \ldots, x_n]$ se define dando la característica del cuerpo K, las variables $x_1, \ldots, x_n$, y el orden monomial que fijamos. Si cambiamos el orden monomial, cambiaremos de anillo para Singular. Definimos por ejemplo el anillo $\mathbb{Q}[x, y, z]$ con el orden *grevlex* al que llamamos `A` de la manera siguiente:

```
> ring A=0,(x,y,z),dp;
```

Los órdenes *lex*, *glex* y *grevlex* se codifican en Singular con `lp`, `Dp` y `dp` respectivamente. Recomiendo usar el manual online para ver cómo definir otros órdenes monomiales, por

ejemplo un orden producto o un orden pesado. En Singular también se pueden definir órdenes locales.

Luego podemos definir un polinomio o un ideal. Definamos por ejemplo el polinomio $x^2y^3z^3 + y^3z^2 - x^4y - xyz^2$ de `A` al que llamanos `P`:

```
> poly P=x2y3z3+y3z2-x4y-xyz2;
```

Si le preguntamos a continuación lo que contiene la variable `P` nos contestará:

```
> P;
x2y3z3-x4y+y3z2-xyz2
```

Observamos que ha reordenado los monomios del soporte de nuestro polinomio de mayor a menor usando el orden monomial que hemos definido sobre el anillo `A`, en este caso el *grevlex*.

Si queremos reordenar los monomios del polinomio usando otro orden monomial, por ejemplo *lex* y *glex*, podemos cambiar de anillo. Los objetos definidos en un anillo no están definidos en otro anillo pero podemos pasarlos de uno a otro (habiendo definido previamente ambos anillos) usando el comando `imap` que define la aplicación identidad entre un anillo previamente definido y el anillo en el que nos encontramos en este momento. Por ejemplo podemos definir el anillo $\mathbb{Q}[x, y, z]$ dotado ahora del orden *lex*, al que llamaremos `A2` (no podemos llamarlo de nuevo `A` ya que si lo hacemos destruiremos el anillo `A` previamente definido y con el todos los objetos allí definidos), e importar desde el anillo `A` el polinomio `P` al que seguimos llamando `P` (también podríamos cambiarle el nombre):

```
> ring B=0,(x,y,z),lp;
> poly P=imap(A,P);
> P;
-x4y+x2y3z3-xyz2+y3z2
```

El anillo en el que se trabajará es el último que hemos definido. Si queremos volver a un anillo previamente definido haremos lo siguiente:

```
> setring A;
> P;
x2y3z3-x4y+y3z2-xyz2
```

Podemos ahora definir en el anillo `A` el ideal `I` generado por los polinomios f_1, f_2 y f_3 del ejemplo 11 y pedir una base de Gröbner. Existen dos comandos para calcular una base de Gröbner, `std` y `groebner`. La diferencia entre los dos es el método empleado para el cálculo; véase el manual online para entender esta diferencia. En los ejemplos que trataremos en estas notas, usaremos indistintamente cualquiera de los dos comandos. Cabe observar que el resultado que nos proporciona Singular no tiene porque ser la base de Gröbner reducida (puede serlo o no). Para forzar que el resultado del cálculo obtenido usando `std` o `groebner` sea la base de Gröbner reducida usando el comando `option(redSB)`:

```
> option(redSB);
> ideal I=xy-z2,x2-yz,y3-xz2;
> ideal sI=std(I);
> sI;
sI[1]=xy-z2
sI[2]=x2-yz
sI[3]=y2z-xz2
sI[4]=y3-xz2
sI[5]=yz3-z4
sI[6]=xz3-z4
```

Obviamente los ideales `I` y `sI` definidos en el ejemplo anterior son idénticos, cambia simplemente el sistema de generadores.

Con estas indicaciones básicas ya podemos empezar a manejar el programa y resolver, por ejemplo, algunos de los ejercicios propuestos en la sección 5. Iremos descubriendo más funciones interesantes en la sección 4 pero el lector ya puede ir experimentando solo y trabajar con sus ejemplos favoritos.

4. Aplicaciones

Ya hemos visto como usar las bases de Gröbner para resolver el problema de pertenencia (corolario 18) y para determinar si dos ideales polinomiales coinciden o no (nota 31). Veremos en esta sección otros problemas que podemos resolver utilizándolas.

4.1. Eliminación de variables, ecuaciones implícitas

El orden *lex* es conocido por ser bastante malo desde un punto de visto computacional. Construir una base de Gröbner para este orden cuesta en general más que para otro orden monomial, por ejemplo el *grevlex*. En esta sección veremos que el orden *lex* también tiene una propiedad que lo hace válido para un problema que no es nada trivial desde un punto de vista computacional y que aporta mucha información acerca del ideal (y de la variedad algebraica asociada), el problema de *eliminación de variables*[5]: dados un ideal I de A y un entero ℓ, $1 \leq \ell < n$, ¿cómo determinar de manera efectiva un sistema de generadores del ideal $I \cap K[x_{\ell+1}, \ldots, x_n]$ a partir de un sistema de generadores de I? Empezamos definiendo el tipo de órdenes monomiales que permitirán contestar a esta pregunta usando las bases de Gröbner.

Definición 33. Un orden monomial $>$ sobre A es un *orden de eliminación para las ℓ primeras variables* ($1 \leq \ell < n$) si, para todo par de monomios $\mathbf{x}^\alpha, \mathbf{x}^\beta$ de A,

$$\mathbf{x}^\alpha \notin (x_1, \ldots, x_\ell) \text{ y } \mathbf{x}^\beta \in (x_1, \ldots, x_\ell) \quad \Longrightarrow \quad \mathbf{x}^\beta > \mathbf{x}^\alpha \,. \tag{5}$$

Como consecuencia directa de la definición tenemos que si $>$ es un orden de eliminación para las ℓ primeras variables, para todo polinomio f de A, tenemos que

$$\operatorname{in}(f) \in K[x_{\ell+1}, \ldots, x_n] \quad \Longrightarrow \quad f \in K[x_{\ell+1}, \ldots, x_n] \,. \tag{6}$$

Veamos algunos ejemplos de orden de eliminación:

- El orden *lex* es un orden de eliminación para las ℓ primeras variables para todo ℓ, $1 \leq \ell < n$.

[5] El famoso poema de Abhyankar *Eliminate, eliminate, eliminate, Eliminate the eliminators of elimination theory* es una respuesta a los detractores de los métodos constructivos en geometría algebraica como A. Weil que predicaba por la eliminación de la Teoría de Eliminación en geometría algebraica; véase [10, p. 310] para esta nota histórica.

- Un orden graduado (por ejemplo *glex* o *grevlex*) nunca es un orden de eliminación ya que cualquier par de monomios $\mathbf{x}^\alpha, \mathbf{x}^\beta$ de A con $\deg \mathbf{x}^\alpha > \deg \mathbf{x}^\beta$ incumplirá la propiedad (5).
- El orden producto definido en el ejercicio 2 de la sección 5 es un orden de eliminación.
- El orden de eliminación de Bayer y Stillman está definido de la manera siguiente:

$$\mathbf{x}^\beta >_{BS} \mathbf{x}^\alpha \Longleftrightarrow [\sum_{i=1}^{\ell} \beta_i > \sum_{i=1}^{\ell} \alpha_i] \text{ ó } [\sum_{i=1}^{\ell} \beta_i = \sum_{i=1}^{\ell} \alpha_i \text{ y } \mathbf{x}^\beta >_{grevlex} \mathbf{x}^\alpha] .$$

  Es fácil justificar se define de esta manera un orden monomial, y que es de eliminación para las ℓ primeras variables.

Los órdenes de eliminación juegan un papel importante en el problema de eliminación de variables antes planteado por el resultado siguiente:

Teorema 34. *Sean I un ideal de A y $>_\ell$ un orden de eliminación sobre A para las ℓ primeras variables con $1 \leq \ell < n$. Si $\mathcal{G}$ es una base de Gröbner de I para el orden $>_\ell$, entonces $\mathcal{G} \cap K[x_{\ell+1}, \ldots, x_n]$ es una base de Gröbner de $I \cap K[x_{\ell+1}, \ldots, x_n]$ para el orden inducido por $>_\ell$ sobre $K[x_{\ell+1}, \ldots, x_n]$.*

Este resultado proporciona una respuesta al problema de eliminación de variables ya que el conjunto $\mathcal{G}$ es finito y es por tanto muy fácil determinar $\mathcal{G} \cap K[x_{\ell+1}, \ldots, x_n]$ que es, por los teoremas 34 y 16, un sistema de generadores del ideal $I \cap K[x_{\ell+1}, \ldots, x_n]$.

Demostración. Sean $\mathcal{G}_1 = \{g_1, \ldots, g_r\}$ el subconjunto de $\mathcal{G}$ formado por los elementos que no involucran las ℓ primeras variables, es decir $\mathcal{G}_1 = \mathcal{G} \cap K[x_{\ell+1}, \ldots, x_n]$, y $\mathcal{G}_2$ el subconjunto de $\mathcal{G}$ formado por los demás elementos de $\mathcal{G}$. Está claro que $\mathcal{G}_1$ es un subconjunto finito de $I_\ell := I \cap K[x_{\ell+1}, \ldots, x_n]$ y vamos a demostrar que es una base de Gröbner de I_ℓ respecto del orden orden inducido por $>_\ell$ sobre $K[x_{\ell+1}, \ldots, x_n]$, es decir, por la definición 15, que $\operatorname{in}(I_\ell) = (\operatorname{in}(g_1), \ldots, \operatorname{in}(g_r))$. Observamos primero que para todo $f \in \mathcal{G}_2$, $\operatorname{in}(f) \notin K[x_{\ell+1}, \ldots, x_n]$ por la propiedad (6) antes mencionada, es decir que los monomios iniciales de los elementos de $\mathcal{G}_2$ involucran todos al menos una de las ℓ primeras variables. Si tomamos por tanto un elemento $g \in I_\ell$, como su monomial inicial no involucra ninguna de las ℓ primeras variables, no puede ser múltiplo del monomio inicial de un elemento de $\mathcal{G}_2$, y como $\operatorname{in}(g) \in \operatorname{in}(I)$, tiene que ser múltiplo del monomio inicial de algún elemento de $\mathcal{G}_1$. Esto justifica que $\operatorname{in}(I_\ell) \subset (\operatorname{in}(g_1), \ldots, \operatorname{in}(g_r))$ y como la otra inclusión es trivial, el resultado queda demostrado. □

Ejemplo 35. Consideramos el ideal $I = (xy^2 - xz + y, xy - z, xy - yz^4)$ de $\mathbb{Q}[x, y, z]$. Podemos calcular la base de Gröbner reducida de I para el orden *lex* usando Singular[6].

```
> option(redSB);
> ring A1=0,(x,y,z),lp;
> ideal I=xy2-xz+y,xy-z,xy-yz4;
> groebner(I);
_[1]=z9-z2-z
_[2]=y+z8-z7+z6-z5-z
_[3]=xz-z5
```

Como el orden *lex* es un orden de eliminación tanto para la primera variable como para las dos primeras, de este cálculo de base de Gröbner deducimos que $I \cap \mathbb{Q}[z] = (z^9 - z^2 - z)$ e $I \cap \mathbb{Q}[y, z] = (y + z^8 - z^7 + z^6 - z^5 - z, z^9 - z^2 - z)$. Podríamos haber obtenido esta información usando el comando `eliminate` de Singular que elimina las variables que le indiquemos (damos el producto de las variables que queremos eliminar). De esta manera dejamos el programa seleccionar el mismo el orden de eliminación que estime mejor.

```
> eliminate(I,x*y);
_[1]=z9-z2-z
> eliminate(I,x);
_[1]=z9-z2-z
_[2]=y+z8-z7+z6-z5-z
```

La eliminación de variables resultará muy útil en algunas de las aplicaciones que presentaremos en las próximas secciones. También se utiliza para encontrar ecuaciones implícitas de variedades algebraicas definidas parametricamente. Véamos un ejemplo ([10, p. 308]): si consideramos el subconjunto $\mathcal{C}$ de $\mathbb{P}^2_{\mathbb{C}}$ formado por todos los puntos de la forma $(s^3 : s^2t + st^2 : t^3)$ para $(s : t) \in \mathbb{P}^1_{\mathbb{C}}$, está claramente contenido en la variedad algebraica $V(I)$ definida por el ideal I formado por todos los polinomios homogéneos F de $\mathbb{C}[x, y, z]$ tales que $F(s^3, s^2t + st^2, t^3)$ es identicamente nulo. De hecho $V(I)$ es la variedad algebraica más pequeña que contiene a $\mathcal{C}$, y $\varphi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}},\ (s : t) \mapsto (s^3 : s^2t + st^2 : t^3)$

[6]Iniciamos aquí una nueva sesión de trabajo con Singular que terminará al final de la sección 4. Se iran definiendo anillos e ideales que podrán ser utilizados en distintas partes de esta sección.

es una parametrización de la variedad $V(I)$. Determinar el ideal I, que en nuestro caso es principal, no es un problema fácil desde el punto de vista computacional. Consiste en pasar de una descripción paramétrica de nuestra variedad a sus ecuaciones implícitas. Pero el ideal I no es más que la intersección del ideal $(x-s^3, y-s^2t-st^2, z-t^3) \subset \mathbb{C}[x,y,z,s,t]$ con el subanillo $\mathbb{C}[x,y,z]$ y por tanto $I = (x-s^3, y-s^2t-st^2, z-t^3) \cap \mathbb{C}[x,y,z]$ se puede determinar eliminando variables.

```
> ring A2=0,(x,y,z,s,t),dp;
> ideal I=x-s3,y-s2t-st2,z-t3;
> eliminate(I,s*t);
_[1]=y3-x2z-3xyz-xz2
```

El problema de encontrar las ecuaciones implícitas puede complicarse mucho cuando el ideal I de las ecuaciones implícitas no es principal pero se realiza bien en ejemplos razonables eliminando variables. Veámos otro ejemplo: si consideramos la curva monomial afín definida de manera paramétrica por $\mathcal{C} = \{(t^3, t^7, t^{11}, t^{13}, t^{17}) \in \mathbb{A}^5_{\mathbb{Q}},\ t \in \mathbb{Q}\}$, su ideal de definición es el ideal I de $\mathbb{Q}[x_1, \ldots, x_5]$ engendrado por los polinomios $x_3x_4 - x_2x_5$, $x_2x_4 - x_1x_5$, $x_2^2 - x_1x_3$, $x_4^3 - x_3^2x_5$, $x_3^3 - x_1x_4x_5$, $x_2x_3^2 - x_1x_4^2$, $x_1^2x_3 - x_5$, $x_1^2x_2 - x_4$, $x_1^3x_5 - x_4^2$, $x_1^3x_4 - x_3^2$, $x_1^6 - x_2x_3$. Se obtiene de la siguiente manera:

```
> ring A3=0,(x(1..5),t),dp;
> ideal I=x(1)-t3,x(2)-t7,x(3)-t11,x(4)-t13,x(5)-t17;
> eliminate(I,t);
_[1]=x(3)*x(4)-x(2)*x(5)
_[2]=x(2)*x(4)-x(1)*x(5)
_[3]=x(2)^2-x(1)*x(3)
_[4]=x(4)^3-x(3)^2*x(5)
_[5]=x(3)^3-x(1)*x(4)*x(5)
_[6]=x(2)*x(3)^2-x(1)*x(4)^2
_[7]=x(1)^2*x(3)-x(5)
_[8]=x(1)^2*x(2)-x(4)
_[9]=x(1)^3*x(5)-x(4)^2
_[10]=x(1)^3*x(4)-x(3)^2
_[11]=x(1)^6-x(2)*x(3)
```

4.2. Intersección de ideales

La eliminación de variables también resultará útil para otros problemas, por ejemplo para determinar la intersección de dos ideales I y J de A. Introducimos una nueva variable t y consideramos dos subconjuntos de $A[t]$, $tI = \{tf \,/\, f \in I\}$ y $(1-t)I = \{(1-t)f \,/\, f \in I\}$. Son dos ideales de $A[t]$ y tenemos que

$$I \cap J = (tI + (1-t)J) \cap A\,. \tag{7}$$

En efecto, todo polinomio f de $I \cap J$ puede verse como un elemento de $A[t]$ que no involucra la variable t. Como $f = tf + (1-t)f$, usando que $f \in I$ y que $f \in J$, obtenemos que $f \in tI + (1-t)J$ por lo que $I \cap J \subset (tI + (1-t)J) \cap A$. Reciprocamente, tomemos un polinomio $f \in A[t]$ que pertenezca a $tI + (1-t)J$ y no involucre la variable t: existen $q_1 \in I.A[t]$ y $q_2 \in J.A[t]$ tales que $f = tq_1 + (1-t)q_2$. Sustituimos ahora t por 1 en esta igualdad. Como f no involucra t, en el lado izquierdo obtenemos f y concluimos que f coincide con el polinomio obtenido al sustituir t por 1 en $q_1 \in I.A[t]$ por lo que $f \in I$. Sustituyendo ahora t por 0 obtenemos que $f \in J$ y queda justificada la otra inclusión.

La propiedad (7) permite determinar un sistema de generadores de $I \cap J$ simplemente introduciendo una nueva variable t y eliminando t del ideal $tI + (1-t)J$.

Apliquemos este método en un ejemplo fácil que podemos tratar a mano. Todos sabemos que si consideramos los dos ideales principales $I = (x)$ e $J = (y)$ de $K[x, y]$, entonces $I \cap J = (xy)$. Para aplicar el método anterior para confirmar este resultado, consideramos el ideal $tI + (1-t)J$ de $K[t, x, y]$ que no es más que el ideal $L = (tx, y - ty)$. Tenemos que calcular una base de Gröbner de L para un orden de eliminación para la primera variable, t. Elegimos el orden *lex*. El S-polinomio de $f_1 = tx$ y $f_2 = y - ty$ es $f_3 = S(f_1, f_2) = yf_1 + xf_2 = xy$ que añadimos a nuestra base de Gröbner ya que xy no es múltiplo ni de tx, ni de ty. Finalmente, $S(f_1, f_3) = yf_1 - tf_3 = 0$ y $S(f_2, f_3) = -xf_2 - tf_3 = -xy \to_{f_3} 0$, por lo que $\{tx, ty - y, xy\}$ es la base de Gröbner reducida de L respecto del orden *lex*. Por (7) y el teorema 34, $I \cap J = (xy)$.

Usaremos ahora Singular en un ejemplo donde no es tan fácil determinar el resultado a mano sin usar un ordenador.

```
> ring A4=0,(x,y),dp;
> ideal I=x2+y3-1,x-xy+3; ideal J=x2y-1;
> ring A5=0,(x,y,t),dp;
> ideal I=imap(A4,I); ideal J=imap(A4,J);
> ideal L=t*I+(1-t)*J;
> eliminate(L,t);
_[1]=x3y2-x3y-3x2y-xy+x+3
_[2]=x2y4+x4y-x2y-y3-x2+1
_[3]=x5y+3x2y3+3x2y2-x3+3x2y-3y2-3y-3
```

Singular tiene un comando, `intersect`, que permite calcular la intersección de ideales directamente.

```
> setring A4;
> intersect(I,J);
_[1]=x3y2-x3y-3x2y-xy+x+3
_[2]=x2y4+x4y-x2y-y3-x2+1
_[3]=x5y+3x2y3+3x2y2-x3+3x2y-3y2-3y-3
```

Véamos ahora que la intersección (y por tanto la eliminación de variables) permite construir el máximo divisor común (m.c.d.) y el mínimo común múltiplo (m.c.m.) de dos polinomios en varias variables.

Dados dos polinomios no nulos f y g de A, se demuestra (usando que A es un dominio de factorización única) que existe un único polinomio unitario[7] de A que sea divisor común a f y g y múltiplo de cualquier otro divisor común a f y g. Es el máximo divisor común de f y g y lo denotaremos por $\mathrm{mcd}(f,g)$. También existe un único polinomio unitario de A que sea múltiplo común a f y g y divisor de cualquier otro múltiplo común a f y g, el mínimo común múltiplo de f y g denotado por $\mathrm{mcm}(f,g)$. La relación entre estos dos polinomios es la siguiente (véase, por ejemplo, [5, Prop. 14, p.187]): existe una constante a de K no nula (el producto de los coeficientes dominantes de f y g) tal que

$$f \times g = a \times \mathrm{mcd}(f,g) \times \mathrm{mcm}(f,g)\,. \tag{8}$$

[7] Si no queremos que esta definición dependa de un orden monomial sobre A, tenemos que quitar la condición 'unitario'. La unicidad, tanto del m.c.d. como del m.c.m., es entonces módulo el producto por constantes no nulas.

Además, si tomamos ahora dos ideales principales (f) y (g) de A, tenemos que $(f) \cap (g)$ también es principal y

$$(f) \cap (g) = (\text{mcm}(f, g)) . \tag{9}$$

Combinando (8) y (9), y dado que sabemos determinar la intersección de dos ideales, tenemos un método para calcular el m.c.d. y el m.c.m. de dos polinomios de A.

```
> poly f=x3-x2y-3x2+xy-y2-3y; ideal ff=f;
> poly g=x3y+xy2+2x2+2y; ideal gg=g;
> ideal MCM=intersect(ff,gg);
> MCM;
MCM[1]=x4y-x3y2-3x3y+x2y2-xy3+2x3-2x2y-3xy2-6x2+2xy-2y2-6y
> f*g/MCM[1];
x2+y
```

De nuevo, hay comandos de Singular que calculan directamente el m.c.d y el m.c.m, `gcd` y `lcm` respectivamente, usando métodos más eficientes que el que hemos presentado aquí. Observamos que el comando `lcm` no forma parte de los comandos del núcleo de Singular. Está en la librería `poly.lib` que tenemos por tanto que cargar.

```
> gcd(f,g);
x2+y
> LIB "poly.lib";
> lcm(f,g);
x4y-x3y2-3x3y+x2y2-xy3+2x3-2x2y-3xy2-6x2+2xy-2y2-6y
```

4.3. Cociente de dos ideales

Otra operación entre ideales que es importante tanto en álgebra conmutativa como en geometría algebraica, es el cociente.

Definición 36. Dados dos ideales $\cdot\text{I}\cdot$ y J de A, el siguiente subconjunto de A,

$$I : J = \{f \in A \,/\, fg \in I, \forall\, g \in J\}$$

es un ideal de A llamado el *cociente de I por J*. Está formado por todos los elementos de A que llevan, por el producto, a todo J dentro de I.

La interpretación geométrica de esta operación viene reflejada en el siguiente resultado ([5, Cor. 8 p. 193]): si V y W son dos variedades algebraicas afines, $I(V \backslash W) = I(V) : I(W)$.

Uno de los usos importantes de está operación es que permite determinar si un ideal está o no contenido en otro. En efecto, para todo par de ideales I, J de A, se tiene que

$$J \subset I \iff I : J = (1)\,. \tag{10}$$

Nos preguntamos ahora cómo construir el cociente de dos ideales I y J de A. Lo primero que observamos es que, usando que ya sabemos calcular la intersección de ideales, el problema se reduce al caso en el que J es principal usando que si conocemos un sistema de generadores de J, $\{g_1, \ldots, g_t\}$, entonces

$$I : (g_1, \ldots, g_t) = \bigcap_{i=1}^{t} I : (g_i)\,. \tag{11}$$

Y el cálculo del cociente cuando el segundo ideal es principal se realiza usando el siguiente resultado:

Proposición 37. *Dados un ideal I y un polinomio g de A, si $I \cap (g) = (h_1, \ldots, h_s)$ entonces necesariamente cada h_i es un múltiplo de g, y*

$$I : (g) = \left(\frac{h_1}{g}, \ldots, \frac{h_s}{g}\right).$$

Demostración. Está claro que cada generador de $I \cap (g)$ es múltiplo de g ya que pertenece a (g). Como cada elemento del conjunto de polinomios $\{\frac{h_1}{g}, \ldots, \frac{h_s}{g}\}$ multiplicado por g proporciona un elemento de I, tenemos que $(\frac{h_1}{g}, \ldots, \frac{h_s}{g}) \subset I : (g)$. Reciprocamente, si tomamos un polinomio f en $I : (g)$, entonces $fg \in I$ y como también $fg \in (g)$, fg es una combinación de $h_1, \ldots, h_s$. Simplificando por g obtenemos el resultado. □

En el siguiente ejemplo calculamos $I : J$ para los ideales $I = (x^2 + z, xy + y^2 + z, xz - y^3 - 2yz, y^4 + 3y^2z + z^2)$ y $J = (x^2 + z, xy + y^2 + z, x^3 - yz)$ de $\mathbb{Q}[x, y, z]$. Dado que los dos primeros generadores de J, g_1 y g_2, son también generadores de I, por (10) tenemos que $I : (g_1) = I : (g_2) = (1)$ y por tanto aplicando (11) deducimos que $I : J = I : (g_3)$. Determinamos este cociente usando Singular y aplicando la proposición 37, y terminamos comprobando nuestro resultado con el comando `quotient` que determina el cociente de dos ideales:

```
> ring A6=0,(x,y,z),dp;
> ideal I=x2+z,xy+y2+z,xz-y3-2yz,y4+3y2z+z2;
> ideal J=x2+z,xy+y2+z,x3-yz;
> ideal Q=intersect(I,J[3]);
> Q;
Q[1]=x4y+x3y2+x3z-xy2z-y3z-yz2
Q[2]=x5+x3z-x2yz-yz2
Q[3]=x3y3-x4z+2x3yz-y4z+xyz2-2y2z2
> Q/J[3];
_[1,1]=xy+y2+z
_[1,2]=x2+z
_[1,3]=y3-xz+2yz
> quotient(I,J);
_[1]=xy+y2+z
_[2]=x2+z
_[3]=y3-xz+2yz
```

4.4. El problema de pertenencia al radical

Un problema más fácil que el cálculo del radical de un ideal es el problema de pertenencia al radical: dados un ideal I de A y un polinomio f de A, ¿cómo determinar si $f \in \sqrt{I}$? Por supuesto si sabemos construir $\sqrt{I}$, podemos responder usando la solución que hemos dado al problema de pertenencia, pero el siguiente resultado permite contestar a la pregunta sin construir el radical de I:

Proposición 38. *Dados un ideal $I \subset A$ y un polinomio $f \in A$, tomamos una nueva indeterminada w y consideramos el ideal $\tilde{I}$ de $A[w]$ engendrado por I y por el polinomio $1 - wf$, es decir $\tilde{I} = I.A[w] + (1 - wf)$. Las tres propiedades siguientes son equivalentes:*

1. $f \in \sqrt{I}$;
2. $1 \in \tilde{I}$;
3. $\{1\}$ *es la base de Gröbner reducida de $\tilde{I}$ respecto de un orden monomial arbitrario sobre $A[w]$.*

Demostración. Está claro que 2 y 3 son equivalentes. Para la equivalencia de 1 y 2, véase por ejemplo [5, Prop. 8, p.176]. Observamos que esta prueba utiliza el teorema 2 pero

que el resultado es cierto sobre un cuerpo arbitrario (se pasa al cierre algebraico para la demostración). Para otra demostración que relaciona el problema de pertenencia al radical con la construcción de la saturación $I : f^{\infty}$, véase [12, Prop. 3.7]. □

Ilustraremos el método anterior con un ejemplo sencillo. En $\mathbb{Q}[x, y, z]$, consideramos el ideal monomial $I = (x^3, x^2y, y^3z, y^2z^7, xyz)$. En este caso, es fácil demostrar que $\sqrt{I} = (x, yz)$ por lo que $x \in \sqrt{I}$ y $z \notin \sqrt{I}$. Lo comprobaremos ahora con Singular usando el método anterior.

```
> ideal L=x3,x2y,y3z,y2z7,xyz;
> ring A7=0,(x,y,z,w),dp;
> ideal I=imap(A6,L);
> ideal J=I,1-w*x;
> groebner(J);
_[1]=1
> ideal K=I,1-w*z;
> groebner(K);
_[1]=zw-1
_[2]=y2
_[3]=xy
_[4]=x3
```

En la librería `primdec.lib` de Singular encontraremos la implementación de varios algoritmos para la construcción de una descomposición primaria y del radical de un ideal polinomial. Estos algoritmos son más avanzados y exceden el contenido de este curso. Podemos usar el sencillo ejemplo anterior para ver como funciona el comando `radical` de la librería `primdec.lib` y veremos en la sección 5 un problema menos trivial.

```
> setring A6;
> LIB "primdec.lib";
> radical(L);
_[1]=x
_[2]=yz
```

4.5. Primeras sicigias, sistemas minimales de generadores

Veámos de pasada una aplicación muy potente de las bases de Gröbner en álgebra conmutativa: el cálculo de sicigias.

Definición 39. Dado un conjunto $\mathcal{F} = \{f_1, \ldots, f_m\}$ de polinomios distintos de A, una *sicigia* de $\mathcal{F}$ es una relación polinomial lineal entre los elementos de $\mathcal{F}$, es decir una relación

$$q_1 f_1 + \cdots + q_m f_m = 0 \tag{12}$$

con $q_1, \ldots, q_m \in A$. Una sicigia se suele representar en forma vectorial, es decir que la sicigia de $\mathcal{F}$ correspondiente a la relación (12) será el vector $s = (q_1, \ldots, q_m)^t \in A^m$. El problema de describir las sicigias de $\mathcal{F}$ consiste en encontrar todas las relaciones de este tipo entre los elementos de $\mathcal{F}$. Se demuestra que el conjunto de todas las sicigias de $\mathcal{F}$, denotado por $\mathrm{Sic}(\mathcal{F})$, es un submódulo finitamente generado de A^m. Describir por tanto las sicigias de $\mathcal{F}$ consiste en dar un conjunto finito de generadores del submódulo $\mathrm{Sic}(\mathcal{F})$ de A^m, es decir un número finito de relaciones del tipo (12) tal que cualquier otra relación sea una combinación A-lineal de estas relaciones.

Nota 40.

1. En lugar de hablar de sicigias del conjunto de polinomios $\mathcal{F}$ se suele hablar de sicigias del ideal I de A engendrado por $\mathcal{F}$ pero esto es un abuso ya que las sicigias dependen (y mucho) del sistema de generadores elegido. Como no entraremos en los detalles de lo que es invariante para el ideal I (cuando I es homogéneo, o graduado respecto de alguna graduación), hablaremos aquí de sicigias de un conjunto de polinomios.

2. Cuando tenemos más de dos polinomios, siempre hay sicigias no triviales, es decir que $\mathrm{Sic}(\mathcal{F})$ nunca es el módulo nulo si $m \geq 2$. En efecto, al menos siempre tenemos las llamadas *relaciones de Koszul* que son aquellas de la forma $q_{ij} f_i + q_{ji} f_j = 0$ para $q_{ij} = f_j$ y $q_{ji} = -f_i$.

Saber describir las sicigias permite, por ejemplo, determinar si un sistema de generadores $\mathcal{F} = \{f_1, \ldots, f_m\}$ de un ideal I de A es o no minimal. En efecto si $\mathcal{F}$ no es minimal, al menos uno de los elementos de $\mathcal{F}$, digamos f_i, se expresa como combinación de los demás. Esta relación proporciona un elemento de $\mathrm{Sic}(\mathcal{F})$ que es un vector cuya i-ésima coordenada es una constante no nula. Una sicigia con esta propiedad tiene por tanto que aparecer en cualquier sistema de generadores del módulo $\mathrm{Sic}(\mathcal{F})$. Reciprocamente, si existe tal sicigia,

está claro que el sistema de generadores $\mathcal{F}$ no es minimal ya que esta sicigia proporciona una relación que expresa f_i en función de los demás elementos de $\mathcal{F}$.

Un importante resultado que presentaremos a continuación dice que cuando tenemos una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_t\}$ respecto de un orden monomial arbitrario, entonces podemos describir $\mathrm{Sic}(\mathcal{G})$ sin esfuerzo adicional.

Si $\mathcal{G}$ es una base de Gröbner del ideal I de A engendrado por $\mathcal{G}$, por el criterio de Buchberger tenemos que para todo i, j con $1 \leq i < j \leq t$, el S-polinomio de g_i y g_j, $S(g_i, g_j)$, se expresa en función de los elementos de $\mathcal{G}$ con una relación como las descritas en la definición 12 y con $r = 0$. Como por otra parte, $S(g_i, g_j)$ es una combinación de g_i y g_j, cada propiedad $S(g_i, g_j) \to_{\mathcal{G}} 0$ proporciona una sicigia no trivial de $\mathcal{G}$ que denotaremos por s_{ij}.

Véamos un ejemplo sencillo para ilustrar esta relación entre reducción a cero de los S-polinomios y sicigia. En el ejemplo 25, hemos visto que $\mathcal{G} = \{f_1, f_2, f_3\}$ es una base de Gröbner del ideal I de $\mathbb{Q}[x, y]$ engendrado por $f_1 = xy - 1$, $f_2 = y^2 - 1$ y $f_3 = x - y$ respecto del orden *lex*. Para ello hemos reducido cada S-polinomio de la manera siguiente:

- $S(f_1, f_2) = yf_1 - xf_2$ se reduce a cero módulo $\mathcal{G}$ ya que $S(f_1, f_2) = x - y = f_3$,
- $S(f_1, f_3) = f_1 - yf_3 \to_{\mathcal{G}} 0$ ya que $S(f_1, f_3) = y^2 - 1 = f_2$, y
- $S(f_2, f_3) = xf_2 - y^2 f_3 \to_{\mathcal{G}} 0$ ya que $S(f_2, f_3) = -x + y^3 = -f_3 + yf_2$.

Las sicigias no triviales de $\mathcal{G}$ obtenidas a partir de estas tres reducciones son

$$s_{12} = \begin{pmatrix} y \\ -x \\ -1 \end{pmatrix}, \; s_{13} = \begin{pmatrix} 1 \\ -1 \\ -y \end{pmatrix} \text{ y } s_{23} = \begin{pmatrix} 0 \\ x - y \\ -y^2 + 1 \end{pmatrix}. \tag{13}$$

Observamos que la primera (también la segunda) de estas sicigias tiene alguna entrada constante no nula lo cual confirma que $\mathcal{G}$ no genera I minimalmente, cosa que ya sabíamos ya que $I = (f_1, f_2)$.

El siguiente resultado nos dice que las sicigias s_{ij} obtenidas de esta manera nos permiten obtener todas las sicigias de $\mathcal{G}$:

Teorema 41. *Si $\mathcal{G} = \{g_1, \ldots, g_t\}$ es una base de Gröbner del ideal I de A engendrado por $\mathcal{G}$ y si, para todo i, j con $1 \leq i < j \leq t$, denotamos por s_{ij} la sicigia de $\mathcal{G}$ obtenida a partir de la reducción $S(g_i, g_j) \to_{\mathcal{G}} 0$ tal como lo hemos explicado antes, entonces el A-módulo $Sic(\mathcal{G}) \subset A^m$ está engendrado por $\{s_{ij}\,;\; 1 \leq i < j \leq t\}$.*

Para una demostración de este resultado, nos referimos a [6, Chapter 5.3, Thm. 3.2].

Pero la pregunta original no era esta. Nos gustaría, dado $\mathcal{F} = \{f_1, \ldots, f_m\}$ que no sea necesariamente una base de Gröbner del ideal I de A engendrado por $\mathcal{F}$, poder describir $\mathrm{Sic}(\mathcal{F})$. Esto también se puede hacer, calculando primero una base de Gröbner $\mathcal{G}$ de I respecto de un orden monomial arbitrario, aplicando luego el teorema 41 para describir $\mathrm{Sic}(\mathcal{G})$, y finalmente volviendo al sistema de generadores original para encontrar sus sicigias, $\mathrm{Sic}(\mathcal{F})$. No entraremos en los detalles de este método, pero se puede encontrar en [6, Chapter 5.3, Prop. 3.8]. Este método esta implementado en Singular y veremos ahora en un ejemplo como utilizar el comando `syz` (de la palabra en inglés *syzygy* para sicigia):

```
> setring A4;
> poly f1=xy-1; poly f2=y2-1; poly f3=x-y;
> ideal L=f1,f2,f3;
> ideal M=f1,f2;
> print(syz(L));
-1,-y,
 1, x,
 y, 1
> print(syz(M));
-y2+1,
 xy-1
```

Observamos que cuando solicitamos `print(syz(L))`, Singular sólo nos da dos de los tres generadores de $\mathrm{Sic}(\mathcal{G})$ que hemos encontrado en (13). Las dos sicigias proporcionadas por Singular son $-s_{13}$ y $-s_{12}$. La razón es que el tercer generador dado por el teorema 41 es, en este ejemplo, supérfluo ya que $s_{23} = ys_{13} - s_{12}$. Por alguna razón, Singular lo ha eliminado. La respuesta es por tanto la misma que la que habíamos encontrado a mano en (13).

Terminaremos esta sección diciendo que las nociones de orden monomial y de base de Gröbner se generalizan facilmente de ideales a módulos. Esto nos permite, una vez determinado el módulo $\mathrm{Sic}(\mathcal{F})$ como antes, de calcular una base de Gröbner de este módulo y, aplicando el resultado análogo al teorema 41 para módulos, de determinar las sicigias de $\mathrm{Sic}(\mathcal{F})$, es decir las llamadas segundas sicigias de $\mathcal{F}$, y así sucesivamente. Se llega de esta manera a la construcción de una resolución libre del ideal de partida e incluso se puede, usando bases de Gröbner, dar una prueba constructiva del famoso Teorema de las Sicigias

de Hilbert. La demostración requiere un teorema de Schreyer que viene, esencialmente, a definir un orden monomial apropiado al cálculo de sicigias; véase por ejemplo [10, Chapter 15]. Nos referimos a [6] y [12] para un tratamiento exhaustivo de las bases de Gröbner para módulos y la construcción de resoluciones de A-módulos finitamente generados.

4.6. Coloración de grafos, resolución de sudokus

Presentaremos ahora una curiosa aplicación de las bases de Gröbner, más alejada de las áreas del álgebra conmutativa y de la geometría algebraica, y que se situa más bien en el ámbito de la combinatoria. Se trata del problema de la coloración de grafos. Los resultados que presentamos aquí, y muchos más, se pueden encontrar en el precioso artículo de Hillar y Windfeldt [15]. Estos resultados no pretenden ser más eficientes que los métodos combinatorios para resolver este tipo de problemas, aunque pueden llegar a serlo, pero son, como poco, muy curiosos ya que ofrecen un puente más entre el álgebra conmutativa y la combinatoria.

Empezaremos introduciendo las nociones necesarias para enunciar los problemas que aquí nos planteamos. Dado un grafo G (simple y no dirigido) con n vértices, denotamos por $V = \{1, \ldots, n\}$ el conjunto de sus vértices y por E el conjunto de sus aristas. Denotaremos por (i, j) la arista entre los vértices i y j. Tomando un conjunto de k colores, $C_k = \{c_1, \ldots, c_k\}$, con $1 \leq k < n$, diremos que G es *k-coloreable* si se puede pintar cada vértice de G de un color de C_k de manera que dos vértices de G adjacentes (es decir unido por una arista de G) no tengan el mismo color. Dicho de otra manera, G es k-coloreable si podemos definir una aplicación $\nu : V \to C_k$ tal que, para toda arista $(i, j) \in E$, $\nu(i) \neq \nu(j)$.

(P1) El primer problema que nos planteamos es determinar, usando bases de Gröbner, cuando G es k-coloreable.

(P2) El segundo consiste en tomar ahora un grafo k-coloreable G y determinar si existe una única manera de colorear G con k colores. Por supuesto, la unicidad que planteamos aquí es módulo permutación de los colores, es decir que si sólo permutamos los colores, consideraremos que estamos hablando de la misma k-coloración de G.

El tratamiento algebraico de este problema requiere introducir un cuerpo K que suponemos algebraicamente cerrado y cuya característica no divida a k. En $A = K[x_1, \ldots, x_n]$, consideramos entonces el ideal $I_{G,k}$ siguiente:

$$I_{G,k} = (x_i^k - 1\,;\ i \in V) + (x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1}\,;\ (i,j) \in E)\,.$$

Vamos a justificar primero que si $I_{G,k} \neq (1)$, es decir si $V(I_{G,k}) \neq \emptyset$ por el teorema 2, $I_{G,k}$ es un ideal 0-*dimensional*, es decir que $V(I_{G,k})$ está formado por un número finito de puntos de $\mathbb{A}^n_K$. Podríamos hacer incluido en la sección 4 de estas notas un apartado sobre ideales 0-dimensionales y bases de Gröbner. Preferimos referirnos a los estupendos [5, Chapter 5.3] y [12, Chapter 3.3], y recordar lo fundamental en el siguiente resultado:

Teorema 42. *Si K es un cuerpo algebraicamente cerrado e I es un ideal propio de A ($I \neq (1)$), las siguientes propiedades son equivalentes:*

1. *I es 0-dimensional;*
2. *A/I es un K-espacio vectorial de dimensión finita;*
3. *Fijado un orden monomial arbitrario $>$, el conjunto de los monomios de A que no pertenecen a $\mathrm{in}\,(I)$ es finito;*
4. *Fijado un orden monomial arbitrario $>$, en cualquier base de Gröbner $\mathcal{G}$ de I respecto de $>$, y para todo i, $1 \leq i \leq n$, existe un elemento de $\mathcal{G}$ cuyo monomio inicial sea una potencia de x_i.*

Nota 43. La equivalencia entre 2 y 3 en el resultado anterior se deduce de un resultado más preciso ([5, Prop. 4, Chapter 5.3]): para cualquier ideal I de A, el conjunto de las imágenes en A/I de los monomios de A que no pertenecen a $\mathrm{in}\,(I)$ forma una base del K-espacio vectorial A/I.

Volvemos ahora al ideal $I_{G,k}$. La primera parte de sus generadores, $\{x_i^k - 1\,;\ i \in V\}$, nos permite afirmar, usando la propiedad 4 del teorema 42, que $I_{G,k}$ es 0-dimensional. La relación entre el ideal $I_{G,k}$ y los problemas (P1) y (P2) planteados al principio de esta sección está reflejada en los dos resultados siguientes que recogen parcialmente el contenido de los teoremas 1.1 y 1.9 de [15].

Teorema 44 (grafos k-coloreables)**.** *Las propiedades siguientes son equivalentes:*

1. *G no es k-coloreable;*
2. *$V(I_{G,k}) = \emptyset$;*
3. *$I_{G,k} = (1)$;*
4. *$\{1\}$ es la base de Gröbner reducida de $I_{G,k}$ respecto de cualquier orden monomial.*

Teorema 45 (unicidad de la k-coloración)**.** *Si $I_{G,k} \neq (1)$, G es k-coloreable y las propiedades siguientes son equivalentes:*

1. *G es k-coloreable de manera única;*
2. *la dimensión de $A/I_{G,k}$ como K-espacio vectorial es $k!$;*
3. *el número de monomios de A que no pertenece a $\operatorname{in}(I_{G,k})$, el ideal inicial de $I_{G,k}$ respecto de un orden monomial arbitrario, es $k!$.*

Ilustraremos el uso de estos resultados con unos ejemplos sencillos. Consideramos dos grafos cuyo conjunto de vértices es $\{1,2,3\}$: el grafo G_1 cuyo conjunto de aristas es $\{(1,2),(2,3)\}$ (*path*, camino), y el grafo G_2 cuyo conjunto de aristas es $\{(1,2),(2,3),(1,3)\}$ (3-ciclo). Está claro que G_1 es 2-coloreable mientras G_2 no lo es (requiere 3 colores). Comprobamos estas propiedades aplicando la propiedad 4 del teorema 44:

```
> setring A6;
> ideal IG12=x^2-1,y^2-1,z^2-1,x+y,y+z;
> groebner(IG12);
_[1]=y+z
_[2]=x-z
_[3]=z2-1
> ideal IG22=x^2-1,y^2-1,z^2-1,x+y,y+z,x+z;
> groebner(IG22);
_[1]=1
```

Está claro además que G_1 es unicamente 2-coloreable. De nuevo vamos a comprobarlo usando el teorema 45. El comando `lead` nos permite obtener que $\operatorname{in}(I_{G_1,2}) = (x, y, z^2)$ por lo que $\{1, z\}$ es el conjunto de los monomios de $\mathbb{Q}[x,y,z]$ que no pertenecen a $\operatorname{in}(I_{G_1,2})$. Por la propiedad 3 del teorema 45 deducimos que efectivamente G_1 es unicamente 2-coloreable.

```
> lead(groebner(IG12));
_[1]=y
_[2]=x
_[3]=z2
```

Si consideramos ahora un tercer grafo, G_3, cuyos conjuntos de vértices y aristas sean $\{1,2,3,4\}$ y $\{(1,2),(2,3),(3,4)\}$ respectivamente, también es unicamente 2-coloreable. Además es 3-coloreable pero no lo es de manera única.

```
> setring A7;
> ideal IG32=x^2-1,y^2-1,z^2-1,w^2-1,x+y,y+z,z+w;
> ideal sIG32=groebner(IG32);
> lead(sIG32);
_[1]=z
_[2]=y
_[3]=x
_[4]=w2
> vdim(sIG32);
2
> ideal IG33=x^3-1,y^3-1,z^3-1,w^3-1,x^2+xy+y^2,y^2+yz+z^2,z^2+zw+w^2;
> ideal sIG33=groebner(IG33);
> lead(sIG33);
_[1]=z2
_[2]=y2
_[3]=x2
_[4]=w3
> vdim(sIG33);
24
```

Observamos el uso del comando `vdim` que cuenta el número de monomios de A que no están en $\operatorname{in}(I)$ y determina por tanto, tal como lo hemos observado en la nota 43, la dimensión de A/I como K-espacio vectorial.

Veámos ahora un ejemplo más complejo para el cual la respuesta a los problemas (P1) y (P2) no es tan evidente. Se trata del grafo G con 12 vértices y 23 aristas pintado en [15, Fig. 1]. El ideal $I_{G,3}$ tiene por tanto 35 generadores y el siguiente cálculo permite afirmar que G es únicamente 3-coloreable.

```
> ring A8=0,x(1..12),dp;
> ideal I=x(1)^3-1,x(2)^3-1,x(3)^3-1,x(4)^3-1,x(5)^3-1,x(6)^3-1,
x(7)^3-1,x(8)^3-1,x(9)^3-1,x(10)^3-1,x(11)^3-1,x(12)^3-1,
(x(1)+x(2))^2-x(1)*x(2),(x(1)+x(6))^2-x(1)*x(6),(x(1)+x(12))^2-x(1)*x(12),
(x(1)+x(4))^2-x(1)*x(4),(x(2)+x(5))^2-x(2)*x(5),(x(2)+x(7))^2-x(2)*x(7),
(x(2)+x(3))^2-x(2)*x(3),(x(3)+x(8))^2-x(3)*x(8),(x(3)+x(10))^2-x(3)*x(10),
(x(4)+x(9))^2-x(4)*x(9),(x(4)+x(11))^2-x(4)*x(11),(x(5)+x(6))^2-x(5)*x(6),
(x(6)+x(7))^2-x(6)*x(7),(x(7)+x(8))^2-x(7)*x(8),(x(8)+x(9))^2-x(8)*x(9),
(x(9)+x(10))^2-x(9)*x(10),(x(10)+x(11))^2-x(10)*x(11),
(x(11)+x(12))^2-x(11)*x(12),(x(12)+x(5))^2-x(12)*x(5),(x(5)+x(9))^2-x(5)*x(9),
(x(6)+x(10))^2-x(6)*x(10),(x(7)+x(11))^2-x(7)*x(11),(x(8)+x(12))^2-x(8)*x(12);
> ideal gI=groebner(I);
> gI;
gI[1]=x(10)+x(11)+x(12)
gI[2]=x(9)-x(11)
gI[3]=x(8)+x(11)+x(12)
gI[4]=x(7)-x(12)
gI[5]=x(6)-x(11)
gI[6]=x(5)+x(11)+x(12)
gI[7]=x(4)-x(12)
gI[8]=x(3)-x(12)
gI[9]=x(2)-x(11)
gI[10]=x(1)+x(11)+x(12)
gI[11]=x(11)^2+x(11)*x(12)+x(12)^2
gI[12]=x(12)^3-1
> vdim(gI);
6
```

Podríamos haber planteado un tercer problema sobre coloración de grafos que también se puede puede resolver con bases de Gröbner pero que no abordaremos aquí:

(P3) Si tomamos un grafo k-coloreable y damos una k-coloración parcial (es decir que pintamos algunos de sus vértices), ¿cómo determinar si existe una única k-coloración compatible con esta k-coloración parcial? Y si es el caso, ¿cómo determinarla?

Curiosamente, este último problema está relacionado con el problema de la resolución de un sudoku. En efecto, a la tabla vacía 9×9 de un sudoku, podemos asociarle un grafo G_s

con 81 vértices (uno por cada celda de la tabla) donde traduciremos las reglas del sudoku con las aristas de G_s: ponemos una arista entre dos vértices de G_s cuando estos vértices corresponden a dos celdas de la tabla que no pueden recibir el mismo número, es decir las celdas situadas en una misma fila, una misma columna, o una misma subtabla 3×3 (de las 9 subtablas destacadas en un sudoku). Hecha esta asociación entre la tabla vacía de un sudoku y este grafo G_s, vemos que un sudoku resuelto corresponde a una coloración de G_s con 9 colores, los números entre 1 y 9. Visto de esta manera, está claro que el grafo G_s es 9-coloreable (porque existen sudokus resueltos que cumplen las reglas) y que no lo es de manera única (porque existen varios sudokus resueltos cumpliendo las reglas, de hecho existen muchos y por eso varios periódicos pueden proponer cada día resolver alguno!). Estas dos propiedades de G_s se podrían verificar usando Singular y los teoremas 44 y 45 (dejamos este ejercicio para quién tenga la paciencia de introducir el ideal $I_{G_s,9}$ en Singular!). Resolver un sudoku es por tanto equivalente a encontrar, dada una 9-coloración parcial del grafo G_s, una coloración total de G_s que sea compatible. Un sudoku estará bien planteado, es decir tendrá una solución única, cuando la correspondiente coloración parcial de G_s proporciona una única 9-coloración de G_s compatible. Y reconocemos aquí el problema (P3) antes planteado. Por supuesto, las bases de Gröbner no proporcionan una manera eficiente de resolver sudokus pero no deja de ser una aplicación curiosa, bonita e inesperada.

5. Ejercicios

Órdenes monomiales

Ejercicio 1.– Ordena los monomios de los siguientes polinomios de mayor a menor para el orden lexicográfico (*lex*), para el orden lexicográfico graduado (*glex*) y para el orden lexicográfico inverso graduado (*grevlex*). Verifica luego tu respuesta usando Singular.

1. $2xy^2 + 3x + 4y^2 \in K[x, y]$;
2. $x^2y^3z^3 - x^4y + y^3z^2 - xyz^2 \in K[x, y, z]$.

Ejercicio 2.– (orden producto) Consideramos dos grupos de variables, $\mathbf{x} = \{x_1, \ldots, x_n\}$ e $\mathbf{y} = \{y_1, \ldots, y_m\}$ y el anillo de polinomios $A := K[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Si $>_x$ es un orden monomial sobre $K[x_1, \ldots, x_n]$ y $>_y$ un orden monomial sobre $K[y_1, \ldots, y_m]$, definimos la siguiente relación $>_{pr}$ entre monomios de A: dados dos monomios $\mathbf{x}^\alpha, \mathbf{x}^\beta$ en las

variables $\mathbf{x}$ y dos monomios $\mathbf{y}^\gamma, \mathbf{y}^\delta$ en las variables $\mathbf{y}$,

$$\mathbf{x}^\beta \mathbf{y}^\delta >_{pr} \mathbf{x}^\alpha \mathbf{y}^\gamma \iff [\mathbf{x}^\beta >_x \mathbf{x}^\alpha] \text{ ó } [\mathbf{x}^\alpha = \mathbf{x}^\beta \text{ e } \mathbf{y}^\delta >_y \mathbf{y}^\gamma].$$

1. Prueba que $>_{pr}$ es un orden monomial sobre A (llamado *orden producto*).
2. Justifica que si M es un monomio de A solo en las variables $\mathbf{y}$ y si N es un monomio de A donde aparece al menos una de las variables $\mathbf{x}$, entonces $N >_{pr} M$, es decir que $>_{pr}$ es un orden de eliminación sobre A para las n primeras variables.
3. Prueba que si los órdenes $>_x$ y $>_y$ son los órdenes lexicográficos sobre $K[x_1, \ldots, x_n]$ y $K[y_1, \ldots, y_m]$ respectivamente, entonces $>_{pr}$ es el orden lexicográfico sobre A.
4. Observa como se puede generalizar la definición de orden producto anterior con más de dos grupos de variables.
5. Justifica que el orden lexicográfico sobre $K[x_1, \ldots, x_n]$ es un orden producto con n grupos de variables.

Ejercicio 3.– (orden matricial) Por la nota 7, cualquier orden monomial es un orden matricial, es decir que es de la forma $>_M$ para alguna matriz M inversible, $n \times n$ y con entradas enteras (siendo n el número de variables en el anillo de polinomios en el que estamos trabajando). Determina matrices M_1, M_2 y M_3 tales que $(>_{lex}) = (>_{M_1})$, $(>_{glex}) = (>_{M_2})$ y $(>_{grevlex}) = (>_{M_3})$. Si consideramos ahora el orden producto $>_{pr}$ definido en el ejercicio anterior, expresa la matriz $(n+m) \times (n+m)$ asociada a este orden en función de las matrices definiendo los ordenes $>_x$ y $>_y$.

Algoritmo de división en varias variables

Ejercicio 4.– Fijamos sobre $\mathbb{Q}[x, y, z]$ el orden *grevlex*. Divide el polinomio $f = x^2y^3z^3 + x^4y + y^3z^2 + xyz^2 \in \mathbb{Q}[x, y, z]$ por la lista ordenada de polinomios $[f_1, f_2, f_3]$ con $f_1 = xy - z^2$, $f_2 = x^2 - yz$, $f_3 = y^3 - xz^2$ (ejemplo 11). Repite el ejercicio con la lista $[f_3, f_1, f_2]$. Verifica tu respuesta con Singular.

Primeros pasos con bases de Gröbner

Ejercicio 5.– Demuestra (directamente usando la definición) que el conjunto de polinomios $\{x + z, y - z\} \subset \mathbb{Q}[x, y, z]$ es una base de Gröbner del ideal I que genera para el orden *lex*.

Ejercicio 6.– Deduce del Ejercicio 4 que $\{f_1, f_2, f_3\}$ no es una base de Gröbner del ideal $I = \langle f_1, f_2, f_3\rangle$ para el orden *grevlex*.

Criterio y algoritmo de Buchberger

Ejercicio 7.– Determina la base de Gröbner reducida del ideal $I = \langle f_1, f_2, f_3\rangle$ para el orden *grevlex* siendo f_1, f_2, f_3 los polinomios definidos en el ejemplo 11. Verifica tu respuesta con Singular.

Ejercicio 8.– Fijamos un orden monomial $>$ sobre $A = K[x_1, \ldots, x_n]$. Dado un conjunto finito de polinomios $\mathcal{G}$ de A, si tenemos dos elementos f y g de $\mathcal{G}$ tales que $\mathrm{mcd}(\mathrm{in}\,(f), \mathrm{in}\,(g)) = 1$, demuestra que entonces $S(f, g) \to_{\mathcal{G}} 0$. Observa que esto puede simplificar bastante las cosas a la hora de aplicar el criterio de Buchberger para comprobar si un conjunto de generadores finito de un ideal dado es o no una base de Gröbner. Vuelve ahora al ejercicio 5 y da una respuesta inmediata a la pregunta allí planteada.

Ejercicio 9.– Para todo entero $\ell \geq 1$, consideramos el conjunto $\mathcal{G} = \{x_1^\ell - 1, \ldots, x_n^\ell - 1\}$ y sea I el ideal de A engendrado por $\mathcal{G}$. Demuestra que $\mathcal{G}$ es una base de Gröbner universal de I.

Bases de Gröbner de ideales monomiales y binomiales

Ejercicio 10.– Sea M un ideal monomial de $A := K[x_1, \ldots, x_n]$ arbitrario.

1. Demuestra la propiedad 2 de la proposición 3, es decir que M admite un único sistema minimal de generadores formado por monomios, $\mathcal{M}$, y que $\mathcal{M}$ es la base de Gröbner reducida de M respecto de cualquier orden monomial sobre A.

2. Proporciona un método eficiente para determinar si un ideal es o no monomial y determina usando Singular cual de los 2 ideales de $\mathbb{Q}[x, y, z]$ siguientes es monomial:

   - $I = \langle x^5y^7z + x^6y^3z^4, x^6y^3z^3 + x^8yz^3, x^6y^8z^2 + x^4y^8z^4, x^7yz^2\rangle$;
   - $J = \langle x^5y^7z + x^6y^3z^4, x^6y^3z^3 + x^6yz^5, x^6y^8z^2 + x^4y^8z^4, x^7yz^2\rangle$.

Ejercicio 11.– Se dice que un ideal I de $K[x_1, \ldots, x_n]$ es *binomial* si admite un sistema de generadores formado por diferencias de monomios. Probar que, dado un órden

monomial arbitrario, la base de Gröbner reducida de un ideal binomial es binomial (es decir que está formada por diferencias de monomios).

Primeras aplicaciones en álgebra conmutativa y geometría algebraica

Ejercicio 12.– (comparación de dos ideales en un anillo de polinomios) Consideramos los dos ideales I y J de $\mathbb{Q}[x,y,z]$ siguientes:

$$\begin{aligned} I &:= (x^2+z, xy+y^2+z, xz-y^3-2yz, y^4+3y^2z+z^2), \\ J &:= (x^2+z, xy+y^2+z, x^3-yz). \end{aligned}$$

Compara estos dos ideales usando Singular, es decir determina cual de las siguientes afirmaciones es cierta (si es que alguna lo es): $I \subset J$, $J \subset I$, $I = J$.

Ejercicio 13.– (ecuaciones implícitas) Consideramos el siguiente conjunto $\mathcal{C}$ de puntos de $\mathbb{Q}^3$:

$$\mathcal{C} := \{(t, t^2, t^3) \in \mathbb{Q}^3;\, t \in \mathbb{Q}\}\,.$$

Denotamos por $I := I(C)$ al ideal formado por todos los polinomios de $A := \mathbb{Q}[x,y,z]$ que se anulan en todos los puntos de C.

1. Justifica que $\langle y - x^2, z - x^3\rangle \subset I$.

2. Prueba que todo polinomio $f \in \mathbb{Q}[x,y,z]$ se escribe de la forma

$$f = h_1.(y - x^2) + h_2.(z - x^3) + r$$

con $h_1, h_2 \in \mathbb{Q}[x,y,z]$ y $r \in \mathbb{Q}[x]$. Deduce que $I = \langle y - x^2, z - x^3\rangle$.

Ejercicio 14.– (pertenencia al radical) Utiliza Singular y la proposición 38 para demostrar que los ideales I y J dados a continuación son distintos pero tienen el mismo radical: $I = (x^2z^2 + x^3, xz^4 + 2x^2z^2 + x^3, y^2z - 2yz^2 + z^3, x^2y + y^3)$, $J = (xz^2 + x^2, yz^2 - z^3, x^2y - x^2z, y^4 - x^3, x^4z - x^3z, z^6 + x^4, x^5 - x^4)$. Comprueba el resultado calculando el radical de ambos ideales con el comando `radical` de la librería `primdec.lib` de Singular.

Referencias

[1] Abbott J.; Bigatti A. M.; Robbiano L. Cocoa *5.0 a system for doing computation in commutative algebra.* University of Genova (2013), available at `http://cocoa.dima.unige.it` .

[2] Adams W. W.; Loustaunau P. *An introduction to Gröbner bases.* Graded Studies in Mathematics **3**, Amer. Math. Soc., 1994 .

[3] Bayer D.; Mumford D. *What can be computed in algebraic geometry?.* In: D. Eisenbud and L. Robbiano (Eds.), *Computational algebraic geometry and commutative algebra* (Cortona 1991), Cambridge University Press, 1-48, 1993 .

[4] Bigatti A. M.; Gimenez P.; Sáenz de Cabezón E.(Eds.) *Monomial ideals, computations and applications.* Lecture Notes in Mathematics **2083**, Springer, 2013 .

[5] Cox D.; Little J.; O'Shea D. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Undergraduate Texts in Mathematics, 2nd. edition, Springer, 1997 .

[6] Cox D.; Little J.;O'Shea D. *Using algebraic geometry.* Graduate Texts in Mathematics **185**, Springer, 1998 .

[7] Decker W.; Greuel G.-M.; Pfister G.; Schönemann H. *Singular 3-1-6, a computer algebra system for polynomial computations.* University of Kaiserslautern (2012), available at `http://www.singular.uni-kl.de` .

[8] Decker W.; Lossen C. *Computing in algebraic geometry. A quick start using Singular.* Algorithms and Computation in Mathematics **16**, Springer, 2006 .

[9] Decker W.; Pfister G. *A first course in computational algebraic geometry.* African Institute of Mathematics (AIMS) Library Series, Cambridge University Press, 2013 .

[10] Eisenbud D. *Commutative algebra with a view toward algebraic geometry.* Graduate Texts in Mathematics **150**, Springer, 1995 .

[11] Eisenbud D.; Grayson D. R.; Stillman M.; Sturmfels B.(Eds.) *Computations in algebraic geometry with Macaulay2.* Algorithms and Computation in Mathematics **8**, Springer, 2002 .

[12] Ene V.; Herzog J. *Gröbner bases in commutative algebra.* Graded Studies in Mathematics **130**, Amer. Math. Soc., 2012 .

[13] Grayson D. R.; Stillman M. E. *Macaulay2 1.6, a software system for research in algebraic geometry.* University of Illinois/Cornell University (2013), available at `http://www.math.uiuc.edu/Macaulay2` .

[14] Greuel G.-M.; Pfister G. *A* Singular *introduction to commutative algebra.* Springer, 2002 .

[15] Hillar C. J.; Windfeldt T. *Algebraic characterization of uniquely vertex colorable graphs.* Journal of Combinatorial Theory, Series B, **98** (2008) 400-414 .

[16] Kreuzer M.; Robbiano L. *Computational commutative algebra.* Vol. I and II. Springer, 2000 and 2005 .

[17] Lejeune-Jalabert M. *Effectivité de calculs polynomiaux.* Cours de D.E.A., Institut Fourier, Grenoble, 1984-85 .

[18] Sturmfels B. *Gröbner bases and convex polytopes.* University Lecture Series **8**, Amer. Math. Soc., 1996 .

[19] Vasconcelos W. V. *Computational methods in commutative algebra and algebraic geometry.* Algorithms and Computation in Mathematics **2**, Springer, 1998 .