Capítulo XII

Aplicaciones de las bases de Groebner

Introducción

Las aplicaciones de la Matemática se han desarrollado enormemente en los últimos tiempos por el uso del Cálculo Simbólico. De este desarrollo, basado en el uso de los anillos de polinomios, una gran parte se fundamenta en las bases de Groebner, ya que nos permiten realizar cálculos mediante algoritmos más o menos eficientes y, en consecuencia, obtener resultados efectivos sobre los problemas planteados.

¿Qué problemas se pueden abordar?

En principio todos aquellos que sean susceptibles de ser expresados mediante ecuaciones polinómicas en una o varias variables. Ya hemos estudiado algunas aplicaciones de las bases de Groebner, principalmente a la aritmética de ideales. A este respecto vamos a recordar los siguiente hechos básicos relativos a la teoría de bases de Groebner.

1. Para el cálculo con ideales de anillos de polinomios una herramienta fundamental es el uso de órdenes monomiales, que son generalizaciones del orden usual en $\mathbb{N}$.

2. Fijado un orden monomial, cada polinomio se puede escribir de forma única. Dado un monomio, éste se representa mediante una n–upla, utilizando los coeficientes de las indeterminadas. Dado un polinomio no nulo, existe un término líder, formado por el coeficiente líder y el monomio líder.

1132-00.tex

3. Dado un ideal $\mathfrak{a} \subseteq K[X_1,\dots,X_n]$, sus polinomios no nulos determinan un monoideal $\mathrm{Exp}(\mathfrak{a})$ de $\mathbb{N}^n$.

4. Una base de Groebner para $\mathfrak{a}$ es un conjunto de polinomios $\{F_1,\dots,F_t\} \subseteq \mathfrak{a}$ tales que el conjunto $\{\exp(F_1),\dots,\exp(F_t)\}$ es un sistema de generadores del monoideal $\mathrm{Exp}(\mathfrak{a})$. Cada ideal no nulo tiene una base de Groebner. Para conseguir unicidad consideramos un tipo especial de bases de Groebner: *las bases de Groebner reducidas*. De esta forma podemos comparar ideales considerando bases de Groebner (reducidas).

5. Para órdenes monomiales adecuados, dado un ideal $\mathfrak{a} \subseteq K[X_1,\dots,X_n]$ con base de Groebner $\mathbb{G}$, el ideal $\mathfrak{a} \cap K[X_1,\dots,X_i] \subseteq K[X_1,\dots,X_i]$ tiene base de Groebner $\mathbb{G} \cap K[X_1,\dots,X_i]$. (Teoría de la eliminación.)

6. Como consecuencia tenemos algoritmos efectivos para determinar bases de Groebner de la intersección de ideales y así como de otros ideales dentro de la teoría aritmética de ideales de un anillo de polinomios.

Todo problema interno de la teoría de ideales en anillos de polinomios $K[X_1,\dots,X_n]$, donde K es un cuerpo, se puede abordar con el uso de bases de Groebner; siendo su resolución más ó menos complicada en función de la complejidad de los mismos. (Test de primalidad, descomposición primaria, etc.)
A partir de esta situación inicial podemos considerar ligeras modificaciones y tratar de abordar la teoría resultante; veamos algunos ejemplos.

1. En vez de un cuerpo K, es de interés determinar la aritmética de los ideales del anillo de polinomios sobre un anillo (conmutativo) A; esto es, de $A[X_1,\dots,X_n]$. En este caso, aún cuando $A = \mathbb{Z}$, el anillo de los números enteros, que es un dominio euclídeo, la complejidad de la teoría es grande.

2. En vez del anillo conmutativo $K[X_1,\dots,X_n]$, en ciertos casos es de interés considerar anillos no conmutativos: álgebras de caminos, álgebras de operadores diferenciales, extensiones de Ore, etc. También en este caso la complejidad aumenta, a la par de las posibles aplicaciones.

El objetivo de este capítulo es estudiar algunas aplicaciones de la teoría de polinomios, en las que la herramienta fundamental son las bases de Groebner, y la aritmética de polinomios con coeficientes en un cuerpo K.

59. Interpolación

Sea K un cuerpo; por ejemplo $K = \mathbb{R}$ ó $\mathbb{C}$.

Método de interpolación de Lagrange

Se considera una función $f : K^n \longrightarrow K$ de la que conocemos su valor en algunos puntos $x_1, \ldots, x_t \in K^n$, estamos interesados en determinar una aproximación a f, en este caso en un polinomio $F \in K[X_1, \ldots, X_n]$ tal que $F(x_i) = f(x_i)$, para $i = 1, \ldots, t$.

Dado un conjunto de puntos distintos $x_1, \ldots, x_t \in K^n$ determinamos un polinomio $F \in K[X_1, \ldots, X_n]$ tal que $F(x_1), \ldots, F(x_t)$ tomen unos valores dados $v_1, \ldots, v_t \in K$. Esto es, el problema que se plantea es: dados $x_1, \ldots, x_t \in K^n$, distintos, y $v_1, \ldots, v_t \in K$, determinar todos los polinomios $F \in K[X_1, \ldots, X_n]$ tales que $F(x_i) = v_i$ para cada $i = 1, \ldots, t$.

Una forma de determinar estos polinomios F es considerar el conjunto

$$\mathfrak{a} = \{F \in K[X_1, \ldots, X_n] \mid \ F(x_i) = 0, \text{ para cada } i = 1, \ldots, t\}.$$

Lema. 59.1.
Con la notación anterior $\mathfrak{a}$ *es un ideal cofinito de* $K[X_1, \ldots, X_n]$.

Observa que los polinomios F que son solución al problema de interpolación forman una clase módulo $\mathfrak{a}$, y que, por lo tanto, la solución al problema de interpolación es única módulo $\mathfrak{a}$.

Sabemos que si $\mathbb{G}$ es una base de Groebner del ideal $\mathfrak{a}$, cada clase módulo $\mathfrak{a}$ tiene un único representante de la forma $\sum_{\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(\mathbb{G})} c_\alpha X^\alpha$. Observa que esta suma es finita ya que el ideal $\mathfrak{a}$ es cofinito, y por tanto $\mathbb{N}^n \setminus \mathrm{Exp}(\mathbb{G})$ es un conjunto finito.

Para determinar una solución F basta considerar un elemento genérico, el cual será de la forma $\sum_{\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(\mathbb{G})} c_\alpha X^\alpha$, e imponer las condiciones iniciales, esto es:

$$\sum_{\alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(\mathbb{G})} c_\alpha x_i^\alpha = v_i, \text{ para } i = 1, \ldots, t.$$

Éste es un sistema de ecuaciones lineales en las indeterminadas $\{c_\alpha \mid \ \alpha \in \mathbb{N}^n \setminus \mathrm{Exp}(\mathbb{G})\}$, los coeficientes de F, y cada solución de este sistema proporciona los coeficientes de una solución al problema de la interpolación.

1132-01.tex

Teorema. 59.2.
Existe solución al problema de interpolación de Lagrange y es única módulo $\mathfrak{a}$.

Según se tome el orden monomial tendremos un tipo u otro de ideales; por ejemplo, si el orden es el lexicográfico, primarán unas variables respecto a otras; si el orden es graduado primarán unos grados respecto a otros.

Ejercicio. 59.3.
Se considera los puntos $x_0=(0,0,0), x_1=(0,0,1), x_2=(1,0,0), x_3=(1,1,0), x_4=(1,2,1), x_5=(1,1,2)$ *y los valores* $v_0=1, v_1=2, v_2=1, v_3=0, v_4=2, v_5=-1$. *Obtener un polinomio de interpolación que en los puntos* x_i *tome los valores* v_i.
Ref.: 1132e_023 SOLUCIÓN

SOLUCIÓN. Ejercicio (59.3.)
Para obtener un polinomio de interpolación, determinamos el ideal de cada uno de los puntos:

$$\begin{array}{ll}\mathfrak{a}_0=(X_1,X_2,X_3) & \mathfrak{a}_3=(X_1-1,X_2-1,X_3)\\ \mathfrak{a}_1=(X_1,X_2,X_3-1) & \mathfrak{a}_4=(X_1-1,X_2-2,X_3-1)\\ \mathfrak{a}_2=(X_1-1,X_2,X_3) & \mathfrak{a}_5=(X_1-1,X_2-1,X_3-2)\end{array}$$

El ideal $\mathfrak{a}$ es la intersección de estos ideales.

$$\mathfrak{a}=(X_3^3-3X_3^2+2X_3, X_2X_3^2-X_3^2-X_2X_3+X_3, X_2^2-X_3X_2-X_2+X_3^2-X_3,\\ -X_3^2+2X_1X_3-X_2X_3+X_3, X_1X_2-X_2, X_1^2-X_1).$$

Hemos utilizado el orden lexicográfico, por lo que la base de Groebner obtenida depende fuertemente de este orden. El complemento de $\mathrm{Exp}(\mathfrak{a})$ es:

$$\mathrm{Exp}(\mathfrak{a})=\{(2,0,0),(1,1,0),(1,0,1),(0,2,0),(0,1,2),(0,0,3)\}+\mathbb{N}^3$$

Como consecuencia $\mathbb{N}^3\backslash\mathrm{Exp}(\mathfrak{a})$ está contenido en el cubo determinado por $(2,0,0),(0,2,0)$ y $(0,0,3)$, y no son múltiplos de los elementos de $\mathrm{Exp}(\mathfrak{a})$, tenemos:

$$\mathbb{N}^3\setminus\mathrm{Exp}(\mathfrak{a})=\{(0,0,0),(0,0,1),(0,0,2),(0,1,0),(0,1,1),(1,0,0)\}.$$

Un representante de un elemento del cociente $K[X_1,X_2,X_3]/\mathfrak{a}$ es de la forma:

$$F(X)=a_{000}+a_{001}X_3+a_{002}X_3^2+a_{010}X_2+a_{011}X_2X_3+a_{100}X_1.$$

Si se verifica $F(x_i) = v_i$, para $i = 0, 1, \ldots, 5$, se tienen la relaciones:

$$\left.\begin{aligned} a_{0,0,0} &= 1 \\ a_{0,0,0} + a_{0,0,1} + a_{0,0,2} &= 2 \\ a_{0,0,0} + a_{1,0,0} &= 1 \\ a_{0,0,0} + a_{0,1,0} + a_{1,0,0} &= 0 \\ a_{0,0,0} + a_{0,0,1} + a_{0,0,2} + 2a_{0,1,0} + 2a_{0,1,1} + a_{1,0,0} &= 2 \\ a_{0,0,0} + 2a_{0,0,1} + 4a_{0,0,2} + a_{0,1,0} + 2a_{0,1,1} + a_{1,0,0} &= -1 \end{aligned}\right\}$$

Con soluciones

$$a_{\{0,0,0\}} = 1, a_{\{0,0,1\}}\frac{7}{2}, a_{\{0,0,2\}} = -\frac{5}{2}, a_{\{1,0,0\}} = 0, a_{\{0,1,0\}} = -1, a_{\{0,1,1\}} = 1.$$

que define el polinomio

$$F(X_1, X_2, X_3) = \frac{-5X_3^2}{2} + X_2X_3 + \frac{7X_3}{2} - X_2 + 1.$$

□

Método de interpolación de Hermite

Si complementamos el método de interpolación de Lagrange mediante el uso de valores para las derivadas, se tiene el método de interpolación de Hermite. Se trata en este caso de determinar un polinomio $F \in K[X_1, \ldots, X_n]$ tal que en un conjunto finito de puntos $x_1, \ldots, x_t \in K^n$ (distintos) tomen valores dados $v_1, \ldots, v_t \in K$, y que para vectores unitarios w_{i,j_i} se tenga

$$D^{(h)}_{w_{i,j_i}} F(x_i) = v_{i,j_i,h}, \text{ para } i = 1, \ldots, t,\ j_i = 1, \ldots, s(i),\ h = 1, \ldots, s(i, j_i).$$

(En este caso $D^{(h)}_{w_{i,j_i}} F(x_i)$ es el valor de la derivada h–ésima de F según la dirección indicada por el vector w_{i,j_i}.)

Lema. 59.4.
Con la notación anterior el conjunto

$$\mathfrak{a} = \{F \in K[X_1, \ldots, X_n] \mid\ F(x_i) = 0 \text{ y } D^{(h)}_{w_{i,j_i}} F(x_i) = 0 \text{ para todo } i, j_i, h\}.$$

es un ideal cofinito.

Para la demostración de este Lema consideramos un vector w_{i,j_i}, y el ideal

$$\mathfrak{a}_{i,j_i} = \{F \in K[X_1, \ldots, X_n] \mid\ F(x_i) = 0,\ D^{(h)}_{w_{i,j_i}}(x_i) = 0\}.$$

Utilizando que h varía en $\{1,\dots,s(i,j_i)\}$ probamos que $\mathfrak{a}_{i,j_i}$ es un ideal. Tenemos que $\mathfrak{a}=\cap_{i,j_i}\mathfrak{a}_{i,j_i}$.
De forma análoga al método de interpolación de Lagrange, dada una base de Groebner $\mathbb{G}$ de $\mathfrak{a}$, el cociente $K[X_1,\dots,X_n]/\mathfrak{a}$ es un espacio vectorial de dimensión finita, y cada solución al problema de interpolación de Hermite está unívocamente determinada módulo $\mathfrak{a}$.
Dada una base de Groebner $\mathbb{G}$ de $\mathfrak{a}$, cada clase módulo $\mathfrak{a}$ tiene un único representante de la forma $\sum_{\alpha\in\mathbb{N}^n\setminus \mathrm{Exp}(\mathbb{G})} c_\alpha X^\alpha$. Para determinar una solución basta considerar el sistema de ecuaciones lineales

$$\sum_{\alpha\in\mathbb{N}^n\setminus \mathrm{Exp}(\mathbb{G})} c_\alpha X^\alpha = v_i,$$

$$D^{(h)}_{w_{i,j_i}} \sum_{\alpha\in\mathbb{N}^n\setminus \mathrm{Exp}(\mathbb{G})} c_\alpha X^\alpha = v_{i,j_i,h},$$

para todos i, j_i, h.

Teorema. 59.5.
La solución al problema de interpolación de Hermite es única módulo $\mathfrak{a}$.

Método de interpolación de Birkhoff

En el método de interpolación de Hermite, para conseguir la unicidad es decisivo que no existan huecos en las condiciones iniciales. Cuando existen huecos, esto es, existe un valor para $D^{(h+1)}_w F(x_i)$ y no existe $D^{(h)}_w F(x_i)$, podemos proceder suponiendo que tenemos definida $D^{(h)}_w F(x_i)$, determinar el correspondiente ideal $\mathfrak{a}$, y tener en cuenta que a la hora de calcular el polinomio de interpolación aparecerá un parámetro: el valor de $D^{(h)}_w F(x_i)$. Tendremos así la solución dependiente de un cierto número de parámetros: *los huecos*.

Elección del orden monomial

En los problemas de interpolación por medio de bases de Groebner el orden monomial utilizado es importante, pues permite obtener polinomios de interpolación con unas u otras características. Por ejemplo, un orden lexicográfico producirá polinomios en los que algunas indeterminadas tendrán grados altos, y un orden graduado producirá polinomios en los que los grados de las distintas indeterminadas son semejantes. Sin embargo, conviene tener en cuenta que para calcular la intersección el orden monomial utilizado debe ser un orden de eliminación, por lo que no podremos, en general, usar un orden graduado; podemos, una vez calculada la intersección, determinar una base de Groebner para el orden que elijamos.

Ejercicio. 59.6.
Estudia ejemplos de las diversas situaciones considerando puntos en $\mathbb{Q}^2$ y en $\mathbb{Q}^3$, con valores en $\mathbb{Q}$.
Ref.: 1132e_003 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (59.6.)
HACER □

Superficies en $\mathbb{R}^3$

Queremos determinar una superficie en $\mathbb{R}^3$ conociendo algunos puntos de la misma.
Dados puntos $(a_1,b_1,c_1),\dots,(a_t,b_t,c_t)$, para determinar un polinomio $F\in\mathbb{R}[X,Y,Z]$ que verifique $F(a_i,b_i,c_i)=0$, para cada $i=1,\dots,t$, procedemos como sigue:

(1) Determinamos el ideal $\mathfrak{a}=\{F\in\mathbb{R}^3 \mid F(a_i,b_i,c_i)=0\}$, que es el ideal $\cap_{i=1}^t(X-a_i,Y-b_i,Z-c_i)$.
(2) Si existen relaciones extra del tipo $D_w^{(h)}F(a_i,b_i,c_i)=v_{i,w,h}$, $h=0,\dots,s$, hay que cambiar el ideal $\mathfrak{a}$ para incluir éstas, y determinar los polinomios que verifican además estas relaciones.

Ejercicio. 59.7.
Determina una superficie que contenga a los puntos $x_1=(0,0,0), x_2=(1,1,1)$ y $x_3=(1,0,1)$.
Ref.: 1132e_004 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (59.7.)
Es claro que basta determinar el ideal intersección

$$(X,Y,X)\cap(X-1,Y-1,Z-1)\cap(X-1,Y,Z-1).$$

Su valor es:

$$\left\{YZ-Y,Y^2-Y,XZ-X,XY-Y,X^2-X\right\}.$$

En este caso tenemos todos los polinomios que se anulan en los puntos dados. □

El siguiente método permite imponer una condición adicional, y por lo tanto *limitar* el conjunto de soluciones.

SOLUCIÓN. Vamos a determinar un polinomio $F(X,Y)$ que en los puntos $(0,0),(1,1)$ y $(1,0)$ tome los valores $0,1$ y 1, respectivamente. Primero determinamos el ideal

$$\mathfrak{a}=(X,Y)\cap(X-1,Y-1)\cap(X-1,Y)=(X^2-X,XY-Y,Y^2-Y).$$

En consecuencia $\exp(\mathbb{G}) = \{(2,0),(1,1),(0,2)\}$, y $\mathbb{N}^2 \setminus \mathrm{Exp}(\mathbb{G}) = \{(0,0),(1,0),(0,1)\}$. Un elemento genérico de $K[X,Y]/\mathfrak{a}$ es de la forma $c_0+c_1X+c_2Y$; para que verifique las condiciones del enunciado debe verificar:

$$\left.\begin{array}{rrrr} c_0 & +c_1 0 & +c_2 0 & =0 \\ c_0 & +c_1 & +c_2 & =1 \\ c_0 & +c_1 & +c_2 0 & =1 \end{array}\right\}$$

La solución es: $c_0 = 0, c_1 = 1, c_2 = 0$. La superficie que pasa por x_1, x_2 y x_3 es: $Z = X$, que es un plano. □

Ejercicio. 59.8.
Determina una superficie que contenga a los puntos $x_1 = (0,0,0), x_2 = (1,1,1), x_3 = (1,0,1)$ *y* $x_4 = (1,-1,2)$.
Ref.: 1132e_005 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (59.8.)
Vamos a determinar un polinomio $F(X,Y)$ que en los puntos $(0,0),(1,1),(1,0)$ y $(1,-1)$ tome los valores $0,1,1$ y 2, respectivamente. Primero determinamos el ideal

$$\mathfrak{a} = (X,Y) \cap (X-1,Y-1) \cap (X-1,Y) \cap (X-1,Y+1) = (X^2-X, XY-Y, Y^3-Y).$$

En consecuencia $\exp(\mathbb{G}) = \{(2,0),(1,1),(0,3)\}$, y $\mathbb{N}^2 \setminus \mathrm{Exp}(\mathbb{G}) = \{(0,0),(1,0),(0,1),(0,2)\}$. Un elemento genérico de $K[X,Y]/\mathfrak{a}$ es de la forma $c_0+c_1X+c_2Y+c_3Y^2$; para que verifique las condiciones del enunciado debe verificar:

$$\left.\begin{array}{rrrrr} c_0 & +c_1 0 & +c_2 0 & +c_3 0 & =0 \\ c_0 & +c_1 & +c_2 & +c_3 & =1 \\ c_0 & +c_1 & +c_2 0 & +c_3 0 & =1 \\ c_0 & +c_1 & -c_2 & +c_3 & =2 \end{array}\right\}$$

La solución es: $c_0 = 0, c_1 = 1, c_2 = \frac{-1}{2}, c_3 = \frac{1}{2}$. La superficie que pasa por x_1, x_2, x_3 y x_4 es: $Z = X - \frac{Y}{2} + \frac{Y^2}{2}$, que no es un plano. □

Esta técnica no podemos aplicarla cuando consideramos puntos con las mismas coordenadas, por ejemplo: para determinar una superficie que contenga a los puntos $x_1 = (0,0,0)$, $x_2 = (0,0,1)$, $x_3 = (0,1,0)$, $x_4 = (0,1,1)$, $x_5 = (1,0,0)$, $x_6 = (1,0,1)$, $x_7 = (1,1,0)$, $x_8 = (1,1,1)$. Para esto, como veremos más adelante, necesitamos ver otro modo de dar las ecuaciones de una superficie.

Sin embargo, en algunas ocasiones podemos obtener la ecuación de la superficie que contiene a un cierto número de puntos: $x_1, x_2, \ldots, x_t$ determinando un polinomio $F \in K[X,Y,Z]$ tal que $F(x_i) = 0$. Más en general; dados puntos $x_1, x_2 \ldots, x_t$ y valores $v_1, v_2, \ldots, v_t$, veamos un ejemplo en el que calcularemos un polinomio F tal que $F(x_i) = v_i$ para $i = 1, 2, \ldots, t$.

Ejercicio. 59.9.
Dados los puntos $x_1=(0,0,0), x_2=(1,1,1), x_3=(1,0,1), x_4=(0,-1,2)$*, determina un polinomio* F *tal que* $F(x_i)=v_i$*, para* $i=1,2,3,4$*, siendo* $v_1=4, v_2=5, v_3=-1, v_4=0$.
Ref.: 1132e_006 SOLUCIÓN

SOLUCIÓN. Ejercicio (59.9.)
Primero determinamos el ideal, dando su base de Groebner, $\mathbb{G}$.

$$\begin{aligned}\mathfrak{a} &= (X,Y,Z)\cap(X-1,Y-1,Z-1)\cap(X-1,Y,Z-1)\cap(X,Y+1,Z-2)\\ &= (X-2Z+Z^2, Y^2-Y-Z^2+Z, 2YZ-2Y+Z^2-Z, Z^3-3Z^2+2Z).\end{aligned}$$

Tenemos $\exp(\mathbb{G})=\{(1,0,0),(0,2,0),(0,1,1),(0,0,3)\}$. En consecuencia

$$\mathbb{N}^3\setminus \operatorname{Exp}(\mathbb{G}) = \{(0,0,0),(0,1,0),(0,0,1),(0,0,2)\},$$

y un elemento genérico de $K[X,Y,Z]/\mathfrak{a}$ se escribe en la forma $c_0+c_1Y+c_2Z+c_3Z^2$. Al imponer que tome en los puntos los valores dados, tenemos un sistema de ecuaciones lineales en las indeterminadas c_0,c_1,c_2,c_3.

$$\left.\begin{array}{rrrrl} c_0 & & & & =4\\ c_0 & +c_1 & +c_2 & +c_3 & =5\\ c_0 & & +c_2 & +c_3 & =-1\\ c_0 & -c_1 & +2c_2 & +4c_3 & =0\end{array}\right\}$$

Cuya solución es: $c_0=4, c_1=6, c_2=-11, c_3=6$, y en consecuencia el polinomio F es:

$$F(X,Y,Z)=6Y+6Z^2-11Z+4.$$

□

Ejercicio. 59.10.
Supongamos que en el ejercicio anterior agregamos la condición $\frac{d}{dX}F(x_1)=1$.
Ref.: 1132e_007 SOLUCIÓN

SOLUCIÓN. Ejercicio (59.10.)
En este caso el ideal asociado al punto x_1 es

$$\{F\in K[X,Y,Z]\mid\ F(x_1)=0=\frac{d}{dX}F(x_1)\}.$$

Por tanto se tiene

$$F = H_1X + H_2Y + H_3Z,$$
$$\tfrac{d}{dX}F = \tfrac{d}{dX}H_1X + H1 + \tfrac{d}{dX}H_2Y + \tfrac{d}{dX}H_3Z,$$

Al evaluar en x_1 se tiene:

$$0 = \tfrac{d}{dX}F = H_1(x_1),$$

De aquí se tiene $H_1 \in (X,Y,Z)$, y por tanto $H_1 = H_{11}X + H_{12}Y + H_{13}Z$, entonces

$$F = H_1X + H_2Y + H_3Z = (H_{11}X + H_{12}Y + H_{13}Z)X + H_2Y + H_3Z = K_1X^2 + K_2Y + K_3Z.$$

El ideal de x_1 es: (X_2,Y,Z). Al introducir este ideal en el desarrollo del problema, tenemos que calcular

$$\mathfrak{a} = (X^2,Y,Z) \cap (X-1,Y-1,Z-1) \cap (X-1,Y,Z-1) \cap (X,Y+1,Z-2)$$
$$\{2Z - 3Z^2 + Z^3, -2Y - Z + 2YZ + Z^2, -Y + Y^2 + Z - Z^2, -2Z + XZ + Z^2, -2Y + 2XY + Z - Z^2,$$
$$X^2 - 2Z + Z^2\}. \quad \text{(XII.1)}$$

Tenemos $\exp(\mathbb{G}) = \{(0,0,3),(0,1,1),(1,0,1),(0,2,0),(0,1,0),(2,0,0)\}$. En consecuencia,

$$M^3 \setminus \mathrm{Exp}(\mathbb{G}) = \{(0,0,0),(1,0,0),(0,1,0),(1,1,0),(0,0,1),(0,0,2)\}.$$

Un elemento genérico de $K[X,Y,Z]/\mathfrak{a}$ se escribe como $c_0 + c_1X + c_2Y + c_3XY + c_4Z + c_5Z^2$. Al imponer que tome en los puntos los valores dados, tenemos un sistema de ecuaciones lineales en las indeterminadas $c_0,\ldots,c_5$.

$$\left.\begin{array}{rrrrrrr} c_0 & & & & & = & 4 \\ & c_1 & & & & = & 1 \\ c_0 & +c_1 & +c_2 & +c_3 + & c_4 + & c_5 = & 5 \\ c_0 & +c_1 & & + & c_4 + & c_5 = & -1 \\ c_0 & & -c_2 & & +2c_4 + 4c_5 = & & 0 \end{array}\right\}$$

Cuya solución es: $c_0 = 4$, $c_1 = 1$, $c_3 = 6 - c_2$, $c_4 = -10 - \frac{c_2}{2}$, $c_5 = 4 + \frac{c_2}{2}$, y el polinomio pedido es: $F(X,Y,Z) = 4 + X + c_2Y + (6-c_2)XY - \frac{20+c_2}{2}Z + \frac{8+c_2}{2}Z^2$. □

Superficies definidas por funciones coordenadas

Supongamos que queremos determinar una superficie de ecuación $F = 0$, siendo $F \in \mathbb{R}[X,Y,Z]$, con ecuaciones paramétricas

$$X = X(t,s)$$
$$Y = Y(t,s)$$
$$Z = Z(t,s)$$

con la información inicial dada por la tabla siguiente:

(t,s)	$X(t,s)$	$Y(t,s)$	$Z(t,s)$
(t_1,s_i)	x_i	y_i	z_i
$(0,0)$	1	-1	2
$(0,1)$	2	1	0
$(1,0)$	3	-2	1
$(t_i,s_i),w_{i,j_i},h$	$x_{i,j_i,h}$	$y_{i,j_i,h}$	$z_{i,j_i,h}$
$(0,0),(1,0),1$	1	-1	0
$(0,0),(0,1),1$	1	-1	-1
$(0,0),(1,0),2$	0	-2	2

Determinamos un polinomio $F_X \in \mathbb{R}[T,S]$ que resuelve el problema de interpolación dado por:

(t,s)	$X(t,s)$
(t_1,s_i)	x_i
$(0,0)$	1
$(0,1)$	2
$(1,0)$	3
$(t_i,s_i),w_{i,j_i},h$	$x_{i,j_i,h}$
$(0,0),(1,0),1$	1
$(0,0),(0,1),1$	1
$(0,0),(1,0),2$	0

Repitiendo el proceso para Y y para Z, se obtienen polinomios $F_X, F_Y, F_Z \in \mathbb{R}[T,S]$ que son las ecuaciones paramétricas de nuestra superficie. En este caso es:

$$\begin{aligned} X &= F_X(T,S) \\ Y &= F_Y(T,S) \\ Z &= F_Z(T,S) \end{aligned}$$

Para obtener una ecuación implícita de la superficie, basta con eliminar las indeterminadas T y S en las anteriores ecuaciones; obteniendo así la ecuación buscada: $F = 0$, con $F \in \mathbb{R}[X,Y,Z]$.

Actividades

Ejercicio. 59.11. (Circunferencia)
Dados los puntos $x_1 = (1,0)$, $x_2 = (0,1)$, $x_3 = (-1,0)$ *y* $x_4 = (0,-1)$.
(1) Determina los polinomios $F \in \mathbb{R}[X,Y]$ *tal que* $F(x_i) = 0$, *para* $i = 1,2,3,4$.

Se consideran además los puntos $x_5=(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}})$, $x_6=(-\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}})$, $x_7=(-\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}})$, $x_8=(\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}})$.

(2) *Determina un polinomio* $F\in\mathbb{R}[X,Y]$ *tal que* $F(x_i)=0$ *para* $i=1,\dots,8$.

Imponemos las condiciones $\frac{d}{dX}F(x_i)=v_{X,i}$ *y* $\frac{d}{dY}F(x_i)=v_{Y,i}$.

(3) *Determina los polinomios* $F\in\mathbb{R}[X,Y]$ *tales que* $F(x_i)=0$, *para* $i=1,2,3,4$ *y* $\frac{d}{dX}F(x_i)=v_{X,i}$, *siendo* $v_{X,1}=2$, $v_{X,2}=0$, $v_{X,3}=-2$, $v_{X,4}=0$.

(4) *Determina los polinomios* $F\in\mathbb{R}[X,Y]$ *verificando las condiciones de (3) y la condición* $\frac{d}{dY}F(x_i)=v_{Y,i}$, *siendo* $v_{Y,1}=0$, $v_{Y,2}=2$, $v_{Y,3}=0$, $v_{Y,4}=-2$.

(5) *Determina los polinomios* $F\in\mathbb{R}[X,Y]$ *verificando las condiciones de (3) y la condición* $\frac{d^2}{dX^2}F(x_i)=w_{X,i}$, *siendo* $w_{X,1}=2$, $w_{X,2}=2$, $w_{X,3}=2$, $w_{X,4}=2$.

Ref.: 1132e_008 SOLUCIÓN

SOLUCIÓN. Ejercicio (59.11.)

HACER □

Ejercicio. 59.12.

Dados los puntos $x_1=(1,0)$, $x_2=(0,1)$, $x_3=(-1,0)$ *y* $x_4=(0,-1)$.*Tarea a realizar.*

(1) *Determina los polinomios* $F\in\mathbb{R}[X,Y]$ *tal que* $F(x_i)=v_i$, *para* $i=1,2,3,4$. *Tomar*

$$v_1=1;\qquad v_2=2;\qquad v_3=1;\qquad v_4=0.$$

(2) *Determina los polinomios* $F\in\mathbb{R}[X,Y]$ *tal que* $F(x_i)=v_i$, *para* $i=1,2,3,4$, *y*

$$\frac{d}{dY}F(x_1)=1;\qquad \frac{d}{dX}F(x_2)=0;\qquad \frac{d}{dY}F(x_3)=-1;\qquad \frac{d}{dX}F(x_4)=0.$$

Ref.: 1132e_009 SOLUCIÓN

SOLUCIÓN. Ejercicio (59.12.)

HACER □

60. Grafos

Dado un grafo $G = (V, L)$, una **coloración** de G consiste en asignar un color a cada vértice de forma que dos vértices, entre los que existe un lado, tienen colores distintos. Observa que una coloración es una aplicación $c : V \to C$ del conjunto de vértices V al conjunto de colores C, que verifica ciertas condiciones; si $v = \{v_1, v_2\} \in L$ es un lado, entonces $c(v_i) \neq c(v_j)$.

Existe una amplia teoría sobre coloraciones de grafos. Vamos a estudiar un aspecto de la teoría en el que podremos hacer uso de los anillos de polinomios y de las bases de Groebner.

Supongamos que queremos dar a un grafo G una coloración con d colores, esto es, una **d–coloración**. En este caso asignamos a cada color un valor, sea ξ^j, siendo ξ una raíz d–ésima primitiva de la unidad. Como tenemos d raíces d–ésimas de la unidad, podemos asignar una a cada uno de los colores. Así pues dar una coloración es definir una aplicación $c : V \to \{\xi_0, \dots, \xi_{d-1}\} = \{\xi^j \mid j = 0, \dots, d-1\}$, para ξ una raíz primitiva d–ésima de la unidad.

Si los vértices son $V = \{1, \dots, t\}$ y llamamos x_i al valor asignado al vértice i, se tiene $x_i^d - 1 = 0$. Por otro lado para dos vértices i, j se tiene

$$(x_i - x_j)(x_i^{d-1} + x_i^{d-2}x_j + \cdots + x_i x_j^{d-2} + x_i^{d-1}) = x_i^d - x_j^d = 0.$$

Si i y j están unidos por un lado, se tiene $x_i - x_j \neq 0$, y por tanto $x_i^{d-1} + x_i^{d-2}x_j + \cdots + x_i x_j^{d-2} + x_i^{d-1} = 0$.

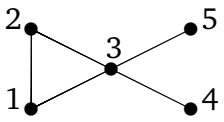
Como consecuencia, los valores x_i son raíces del siguiente sistema de ecuaciones polinómicas:

$$\begin{cases} X_i^d - 1 = 0, & i \in V, \\ X_i^{d-1} + X_i^{d-2}X_j + \cdots + X_i X_j^{d-2} + X_i^{d-1} = 0 & \{i, j\} \in L. \end{cases}$$

Cada solución de este sistema es una coloración del grafo.

Para futuras aplicaciones, llamamos $\mathfrak{a}(G, d)$ al ideal generado por los polinomios anteriores; cada elemento de $V(\mathfrak{a}(G, d))$, el conjunto de ceros de este ideal, corresponde a una d-coloración. Llamamos $\mathfrak{a}(G, d)$ el **ideal de d–coloración** del grafo G.

Veamos el siguiente ejemplo.



Vamos a colorear con 2 y 3 colores.

1132-02.tex

Para dos colores tenemos que resolver el sistema:

$$\left.\begin{array}{l} X_1^2-1=0 \\ X_2^2-1=0 \\ X_3^2-1=0 \\ X_4^2-1=0 \\ X_5^2-1=0 \end{array}\right\} \left.\begin{array}{l} X_1+X_2=0 \\ X_1+X_3=0 \\ X_2+X_3=0 \\ X_3+X_4=0 \\ X_3+X_5=0 \end{array}\right\}$$

$$\mathbf{> GroebnerBasis[\{X_1^2-1, X\_2^2-1, X_3^2-1, X_4^2-1, X_5^2-1, X_1+X_2, X_1+X_3, X_2+X_3, X_3+X_4, X_3+X_5\}, \{X_1, X_2, X_3, X_4, X_5\}]}$$

la base de Groebner del ideal generado por estos polinomios es trivial: $\{1\}$. En consecuencia no existe una coloración del grado con dos colores. Lo cual, por otro lado es evidente por la existencia del subgrafo completo $\{1,2,3\}$.

Para tres colores tenemos que resolver el sistema:

$$\left.\begin{array}{l} X_1^3-1=0 \\ X_2^3-1=0 \\ X_3^3-1=0 \\ X_4^3-1=0 \\ X_5^3-1=0 \end{array}\right\} \left.\begin{array}{l} X_1^2+X_1X_2+X_2^2=0 \\ X_1^2+X_1X_3+X_3^2=0 \\ X_2^2+X_2X_3+X_3^2=0 \\ X_3^2+X_3X_4+X_4^2=0 \\ X_3^2+X_3X_5+X_5^2=0 \end{array}\right\}$$

$$\mathbf{> GroebnerBasis[\{X_1^3-1, X_2^3-1, X_3^3-1, X_4^3-1, X_5^3-1, X_1^2+X_1X_2+X_2^2, X_1^2+X_1X_3+X_3^2, X_2^2+X_2X_3+X_3^2, X_3^2+X_3X_4+X_4^2, X_3^2+X_3X_5+X_5^2\}, \{X_1, X_2, X_3, X_4, X_5\}]}$$

la base de Groebner del ideal generado por estos polinomios es:

$$\{X_1+X_2+X_3, X_2^2+X_2X_3-X_3X_5-X_5^2, X_3^2+X_3X_5+X_5^2, X_3X_4+X_4^2-X_3X_5-X_5^2, -1+X_4^3, -1+X_5^3\}.$$

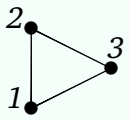
Para averiguar cuántas coloraciones distintas existen, tenemos que calcular la co–dimensión de este ideal, esto es, el número de soluciones distintas. En Mathematica usamos la orden:

$$\mathbf{L = Solve[\{-1+X_5^3 == 0, -1+X_4^3 == 0, X_3X_4+X_4^2-X_3X_5-X_5^2 == 0, X_3^2+X_3X_5+X_5^2 == 0, X_2^2+X_2X_3-X_3X_5-X_5^2 == 0, X_1+X_2+X_3 == 0\}, \{X_1, X_2, X_3, X_4, X_5\}]}$$

Length[L]

Por lo tanto el número de 3–coloraciones distintas es 24. Que, eliminado las permutaciones de tres elementos, nos dan cuatro coloraciones esencialmente distintas.

Ejercicio. 60.1.
Prueba que el siguiente grafo tiene una única 3-coloración.



Ref.: 1132e_010 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (60.1.)
HACER □

Sudoku

El problema de resolver un sodoku se puede plantear en términos de colorear un grafo. Imaginemos que tenemos un sudoku 9×9. Cada casilla será un vértice del grafo, y habrá un lado entre cada dos vértices que estén en la misma fila, en la misma columna, o en el mismo cuadrado básico 3×3. Tenemos $9 \times 9 = 81$ vértices y de cada vértice salen $8 + 8 + 4 = 20$ lados.

Resolver un sudoku consiste en colorear el correspondiente grafo con nueve colores, y por tanto es un problema que ya hemos resuelto. Sin embargo en la práctica la resolución consume mucho tiempo. Veamos el caso de un sudoku 4×4. En este caso tenemos $4 \times 4 = 16$ vértices, que podemos representar por $v_{i,j}$, en donde i y j varían entre 1 y 4. Además de cada vértice salen $3 + 3 + 1 = 7$ lados. Tenemos por tanto $16 + \frac{7 \times 16}{2} = 72$ ecuaciones:

Ver archivo en Mathematica “sudoku4x4-b.nb".

Los vértices:

```
> Var = Flatten[Table[Subscript[v, i, j], {i, 1, 4}, {j, 1, 4}]]

> EcuVert = Table[Var[[i]]^4 - 1, {i, 1, Length[Var]}]
```

Los lados:

```
> Lado1[i_, j_]:=
    Join[Table[{Subscript[v,i,j],Subscript[v,i,k]},{k,j+1,4}],
        Table[{Subscript[v,i,j],Subscript[v,k,j]},{k,i+1,4}]]
```

```
> Lados2=
    Flatten[Join[Table[Lado1[i,j],{i,1,4},{j,i,4}],
        Table[Lado1[i,j],{i,1,4},{j,1,i-1}]],2];

> Lados3=
    {{Subscript[v,1,1],Subscript[v,2,2]},
        {Subscript[v,1,2],Subscript[v,2,1]},
        {Subscript[v,1,3],Subscript[v,2,4]},
        {Subscript[v,1,4],Subscript[v,2,3]},
        {Subscript[v,3,1],Subscript[v,4,2]},
        {Subscript[v,3,2],Subscript[v,4,1]},
        {Subscript[v,3,3],Subscript[v,4,4]},
        {Subscript[v,3,4],Subscript[v,4,3]}};

> Lados= Sort[Join[Lados2, Lados3]];
```

Ecuaciones de los lados:

```
> Ecuacion[x_, y_] := x^3 + x^2 y + x y^2 + y^3

> Ecuacion2[L_] := Ecuacion[L[[1]], L[[2]]]

> EcuLados = Map[Ecuacion2, Lados];
```

Ecuaciones del Sudoku 4×4:

```
> EcuSudoku = Join[EcuVert, EcuLados];
```

Como todos conocemos, al resolver un sudoku tenemos algunas casillas a las que previamente les hemos asignado un valor. Por tanto las correspondientes indeterminadas no son tales, puesto que ya conocemos su valor. Veamos un ejemplo.

Ejemplo.

Vamos a estudiar el caso en el que $v_{1,1} = 1$, $v_{1,4} = -1$, $v_{2,1} = -1$, $v_{2,2} = I$, $v_{3,3} = 1$, $v_{4,4} = I$, que corresponde al sudoku:

1			-1
-1	I		
		1	
			I

```
> CondInicial=
    {Subscript[v,1,1]-1,
     Subscript[v,1,4]+1,
     Subscript[v,2,1]+1,
```

```
     Subscript[v,2,2]-I,
     Subscript[v,3,3]-1,
     Subscript[v,4,4]-I};

> EcuSudokuEjemplo=Join[EcuSudoku,CondInicial];

> GB=GroebnerBasis[EcuSudokuEjemplo, Var]

> Sistema=Table[GB[[i]]==0,{i,1,Length[GB]}];

> SO=Solve[Sistema, Var];

> Length[SO]

> Table[Sort[SO[[i]],#1[[1,2]]<#2[[1,2]]&],{i,1,Length[SO]}];

> MatrixForm[%]
```

Observa que en este caso se tiene una solución única.

Problema. 60.2.
(1) ¿Cuál es el número mínimo de casillas que tienen que ser ocupadas para que la solución de un sudoku 4×4 *sea única?*
Observa que en el ejemplo anterior hemos utilizado exactamente seis casillas.
(2) ¿Cuáles pueden ser estas casillas?

Otro método

En este caso podríamos también haber trabajado en el cuerpo $\mathbb{F}_5$, que tiene exactamente cuatro raíces cuartas de la unidad: todos los elementos no nulo. El desarrollo es exactamente el mismo que hemos expuesto, si bien el tiempo de cálculo empleado puede ser menor.

Otro método

Siguiendo con el problema de resolver un sudoku 4×4, podemos trabajar, en vez de en el conjunto de las raíces cuartas de la unidad, en el cuerpo $\mathbb{F}_4$. Este cuerpo es $\mathbb{F}_4 = \mathbb{Z}_2[X]/(X^2+X+1)$. De esta forma una coloración es dar una aplicación $c : V \longrightarrow \mathbb{F}_4$; si llamamos $c(v_{i,j}) = x_{i,j}$, resulta que cada uno de estos valores es un elemento de $\mathbb{F}_4$, y por tanto verifica la ecuación $X^4 - X = 0$. Dados dos vértices v y w unidos por un lado, se tiene $v - w \neq 0$, y por otro lado $v^4 - v = 0 = w^4 - w$; tenemos entonces $v^4 - w^4 = v - w$, y si $v - w \neq 0$, entonces $v^3 + v^2 w + v w^2 + w^3 = \dfrac{v^4 - w^4}{v - w} = 1$.

Los lados del grafo son:

Filas y Columnas:
$\{v_{1,1}, v_{1,2}\}, \{v_{1,1}, v_{1,3}\}, \{v_{1,1}, v_{1,4}\}, \{v_{1,1}, v_{2,1}\},$
$\{v_{1,1}, v_{3,1}\}, \{v_{1,1}, v_{4,1}\}, \{v_{1,2}, v_{1,3}\}, \{v_{1,2}, v_{1,4}\},$
$\{v_{1,2}, v_{2,2}\}, \{v_{1,2}, v_{3,2}\}, \{v_{1,2}, v_{4,2}\}, \{v_{1,3}, v_{1,4}\},$
$\{v_{1,3}, v_{2,3}\}, \{v_{1,3}, v_{3,3}\}, \{v_{1,3}, v_{4,3}\}, \{v_{1,4}, v_{2,4}\},$
$\{v_{1,4}, v_{3,4}\}, \{v_{1,4}, v_{4,4}\}, \{v_{2,2}, v_{2,3}\}, \{v_{2,2}, v_{2,4}\},$
$\{v_{2,2}, v_{3,2}\}, \{v_{2,2}, v_{4,2}\}, \{v_{2,3}, v_{2,4}\}, \{v_{2,3}, v_{3,3}\},$
$\{v_{2,3}, v_{4,3}\}, \{v_{2,4}, v_{3,4}\}, \{v_{2,4}, v_{4,4}\}, \{v_{3,3}, v_{3,4}\},$
$\{v_{3,3}, v_{4,3}\}, \{v_{3,4}, v_{4,4}\}, \{v_{2,1}, v_{2,2}\}, \{v_{2,1}, v_{2,3}\},$
$\{v_{2,1}, v_{2,4}\}, \{v_{2,1}, v_{3,1}\}, \{v_{2,1}, v_{4,1}\}, \{v_{3,1}, v_{3,2}\},$
$\{v_{3,1}, v_{3,3}\}, \{v_{3,1}, v_{3,4}\}, \{v_{3,1}, v_{4,1}\}, \{v_{3,2}, v_{3,3}\},$
$\{v_{3,2}, v_{3,4}\}, \{v_{3,2}, v_{4,2}\}, \{v_{4,1}, v_{4,2}\}, \{v_{4,1}, v_{4,3}\},$
$\{v_{4,1}, v_{4,4}\}, \{v_{4,2}, v_{4,3}\}, \{v_{4,2}, v_{4,4}\}, \{v_{4,3}, v_{4,4}\}$
Cuadrículas:
$\{v_{1,1}, v_{2,2}\}, \{v_{1,2}, v_{2,1}\}, \{v_{1,3}, v_{2,4}\}, \{v_{1,4}, v_{2,3}\},$
$\{v_{3,1}, v_{4,2}\}, \{v_{3,2}, v_{4,1}\}, \{v_{3,3}, v_{4,4}\}, \{v_{3,4}, v_{4,3}\}$

Las ecuaciones son:

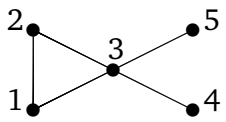
$$
\begin{gathered}
v_{1,1}^4 - v_{1,1}, v_{1,2}^4 - v_{1,2}, v_{1,3}^4 - v_{1,3}, v_{1,4}^4 - v_{1,4}, v_{2,1}^4 - v_{2,1}, v_{2,2}^4 - v_{2,2}, v_{2,3}^4 - v_{2,3}, \\
v_{2,4}^4 - v_{2,4}, v_{3,1}^4 - v_{3,1}, v_{3,2}^4 - v_{3,2}, v_{3,3}^4 - v_{3,3}, v_{3,4}^4 - v_{3,4}, v_{4,1}^4 - v_{4,1}, v_{4,2}^4 - v_{4,2}, \\
v_{4,3}^4 - v_{4,3}, v_{4,4}^4 - v_{4,4}, \\
v_{1,1}^3 + v_{1,2}v_{1,1}^2 + v_{1,2}^2 v_{1,1} + v_{1,2}^3 + 1, v_{1,1}^3 + v_{1,3}v_{1,1}^2 + v_{1,3}^2 v_{1,1} + v_{1,3}^3 + 1, \\
v_{1,1}^3 + v_{1,4}v_{1,1}^2 + v_{1,4}^2 v_{1,1} + v_{1,4}^3 + 1, v_{1,1}^3 + v_{2,1}v_{1,1}^2 + v_{2,1}^2 v_{1,1} + v_{2,1}^3 + 1, \\
v_{1,1}^3 + v_{2,2}v_{1,1}^2 + v_{2,2}^2 v_{1,1} + v_{2,2}^3 + 1, v_{1,1}^3 + v_{3,1}v_{1,1}^2 + v_{3,1}^2 v_{1,1} + v_{3,1}^3 + 1, \\
v_{1,1}^3 + v_{4,1}v_{1,1}^2 + v_{4,1}^2 v_{1,1} + v_{4,1}^3 + 1, v_{1,2}^3 + v_{1,3}v_{1,2}^2 + v_{1,3}^2 v_{1,2} + v_{1,3}^3 + 1, \\
v_{1,2}^3 + v_{1,4}v_{1,2}^2 + v_{1,4}^2 v_{1,2} + v_{1,4}^3 + 1, v_{1,2}^3 + v_{2,1}v_{1,2}^2 + v_{2,1}^2 v_{1,2} + v_{2,1}^3 + 1, \\
v_{1,2}^3 + v_{2,2}v_{1,2}^2 + v_{2,2}^2 v_{1,2} + v_{2,2}^3 + 1, v_{1,2}^3 + v_{3,2}v_{1,2}^2 + v_{3,2}^2 v_{1,2} + v_{3,2}^3 + 1, \\
v_{1,2}^3 + v_{4,2}v_{1,2}^2 + v_{4,2}^2 v_{1,2} + v_{4,2}^3 + 1, v_{1,3}^3 + v_{1,4}v_{1,3}^2 + v_{1,4}^2 v_{1,3} + v_{1,4}^3 + 1, \\
v_{1,3}^3 + v_{2,3}v_{1,3}^2 + v_{2,3}^2 v_{1,3} + v_{2,3}^3 + 1, v_{1,3}^3 + v_{2,4}v_{1,3}^2 + v_{2,4}^2 v_{1,3} + v_{2,4}^3 + 1, \\
v_{1,3}^3 + v_{3,3}v_{1,3}^2 + v_{3,3}^2 v_{1,3} + v_{3,3}^3 + 1, v_{1,3}^3 + v_{4,3}v_{1,3}^2 + v_{4,3}^2 v_{1,3} + v_{4,3}^3 + 1, \\
v_{1,4}^3 + v_{2,3}v_{1,4}^2 + v_{2,3}^2 v_{1,4} + v_{2,3}^3 + 1, v_{1,4}^3 + v_{2,4}v_{1,4}^2 + v_{2,4}^2 v_{1,4} + v_{2,4}^3 + 1, \\
v_{1,4}^3 + v_{3,4}v_{1,4}^2 + v_{3,4}^2 v_{1,4} + v_{3,4}^3 + 1, v_{1,4}^3 + v_{4,4}v_{1,4}^2 + v_{4,4}^2 v_{1,4} + v_{4,4}^3 + 1, \\
v_{2,1}^3 + v_{2,2}v_{2,1}^2 + v_{2,2}^2 v_{2,1} + v_{2,2}^3 + 1, v_{2,1}^3 + v_{2,3}v_{2,1}^2 + v_{2,3}^2 v_{2,1} + v_{2,3}^3 + 1, \\
v_{2,1}^3 + v_{2,4}v_{2,1}^2 + v_{2,4}^2 v_{2,1} + v_{2,4}^3 + 1, v_{2,1}^3 + v_{3,1}v_{2,1}^2 + v_{3,1}^2 v_{2,1} + v_{3,1}^3 + 1, \\
v_{2,1}^3 + v_{4,1}v_{2,1}^2 + v_{4,1}^2 v_{2,1} + v_{4,1}^3 + 1, v_{2,2}^3 + v_{2,3}v_{2,2}^2 + v_{2,3}^2 v_{2,2} + v_{2,3}^3 + 1, \\
v_{2,2}^3 + v_{2,4}v_{2,2}^2 + v_{2,4}^2 v_{2,2} + v_{2,4}^3 + 1, v_{2,2}^3 + v_{3,2}v_{2,2}^2 + v_{3,2}^2 v_{2,2} + v_{3,2}^3 + 1, \\
v_{2,2}^3 + v_{4,2}v_{2,2}^2 + v_{4,2}^2 v_{2,2} + v_{4,2}^3 + 1, v_{2,3}^3 + v_{2,4}v_{2,3}^2 + v_{2,4}^2 v_{2,3} + v_{2,4}^3 + 1, \\
v_{2,3}^3 + v_{3,3}v_{2,3}^2 + v_{3,3}^2 v_{2,3} + v_{3,3}^3 + 1, v_{2,3}^3 + v_{4,3}v_{2,3}^2 + v_{4,3}^2 v_{2,3} + v_{4,3}^3 + 1, \\
v_{2,4}^3 + v_{3,4}v_{2,4}^2 + v_{3,4}^2 v_{2,4} + v_{3,4}^3 + 1, v_{2,4}^3 + v_{4,4}v_{2,4}^2 + v_{4,4}^2 v_{2,4} + v_{4,4}^3 + 1, \\
v_{3,1}^3 + v_{3,2}v_{3,1}^2 + v_{3,2}^2 v_{3,1} + v_{3,2}^3 + 1, v_{3,1}^3 + v_{3,3}v_{3,1}^2 + v_{3,3}^2 v_{3,1} + v_{3,3}^3 + 1, \\
v_{3,1}^3 + v_{3,4}v_{3,1}^2 + v_{3,4}^2 v_{3,1} + v_{3,4}^3 + 1, v_{3,1}^3 + v_{4,1}v_{3,1}^2 + v_{4,1}^2 v_{3,1} + v_{4,1}^3 + 1, \\
v_{3,1}^3 + v_{4,2}v_{3,1}^2 + v_{4,2}^2 v_{3,1} + v_{4,2}^3 + 1, v_{3,2}^3 + v_{3,3}v_{3,2}^2 + v_{3,3}^2 v_{3,2} + v_{3,3}^3 + 1, \\
v_{3,2}^3 + v_{3,4}v_{3,2}^2 + v_{3,4}^2 v_{3,2} + v_{3,4}^3 + 1, v_{3,2}^3 + v_{4,1}v_{3,2}^2 + v_{4,1}^2 v_{3,2} + v_{4,1}^3 + 1, \\
v_{3,2}^3 + v_{4,2}v_{3,2}^2 + v_{4,2}^2 v_{3,2} + v_{4,2}^3 + 1, v_{3,3}^3 + v_{3,4}v_{3,3}^2 + v_{3,4}^2 v_{3,3} + v_{3,4}^3 + 1, \\
v_{3,3}^3 + v_{4,3}v_{3,3}^2 + v_{4,3}^2 v_{3,3} + v_{4,3}^3 + 1, v_{3,3}^3 + v_{4,4}v_{3,3}^2 + v_{4,4}^2 v_{3,3} + v_{4,4}^3 + 1, \\
v_{3,4}^3 + v_{4,3}v_{3,4}^2 + v_{4,3}^2 v_{3,4} + v_{4,3}^3 + 1, v_{3,4}^3 + v_{4,4}v_{3,4}^2 + v_{4,4}^2 v_{3,4} + v_{4,4}^3 + 1, \\
v_{4,1}^3 + v_{4,2}v_{4,1}^2 + v_{4,2}^2 v_{4,1} + v_{4,2}^3 + 1, v_{4,1}^3 + v_{4,3}v_{4,1}^2 + v_{4,3}^2 v_{4,1} + v_{4,3}^3 + 1, \\
v_{4,1}^3 + v_{4,4}v_{4,1}^2 + v_{4,4}^2 v_{4,1} + v_{4,4}^3 + 1, v_{4,2}^3 + v_{4,3}v_{4,2}^2 + v_{4,3}^2 v_{4,2} + v_{4,3}^3 + 1, \\
v_{4,2}^3 + v_{4,4}v_{4,2}^2 + v_{4,4}^2 v_{4,2} + v_{4,4}^3 + 1, v_{4,3}^3 + v_{4,4}v_{4,3}^2 + v_{4,4}^2 v_{4,3} + v_{4,4}^3 + 1
\end{gathered}
$$

Estamos trabajando en el anillo $\mathbb{F}_4[v_{i,j}]$, y en él tenemos el ideal $\mathfrak{a}$ generado por los polinomios anteriores; podemos pasar al anillo $\mathbb{F}_2[X, v_{i,j}]$, y considerar el ideal $\mathfrak{b}$ generado por estos mismos polinomios junto con el polinomio X^2+X+1. Este cambio es importante, ya que ahora podemos trabajar sencillamente módulo 2. Otro problema es calcular una solución; los valores de las soluciones están en el conjunto $\{0, 1, x, x+1\} = \mathbb{F}_4$.

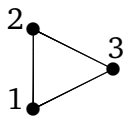
Grafos unívocamente coloreables

Dado grafo G que es d–coloreable, esto es, admite una d–coloración, decimos que G es **unívocamente d–coloreable** si para cada dos d–coloraciones distintas c_1 y c_2 existe una biyección $\theta : C \to C$ del conjunto de colores tal que $c_2 = \theta \circ c_1$. Observa que si G es unívocamente d–coloreable, entonces el conjunto $V(\mathfrak{a}(G,d))$ tiene exactamente $d!$ elementos, esto es, uno por cada permutación del conjunto de colores.

Observa que el grafo



no es unívocamente 3–coloreable; en cambio sí lo es el grafo



Observación. 60.3.
Observa que todo grafo d–completo es unívocamente d–coloreable.

Problema. 60.4.
El problema planteado es cómo determinar cuando un grafo d–coloreable es unívocamente d–coloreable.

Hacemos el siguiente desarrollo. Dada una coloración c, podemos suponer que los vértices $\{v_1,\dots,v_s\}$ están coloreados de forma que los d últimos vértices lo están con los d colores. Asignamos a los vértices $v_1,\dots,v_s$ las indeterminadas $X_1 > \cdots > X_{s-d} > Y_1 > \ldots > Y_d$, y los polinomios:

$$\begin{array}{ll}
U_d(Y_d) := Y_d^d - 1. & \\
U_i(Y_i,\dots,Y_d) := \sum_{\alpha_i+\cdots+\alpha_d=i} Y_i^{\alpha_i}\cdots Y_d^{\alpha_d}, & \text{si } i = 1,\dots,d-1. \\
V_{i,j_i}(X_{j_i},Y_i) := X_{j_i} - Y_i, & \text{si } c(v_{j_i}) = c(v_i), \quad \text{para } i = 2,\dots,d. \\
V_{1,j_1}(X_{j_i},Y_1) = X_{j_1} + Y_2 + \cdots + Y_d, & \text{si } c(v_{j_1}) = c(v_1).
\end{array}$$

Los grafos unívocamente d–coloreables se pueden caracterizar mediante el siguiente teorema:

Teorema. 60.5. ((Hillar/Windfeldt:2008, [13]))
Sea G un grafo con una d–coloración c. Con la notación anterior son equivalentes:

(a) G es unívocamente d–coloreable.
(b) $\{U_d\} \cup \{U_i \mid i = 1\ldots, d-1\} \cup \{V_{i,j_i} \mid j_i;\ i = 2,\ldots,d\} \cup \{V_{1,j_1} \mid j_1\} \subseteq \mathfrak{a}(G,d)$.
(c) $\{U_d\} \cup \{U_i \mid i = 1\ldots, d-1\} \cup \{V_{i,j_i} \mid j_i;\ i = 2,\ldots,d\} \cup \{V_{1,j_1} \mid j_1\}$ es una base de Groebner reducida de $\mathfrak{a}(G,d)$.

DEMOSTRACIÓN. HACER □

El objetivo de este Teorema es hacer que $\mathrm{Exp}(\mathfrak{a}(G,d))$ sea igual al monoideal generado por

$$\{Y_d^d, Y_{d-1}^{d-1}, \ldots, Y_2^2, Y_1, X_{s-d}, \ldots, X_1\},$$

y por tanto en este caso tendremos que $\mathbb{N}^s \setminus \mathrm{Exp}(\mathfrak{a}(G,d))$ tiene cardinal $d!$

Ciclos en grafos

Dado un grafo $G = (V,E)$ con vértices $\{v_1,\ldots,v_s\}$ y un entero positivo $d \leq s$, estamos interesados en estudiar si G contiene ciclos de longitud d. Para esto consideramos indeterminadas $X_1,\ldots,X_s$ e $Y_1,\ldots,Y_s$.
Si el grafo contiene un ciclo de longitud d y v_i es un vértice de este ciclo, consideramos $y_i = 1$, en caso contrario escribimos $y_i = 0$. Como consecuencia se tiene $y_1 + \cdots + y_s = d$ e $y_i(y_i - 1) = 0$ para cada índice i. Por lo tanto tenemos que estudiar el sistema de ecuaciones:

$$\left.\begin{array}{l} Y_1 + \cdots + Y_s - d = 0, \\ Y_1(Y_1-1) = 0 \\ \vdots \\ Y_s(Y_s-1) = 0 \end{array}\right\}$$

Dado un vértice v_i con $y_i = 1$, tomamos $x_i = k$, si v_i ocupa el lugar k en el ciclo. Como consecuencia se tiene $(x_i-1)\cdots(x_i-d) = 0$, y por tanto, para cada índice i tenemos $y_i(x_i-1)\cdots(x_i-d) = 0$. Realmente si $y_i = 0$, no nos interesa el posible valor de x_i, por esto no supone una restricción el suponer que se tiene $(x_i-1)\cdots(x_i-d) = 0$, y por lo que tenemos que estudiar las ecuaciones:

$$\left.\begin{array}{l} (X_1-1)\cdots(X_1-d) = 0 \\ \vdots \\ (X_s-1)\cdots(X_s-d) = 0 \end{array}\right\}$$

Supongamos que v_i ocupa el lugar k en el ciclo, otro vértice v_j ocupará el lugar siguiente, $k+1$ ó 1, según el caso. Se tendrá, en cualquier caso, que $y_j = 1$. Tenemos:

1. Si $x_i = k < d$, entonces $x_j = k+1$, y se tiene $x_i - x_j + 1 = 0$.
2. Si $x_i = k = d$, entonces $x_j = 1$, y se tiene $x_i - x_j - (d-1) = 0$.

Para $y_i = 1$ e $y_j = 1$, se tiene:

1. Si $x_i < d$ y la dirección en el ciclo es de v_i a v_j, entonces $x_j = k+1$, y como antes tenemos $x_i - x_j + 1 = 0$.
2. Si $x_i > 2$ y la dirección en el ciclo es de v_j a v_i, entonces se obtiene el caso anterior intercambiando i y j.
3. Si $x_i = d$ y la dirección en el ciclo es de v_i a v_j, entonces $x_j = 1$, y como antes tenemos $x_i - x_j - (d-1) = 0$.
4. Si $x_i = 1$ y la dirección en el ciclo es de v_j a v_i, entonces se obtiene el caso anterior intercambiando i y j.

Tenemos pues la relación $(x_i - x_j + 1)(x_i - x_j - (d-1)) = 0$ para cada j tal que $\{i,j\} \in E$ y la dirección en el ciclo es de v_i a v_j. Podemos escribir esta relación $y_i(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0$
Si $\{i,j\} \in E$ y se tiene $y_i = 1$, $y_j = 0$, entonces no nos interesan las relaciones de x_i y x_j. Por tanto, siguiendo con la notación anterior tendremos $y_i(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0$, que es $x_i x_i = 0$, de donde $x_i = 0$, pero esto no es posible!!!!
Si $\{i,j\} \in E$ y se tiene $y_i = 0$, las relaciones de x_i y x_j no nos interesan. Por tanto, siguiendo con la notación anterior tendremos $y_i(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0$, que proporciona $0 = 0$.
Juntando ahora todas estas relaciones tenemos $y_i \prod_{\{i,j\}\in E}(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0$.
De esta forma, como el producto tiene al menos dos factores y algún y_j no nulo, los factores con $y_j = 0$ que dan un factor x_i^2 podemos simplificarlos ya que los x_i son no nulos.
Esto nos da las relaciones:

$$y_i \prod_{\{i,j\}\in E}(x_i - y_j x_j + y_j)(x_i - y_j x_j - y_j(d-1)) = 0\Big\}_{i=1,\dots,s}$$

y por lo tanto tenemos que estudiar las ecuaciones:

$$Y_i \prod_{\{i,j\}\in E}(X_i - Y_j X_j + Y_j)(X_i - Y_j X_j - Y_j(d-1)) = 0\Big\}_{i=1,\dots,s}$$

Como consecuencia si el grafo G tiene un ciclo de longitud d, entonces el siguiente sistema tiene una solución.

$$\begin{array}{l} Y_1 + \cdots + Y_s - d = 0, \\ Y_i(Y_i - 1) = 0\Big\}_{i=1,\dots,s} \\ (X_i - 1)\cdots(X_i - d) = 0\Big\}_{i=1,\dots,s} \\ Y_i \prod_{\{i,j\}\in E}(X_i - Y_j X_j + Y_j)(X_i - Y_j X_j - Y_j(d-1))\Big\}_{i=1,\dots,s} \end{array}$$

A estas ecuaciones podemos agregar otras que se deducen fácilmente de los posibles valores de los y_i y los x_i. Por ejemplo se tiene $y_1 x_1 + \cdots + y_s x_s = 1 + \cdots + d = \frac{d(d+1)}{2}$, y si consideramos x_i^2, entonces se tendrá $y_1 x_1^2 + \cdots + y_s x_s^2 = 1^2 + \cdots + d^2 = \frac{d(d+1)(2d+1)}{6}$; de esta forma, al aumentar el número de ecuaciones podremos resolver más fácilmente el sistema.

Teorema. 60.6.
Dado un grafo $G = (V,E)$ con vértices $V = \{v_1, \dots, v_s\}$ y $d < s$ un entero positivo, son equivalentes:

(a) G contiene un ciclo de longitud d.
(b) El sistema de ecuaciones

$$\begin{array}{l} Y_1+\cdots+Y_s-d=0,\\ Y_i(Y_i-1)=0\big\}_{i=1,\dots,s}\\ (X_i-1)\cdots(X_i-d)=0\big\}_{i=1,\dots,s}\\ Y_i\prod_{\{i,j\}\in E}(X_i-Y_jX_j+Y_j)(X_i-Y_jX_j-Y_j(d-1))\big\}_{i=1,\dots,s}\end{array}$$

tiene una solución.

Según lo anterior, cada solución dará un ciclo de longitud d de G.

Observación: Tenemos que limitar las posibles permutaciones cíclicas de los vértices que conforman el ciclo.

DEMOSTRACIÓN. Sólo es necesario probar que si $x_1,\dots,x_s,y_1,\dots,y_s$ es una solución del sistema, entonces existe un ciclo de longitud d en el grafo.
Consideramos los índices i tales que $y_i\neq 0$; estos son los vértices del ciclo. Vamos a ver que estos vértices forman un ciclo. Para $y_i\neq 0$ tenemos que existe un índice j tal que $y_j\neq 0$ y $x_i-x_j+1=0$ ó $x_i-x_j-(d-1)=0$. En el primer caso $x_j=x_i+1$, y en el segundo $x_i+1=x_j+d$; como $x_i,x_j\in\{1,\dots,d\}$, se tiene $x_i=d$ y $x_j=1$. Ahora un simple razonamiento sobre el principio del palomar prueba que los x_i para los que $y_i\neq 0$ recorren el conjunto $\{1,\dots,d\}$, y tenemos un ciclo. □

En un grafo G un **camino de Hamilton** es un camino que pasa una vez por cada vértice; si el camino de Hamilton es cerrado, entonces se llama un **ciclo de Hamilton**. El resultado que acabamos de probar nos sirve para comprobar si un grafo tiene un ciclo de Hamilton.

Corolario. 60.7.
Dado un grafo $G=(V,E)$ con vértices $V=\{v_1,\dots,v_s\}$, son equivalentes:
(a) G contiene un ciclo de Hamilton.
(b) El sistema de ecuaciones

$$\begin{array}{l} Y_1+\cdots+Y_s-s=0,\\ Y_i(Y_i-1)=0\big\}_{i=1,\dots,s}\\ \textit{(Irrelevantes, ya que todos los } y_i \textit{ valdrán 1)}\\ (X_i-1)\cdots(X_i-s)=0\big\}_{i=1,\dots,s}\\ \prod_{\{i,j\}\in E}(X_i-X_j+1)(Y_i-X_j-(d-1))\big\}_{i=1,\dots,s}\end{array}$$

tiene una solución.

Según lo anterior, cada solución dará un ciclo de Hamilton de G.

Caminos en un grafo

Dado un grafo orientado $G=(V,E)$ con vértices $\{v_1,\dots,v_s\}$, y sin ciclos, y un entero positivo $d\leq s$, estamos interesados en estudiar si G tiene caminos de longitud $d-1$ (d vértices y $d-1$ lados). Para esto consideramos indeterminadas $X_1,\dots,X_s$ e $Y_1,\dots,Y_s$.
Si el grafo contiene un camino de longitud $d-1$ y v_i es un vértice de este camino, consideramos $y_i=1$, en caso contrario escribimos $y_i=0$. Como consecuencia se tienen las relaciones:

$$\begin{array}{l} y_1+\cdots+y_s=d,\\ y_i(y_i-1)=0, \text{ para todo índice } i,\end{array}$$

$$\left.\begin{array}{l} Y_1+\cdots+Y_s-d=0,\\ Y_1(Y_1-1)=0\\ \vdots\\ Y_s(Y_s-1)=0\end{array}\right\}$$

Dado un vértice v_i con $y_i=1$, consideramos $x_i=d-k$, si v_i ocupa el lugar k en el camino. Como consecuencia se tiene $(x_i-(d-1))\cdots(x_i-1)x_i=0$. Tenemos entonces que estudiar las ecuaciones:

$$\begin{array}{l} X_1(X_1-1)\cdots(X_1-(d-1))=0\\ \vdots\\ X_s(X_s-1)\cdots(X_s-(d-1))=0\end{array}$$

Supongamos que v_i ocupa el lugar k en el camino, es decir $x_i=d-k$; otro vértice v_j ocupará el lugar siguiente, $k+1$, y por tanto se tiene $x_j=d-(k+1)$. En cualquier caso, si se tiene $y_j=1$, tenemos que $x_i-x_j-1=0$, si $\{i,j\}\in E$, y de igual manera se cumple que $y_i(x_i-y_jx_j-y_j)=0$ Juntando ahora todas estas relaciones tenemos $y_i\prod_{\{i,j\}\in E}(x_i-y_jx_j-y_j)=0$.
Tenemos, por tanto, que estudiar las ecuaciones:

$$Y_i\prod_{\{i,j\}\in E}(X_i-Y_jX_j-Y_j)=0\Big\}_{i=1,\dots,s}$$

Como consecuencia si el grafo G tiene un camino de longitud $d-1$, entonces el siguiente sistema tiene una solución.

$$\begin{array}{l} Y_1+\cdots+Y_s-d=0,\\ Y_1X_1+\cdots+Y_sX_s-\frac{d(d+1)}{2}=0, \text{ (opcional)}\\ Y_1X_1^2+\cdots+Y_sX_s^2-\frac{d(d+1)(2d+1)}{6}=0, \text{ (opcional)}\\ Y_i(Y_i-1)=0\Big\}_{i=1,\dots,s}\\ X_i(X_i-1)\cdots(X_i-(d-1))=0\Big\}_{i=1,\dots,s}\\ Y_i\prod_{\{i,j\}\in E}(X_i-Y_jX_j+Y_j)=0\Big\}_{i=1,\dots,s}\end{array}$$

Observa que no consideramos ciclos, pues no tenemos contemplada la posibilidad de asignar dos valores distintos a la variable X_i.

Teorema. 60.8.
Dado un grafo $G=(V,E)$ con vértices $V=\{v_1,\dots,v_s\}$, y sin ciclos, y $d\leq s$ un entero positivo, son equivalentes:

(a) G contiene un camino de longitud $d-1$.
(b) El sistema de ecuaciones

$$\begin{aligned}
&Y_1+\cdots+Y_s-d=0,\\
&Y_1X_1+\cdots+Y_sX_s-\frac{d(d+1)}{2}=0,\ \textit{(opcional)}\\
&Y_1X_1^2+\cdots+Y_sX_s^2-\frac{d(d+1)(2d+1)}{6}=0,\ \textit{(opcional)}\\
&Y_i(Y_i-1)=0\}_{i=1,\dots,s}\\
&X_i(X_i-1)\cdots(X_i-(d-1))=0\}_{i=1,\dots,s}\\
&Y_i\textstyle\prod_{\{i,j\}\in E}(X_i-Y_jX_j+Y_j)=0\}_{i=1,\dots,s}
\end{aligned}$$

tiene una solución.

Según lo anterior, cada solución dará un camino de longitud $d-1$ de G.

Actividades

Ejercicio. 60.9. (Sudoku 4×4)
Estudiar la resolución de un sudoku 4×4, considerando coeficientes en los diferentes cuerpos que hemos tratado: $\mathbb{C}$, $\mathbb{F}_5$ y $\mathbb{F}_4$.
Ref.: 1132e_011 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (60.9.)
HACER □

Tarea a realizar para la evaluación es:

Ejercicio. 60.10. (Sudoku 9×9)
Estudiar la resolución de un sudoku 9×9, considerando coeficientes en los cuerpos $\mathbb{C}$ y $\mathbb{F}_9$.
Ref.: 1132e_012 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (60.10.)
HACER □

En general trabajar en el cuerpo $\mathbb{F}_9$ es muy complicado, sobre todo a la hora de obtener una solución del sistema final; por esta razón vamos a considerar una pequeña variación. Vamos a suponer que los colores a utilizar son los elementos de un grupo de orden 9, sea éste C_9, y vamos a suponer que C_9 está incluido en el grupo multiplicativo de un cuerpo de $\mathbb{F}_p$, con p primo, entonces $9\,|\,p-1$, y por tanto p es de la forma $9k+1$. Podremos trabajar pues en un cuerpo de 19 elementos en vez de en $\mathbb{F}_9$. La ventaja es que la resolución del sistema es más sencilla, y la dificultad es que trabajamos módulo 19 en vez de hacerlo módulo 3. En el caso de $\mathbb{F}_{19}$ el único subgrupo cíclico de orden 9 es: $\{1,4,16,7,9,17,11,6,5\}$. Tenemos pues que establecer una diccionario que permita pasar del conjunto $\{1,2,\ldots,9\}$ al conjunto $\{1,4,16,7,9,17,11,6,5\}$ para codificar adecuadamente los datos del sudoku.

Ejercicio. 60.11. (Sudoku 9×9)
Estudiar la resolución de un sudoku 9×9, considerando coeficientes en el cuerpo $\mathbb{F}_{19}$.
Ref.: 1132e_013 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (60.11.)
HACER □

61. Demostración de teoremas geométricos

La demostración de teoremas de la geometría del plano es posible, haciendo uso de la Geometría Algebraica, traduciéndolos a problemas algebraicos sobre anillos de polinomios. Vamos a ver que en algunos casos un problema geométrico dado se puede interpretar algebraicamente mediante el estudio de un sistema de ecuaciones, o más generalmente, de un ideal de un anillo de polinomios, en un número finito de indeterminadas, con coeficientes en un cuerpo. En particular veremos que determinadas construcciones son imposibles al probar que el correspondiente ideal no tiene ceros.

Trabajamos en un anillo de polinomios $K[X_1,\dots,X_n]$ en las indeterminadas $X_1,\dots,X_n$, que en el caso de problemas en el plano se tomará $n=2$, con coeficientes en un cuerpo, que en nuestro caso será $\mathbb{R}$ ó $\mathbb{C}$, y que ampliaremos con más indeterminadas para expresar las relaciones que se cumplen en el teorema a estudiar. Sobre este tipo de anillos los resultados que necesitamos son:

Teorema de la base de Hilbert. *Todo ideal de $K[X_1,\dots,X_n]$ tiene un número finito de generadores.*

Teorema de los Ceros de Hilbert. *Si $\overline{K}$ es un cuerpo algebraicamente cerrado, conteniendo a K, (por ejemplo, si $K=\mathbb{R}$ podemos tomar $\overline{K}=\mathbb{C}$), y $F_1,\dots,F_s\in K[X_1,\dots,X_n]$, entonces los polinomios $F_1,\dots,F_s$ no tienen un cero en común en $\mathbb{A}^n(\overline{K})$ si, y sólo si, existen polinomios $P_1,\dots,P_s\in K[X_1,\dots,X_n]$ tales que $1=P_1F_1+\cdots+P_sF_s$.*

Veamos cómo utilizar estos hechos en el estudio de los ceros de los polinomios de un ideal.

Un ideal $\mathfrak{a}\in\mathbb{C}[X_1,\dots,X_n]$ tiene ceros si, y sólo si, $\mathfrak{a}\neq\mathbb{C}[X_1,\dots,X_n]$. En consecuencia, son equivalentes:

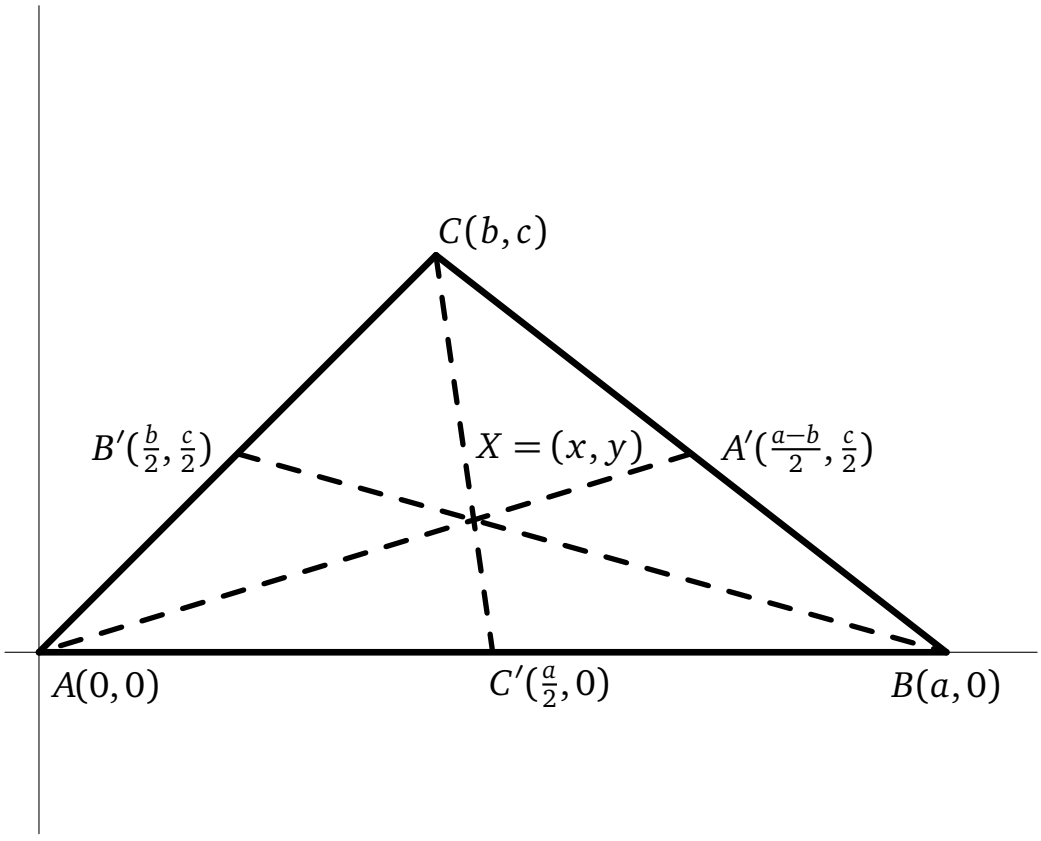
(a) $\mathfrak{a}$ no tiene ceros.
(b) $\mathfrak{a}=\mathbb{C}[X_1,\dots,X_n]$.
(c) $1\in\mathbb{G}$, una base de Groebner reducida de $\mathfrak{a}$.

1132-05.tex

Vamos a probar, mediante el uso de anillos de polinomios, que las medianas de cualquier triángulo se cortan en un punto: **el baricentro**.

Ejercicio. 61.1.
Prueba que las tres medianas de un triángulo se cortan en un punto: el baricentro.
Ref.: 1132e_014 SOLUCIÓN

SOLUCIÓN. Ejercicio (61.1.)
Consideramos un triángulo arbitrario, del que suponemos que uno de sus vértices ocupa el origen, y uno de sus lados está situado sobre el eje de abscisas (el eje X). Ésta es la situación de la figura siguiente, en la que hemos señalados los puntos medios de los lados.



Las rectas que determinan AA', BB' y CC' las llamaremos, respectivamente r, s y t; sus ecuaciones son:

$$\begin{cases} r: cX-(a-b)Y=0 \\ s: c(X-a)+(2a-b)Y-ca=0 \\ t: c(2X-a)+(a-2b)Y=0 \end{cases}$$

La intersección de las rectas r y s es un punto X de coordenadas (x, y). Queremos ver que este punto siempre verifica la ecuación que define t. Si éste no es el caso, se tendría $2cx+(a-2b)y-ca \neq 0$, y por tanto existe un número real z tal que $z(2cx+(a-2b)y-ca)=1$. En consecuencia se tienen las relaciones:

$$\left.\begin{array}{l} cx-(a+b)y=0 \\ cx+(2a-b)y-ca=0 \\ z(2cx+(a-2b)y-ca)-1=0 \end{array}\right\}$$

En el desarrollo realizado, si $2cx+(a-2b)y-ca \neq 0$, entonces este sistema de ecuaciones tendría solución; pero resulta que este sistema define un ideal generado por $\{cX-(a+b)Y, cX+(2a-b)Y-ca, Z(2cX+(a-2b)Y-ca)-1\}$,y cuya base de Groebner reducida

$$> \mathbf{GroebnerBasis}[\{\mathbf{cX-(a+b)Y}, \mathbf{cX+(2a-b)Y-ca}, \mathbf{Z(2cX+(a-2b)Y-ca)-1}\}, \{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}]$$

es igual a $\{1\}$, lo que es una contradicción. En consecuencia $2cx+(a-2b)y-ca$ debe ser siempre cero, y las tres rectas se cortan en un punto. □

Nota. En este caso también podríamos haber resuelto el sistema

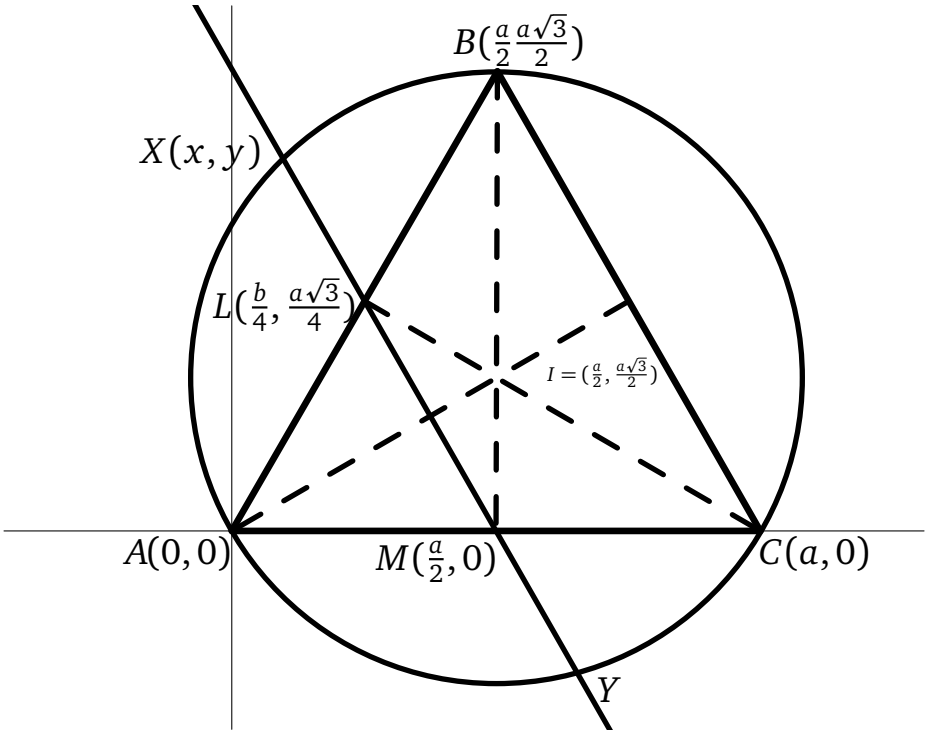
$$\left.\begin{array}{l} cX-(a+b)Y=0 \\ cX+(2a-b)Y-ca=0 \\ 2cX+(a-2b)Y-ca=0 \end{array}\right\}$$

cuya solución es: $(\frac{a+b}{3}, \frac{c}{3})$, y que nos da las coordenadas del punto de corte de las tres medianas: el **baricentro**. Sin embargo el método propuesto nos permite obtener el resultado sin necesidad de calcular los elementos particulares: en este caso el punto X.

Un segundo ejemplo del uso de los métodos computacionales en la demostración de teoremas geométricos es el siguiente:

Ejercicio. 61.2.
Sea ΔABC un triángulo equilátero. Se traza su circunferencia circunscrita. Sean L y M los puntos medios de AB y AC. La recta LM corta a la circunferencia en los puntos X e Y. Prueba que se verifica la relación $\frac{XM}{LM} = \phi$, donde ϕ es la razón áurea.
Ref.: 1132e_015 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (61.2.)



Primero determinamos la recta que contiene a $L = (\frac{a}{4}, \frac{a\sqrt{3}}{4})$ y a $M = (\frac{a}{2}, 0)$:

> **Expand**[$\sqrt{3}$**a**/4((**x**−(**a**/4))/(**a**/2−**a**/4)−(**y**−$\sqrt{3}$**a**/4)/(−$\sqrt{3}$**a**/4))]

El resultado es: $y + \sqrt{3}x - \frac{a\sqrt{3}}{2}$.
A continuación determinamos la circunferencia que circunscribe al triángulo:

> **Expand**[4$\sqrt{3}$((**x**−**a**/2)^2+(**y**−$\sqrt{3}$**a**/6)^2−((**a**/2)^2+($\sqrt{3}$**a**/6)^2))]

El resultado es: $4\sqrt{3}x^2-4a\sqrt{3}x+4\sqrt{3}y^2-4ay$.
Si $\frac{XM}{ML}$ es el número de oro, entonces este número deber igual a $\frac{ML}{LX}$, ya que se tiene:

$$\frac{XM}{ML}=\frac{a}{b}=\frac{b}{a+b}=\frac{ML}{XL};$$

la solución de $\frac{a}{b}=\frac{b}{a+b}$ se obtiene de $a(a+b)=b^2$, esto es, $a^2+ab=b^2$, y por tanto $(\frac{a}{b})^2+\frac{a}{b}=1$. La solución es el número de oro.
Si suponemos que no es cierto, tenemos: $XM\cdot XL\neq ML^2$, y por lo tanto el número $XM^2\cdot XL^2-(ML^2)^2$ es invertible.
Tenemos:

$$\begin{aligned}XM^2&=(x-\tfrac{a}{2})^2+y^2\\ML^2&=(\tfrac{a}{2}-\tfrac{a}{4})^2+(\tfrac{-a\sqrt{3}}{4})^2\\XL^2&=(x-\tfrac{a}{4})^2+(y-\tfrac{a\sqrt{3}}{4})^2\end{aligned}$$

Entonces tenemos una relación:

$$z(XM^2XL^2-(ML^2)^2)-1$$

Al determinar la base de Groebner del ideal generado por

$$\{y+\sqrt{3}x-\frac{a\sqrt{3}}{2},4\sqrt{3}x^2-4a\sqrt{3}x+4\sqrt{3}y^2-4ay,z(XM^2XL^2-(ML^2)^2)-1\},$$

que es justamente el ideal

$$\{y+\sqrt{3}x-\frac{a\sqrt{3}}{2},4\sqrt{3}x^2-4a\sqrt{3}x+4\sqrt{3}y^2-4ay,$$
$$z(((x-\frac{a}{2})^2+y^2)^2((x-\frac{a}{4})^2+(y-\frac{a\sqrt{3}}{4})^2)^2-(((\frac{a}{2}-\frac{a}{4})^2+(-\frac{a\sqrt{3}}{4})^2)^2)^2)-1\}.$$

La base de Groebner es $\{1\}$. Por lo tanto el cociente $\frac{XM}{ML}$ es el número de oro.

```
> GroebnerBasis[{-((√3a)/2) + √3x + y, -4√3ax + 4√3x^2 - 4ay + 4√3y^2,
   z(((x - a/2)^2 + y^2)^2((x - a/4)^2 + (y - a√3/4)^2)^2 - (((a/2 - a/4)^2 + (-a√3/4)^2)^2)^2) - 1},
                                                          {x, y, z, a}]
```

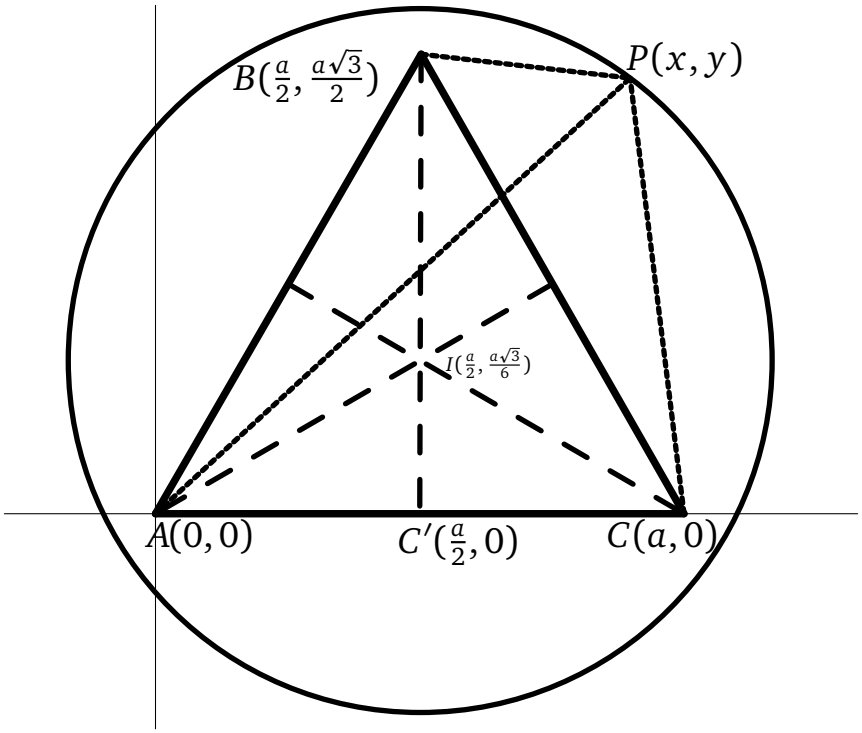
□

Ejercicio. 61.3.
Sea ΔABC un triángulo equilátero de lado a, y consideremos una circunferencia de centro el incentro de ABC y radio arbitrario r. Si P un punto cualquiera de la circunferencia, prueba que

$$PA^2 + PB^2 + PC^2 = a^2 + 3r^2.$$

Ref.: 1132e_016 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (61.3.)



Como el triángulo es equilátero, si uno de los vértices es el origen y otro descansa sobre el eje x, entonces las coordenadas de los puntos son sencillas de utilizar. El incentro, punto en el que se cortan las tres bisectrices coincide con el baricentro, y tiene coordenadas $(\frac{a}{2}, \frac{a\sqrt{3}}{6})$.

La ecuación de la circunferencia de centro $I = (\frac{a}{2}, \frac{a\sqrt{3}}{6})$ y radio r es:

$$\left(x - \frac{a}{2}\right)^2 + \left(y - \frac{a\sqrt{3}}{6}\right)^2 - r^2 = 0.$$

Vamos a determinar los valores de PA^2, PB^2, y PC^2.

$$\begin{cases} PA^2 = x^2 + y^2, \\ PB^2 = \left(x - \frac{a}{2}\right)^2 + \left(y - \frac{a\sqrt{3}}{2}\right)^2, \\ PC^2 = (x-a)^2 + y^2. \end{cases}$$

Tenemos que probar que se verifica

$$PA^2 + PB^2 + PC^2 - (a^2 + 3r^2) = 0;$$

Particularizando a este caso tenemos:

$$x^2 + y^2 + \left(x - \frac{a}{2}\right)^2 + \left(y - \frac{a\sqrt{3}}{2}\right)^2 + (x-a)^2 + y^2 - a^2 - 3r^2 = 0.$$

Si no es cierta esta relación tendremos un número no nulo, que debe tener un inverso w que verificará:

$$w\left(x^2 + y^2 + \left(x - \frac{a}{2}\right)^2 + \left(y - \frac{a\sqrt{3}}{2}\right)^2 + (x-a)^2 + y^2 - a^2 - 3r^2\right) - 1 = 0.$$

Tenemos que estudiar el ideal generado por los elementos:

$$\left(x - \frac{a}{2}\right)^2 + \left(y - \frac{a\sqrt{3}}{6}\right)^2 - r^2 \quad \text{y}$$

$$w\left(x^2 + y^2 + \left(x - \frac{a}{2}\right)^2 + \left(y - \frac{a\sqrt{3}}{2}\right)^2 + (x-a)^2 + y^2 - a^2 - 3r^2\right) - 1$$

en el anillo de polinomios $K[x, y, w, a, r]$.La base de Groebner reducida se obtiene mediante:

$>$ **GroebnerBasis**[{$\mathbf{(x-a/2)^2 + (y-a\sqrt{3}/6)^2 - r^2}$,
$\mathbf{w(x^2 + y^2 + (x-a/2)^2 + (y-a\sqrt{3}/2)^2 + (x-a)^2 + y^2 - a^2 - 3r^2) - 1}$}, {$\mathbf{x, y, w, a, r}$}]

y el resultado es: {1}. En consecuencia la relación es cierta. □

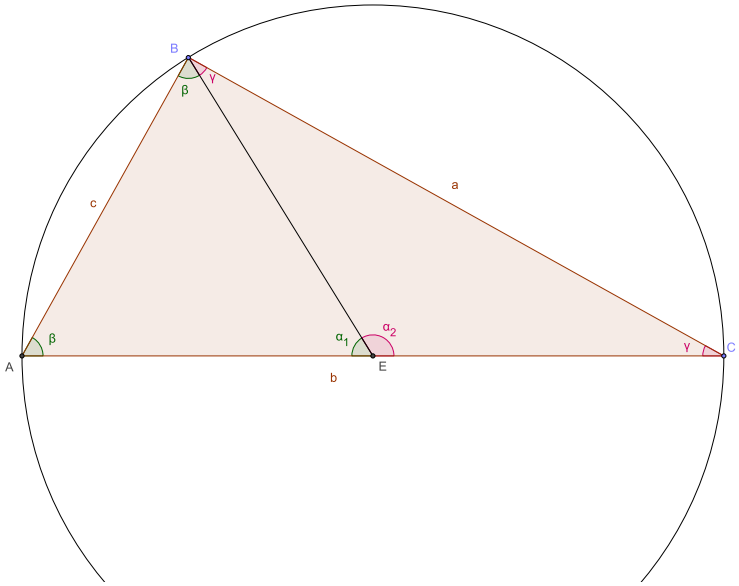
Actividades

Ejercicio. 61.4.
Dado un triángulo ΔABC, siendo AC el lado mayor, prueba que son equivalentes:

(a) ΔABC es un triángulo rectángulo con ángulo recto $\widetilde{B}$.
(b) AC es un diámetro de la circunferencia circunscrita.

Ref.: 1132e_019 *SOLUCIÓN*

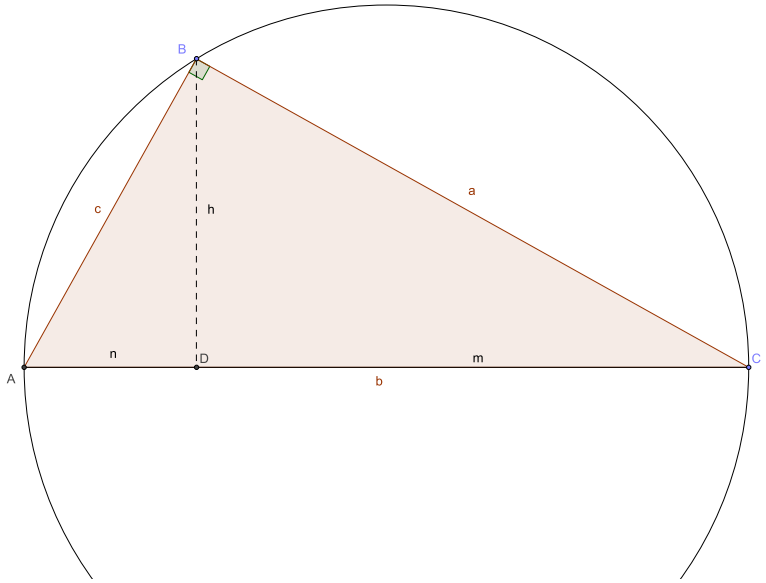
SOLUCIÓN. Ejercicio (61.4.)
Basta observar la siguiente figura:



y utilizar que los tres ángulos (interiores) de un triángulo suman 180^o. □

Ejercicio. 61.5.
Dado un triángulo rectángulo ΔABC con hipotenusa AC, si la altura h divide a ésta en dos segmentos n y m, prueba que se verifica $h^2 = n \times m$.
Ref.: 1132e_020 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (61.5.)
Consideramos la siguiente figura:



Supongamos que el punto A tiene coordenadas $(0,0)$, el punto B tiene coordenadas (n,h), y el punto C tiene coordenadas $(b,0)$, siendo $b = n+m$. Como el triángulo ABC es un triángulo rectángulo con hipotenusa AC, entonces B es un punto de la circunferencia circunscrita, que tiene centro en el punto medio de AC; sus coordenadas son $(\frac{b}{a},0)$, y la ecuación de la circunferencia circunscrita es $(X-\frac{b}{2})^2+Y^2=\left(\frac{b}{2}\right)^2$, entonces se verifica la relación $(n-\frac{b}{2})^2+h^2=\left(\frac{b}{2}\right)^2$.Si no se verifica $h^2 = n\times m$, entonces existe w tal que $w(h^2-nm)-1=0$.En resumen, tenemos las relaciones

$$\left.\begin{array}{r} n+m-b=0 \\ (n-\frac{b}{2})^2+h^2-\left(\frac{b}{2}\right)^2=0 \\ w(h^2-nm)-1=0 \end{array}\right\}$$

Observa que b es un dato del problema; el resto de variables: n,m,h,w, dependen del punto elegido y de la relación $h^2-nm\neq 0$. Al considerar el ideal generado por el conjunto de polinomios

$$\{n+m-b,(n-\frac{b}{2})^2+h^2-\left(\frac{b}{2}\right)^2,w(h^2-nm)-1\},$$

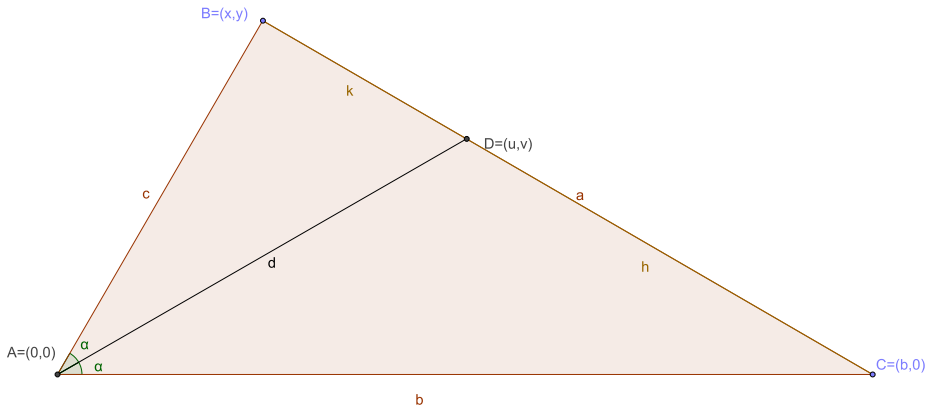
su base de Groebner es $\{1\}$.

$$> \textbf{GroebnerBasis}[\{n+m-b,(n-b/2)^2+h^2-(b/2)^2,w(h^2-nm)-1\},\{n,m,b,h,w\}]$$

En consecuencia no existen soluciones del sistema, lo que es una contradicción, salvo que $h^2-nm=0$, que es justamente lo que queremos probar. □

Ejercicio. 61.6.
Prueba que en todo triángulo ABC, la bisectriz del ángulo $\widetilde{A}$ (ángulo interior) divide al lado BC en dos segmentos que son directamente proporcionales a los otros dos lados.
Ref.: 1132e_000 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (61.6.)
De cara a simplifica los cálculos, suponemos que el triángulo es tal y como aparece en la figura.



El punto $D=(u,v)$ pertenece al segmento BC, por lo tanto tenemos la relación $\frac{u-b}{v-0}=\frac{x-b}{y-0}$, esto es, $y(u-b)=v(x-b)$.
Utilizamos las relaciones del seno y del coseno del ángulo $\widetilde{A}=2\alpha$ y del ángulo α. Tenemos las siguientes relaciones obtenidas directamente de la figura:

$$\left.\begin{array}{ll}\cos(2\alpha)=\frac{x}{c}, & \operatorname{sen}(2\alpha)=\frac{y}{c},\\ \cos(\alpha)=\frac{u}{d}, & \operatorname{sen}(\alpha)=\frac{v}{d},\\ c^2=x^2+y^2, & d^2=u^2+v^2.\end{array}\right\}$$

Por otro lado existen relaciones entre el seno y el coseno de los ángulos doble y mitad; en nuestro caso éstas son:

$$\left.\begin{array}{l}\cos(2\alpha)=\cos^2(\alpha)-\operatorname{sen}^2(\alpha),\\ \operatorname{sen}(2\alpha)=2\operatorname{sen}(\alpha)\cos(\alpha).\end{array}\right\}$$

Tenemos que sen y cos verifican la siguiente relación que nos permite relacionar uno con otro:

$$\text{sen}^2(\alpha)+\cos^2(\alpha)=1, \text{ para cada ángulo } \alpha.$$

Para facilitar los cálculos vamos a escribir simplemente

$$\cos(\alpha)=C_1,\ \text{sen}(\alpha)=S_1,\ \cos(2\alpha)=C_2,\ \text{sen}(2\alpha)=S_2.$$

Reuniendo todas las relaciones tenemos:

$$\left.\begin{array}{l} y(u-b)-v(x-b)=0\\ C_2-\frac{x}{c}=0\\ S_2-\frac{y}{c}=0\\ C_1-\frac{u}{d}=0\\ S_1-\frac{v}{d}=0\\ c^2-x^2-y^2=0\\ d^2-u^2-v^2=0\\ C_2-C_1^2+S_1^2=0\\ S_2-2S_1C_1=0\\ S_2^2+C_2^2-1=0\\ S_1^2+C_1^2-1=0 \end{array}\right\}$$

Ahora hacemos intervenir los segmentos h y k. Queremos probar que $\frac{k}{c}=\frac{h}{b}$, esto es, $kb=hc$. Si esta relación no se cumple, existe w tal que $w(kb-hc)=1$. En términos de las coordenadas de B, D y C se verifica:

$$\left.\begin{array}{l} k^2=(x-u)^2+(y-v)^2\\ h^2=(u-b)^2+v^2\\ (k+h)^2=a^2=(x-b)^2+y^2 \end{array}\right\}$$

Todas estas relaciones

$$\left.\begin{array}{l} w(kb-hc)-1=0\\ k^2-(x-u)^2-(y-v)^2=0\\ h^2-(u-b)^2-v^2=0\\ (k+h)^2-(x-b)^2-y^2=0 \end{array}\right\}$$

también debemos agregarlas a la lista anterior. Ahora queda por estudiar el ideal generado por todos

estos polinomios.

$$\left.\begin{aligned} y(u-b)-v(x-b),\\ cC_2-x,\\ cS_2-y,\\ dC_1-u,\\ dS_1-v,\\ c^2-x^2-y^2,\\ d^2-u^2-v^2,\\ C_2-C_1^2+S_1^2,\\ S_2-2S_1C_1,\\ S_2^2+C_2^2-1,\\ S_1^2+C_1^2-1,\\ w(kb-hc)-1,\\ k^2-(x-u)^2-(y-v)^2,\\ h^2-(u-b)^2-v^2,\\ (k+h)^2-(x-b)^2-y^2. \end{aligned}\right\}$$

Calculamos una base de Groebner del ideal:

$$\begin{aligned} &> \textbf{GroebnerBasis}[\{y(u-b)-v(x-b), cC2-x, cS2-y, dC1-u, dS1-v, c^2-x^2-y^2,\\ &\quad d^2-u^2-v^2, C2-C1^2+S1^2, S2-2S1C1, S2^2+C2^2-1, S1^2+C1^2-1, w(kb-hc)-1,\\ &\quad k^2-(x-u)^2-(y-v)^2, h^2-(u-b)^2-v^2, (k+h)^2-(x-b)^2-y^2\},\\ &\quad \{h,k,x,y,u,v,w,C1,C2,S2,S1,b,c,d\}] \end{aligned}$$

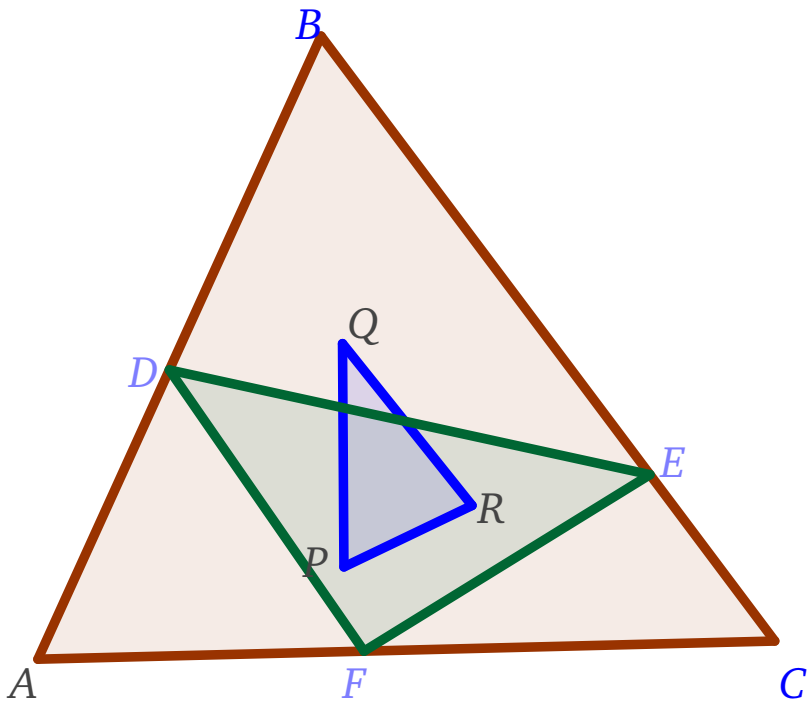
El resultado contiene $-1+\cos(2\alpha)$, luego $\cos(2\alpha)=1$, y por tanto $2\alpha=0$. Esto significa que $B=D=C$, y el triángulo degenera. Podemos imponer pues la condición $C_2-1\neq 0$, y por tanto debemos incluir la relación $t(C_2-1)-1$. Al hacerlo la base de Groebner es:

$$\begin{aligned} &> \textbf{GroebnerBasis}[\{y(u-b)-v(x-b), cC2-x, cS2-y, dC1-u, dS1-v, c^2-x^2-y^2,\\ &\quad d^2-u^2-v^2, C2-C1^2+S1^2, S2-2S1C1, S2^2+C2^2-1, S1^2+C1^2-1, w(kb-hc)-1,\\ &\quad k^2-(x-u)^2-(y-v)^2, h^2-(u-b)^2-v^2, (k+h)^2-(x-b)^2-y^2, t(C2-1)-1\},\\ &\quad \{h,k,x,y,u,v,w,C1,C2,S2,S1,b,c,d,t\}] \end{aligned}$$

que da como resultado $\{1\}$, lo que prueba que salvo el caso degenerado, $2\alpha=0$, no existe solución. Por tanto la hipótesis $\frac{k}{c}=\frac{h}{b}$ es correcta. □

Ejercicio de la Olimpíada Matemática Española del Enero de 2014.

Ejercicio. 61.7.
Sea ABC un triángulo y D, E y F tres puntos cualesquiera sobre los lados AB, BC y CA respectivamente. Llamemos P al punto medio de AE, Q al punto medio de BF y R al punto medio de CD. Probar que el área del triángulo PQR es la cuarta parte del área del triángulo DEF.
Ref.: 1132e_022 SOLUCIÓN

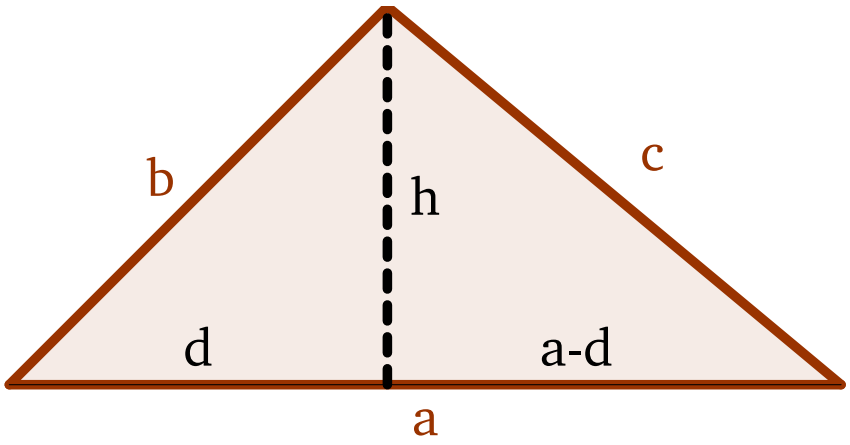


SOLUCIÓN. Ejercicio (61.7.)
HACER □

Ejercicios

Ejercicio. 61.8. (Fórmula de Heron)
Si T es un triángulo de lados a, b, c, prueba que su área es $A = \sqrt{p(p-a)(p-b)(p-c)}$, donde p es el semiperímetro de T, esto es, $p = \frac{a+b+c}{2}$.
Ref.: 1132e_001 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (61.8.)
Consideramos la siguiente situación:



Para probar que $A = \sqrt{p(p-a)(p-b)(p-c)}$, basta probar que $4A^2 = 4p(p-a)(p-b)(p-c)$.
Estudiamos cada uno de los miembros.
Tenemos: $4A^2 = (ah)^2 = a^2h^2 = a^2(b^2-d^2) = (ab)^2 - (ad)^2$.
Por otro lado se tiene:

$$4p(p-a)(p-b)(p-c) = (p(p-c)+(p-b)(p-a))^2 - (p(p-c)-(p-b)(p-a))^2 .$$

Además,

$$p(p-c)+(p-b)(p-a) = 2p^2 - p(a+b+c) + ab = ab.$$

$$\begin{aligned} p(p-c)-(p-b)(p-a) &= p(a+b-c)-ab = \frac{1}{2}(a+b+c)(a+b-c)-ab \\ &= \frac{1}{2}(a^2+b^2-c^2) = \frac{1}{2}(a^2+b^2+h^2-c^2) = \frac{1}{2}(a^2+d^2-(a.d)^2) = ad. \end{aligned}$$

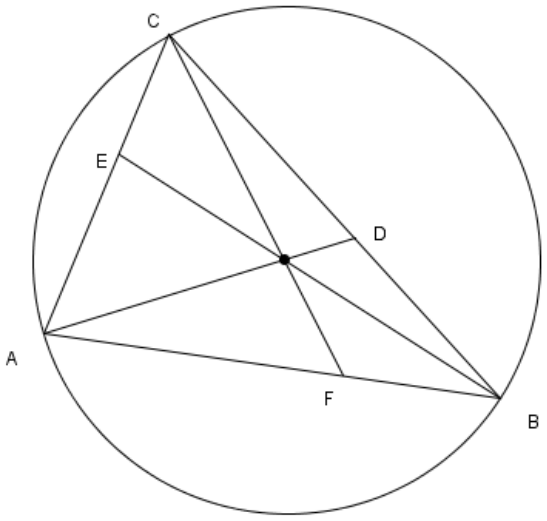
Como consecuencia $4p(p-a)(p-b)(p-c) = (ab)^2 - (ad)^2$. □

Ejercicio. 61.9.
Se considera un triángulo ABC, y puntos D, E y F sobre los lados BC, AC y AB, respectivamente. Demuestra que si los segmentos AD, BE y CF pasan por el centro O de la circunferencia circunscrita al triángulo, y si el radio de ésta es R, entonces se verifica:

$$\frac{1}{AD}+\frac{1}{BE}+\frac{1}{CF}=\frac{2}{R}.$$

Ref.: 1132e_002 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (61.9.)
Considera la siguiente figura



□

62. Ideales de Fermat

Este es un ejemplo del uso de las bases de Groebner en el estudio de ideales de anillos de polinomios. Consideramos el último teorema de Fermat, recordemos que afirma que el polinomio $X^n + Y^n - Z^n$ no tiene soluciones entras no nulas si $n > 2$. Podemos considerar los polinomios $F_n = X^n + Y^n - Z^n$ y el ideal $\mathfrak{a}$ generado por $\{F_n \mid n \geq 1\}$.
Si $K = \mathbb{Q}$, como $K[X,Y,Z]$ es un anillo noetheriano, resulta que $\mathfrak{a}$ es finitamente generado, cabe preguntarse cuál es el menor conjunto de $\{F_n \mid n \leq t\}$ que es un sistema de generadores. Es claro que este conjunto tiene que contener a F_1 y a F_2, ya que no podemos generar ninguno de ellos a partir de los restantes. Recordemos que

$$\begin{aligned} F_1 &= X + Y - Z, \\ F_2 &= X^2 + Y^2 - Z^2, \end{aligned}$$

No ocurre lo mismo con F_3 ó F_4. En efecto, una base de Groebner de $\mathfrak{b} = \langle F_1, F_2 \rangle$ es:

$$\{X + Y - Z, Y^2 - YZ\}.$$

Es claro que

$$Y^2 - YZ = \frac{1}{2}(F_2 - XF_1 + YF_1 - ZF_1) = \frac{1}{2}(F_1(-X + Y - Z) + F_2).$$

Y se tiene

$$\begin{aligned} F_3 &= (X + Y - Z)(X^2 - XY + XZ - YZ + Z^2) + (Y^2 - YZ)(X + Y + 2Z) \\ F_4 &= (X + Y - Z)(X^3 - X^2Y + X^2Z - XYZ + XZ^2 - YZ^2 + Z^3) \\ &\quad + (Y^2 - YZ)(X^2 + Y^2 + XZ + YZ + 2Z^2) \end{aligned}$$

Estamos interesados en obtener una expresión más sencilla de cada F_n en función de F_i con $i < n$. A este respecto tenemos:

$$\begin{aligned} F_3 &= (X^2 - XY + XZ + Y^2 - 2YZ + Z^2)F_1 + 3Z(Y^2 - YZ) \\ F_4 &= (XYZ)F_1 - (XY + XZ + YZ)F_2 + (X + Y + Z)F_3. \end{aligned}$$

También tenemos

$$F_5 = (XYZ)F_2 - (XY + XZ + YZ)F_3 + (X + Y + Z)F_4.$$

Y en general

$$F_{n+3} = (XYZ)F_n - (XY + XZ + YZ)F_{n+1} + (X + Y + Z)F_{n+2}.$$

```
F[n_] := X^n + Y^n - Z^n;

Expand[F[n+3]-(X+Y+Z)F[n+2]+(X Y+X Z+Y Z)F[n+1]-(X Y Z)F[n]]
```

Como consecuencia tenemos el siguiente resultado:

1132-04.tex

Lema. 62.1.
El ideal $\mathfrak{a}$ está generado por $\{F_1, F_2\}$, y para cada $n \geq 1$ se tiene $F_{n+3} = (XYZ)F_n - (XY + XZ + YZ)F_{n+1} + (X + Y + Z)F_{n+2}$.

Ejercicio. 62.2.
Llamamos $\mathfrak{a}$ al ideal de Fermat, esto es, el ideal de $\mathbb{Q}[X, Y, Z]$, generado por los polinomios $\{F_n = X^n + Y^n - Z^n \mid n \geq 1\}$.

(1) Razona la siguiente cuestión. El ideal $\mathfrak{a}$ es finitamente generado, y por lo tanto existe un entero positivo t tal que $\mathfrak{a} = (F_1, F_2, \ldots, F_t)$.
(2) Determina una base de Groebner del ideal $\mathfrak{a}_2 = (F_1, F_2)$.
(3) Expresa F_3 y F_4 en función de esta base.
(4) Prueba, por inducción sobre n, que para cada $n \geq 1$ se tiene $F_{n+3} = (X + Y + Z)F_{n+2} - (XY + XZ + YZ)F_{n+1} + XYZF_n$.

Ref.: 1132e_017 SOLUCIÓN

SOLUCIÓN. Ejercicio (62.2.)
HACER □

Ejercicio. 62.3.
*Prueba el **Teorema de Pappus** utilizando bases de Groebner.*
El teorema de Pappus dice: "dadas dos rectas r y r', puntos A, B, C en r, y A', B', C' en r', siendo B y B' puntos intermedios, si definimos

$$Q = AB' \cap BA', \quad R = BC' \cap CA', \quad S = BC' \cap CB',$$

entonces los puntos Q, R y S están alineados".
Ref.: 1132e_018 SOLUCIÓN

SOLUCIÓN. Ejercicio (62.3.)
HACER □

63. Resultante

Dado un cuerpo K y dos polinomios $F, G \in K[X]$, vamos a estudiar cuando F y G tienen una raíz común en alguna extensión E/K. Si $\alpha \in E$ es una raíz común de F y G, entonces $F(\alpha) = 0 = G(\alpha)$, y por la identidad de Bezout el máximo común divisor D de F y G se escribe como $D = UF + VG$, luego $D(\alpha) = 0$, y por tanto D no es constante.
Tenemos entonces el siguiente resultado:

Proposición. 63.1.
Si K es un cuerpo y $F, G \in K[X]$, entonces F y G tienen una raíz común en una extensión E/K si, y sólo si, $D = \mathrm{mcd}\{F, G\} \neq 1$.

DEMOSTRACIÓN. Solo tenemos que probar que la condición es suficiente. Si D no es constante, existe una extensión E/K en la que D tiene una raíz, y por lo tanto F y G tienen una raíz común en E. □

Veamos otra condición equivalente.

Proposición. 63.2.
Sea K un cuerpo y $F, G \in K[X]$, entonces F y G tienen una raíz en una extensión E/K si, y sólo si, existen $0 \neq A, B \in K[X]$ tales que $\mathrm{gr}(A) < \mathrm{gr}(G)$, $\mathrm{gr}(B) < \mathrm{gr}(F)$ y $AF - BG = 0$.

DEMOSTRACIÓN. ($\Rightarrow$). Como $D = \mathrm{mcd}\{F, G\}$ es no constante, existen A y B tales que $F = BD$ y $G = AD$. Podemos suponer que $\mathrm{gr}(A) < \mathrm{gr}(G)$ y $\mathrm{gr}(B) < \mathrm{gr}(F)$, entonces se tiene la relación: $AF = ABD = BG$.
($\Leftarrow$). De la relación $AF = BG$, si $F = P_1^{e_1} \dots P_t^{e_t}$ es la factorización en irreducibles de F, por ser $\mathrm{gr}(B) < \mathrm{gr}(F)$ se tiene que algún P_i divide a G y $D = \mathrm{mcd}\{F, G\}$ no es constante. □

Si suponemos que

$$F = a_0 + a_1 X + \cdots + a_n X^n$$
$$G = b_0 + b_1 X + \cdots + b_m X^m,$$

son polinomios en $K[X]$, con a_n y b_m no nulos, la relación $AF - BG = 0$ es equivalente a que los elementos

$$F, XF, \dots, X^{m-1}F, G, XG, \dots, X^{n-1}G.$$

1132-03.tex

son linealmente dependientes, y por tanto el determinante

$$\mathrm{Res}(F,G)=\begin{vmatrix} a_0 & a_1 & \cdots\cdots & a_n & \cdots\cdots & \\ 0 & a_0 & a_2 & \cdots\cdots & a_n & \cdots\cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & a_0 & a_2 & \cdots\cdots & a_n \\ b_0 & b_1 & \cdots\cdots & b_m & \cdots\cdots & \\ 0 & b_0 & b_2 & \cdots\cdots & b_m & \cdots\cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & b_0 & b_2 & \cdots\cdots & b_m \end{vmatrix}$$

es igual a cero. El determinante $\mathrm{Res}(F,G)$ se llama la **resultante** de F y G.

Aplicación

Sean $F,G\in K[X,Y]$; al considerar $F,G\in K(Y)[X]$ tenemos que la resultante $\mathrm{Res}(F,G)$ es un polinomio en Y.

El siguiente resultado nos proporciona un método para calcular las soluciones comunes a $F=0$ y $G=0$.

Proposición. 63.3.
Las raíces de $\mathrm{Res}(F,G)=0$ *(en una extensión* E/K*) son:*
(1) las raíces comunes de $a_n(Y)$ *y* $b_m(Y)$ *ó*
(2) las coordenadas y *de las soluciones del sistema* $\{F=0,G=0\}$.

DEMOSTRACIÓN. Sea $\beta\in E$ una raíz de $\mathrm{Res}(F,G)$, si no se verifica (1), se tiene $F(X,\beta)=0$ y $G(X,\beta)=0$ tiene una raíz común, α, en la extensión E de K, y por tanto (α,β) es una solución del sistema. □

Ejemplo. 63.4.
Se consideran los polinomios

$$F=X^2Y^2-X^2+XY+X\in\mathbb{Q}[X,Y],$$
$$G=X^2Y+XY^2-X^2-X+2Y\in\mathbb{Q}[X,Y].$$

Calcula las raíces comunes de F y G.

Primero calculamos la resultante de F y G; en ese caso es:

$$\begin{aligned}\mathrm{Res}(F,G) &= 2Y(-2+3Y^2-Y^3-Y^4+Y^5)\\ &= Y(Y+1)^2(Y-1)(Y-1+i)(Y-1-i).\end{aligned}$$

Las raíces son: 0, 1, -1 (doble), $1+i$ y $1-i$.

Los coeficientes líderes de F y G son, respectivamente, $a_n(Y)=Y^2-1$ y $b_m(Y)=Y-1$, de los cuales 1 es una raíz común.

Cada uno de estos valores puede proporcionar raíces comunes de F y G. Tenemos:

Para $y=0$:

$F=X-X^2$,
$G=-X-X^2$,
Las raíces comunes son: $x=0$.
Una raíz común del sistema original es: $(0,0)$.

Para $y=1$:

$F=2X$,
$G=2$,
No tienen raíces comunes.
En este caso el sistema original no tiene raíces comunes.
Este caso corresponde a la raíz $y=1$ de $a_n(Y)=0=b_m(Y)$.

Para $y=-1$:

$F=0$,
$G=-2-2X^2$,
Las raíces comunes son: $x=i,-i$.
Raíces comunes del sistema original es: $(i,-1),(-i,-1)$.

Para $y=1-i$:

$F=(2-i)X-(1+2i)X^2$,
$G=(2-2i)-(1+2i)X-iX^2$,
Las raíces comunes son: $x=-i$.
Una raíz común del sistema original es: $(-i,1-i)$.

Para $y=1+i$:

$F=(2+i)X-(1-2i)X^2$,
$G=(2+2i)-(1-2i)X+iX^2$,
Las raíces comunes son: $x=i$.
Una raíz común del sistema original es: $(i,1+i)$.

En resumen, las soluciones del sistema

$$\left.\begin{aligned}X^2Y^2-X^2+XY+X=0\\ X^2Y+XY^2-X^2-X+2Y=0\end{aligned}\right\}$$

son:

$$(0,0),(i,-1),(-i,-1),(-i,1-i),(i,1+i).$$

Observación. 63.5.
Observa que la resultante $\mathrm{Res}(F,G)$ en realidad lo que hace es proyectar sobre la recta $X = 0$ el conjunto geométrico formado por las soluciones del sistema, junto con las raíces de los coeficientes líderes. Una vez que se resuelve esta proyección; se determinan las soluciones reales sin más que sustituir éstas en el sistema original.

Teorema de Bezout

Consideramos el anillo $K[X_1,\dots,X_n]$. Un polinomio $F \in K[X_1,\dots,X_n]$ es **homogéneo** de grado r si para cada término $c_\alpha X^\alpha$ se tiene $r = \sum_i \alpha_i$.
Dado un polinomio homogéneo F de grado r, podemos considerarlo como elemento del anillo de polinomios $K[X_1,\dots,X_{n-1}][X_n]$, entonces tiene una expresión $F = F_r + F_{r-1}X_n + \cdots + F_0 X_n^r$, en donde cada F_i es un polinomio homogéneo de grado i en las indeterminadas $X_1,\dots,X_{n-1}$.
Dados $F,G \in K[X_1,\dots,X_n]$ homogéneos, sea $\mathrm{Res}(F,G)$ la resultante en el anillo $K[X_1,\dots,X_{n-1}][X_n]$. De esta forma tenemos que $\mathrm{Res}(F,G)$ es un polinomio en $K[X_1,\dots,X_{n-1}]$.

Lema. 63.6.
Dados $F,G \in K[X_1,\dots,X_n]$, son equivalentes:
(a) $\mathrm{Res}(F,G) = 0$*, esto es, es el polinomio cero,*
(b) F y G tienen un factor común en $K[X_1,\dots,X_n]$.

Cuando F y G son polinomios homogéneos podemos también asegurar que $\mathrm{Res}(F,G)$ es un polinomio homogéneo.

Proposición. 63.7.
Dados $F,G \in K[X_1,\dots,X_n]$ polinomios homogéneos de grados r y s, respectivamente, se tiene que $\mathrm{Res}(F,G)$ *es un polinomio homogéneo, en las indeterminadas $X_1,\dots,X_{n-1}$, de grado rs.*

DEMOSTRACIÓN. Consideramos una nueva indeterminada T y desarrollamos el polinomio

$$\mathrm{Res}(F,G)(TX_1,\dots,TX_{n-1}) = \mathrm{Res}(F(TX_1,\dots,TX_{n-1},X_n), G(TX_1,\dots,TX_{r-1},X_n));$$

tenemos:

$$\mathrm{Res}(F,G)(TX_1,\dots,TX_{n-1}) = \begin{vmatrix} F_0 & TF_1 & T^2F_2 & \dots & T^rF_r & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ G_0 & TG_1 & T^2G_2 & \dots & \dots & T^sG_s & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix}$$

Para calcular este valor multiplicamos las filas 2 y $s+2$ por T, las 3 y $s+3$ por T^2, etc. De esta forma en cada columna tenemos la misma potencia de T; en la columna j tenemos T^{j-1}. Se tiene pues la identidad:

$$T^{1+2+\cdots+s-1}\cdot T^{1+2+\cdots+r-1}\mathrm{Res}(F,G)(TX_1,\ldots,TX_{n-1}) = T^{1+2+\cdots+r+s-1}\mathrm{Res}(F,G)(X_1,\ldots,X_{n-1}).$$

Se tiene:

$$(1+2+\cdots+s-1)+(1+2+\cdots+r-1) = \frac{s(s-1)}{2}+\frac{r(r-1)}{2} = \frac{s^2+r^2-s-r}{2},$$

$$1+2+\cdots+r+s-1 = \frac{(r+s)(r+s-1)}{2} = \frac{s^2+r^2-r-s+2rs}{2}.$$

Por lo tanto resulta $\mathrm{Res}(F,G)(TX_1,\ldots,TX_{n-1}) = T^{rs}\mathrm{Res}(F,G)(X_1,\ldots,X_n)$, y $\mathrm{Res}(F,G)$ es un polinomio homogéneo de grado rs en $X_1,\ldots,X_{n-1}$. □

Podemos ahora estudiar los ceros comunes de dos polinomio homogéneos.

Teorema. 63.8. (Teorema de Bezout)
Sean $F,G\in K[X_1,X_2]$ polinomios homogéneos de grado n y m, respectivamente, que tienen más de nm ceros en común. Entonces F y G tienen un factor común.

DEMOSTRACIÓN. Sean $(a_{1,i},a_{2,i})$ los ceros comunes con $i=0,1,\ldots,nm,\ldots$ Podemos suponer que los $a_{2,i}$ son todos no nulos haciendo una traslación, y que los $a_{1,i}$ son distintos dos a dos.
Reescribimos cada polinomio en términos de $Y_1=\frac{X_1}{X_2}$ y de $Y_2=X_2$, y los consideramos como polinomios en $K[Y_1][Y_2]$ para calcular su resultante. Ésta es $\mathrm{Res}(F,G)\in K[Y_1]$.
Como $(a_{1,i},a_{2,i})$ es un cero de F y de G, se tiene que $(\frac{a_{1,i}}{a_{2,i}},a_{2,i})$ es un cero de los nuevos polinomios, por tanto $\mathrm{Res}(F,G)(\frac{a_{1,i}}{a_{2,i}})=0$, ya que los polinomios $F(\frac{a_{1,i}}{a_{2,i}})$ y $G(\frac{a_{1,i}}{a_{2,i}})$ tienen un cero común. En consecuencia $Y_1-\frac{a_{1,i}}{a_{2,i}}$ es un factor de $\mathrm{Res}(F,G)$, y el grado en Y_1 de $\mathrm{Res}(F,G)$ es mayor que nm, lo que es una contradicción, ya que $\mathrm{Res}(F,G)$ es un polinomio homogéneo de grado nm. □

Teorema. 63.9.
Sea K un cuerpo algebraicamente cerrado, $F,G\in K[X_1,\ldots,X_n]$, $n\geq 3$, polinomios homogéneos que no son constantes en la variable X_n. Existen $k_1,\ldots,k_n\in K$, no todos nulos, tales que $F(k_1,\ldots,k_n)=0=G(k_1,\ldots,k_n)$.

DEMOSTRACIÓN. Tenemos que $\mathrm{Res}(F,G)$ es un polinomio homogéneo en $K[X_1,\ldots,X_{n-1}]$, y como $n-1\geq 2$, tiene al menos un cero, sea éste $(k_1,\ldots,k_{n-1})\neq 0$. Entonces los polinomios $F(k_1,\ldots,k_{n-1},X_n)$ y $G(k_1,\ldots,k_{n-1},X_n)$ tienen resultante nula, luego tienen un factor en común no constante, y por lo tanto existe $k_n\in K$ tal que $F(k_1,\ldots,k_n)=0=G(k_1,\ldots,k_n)$. □

64. Sistemas de números enteros

Cuadrados mágicos

Un cuadrado mágico 3×3 es una tabla de números enteros, del 1 al 9, de forma que la suma de los números en cada fila, en cada columna y en cada diagonal sea la misma. Es fácil ver que estas sumas deben ser igual a 15.

Vamos a plantear un modelo algebraico del cuadrado mágico 3×3. Primero llamamos al número que ocupa la fila i y la columna j por $x_{i,j}$. Tenemos entonces las relaciones de filas:

$$x_{1,1} + x_{1,2} + x_{1,3} = 15, \quad x_{2,1} + x_{2,2} + x_{2,3} = 15, \quad x_{3,1} + x_{3,2} + x_{3,3} = 15,$$

la relaciones de las columnas:

$$x_{1,1} + x_{2,1} + x_{3,1} = 15, \quad x_{1,2} + x_{2,2} + x_{3,2} = 15, \quad x_{1,2} + x_{2,3} + x_{3,3} = 15,$$

y las relaciones de las diagonales:

$$x_{1,1} + x_{2,2} + x_{3,3} = 15, \quad x_{1,3} + x_{2,2} + x_{3,1} = 15.$$

Al considerar todas estas relaciones tenemos un sistema de 8 ecuaciones lineales con 9 incógnitas, que es un sistema compatible indeterminado. Pero estamos interesados en las soluciones comprendidas entre 1 y 9, y todas distintas, por este tenemos que añadir nuevas relaciones, esto es, nuevos generadores al ideal que estamos construyendo.

Al imponer que $x_{1,1}$ tomar valores en $\{1, \dots, 9\}$, aparece la relación:

$$(x_{1,1}-1)(x_{1,1}-2)(x_{1,1}-3)(x_{1,1}-4)(x_{1,1}-5)(x_{1,1}-6)(x_{1,1}-7)(x_{1,1}-8)(x_{1,1}-9) = 0$$

Y esto es necesario hacerlo para los nueve valores $x_{i,j}$, por lo que tendremos las relaciones:

$$(x_{i,j}-1)(x_{i,j}-2)(x_{i,j}-3)(x_{i,j}-4)(x_{i,j}-5)(x_{i,j}-6)(x_{i,j}-7)(x_{i,j}-8)(x_{i,j}-9) = 0\Big\}_{i=1,2,3,j=1,2,3}$$

Al resolver estas relaciones podemos obtener el valor $x_{i,j} = 5$ para todos i y j, por lo que tenemos que agregar las condiciones necesarias para indicar que $x_{i,j} \neq x_{h,k}$ si $(i,j) \neq (h,k)$. Esto es, tenemos que indicar que $x_{i,j} - x_{h,k} \neq 0$. Esta relación la podemos expresar ampliando el anillo en el que estamos trabajando con una nueva indeterminada $u_{i,j,h,k}$ tal que $(x_{i,j} - x_{h,k})u_{i,j,h,k} = 1$; después eliminaremos esta indeterminada para recuperar la relación $x_{i,j} \neq x_{h,k}$. Pero esto tenemos que hacerlo para cada para cuaterna (i,h,j,k) en la que $(i,j) \neq (h,k)$, así pues tenemos $8 + 7 + \cdots + 2 + 1 = 36$ nuevas relaciones del tipo $(x_{i,j} - x_{h,k})u_{i,j,h,k} = 1$.

Todas las relaciones mencionadas nos determinan un ideal, llamémoslo $\mathfrak{a}$, del anillo $\mathbb{Q}[X_{i,j}, U_{i,j,h,k} \mid i,j,h,k]$, y nos interesa conocer el ideal $\mathfrak{a} \cap K[X_{i,j} \mid i,j]$. Para esto el uso de bases de Groebner es una herramienta útil.

1132-07.tex

Variación 1

Las condiciones que hemos impuesto pueden modificarse para hacer más eficiente el cálculo. Por ejemplo todas las relaciones $(X_{i,j}-X_{h,k})U_{i,j,h,k}-1$ pueden agruparse en una solo:

$$U\prod_{(i,j)<(h,k)}(X_{i,j}-X_{h,k})-1$$

De esta forma tenemos una solo indeterminada U en ves de las 36 $U_{i,j,h,k}$ que hemos considerado anteriormente. Reducimos el número de indeterminadas y aumentamos el grado de los polinomios considerados.

Variación 2

El problema de considerar los valores $x_{i,j}$ todos distintos y elementos de $\{1,\ldots,9\}$ podemos tratarlo mediante relaciones del tipo:

$$\sum_{i=1,j=1}^{3,3} x_{i,j}^t=\sum_{i=1}^{9} i^t,\ \text{para } t=1,\ldots,9,$$

en la que conocemos el valor de $\sum_{i=1}^{9} i^t$ para todos los valores de t, por lo que nos quedan completamente determinados los valores de los $x_{i,j}$, todos distintos, y en el conjunto $\{1,\ldots,9\}$.
Tenemos pues un ideal generado por otros generadores que proporciona las mismas soluciones.

Variación 3

Podemos reducir el problema a trabajar en un cuerpo finito, por ejemplo $\mathbb{Z}_1 1$ con la esperanza de que el número de operaciones necesarias sea menor.

Actividad

Estudiar el cuadrado mágico 4×4. En este caso el número de posibles soluciones es mucho mayor.

Kakuro

Kakuro es una clase de enigma lógico que a menudo es referido como una transcripción matemática del crucigrama. Básicamente, los enigmas Kakuro son problemas de programación lineal, y se pueden resolver utilizando las técnicas de matriz matemática, aunque sean resueltos típicamente a mano. Los enigmas de Kakuro son regulares en la mayoría, si no todas, de las publicaciones de matemáticas y de enigma lógico en los Estados Unidos. Dell Magazines propuso los nombres de Cross Sums (Sumas Cruzadas) y Cross Addition (Adición Cruzada), pero también el nombre japonés Kakuro (la abreviación japonésa de kasan kurosu: Adición+Cruz) que parece haber ganado aceptación general y los enigmas aparecen titulados de esta manera ahora en la mayoría de las publicaciones. La popularidad de Kakuro en Japón es inmensa, sólo después del famoso Sudoku entre otras célebres ofertas de la famosa Nikoli.

`http://es.wikipedia.org/wiki/Kakuro`

Kenken

El kenken, también denominado Kenko o KenDoku (versiones no autorizadas se denominan a veces Mathdoku o Calcudoku) es un pasatiempos similar al sudoku. Las reglas son no repetir ningún número en filas o columnas y las regiones marcadas de formas diversas han de estar ocupadas por números que formen la cifra exacta mediante las operaciones indicadas: suma, resta, multiplicación o división. Los dígitos pueden repetirse dentro de una región, siempre que no se encuentren en la misma fila o columna.

`http://es.wikipedia.org/wiki/Kenken`

El kenken consiste en un cuadrado de n filas y n columnas, y se trata de completar filas y columnas con las siguientes condiciones.

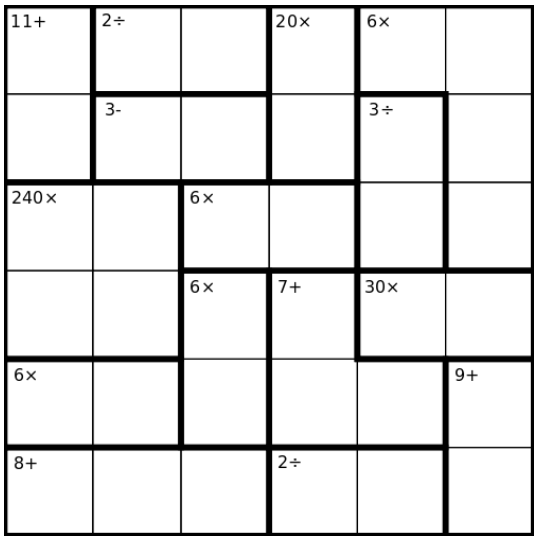
(1) En cada fila y en cada columna sólo se pueden colocar números del 1 al n, no repitiendo números en filas y columnas.
(2) El cuadrado está partido en regiones , en cada una de las cuales aparece un número y una operación. Sa trata de obtener el número dado en cada región con la operación indicada. En el caso de suma y multiplicación no importa el orden, en el caso de resta y división el orden es importanta, en este caso no hay prelación ninguna según la disposición de las casillas.

Si rellenamos la casilla (i,j) con el número $x_{i,j}$, tenemos

(1) Cada fila está rellena con número de 1 a n, por lo que $(x_{i,j}-1)\cdots(x_{i,j}-n)=0$.
(2) Si $j\neq k$, entonces $x_{i,j}\neq x_{i,k}$ si $j\neq k$, por lo que la expresión $x_{i,j}\neq x_{j,k}$ debemos incorporarla como una restricción; en este caso debemos introducir una nueva variable $t_{i;j,k}$ e imponer la relación $(x_{i,j}-x_{i,k})t_{i;j,k}-1=0$. De forma análoga se tendría para $x_{i,j}\neq x_{h,j}$, en donde tendremos que introducir una nueva variable $t_{i,h;j}$ y la relación $(x_{i,j}-x_{h,j})t_{i,h;j}-1=0$.

Estas dos condiciones podemos expresarlas más fácilmente en algunos casos. Por ejemplo si $n=6$, podemos trabajar en $\mathbb{F}_7$. En este caso los valores $x_{i,j}$ pertenecen a $\mathbb{F}_7^\times$, por lo que verifican $x_{i,j}^6=1$. Por tanto si $j\neq k$, tendremos la relación $x_{i,j}^5+x_{i,j}^4x_{i,k}+\cdots+x_{i,j}x_{i,k}^4+x_{i,k}^5=0$.
Además hay que añadir las condiciones que dan los elementos de cada partición. Para la suma y la multiplicación, ya que no importa el orden, no hay problema. Para la resta y la división, cada uno de los elementos de la partición nos da dos posibles relaciones, de las que sólo una es válida. Por ejemplo, si $x_{i,j}$y $x_{i,k}$ son los valores de las casillas de uno de los elementos de la partición, el número a determinar es k, y la operación es "$-$", entonces tendremos una de las relaciones $x_{i,j}-x_{i,k}-k=0$ y $x_{i,k}-x_{i,j}-k=0$. Esto significa que por cada uno de los elementos de la partición con signo "$-$" tendremos que estudiar dos sistemas diferentes, uno que incorpora a $x_{i,j}-x_{i,k}-k=0$. y otro que incorpora a $x_{i,j}-xi,k+k=0$.
Una vez recogida toda la información, tendremos un sistema de ecuaciones polinomiales que es el que tendremos que estudiar.

Veamos el siguiente ejemplo:

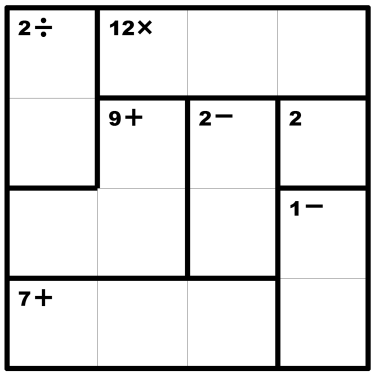


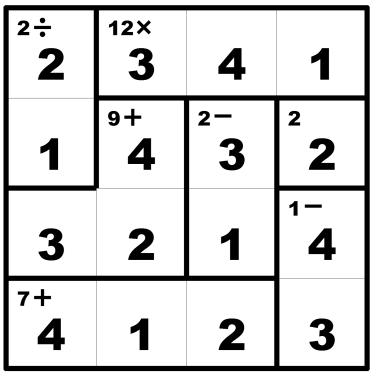
Ejercicio. 64.1.
Estudiar su resolución en Mathematica. Una pista, el elemento $x_{1,5}$ es igual a 1.
Ref.: 1132e_024 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (64.1.)
HACER □

En este caso los cálculos han sido demasiado largos; el tiempo de cálculo depende del paquete que calcule bases de Groebner.

Podemos estudiar casos más sencillos como por ejemplo el siguiente:





Ejercicio. 64.2.
Estudiar su resolución en Mathematica.
Ref.: 1132e_025 *SOLUCIÓN*

SOLUCIÓN. Ejercicio (64.2.)
HACER □

Problema. 64.3.
¿Que ocurre si el kenken es 5×5*?*

65. Programación entera

Soluciones de sistemas de números naturales

Se considera el siguiente sistema de ecuaciones lineales

$$\left.\begin{array}{l} a_{11}s_1 + a_{12}s_2 + \cdots + a_{1m}s_m = b_1 \\ a_{21}s_1 + a_{22}s_2 + \cdots + a_{2m}s_m = b_2 \\ \vdots \\ a_{n1}s_1 + a_{n2}s_2 + \cdots + a_{nm}s_m = b_n \end{array}\right\} \tag{XII.2}$$

y una función $f(s_1,\ldots,s_m) = \sum_{j=1}^m c_j s_j$. Vamos a estudiar el problema de encontrar una solución del sistema $(s_1,\ldots,s_m) \in \mathbb{N}^n$ que minimice la función f cuando $a_{ij}, b_i, c_j \in \mathbb{N}$.

Trasladamos este problema a otro en términos de anillos de polinomios. Primero estudiamos las soluciones enteras al sistema planteado, prescindiendo de la función f. Consideramos indeterminadas $X_1,\ldots,X_n$ y escribimos

$$X_i^{a_{i1}s_1+a_{i2}s_2+\cdots+a_{im}s_m} = X_i^{b_i}, \quad i = 1,\ldots,n.$$

Y por tanto

$$X_1^{a_{11}s_1+a_{12}s_2+\cdots+a_{1m}s_m} \cdots X_n^{a_{n1}s_1+a_{n2}s_2+\cdots+a_{nm}s_m} = X_1^{b_1}\cdots X_n^{b_n},$$

que podemos reordenar como

$$(X_1^{a_{11}}\cdots X_n^{a_{n1}})^{s_1}\cdots(X_1^{a_{1m}}\cdots X_n^{a_{nm}})^{s_m} = X_1^{b_1}\cdots X_n^{b_n}.$$

Si definimos la aplicación $h : K[Y_1,\ldots,Y_m] \to K[X_1,\ldots,X_n]$ mediante $h(Y_j) = X_1^{a_{1j}}\cdots X_n^{a_{nj}}$, se tiene

$$h(Y_1^{s_1}\cdots Y_m^{s_m}) = (X_1^{a_{11}}\cdots X_n^{a_{n1}})^{s_1}\cdots(X_1^{a_{1m}}\cdots X_n^{a_{nm}})^{s_m}$$

Como consecuencia:

Lema. 65.1.
Con la notación anterior, son equivalentes:
(a) El sistema (XII.2) *tiene una solución* $(s_1,\ldots,s_m) \in \mathbb{N}^m$.
(b) $X_1^{b_1}\cdots X_n^{b_n}$ *es la imagen de por* h *de un monomio en* $K[Y_1,\ldots,Y_m]$.

En este caso se tiene que $h(Y_1^{s_1}\cdots Y_m^{s_m}) = X_1^{b_1}\cdots X_n^{b_n}$ *si, y sólo si,* $(s_1,\ldots,s_m) \in \mathbb{N}^m$ *y es una solución.*

1132-06.tex

DEMOSTRACIÓN. Es obvio. □

En realidad nos gustaría que fuese suficiente el que $X_1^{b_1}\cdots X_n^{b_n}\in \mathrm{Im}(h)$ para tener una solución del sistema, y éste es precisamente el caso debido a la definición de h.

Proposición. 65.2.
Con la notación anterior, son equivalentes:
(a) $X_1^{b_1}\cdots X_n^{b_n}\in \mathrm{Im}(h)$.
(b) Existe $Y_1^{s_1}\cdots Y_m^{s_m}\in K[Y_1,\ldots,Y_m]$ *tal que* $X_1^{b_1}\cdots X_n^{b_n}=h(Y_1^{s_1}\cdots Y_m^{s_m})$.

DEMOSTRACIÓN. Ya conocemos como determinar el núcleo de h y su imagen; para ello utilizábamos el ideal $\mathfrak{c}=\langle Y_1-X_1^{a_{11}}\cdots X_n^{a_{n1}},\ldots,Y_m-X_1^{a_{1m}}\cdots X_n^{a_{nm}}\rangle$, calculábamos una base de Groebner $\mathbb{G}$ de $\mathfrak{c}$, y teníamos $\mathrm{Ker}(h)=\mathfrak{c}\cap K[Y_1,\ldots,Y_m]$; si la base de Groebner se calcula con un orden de eliminación en el que $X_i>Y_j$, se tiene una base de Groebner de $\mathrm{Ker}(h)$; por otro lado $F\in\mathrm{Im}(h)$ si, y sólo si $R(F,\mathbb{G})\in K[Y_1,\ldots,Y_m]$. Si $X_1^{b_1}\cdots X_n^{b_n}\in\mathrm{Im}(h)$, entonces existe $F\in K[Y_1,\ldots,Y_m]$ tal que $h(F)=X_1^{b_1}\cdots X_n^{b_n}$. Vamos a razonar que F es un monomio. Esto será consecuencia de cómo está generado $\mathfrak{c}$; observa que si construimos una base de Groebner a partir de los generadores dados, ésta está formada por elementos del tipo $X^{\alpha_1}Y^{\beta_1}-X^{\alpha_2}Y^{\beta_2}$, con $\alpha_1,\alpha_2\in\mathbb{N}^n$ y $\beta_1,\beta_2\in\mathbb{N}^m$; al dividir $X_1^{b_1}\cdots X_n^{b_n}$ por esta base se obtiene en cada paso un sólo monomio, y como el resto es un elemento de $K[Y_1,\ldots,Y_m]$, se tiene un monomio en los Y_j. □

Tenemos pues que estudiar si $X_1^{b_1}\cdots X_n^{b_n}\in\mathrm{Im}(h)$, y esto se realiza del siguiente modo:

(1) Se considera el ideal $\mathfrak{c}=(Y_j-X_1^{a_{1j}}\cdots X_n^{a_{nj}}\mid j=1,\ldots,m)\subseteq K[X_1,\ldots,X_n,Y_1,\ldots,Y_m]$, y una base de Groebner $\mathbb{G}$ de $\mathfrak{c}$.

(2) $X_1^{b_1}\cdots X_n^{b_n}\in\mathrm{Im}(h)$ si, y sólo si, $R(X_1^{b_1}\cdots X_n^{b_n},\mathbb{G})\in K[Y_1,\ldots,Y_m]$

Ejemplo. 65.3.
Consideramos el sistema

$$\left.\begin{array}{rl} 2s_1+s_2 & =3\\ s_1+s_2+3s_3 & =5\end{array}\right\}$$

Para determinar las soluciones enteras consideramos

$$(X_1^2X_2)^{s_1}(X_1X_2)^{s_2}(X_2^3)^{s_3}=X_1^3X_2^5,$$

y el homomorfismo

$$h:K[Y_1,Y_2,Y_3]\longrightarrow K[X_1,X_2],\qquad h(Y_1)=X_1^2X_2,\ h(Y_2)=X_1X_2,\ h(Y_3)=X_2^3.$$

Su núcleo es $K[Y_1,Y_2,Y_3]\cap \mathfrak{c}$, donde $\mathfrak{c}=\langle Y_1-X_1^2X_3, Y_2-X_1X_2, Y_3-X_2^3\rangle$ y un elemento $F\in K[X_1,X_2]$ pertenece a la imagen si, y sólo si, $R(F,\mathbb{G})\in K[Y_1,Y_2,Y_3]$, donde $\mathbb{G}$ es la base de Groebner de eliminación del ideal $\mathfrak{c}$.

GB1 = **GroebnerBasis**$[G,\{X_1,X_2,Y_1,Y_2,Y_3\}]$

$\mathbb{G}=\{Y_1^3Y_3-Y_2^6, X_2Y_2^4-Y_1^2Y_3, X_2Y_1-Y_2^2, X_2^2Y_2^2-Y_1Y_3, X_2^3-Y_3, X_1Y_3-X_2^2Y_2, X_1Y_2-Y_1, X_1X_2-Y_2\}$
$\mathrm{Ker}(h)=\langle Y_1^3Y_3-Y_2^6\rangle$.

Para ver si $X_1^3X_2^5$ pertenece a la imagen de h sólo tenemos que calcular el resto $R(X_1^3X_2^5,\mathbb{G})$ y ver si pertenece a $K[Y_1,Y_2,Y_3]$. En este caso se tiene
PolynomialReduce$\left[X_1^3X_2^5, \mathbf{GB1}, \{X_1,X_2,Y_1,Y_2,Y_3\}\right][[2]]$

$$R(X_1^3X_2^5,\mathbb{G})=Y_1Y_2Y_3.$$

Como consecuencia, el sistema tiene solución en $\mathbb{N}$. Una solución es $s_1=s_2=s_3=1$.

Ejemplo. 65.4.
Consideramos el sistema

$$\left.\begin{array}{l} 2s_1+s_2 \quad\quad =3 \\ s_1+s_2+3s_3=1 \end{array}\right\}$$

Para determinar las soluciones enteras seguimos el mismo proceso que antes. Finalmente tenemos que comprobar si $X_1^3X_2$ pertenece a la imagen de h sólo tenemos que calcular el resto $R(X_1^3X_2,\mathbb{G})$ y ver si pertenece a $K[Y_1,Y_2,Y_3]$. En este caso se tiene
PolynomialReduce$\left[X_1^3X_2, \mathbf{GB1}, \{X_1,X_2,Y_1,Y_2,Y_3\}\right][[2]]$

$$R(X_1^3X_2,\mathbb{G})=X_1Y_1.$$

Como consecuencia, el sistema **no** tiene solución en $\mathbb{N}$.

Referencias:

(1) Freireich (2000) - Aplicaciones de bases de Gröbner y teorías algebraicas para programación entera.
(2) ADAMS/LOUSTAUNAU - An introduction to Gröbner bases (1994)

Soluciones de sistemas de números enteros

Vamos a considerar ahora un sistema de ecuaciones lineales con coeficientes en $\mathbb{Z}$:

$$\left.\begin{array}{l} a_{11}s_1+a_{12}s_2+\cdots+a_{1m}s_m=b_1 \\ a_{21}s_1+a_{22}s_2+\cdots+a_{2m}s_m=b_2 \\ \vdots \\ a_{n1}s_1+a_{n2}s_2+\cdots+a_{nm}s_m=b_n \end{array}\right\} \qquad \text{(XII.3)}$$

queremos hallar las soluciones $(s_1,\ldots,s_m)\in\mathbb{N}^m$. Para ello definimos

(1) $a_j \geq \max\big(\{|a_{ij}| \mid i=1,\dots,n \text{ y } a_{ij}<0\}\cup\{0\}\big)$. Existen $a'_{ij}\geq 0$ tales que

$$(a_{1j},\dots,a_{n,j}) = (a'_{1j},\dots,a'_{n,j}) + a_j(-1,\dots,-1).$$

(2) $b \geq \max(\{|b_i| \mid i=1,\dots,n \text{ y } b_i<0\}\cup\{0\})$, existen $b'_i\geq 0$ tal que

$$(b_1,\dots,b_n) = (b'_1,\dots,b'_n) + b(-1,\dots,-1).$$

Consideramos variables $X_1,\dots,X_n$, una nueva variable T, el ideal $\mathfrak{t} = \langle X_1\cdots X_n T-1\rangle$ del anillo $K[X_1,\dots,X_n,T]$, y el anillo cociente $K[X_1,\dots,X_n,T]/\mathfrak{t}$. En este anillo se verifica

$$\begin{aligned} &X_1^{a_{1j}}\cdots X_n^{a_{nj}} + \mathfrak{t} = X_1^{a'_{1j}}\cdots X_n^{a'_{nj}}T^{a_j} + \mathfrak{t}, \text{para todo } j=1,\dots,m.\\ &X_1^{b_1}\cdots X_n^{b_n} + \mathfrak{t} = X_1^{b'_1}\cdots X_n^{b'_n}T^{b} + \mathfrak{t}.\end{aligned}$$

Al considerar las expresiones formales

$$X_1^{a_{11}s_1+\cdots+a_{1m}s_m}\cdots X_n^{a_{n1}s_1+\cdots+a_{nm}s_m} = X_1^{b_1}\cdots X_n^{b_n},$$

y su reagrupamiento:

$$\big(X_1^{a_{11}}\cdots X_n^{a_{n1}}\big)^{s_1}\cdots\big(X_1^{a_{1m}}\cdots X_n^{a_{nm}}\big)^{s_m} = X_1^{b_1}\cdots X_n^{b_n},$$

podemos escribir

$$\Big(X_1^{a'_{11}}\cdots X_n^{a'_{n1}}T^{a_1}\Big)^{s_1}\cdots\Big(X_1^{a'_{1m}}\cdots X_n^{a'_{nm}}T^{a_m}\Big)^{s_m} + \mathfrak{t} = X_1^{b'_1}\cdots X_n^{b'_n}T^{b} + \mathfrak{t},$$

y definir una aplicación polinómica

$$h : K[Y_1,\dots,Y_m] \to K[X_1,\dots,X_n,T]/\mathfrak{t}$$

mediante $h(Y_j) = X_1^{a'_{1j}}\cdots X_n^{a'_{nj}}T^{a_j} + \mathfrak{t}$. Se tiene

$$h(Y_1^{s_1}\cdots Y_m^{s_m}) = (X_1^{a'_{11}}\cdots X_n^{a'_{n1}}T^{a_1})^{s_1}\cdots(X_1^{a'_{1m}}\cdots X_n^{a'_{nm}}T^{a_m})^{s_m} + \mathfrak{t}.$$

Como todos los a'_{ij} son no negativos, podemos retomar el proceso anterior para determinar una solución, en $\ltimes$, al sistema con coeficientes en $\mathbb{N}$.

Lema. 65.5.
Con la notación anterior, son equivalentes:
(a) El sistema (XII.3) *tiene una solución* $(s_1,\dots,s_m)\in\mathbb{N}^m$.
(b) $X_1^{b'_1}\cdots X_n^{b'_n}T^{b}+\mathfrak{t}$ *es la imagen de por* h *de un monomio en* $K[Y_1,\dots,Y_m]$.

En este caso se tiene que $h(Y_1^{s_1}\cdots Y_m^{s_m}) = X_1^{b'_1}\cdots X_n^{b'_n}T^{b}+\mathfrak{t}$ *si, y sólo si,* $(s_1,\dots,s_m)\in\mathbb{N}^m$ *y es una solución.*

DEMOSTRACIÓN. Es obvio. □

Proposición. 65.6.
Con la notación anterior, son equivalentes:
(a) $X_1^{b'_1}\cdots X_n^{b'_n}T^b+\mathfrak{t}\in \mathrm{Im}(h)$.
(b) Existe $Y_1^{s_1}\cdots Y_m^{s_m}\in K[Y_1,\ldots,Y_m]$ *tal que* $X_1^{b'_1}\cdots X_n^{b'_n}T^b+\mathfrak{t}=h(Y_1^{s_1}\cdots Y_m^{s_m})$.

DEMOSTRACIÓN. En este caso se tiene que construir el ideal

$$\mathfrak{c}=\langle Y_j-X_1^{a_{1j}}\cdots X_n^{a_{nj}}T^{a_j}, j=1,\ldots,m; X_1\cdots X_nT-1\rangle,$$

y si $\mathbb{G}$ es una base de Groebner para un orden monomial tal que $X_j,T>Y_j$, entonces tenemos una descripción de $\mathrm{Ker}(h)$ y de $\mathrm{Im}(h)$, teniendo que $G\in\mathrm{Im}(h)$ si, y sólo si, $R(G,\mathbb{G})\in K[Y_1,\ldots,Y_m]$. En nuestro caso, como $\mathbb{G}$ está formada por elementos del tipo $X^{\alpha_1}Y^{\beta_1}-X^{\alpha_2}Y^{\beta_2}$, con $\alpha_1,\alpha_2\in\mathbb{N}^n$ y $\beta_1,\beta_2\in\mathbb{N}^m$; al dividir $X_1^{b'_1}\cdots X_n^{b'_n}T^b$ por esta base se obtiene, en cada paso, un sólo monomio, y como el resto es un elemento de $K[Y_1,\ldots,Y_m]$, se tiene un monomio en los Y_j. □

Ejemplo. 65.7.
Resolver, en $\mathbb{N}$, el siguiente sistema

$$\left.\begin{array}{r} s_1+s_2\ -s_3=5\\ s_1-2s_2+3s_3=-5\end{array}\right\}$$

Primero lo transformamos en un sistema con coeficientes en $\mathbb{N}$, para ello necesitamos

$$\begin{aligned} a_1&=\max(\varnothing\cup\{0\})=0\\ a_2&=\max(\{|-2|\}\cup\{0\})=2\\ a_3&=\max(\{|-1|\}\cup\{0\})=1\\ b&=\max(\{|-5|\}\cup\{0\})=5\end{aligned}$$

Tenemos la relaciones:

$$\begin{aligned}(1,1)&=(1,1)+0(-1,-1)\\ (1,-1)&=(3,0)+2(-1,-1)\\ (-1,3)&=(0,4)+1(-1,-1)\\ (5,-5)&=(10,0)+5(-1,-1)\end{aligned}$$

El sistema es:

$$\left.\begin{array}{r} s_1+3s_2\ =10\\ s_1\ +4s_3=0\end{array}\right\}$$

y la relación polinómica es:

$$(X_1X_2)^{s_1}(X_1^3T^2)^{s_2}(X_2^4T)^{s_3}=X_1^{10}X_2^0T^5$$

El ideal $\mathfrak{c}$ es:

$$\mathfrak{c} = \langle Y_1 - X_1X_2, Y_2 - X_1^3T^2, Y_3 - X_2^4T, X_1X_2T - 1\rangle.$$

Su base de Groebner es:

$$\left\{Y_1 - Y_2^4Y_3^3, TY_2^4Y_3^3 - 1, X_2 - Y_2Y_3, X_1 - Y_2^3Y_3^2\right\}$$

El resto de la división de $X_1^{10}X_2^0T^5$ por esta base es: $Y_2^{10}Y_3^5$, y una solución al sistema es:

$$s_1 = 0, \quad s_2 = 10, \quad s_3 = 5.$$

Evidentemente no es la única solución; las otras soluciones provienen de monomios de la forma $Y_2^{10}Y_3^5 + L$, donde $L \in \mathrm{Ker}(h) = (Y_1 - Y_2^4Y_3^3)$. Por ejemplo, en este caso se tiene la solución que corresponde a $Y_1Y_2^6Y_32$, que es

$$s_1 = 1, \quad s_2 = 6, \quad s_3 = 2.$$

También se obtienen soluciones en $\mathbb{Z}$, como por ejemplo

$$s_1 = 2, \quad s_2 = 2, \quad s_3 = -1,$$

que corresponde a $Y_1^2Y_2^2Y_3^{-1}$.

Cálculo de máximos y mínimos

Consideramos ahora una función objetivo a minimizar: $f(s_1,\dots,s_m) = \sum_{j=1}^m c_js_j$, en donde $c_j \in \mathbb{Z}$. Según hemos visto, podemos determinar las soluciones en $\mathbb{N}$ del sistema de ecuaciones lineales con coeficientes en $\mathbb{Z}$ (seguimos en este caso para mayor generalidad). Se trata ahora de considerar un orden monomial que permita determinar si una solución proporciona un mínimo. Seguimos con la misma notación que en apartados anteriores.

Dado un orden monomial $\preceq$ en $\mathbb{N}^m$, vamos a imponerle algunas condiciones que queremos que verifique: Si $h(Y_1^{s_1}\cdots Y_m^{s_m}) = h(Y_1^{r_1}\cdots Y_m^{r_m})$ y $f(s_1,\dots,s_m) \geq f(r_1,\dots,r_m)$, entonces $Y_1^{s_1}\cdots Y_m^{s_m} \preceq Y_1^{r_1}\cdots Y_m^{r_m}$. En este caso diremos que $\preceq$ es un **orden monomial compatible con** h **y** f.

Lema. 65.8.
Si $Y_1^{s_1}\cdots Y_m^{s_m} = R(X_1^{b'_1}\cdots X_n^{b'_n}T^b, \mathbb{G})$, *donde* $(s_1,\dots,s_m)$ *es una solución del sistema y* $\preceq$ *es un orden monomial compatible con* h *y* f, *entonces* $(s_1,\dots,s_m)$ *hace mínimo a* f.

DEMOSTRACIÓN. Supongamos que existe otra solución $(r_1,\dots,r_m)$ tal que $\sum_j c_jr_j < \sum_j c_js_j$, entonces como $h(Y_1^{r_1}\cdots Y_m^{r_m}) = X_1^{b'_1}\cdots X_n^{b'_n}T^b + \mathfrak{t} = h(Y_1^{s_1}\cdots Y_m^{s_m})$, se tiene $Y_1^{r_1}\cdots Y_m^{r_m} - Y_1^{s_1}\cdots Y_m^{s_m} \in \mathrm{Ker}(h)$, y por tanto $R(Y_1^{r_1}\cdots Y_m^{r_m} - Y_1^{s_1}\cdots Y_m^{s_m}, \mathbb{G}) = 0$. Como $\sum_j c_jr_j < \sum_j c_js_j$, se tiene $Y_1^{r_1}\cdots Y_m^{r_m} \preceq Y_1^{s_1}\cdots Y_m^{s_m}$, y por tanto el líder de $Y_1^{r_1}\cdots Y_m^{r_m} - Y_1^{s_1}\cdots Y_m^{s_m}$ es $Y_1^{s_1}\cdots Y_m^{s_m}$, y evidentemente la diferencia no reduce a cero. Por tanto $Y_1^{r_1}\cdots Y_m^{r_m} = Y_1^{s_1}\cdots Y_m^{s_m}$, y tenemos el resultado. □

Observa que cada orden compatible con f y h dará una solución al problema de minimizar f, y el número de soluciones dependerá de los posibles órdenes compatible que podamos encontrar.
En el caso en el que todos los c_j son no negativos, tenemos un modo de construir órdenes compatibles. Basta definir el siguiente para $\beta_1, \beta_2 \in \mathbb{N}^m$:

$$\beta_1 \prec \beta_2 \text{ si } \begin{cases} h(Y^{\beta_1}) < h(Y^{\beta_2}) \text{ ó} \\ h(Y^{\beta_1}) = h(Y^{\beta_2}) \text{ y } f(Y^{\beta_1}) < f(Y^{\beta_2}). \end{cases}$$

Ejemplo. 65.9.
Considera el problema de minimizar la función objetivo $f(s_1, s_2, s_3) = 4s_1 + s_2 + 2s_3$ sujeto a las condiciones

$$\begin{aligned} s_1 + s_2 \ - s_3 \ &= 5 \\ s_1 - 2s_2 + 3s_3 &= -5 \end{aligned}$$

Tenemos que las soluciones del sistema son $(0, 10, 5)$, y otras soluciones, en $\mathbb{N}$, se obtienen sumando $(1, -4, -3)$, por tanto sólo hay dos soluciones $(0, 10, 5)$ y $(1, 6, 2)$. Como en este caso se tiene

$$\begin{aligned} f(0, 10, 5) &= 4 \times 0 + 10 + 2 \times 5 = 20, \\ f(1, 6, 2) &= 4 \times 1 + 6 + 2 \times 2 = 14. \end{aligned}$$

Resulta que el mínimo se alcanza con $(1, 6, 2)$.

66. Cálculo proposicional

Se considera un conjunto de variables $P_0 = \{X_1, \ldots, X_n\}$ y una familia de conectivas F. Cada elemento $f \in F$ tiene una multiplicidad, sea d, lo que significa que f tiene d argumentos: $f(X_{i_1}, \ldots, X_{i_d})$ los valores de f forman un conjunto al que llamaremos P_1', y definimos $P_1 = P_0 \cup P_1$, la unión disjunta de P_0 y P_1'. Suponemos que cada conectiva $f \in F$ puede ahora tomar argumentos en P_1, y llamamos P_2 al conjunto de los valores de todos los $f \in F$. De esta forma construimos conjuntos P_n, para $n \in \mathbb{N} \setminus \{0\}$. Definimos $\mathscr{P} = \cup_{n \in \mathbb{N} \setminus \{0\}} P_n$. Llamamos a $\mathscr{P}$ un **cálculo proposicional**, y a sus elementos los llamamos **proposiciones**.

Ejemplo. 66.1.
(1) La conectiva $f = \neg$ es de multiplicidad 1, y la llamamos la negación.
(2) La conectiva $f = \vee$ es de multiplicidad 2, y la llamamos "o".
(3) La conectiva $f = \wedge$ es de multiplicidad 2, y la llamamos "y".
(4) La conectiva $f = \longrightarrow$ es de multiplicidad 2, y la llamamos "implicación".
(5) La conectiva $f = \longleftrightarrow$ es de multiplicidad 2, y la llamamos "equivalencia".

Dado un cálculo proposicional $\mathscr{P}$, una **valoración** es una aplicación $v : P_0 \longrightarrow \mathbb{F} = \mathbb{F}_2$. Podemos extender cada valoración v a una aplicación $v : \mathscr{P} \longrightarrow \mathbb{F}$ de la siguiente forma. Para cada elemento $f(A_{i_1}, \ldots, A_{i_d}) \in \mathscr{P}$ se define

$$v(f(A_{i_1}, \ldots, A_{i_d})) = f'(v(A_{i_1}), \ldots, v(A_{i_d})),$$

siendo f' la aplicación de $f' : \mathbb{F}^d \longrightarrow \mathbb{F}$ que define a f. En los ejemplos anteriores f' está definido de la siguiente forma:

Ejemplo. 66.2.
(1) $f' : \mathbb{F} \longrightarrow \mathbb{F}$, definida como $f'(x) = x + 1$.
(2) $f' : \mathbb{F}^2 \longrightarrow \mathbb{F}$, definida como $f'(x, y) = x + y + xy$.
(3) $f' : \mathbb{F}^2 \longrightarrow \mathbb{F}$, definida como $f'(x, y) = xy$.
(4) $f' : \mathbb{F}^2 \longrightarrow \mathbb{F}$, definida como $f'(x, y) = xy + x + 1$.
(5) $f' : \mathbb{F}^2 \longrightarrow \mathbb{F}$, definida como $f'(x, y) = xy + 1$.

Por comodidad representamos f' simplemente como f, ya que no hay riesgo de confusión, pues los argumentos a los que se aplica f son proposiciones, y a los que se aplica f' son elementos de $\mathbb{F}$.

Dos proposiciones A y B son **equivalentes** si para cada valoración v se tiene $v(A) = v(B)$.

Dadas dos proposiciones, A y B, diremos que A es una **consecuencia lógica** de B si para cada valoración v tal que $v(B) = 1$, se tiene que $v(A) = 1$, y dadas proposiciones $A, B_1, \ldots, B_m$, diremos que A es una **consecuencia lógica** de $\{B_1, \ldots, B_m\}$ si para cada valoración v tal que $v(B_1) = \cdots = v(B_m) = 1$, se tiene que $v(A) = 1$, y lo representamos por $\{B_1, \ldots, B_m\} \models A$.

De particular interés son aquellas proposiciones A tales que $\varnothing \models A$, las llamamos **tautologías**, y verifican que $v(A) = 1$ para cada valoración v. También podemos escribir $\models A$.

El problema es, dadas proposiciones $A, B_1, \ldots, B_m$, determinar cuando se tiene que $\{B_1, \ldots, B_m\} \models A$.

Abordamos el problema buscando un modelo polinomial en el que expresar nuestro problema.

Dado un cálculo proposicional $\mathscr{P}$ consideramos el anillo de polinomios $\mathbb{F}[X_1, \ldots, X_n]$.

1132-08.tex

(1) Para cada valoración v tenemos un homomorfismo de anillos $v : \mathbb{F}[X_1,\dots,X_n] \longrightarrow \mathbb{F}$, definido dando las imágenes de las indeterminadas; en este caso, $X_i \mapsto v(X_i)$.
(2) Para cada conectiva f, de multiplicidad d, definimos una aplicación $f : \mathbb{F}[X_1,\dots,X_n]^d \longrightarrow \mathbb{F}[X_1,\dots,X_n]$ mediante:

$$f(F_1,\dots,F_d) = \sum_{(a_1,\dots,a_d)\in\mathbb{F}^d} f(a_1,\dots,a_d)G_{a_1}(F_1)\cdots G_{a_d}(F_d),$$

siendo $G_0(F) = 1-F$ y $G_1(F) = -F$, para cada $F \in \mathbb{F}[X_1,\dots,X_n]$.
(3) Definimos ahora una aplicación $\theta : \mathscr{P} \longrightarrow \mathbb{F}[X_1,\dots,X_n]$ mediante
  (1) $\theta(X_i) = X_i$, para cada $X_i \in P_0$.
  (2) $\theta(f(A_{i_1},\dots,A_{i_d})) = f(\theta(A_{i_1}),\dots,\theta(A_{i_d}))$, para cada $f(A_{i_1},\dots,A_{i_d}) \in \mathscr{P}\setminus P_0$.

Ejemplo. 66.3.
(1) Si $f = \neg$, se tiene $\theta(\neg(X)) = \sum_{a\in\mathbb{F}} \neg(a)G_a(X) = G_1(X) = -X$. Para $A \in \mathscr{P}$ se tiene $\theta(\neg A) = -\theta(A)$.
(2) Si $f = \vee$, se tiene

$$\theta(X\vee Y) = \sum_{(a,b)\in\mathbb{F}^2} \vee(a,b)G_a(X)G_b(Y) = X+Y+XY.$$

Para $A,B \in \mathscr{P}$ se tiene $\theta(A\vee B) = \theta(A)+\theta(B)+\theta(A)\theta(B)$.
(3) Si $f = \wedge$, para $A,B \in \mathscr{P}$ se tiene $\theta(A\wedge B) = \theta(A)\theta(B)$.
(4) Si $f = \rightarrow$, para $A,B \in \mathscr{P}$ se tiene $\theta(A\rightarrow B) = \theta(A)\theta(B)+\theta(A)+1$.
(5) Si $f = \leftrightarrow$, para $A,B \in \mathscr{P}$ se tiene $\theta(A\leftrightarrow B) = \theta(A)\theta(B)+1$.

Es posible caracterizar cuando un polinomio $F \in \mathbb{F}[X_1,\dots,X_n]$ pertenece al ideal $(X_1^2-X_1,\dots,X_n^2-X_n)$. Ver el siguiente resultado:

Lema. 66.4.
Sea $F \in \mathbb{F}[X_1,\dots,X_n]$, son equivalentes:
(a) $F \in (X_1^2-X_1,\dots,X_n^2-X_n)$.
(b) $v(F) = 0$ *para cada valoración* v.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si se tiene $F \in (X_1^2-X_1,\dots,X_n^2-X_n)$, como $v(X_i^2-X_i) = 0$, se tiene $v(F) = 0$ para cada valoración v.
(b) $\Rightarrow$ (a). Para cada $i \in \{1,\dots,n\}$ consideramos la valoración v_i definida por $v_i(X_j) = \delta_{ij}$. Como $\mathrm{Ker}(v) = (X_1,\dots,X_{i-1},X_i^2-X_i,X_{i+1},\dots,X_n)$, se tiene $f \in (X_1,\dots,X_{i-1},X_i^2-X_i,X_{i+1},\dots,X_n)$, y por tanto $F \in \cap_{i=1}^n (X_1,\dots,X_{i-1},X_i^2-X_i,X_{i+1},\dots,X_n) = (X_1^2-X_1,\dots,X_n^2-X_n)$. □

Como consecuencia tenemos una caracterización de las tautologías.

Teorema. 66.5.
Sea $A \in \mathscr{P}$, son equivalentes:
(a) $\models A$.
(b) $\theta(A)-1 \in (X_1^2-X_1,\dots,X_n^2-X_n)$.

DEMOSTRACIÓN. Se tiene las equivalencias:

$$\begin{aligned}\models A &\Leftrightarrow v(A)=1 \text{ para todo } v\\ &\Leftrightarrow v\theta(A)=1 \text{ para todo } v\\ &\Leftrightarrow v(\theta(A)-1)=0 \text{ para todo } v\\ &\Leftrightarrow \theta(A)-1 \in (X_1^2-X_1,\dots,X_n^2-X_n).\end{aligned}$$

□

De la misma forma podemos estudiar cuando A es una consecuencia lógica de un conjunto de proposiciones, esto es, cuando $\{B_1,\dots,B_m\} \models A$.
Primero veamos un resultado sobre el anillo de polinomios.

Lema. 66.6.
Sean $G, F_1,\dots,F_m$ polinomios en $\mathbb{F}[X_1,\dots,X_n]$, son equivalentes:
(a) $v(F_1)=\cdots=v(F_m)=0$ *implica* $v(G)=0$ *para toda valoración* v.
(b) $v((G+F_1+\cdots+F_m)(F_1-1)\cdots(F_m-1))=0$ *para toda valoración* v.
(c) $(G+F_1+\cdots+F_m)(F_1-1)\cdots(F_m-1) \in (X_1^2-X_1,\dots,X_n^2-X_n)$.
(d) $G \in (F_1,\dots,F_m,X_1^2-X_1,\dots,X_n^2-X_n)$.

DEMOSTRACIÓN. (a) ⇒ (b). Es inmediato, ya que v es un homomorfismo de anillos.
(b) ⇒ (c). Es consecuencia del Lema (66.4.).
(c) ⇒ (d). Basta desarrollar la expresión.
(d) ⇒ (a). Es similar al Lema (66.4.). □

Ahora podemos establecer el resultado sobre la consecuencia lógica.

Teorema. 66.7.
Sean $A, B_1,\dots,B_m \in \mathscr{P}$, son equivalentes:
(a) $\{B_1,\dots,B_m\} \models A$.
(b) $\theta(A)-1 \in (\theta(B_1)-1,\dots,\theta(B_m)-1,X_1^2-X_1,\dots,X_n^2-X_n)$.

DEMOSTRACIÓN. Se tiene las equivalencias:

$$\begin{aligned}\{B_1,\dots,B_m\}\models A &\Leftrightarrow \text{ si } \nu(B_1)=\cdots=\nu(B_m)=0 \text{ entonces } \nu(A)=1 \text{ para todo } \nu\\ &\Leftrightarrow \text{ si } \nu\theta(B_1)=\cdots=\nu\theta(B_m)=1 \text{ entonces } \nu\theta(A)=1 \text{ para todo } \nu\\ &\Leftrightarrow \text{ si } \nu(\theta(B_1)-1)=\cdots=\nu(\theta(B_m)-1)= \text{ entonces } \nu(\theta(A)-1)=0 \text{ para todo } \nu\\ &\Leftrightarrow \theta(A)-1\in(\theta(B_1)-1,\dots,\theta(B_m)-1,X_1^2-X_1,\dots,X_n^2-X_n).\end{aligned}$$

□

Ejercicio. 66.8.
Prueba que $A\vee(\neg A)$ es una tautología para cada $A\in\mathscr{P}$.

SOLUCIÓN. Tenemos

$$\begin{aligned}\theta(A\vee(\neg A)&=\theta(A)+\theta(\neg A)+\theta(A)\theta(\neg A)\\ &=\theta(A)+\theta(A)+1+\theta(A)(\theta(A)+1)\\ &=\theta(A)^2+\theta(A)+1.\end{aligned}$$

para cada polinomio $F\in\mathbb{F}[X_1,\dots,X_n]$ se verifica $F^2-F\in(X_1^2-X_1,\dots,X_n^2-X_n)$, ya que F es un cuerpo de característica 2, y $(X^i)^2-X^i=X^i(X^i-1)=X^i(X-1)(X^{i-1}+\cdots+X+1)$, si $i\geq 1$. □

Ejercicio. 66.9.
Prueba que $P=((A\to B)\wedge(B\to C))\to(A\to C)$ es una tautología, para cada $A,B\in\mathscr{P}$.

SOLUCIÓN. Para simplificar llamamos $a=\theta(A)$, $b=\theta(B)$ y $c=\theta(C)$, se tiene entonces

$$\begin{aligned}&\theta(((A\to B)\wedge(B\to C))\to(A\to C))\\ =&(ab+a+1)(bc+b+1)(ac+a+1)+(ab+a+1)(bc+b+1)+1\\ =&a^2b^2c^2+a^2b^2+a^2bc^2+a^2bc+a^2c+a^2+abc^2+ab+ac+a+1.\end{aligned}$$

Tenemos que ver si $\theta(P)-1=a^2b^2c^2+a^2b^2+a^2bc^2+a^2bc+a^2c+a^2+abc^2+ab+ac+a$ es un elemento de $(X_1^2-X_1,\dots,X_n^2-X_n)$, para ello basta ver que el resto de la división por $\{a^2-a,b^2-b,c^2-c\}$ es cero. En este caso tenemos que

```
PolynomialReduce[a^2b^2c^2+a^2b^2+a^2bc^2+a^2bc+a^2c+a^2+abc^2+ab+ac+a,
    {a^2-a,b^2-b,c^2-c},{a,b,c},Modulus->2]
```

da como solución

$$\left\{\left\{b^2c^2+b^2+bc^2+bc+c+1,ac^2+a,ab\right\},0\right\}$$

por tanto P es una tautología. □

Ejercicio. 66.10.
Si $U = C \to A$, $V_1 = A \to B$ y $V_2 = B \to C$, estudia si U es una consecuencia lógica de $\{V_1, V_2\}$.

SOLUCIÓN. Al igual que antes utilizamos a, b, c. Se tiene:

$$\begin{aligned}\theta(U) &= \theta(C \to A) = ca + c + 1,\\ \theta(V_1) &= \theta(A \to B) = ab + a + 1,\\ \theta(V_2) &= \theta(B \to C) = bc + b + 1.\end{aligned}$$

por lo tanto tenemos que comprobar si $\theta(U) - 1 \in (\theta(V_1) - 1, \theta(V_2) - 1, X_1^2 - X_1, \ldots, X_n^2 - X_n)$. Esto es, si

$$ca + c \in (ab + a, bc + b, X_1^2 - X_1, \ldots, X_n^2 - X_n).$$

En nuestro caso se tiene que

```
GB=GroebnerBasis[{ab+a,bc+b,a^2-a,b^2-b,c^2-c},{a,b,c},Modulus->2]
```

Luego la base de Groebner es:

$$\left\{c^2 + c, b^2 + b, a^2 + a, bc + b, ac + a, ab + a\right\},$$

y el resto es

```
PolynomialReduce[ca+c,GB,{a,b,c},Modulus->2]
```

da como resultado

$$\{\{0, 0, 0, 1, 0, 0\}, a + c\},$$

por tanto U no es una consecuencia lógica de $\{V_1, V_2\}$. □

Ejercicio. 66.11.
Sea $V = A \wedge B$ y $U = A \vee B$. Prueba que U es una consecuencia lógica de V, para todos $A, B \in \mathscr{P}$.

SOLUCIÓN. Tenemos:

$$\begin{aligned}\theta(U) &= ab + a + b,\\ \theta(V) &= ab.\end{aligned}$$

Tenemos que probar que $\theta(U) - 1 \in (\theta(V) - 1, X_1^2 - X_1, \ldots, X_n^2 - X_n)$, o equivalentemente que $ab + a + b - 1 \in (ab - 1, X_1^2 - X_1, \ldots, X_n^2 - X_n)$.
Primero calculamos una base de Groebner de $(ab - 1, a^2 - a, b^2 - b)$

```
GroebnerBasis[{ab-1,a^2-a,b^2-b},{a,b},Modulus->2]
```

Luego, una base de Groebner es:

$$GB = \{1 + b, 1 + a\},$$

y el resto es:

```
PolynomialReduce[ab+a+b+1,GB,{a,b},Modulus->2]
```

que da el resultado

$$\{\{a + 1, 0\}, 0\}$$

Por tanto U es una consecuencia lógica de V. □

67. Polinomios simétricos

Si consideramos el anillo de polinomios $K[X_1,\dots,X_n]$, para cada $\sigma \in S_n$, el grupo simétrico, definimos un automorfismo

$$\varphi_\sigma : K[X_1,\dots,X_n] \longrightarrow K[X_1,\dots,X_n], \quad \varphi(X_i) = X_{\sigma(i)}, \quad i \in \{1,\dots,n\}.$$

Tenemos así un homomorfismo inyectivo de grupos de S_n a $\mathrm{Aut}(K[X_1,\dots,X_n])$, ya que para $\sigma_1, \sigma_2 \in S_n$ se verifica $\varphi_{\sigma_1}\varphi_{\sigma_2} = \varphi_{\sigma_1\sigma_2}$, por lo que podemos identificar S_n con su imagen en $\mathrm{Aut}(K[X_1,\dots,X_n])$.
Para cada grupo $G \subseteq \mathrm{Aut}(K[X_1,\dots,X_n])$ definimos

$$K[X_1,\dots,X_n]^G = \{F \in K[X_1,\dots,X_n] \mid \varphi(F) = F, \text{ para cada } \varphi \in G\}.$$

Se tiene que $K[X_1,\dots,X_n]^G$ es un subanillo de $K[X_1,\dots,X_n]$ al que llamamos el **subanillo G–invariante** de $K[X_1,\dots,X_n]$, cada $F \in K[X_1,\dots,X_n]$ se llama **polinomio G–invariante**.
En el caso en el que $G = S_n$ los polinomios S_n–invariantes se llaman **polinomios simétricos**, y representamos $K[X_1,\dots,X_n]^{S_n}$ por $\mathrm{Sim}(K[X_1,\dots,X_n])$.
Llamamos **polinomio simétrico elemental** de grado uno al polinomio

$$E_1 = X_1 + \cdots + X_n,$$

polinomio simétrico elemental del grado dos al polinomio

$$E_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n = \sum_{i<j} X_iX_j.$$

En general llamamos **polinomio simétrico elemental** de grado $r \le n$ al polinomio

$$E_r = X_1X_2\cdots X_r + X_1X_2\cdots X_{r+1} + \cdots + X_{n-s+1}\cdots X_n = \sum_{i_1<i_2<\cdots<i_r} X_{i_1}\cdots X_{i_s}.$$

Un polinomio $F \in K[X_1,\dots,X_n]$ se llama **homogéneo** si todos sus monomios tienen el mismo grado total, esto es, si $F = \sum_\alpha c_\alpha X^\alpha$, con $\alpha \in \mathbb{N}^n$, entonces $\sum_{i=1}^n \alpha_i$ es el mismo para todo α con $c_\alpha \neq 0$.
Es claro que todo polinomio $F \in K[X_1,\dots,X_n]$ se puede escribir de forma única como una suma de polinomios homogéneos.
El problema planteado es probar que todo polinomio simétricos se puede escribir como un polinomio en los polinomios simétricos elementales, esto es, si llamamos $\mathrm{Sim}(K[X_1,\dots,X_n])$ al conjunto de los polinomio simétricos. Se tiene:

Teorema. 67.1.
(1) Sim$(K[X_1,\dots,X_n])$ es un subanillo de $K[X_1,\dots,X_n]$.
(2) Sim$(K[X_1,\dots,X_n]) = K[E_1,\dots,E_n]$.

1132-09.tex

Aproximación por división de polinomios

Al trabajar con el anillo de polinomios $K[X_1,\dots,X_n]$ con el orden lexicográfico para $X_1 > \cdots > X_n$, un término $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ se llama **decreciente** si verifica $\alpha_1 \geq \cdots \geq X_n$. Ver [4].
Tenemos un primer resultado sobre polinomios simétricos.

Lema. 67.2.
Si $F \in K[X_1,\dots,X_n]$ es un polinomio simétrico, entonces $\mathrm{lt}(F)$ *es decreciente.*

DEMOSTRACIÓN. Si $\mathrm{lt}(F) = X_1^{\alpha_1}\cdots X_n^{\alpha_n}$, y se tiene $\alpha_1 \geq \cdots \geq \alpha_j < \alpha_{j+1}$, entonces tenemos que $X_1^{\alpha_1}\cdots X_j^{\alpha_j}X_{j+1}^{\alpha_{j+1}}\cdots X_n^{\alpha_n} < X_1^{\alpha_1}\cdots X_j^{\alpha_{j+1}}X_{j+1}^{\alpha_j}\cdots X_n^{\alpha_n}$, lo que es una contradicción, pues ambos son términos de F, y el primero es el líder. □

Ejemplo. 67.3.
Para los polinomios simétricos elementales se tiene:

$$\begin{aligned}&\mathrm{lt}(E_1) = X_1,\\ &\mathrm{lt}(E_2) = X_1X_2,\\ &\dots\\ &\mathrm{lt}(E_i) = X_1\cdots X_i, \text{ para cada } 1 \leq i \leq n.\end{aligned}$$

Lema. 67.4.
Para cada término decreciente $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ se tiene

$$\mathrm{lt}(E_1^{\alpha_1-\alpha_2}\cdots E_{n-1}^{\alpha_{n-1}-\alpha_n}E_n^{\alpha_n}) = X_1^{\alpha_1}\cdots X_n^{\alpha_n}.$$

DEMOSTRACIÓN. Se tiene:

$$\begin{aligned}\mathrm{lt}(E_1^{\alpha_1-\alpha_2}\cdots E_{n-1}^{\alpha_{n-1}-\alpha_n}E_n^{\alpha_n}) &= \mathrm{lt}(E_1)^{\alpha_1-\alpha_2}\cdots\mathrm{lt}(E_{n-1})^{\alpha_{n-1}-\alpha_n}\,\mathrm{lt}(E_n)^{\alpha_n}\\ &= X_1^{\alpha_1-\alpha_2}(X_1X_2)^{\alpha_2-\alpha_3}\cdots(X_1\cdots X_{n-1})^{\alpha_{n-1}-\alpha_n}(X_1\cdots X_n)^{\alpha_n}\\ &= X_1^{\alpha_1}\cdots X_n^{\alpha_n}.\end{aligned}$$

□

Para cada término decreciente $T = X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ llamamos F_T al polinomio $E_1^{\alpha_1-\alpha_2}\cdots E_{n-1}^{\alpha_{n-1}-\alpha_n}E_n^{\alpha_n}$. Éste es un polinomio simétrico con termino líder $T = X_1^{\alpha_1}\cdots X_n^{\alpha_n}$. También podemos representar F_T por $F_{(\alpha_1,\dots,\alpha_n)}$.

Dado un polinomio F consideramos el diagrama de Newton decreciente de F

$$\mathscr{N}_D(F) = \{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0 \text{ y } X^\alpha \text{ es decreciente}\}.$$

Dados dos polinomios $F, G \in K[X_1, \ldots, X_n]$, decimos que G es una **reducción simétrica** de F si existe $\alpha \in \mathscr{N}_D(F)$ tal que $G = F - a_\alpha F_\alpha$. En este caso decimos que F es **simétricamente reducible**.

Lema. 67.5.
Un polinomio $F \in K[X_1, \ldots, X_n]$ es simétricamente reducible si, y solo si, tiene un término decreciente.

Dados dos polinomios $F, G \in K[X_1, \ldots, X_n]$ tales que existen polinomios $G_0 = F, G_1, \ldots, G_t = G$, en los que G_{i+1} es una reducción simétrica de G_i, para $i = 0, \ldots, t-1$, diremos que G es una **reducción simétrica iterada** de F.

Lema. 67.6.
Dado un polinomio $F \in K[X_1, \ldots, X_n]$ simétrico y no nulo, se tiene que 0 es una reducción simétrica iterada de F.

Proposición. 67.7.
Dados dos polinomios $F, G \in K[X_1, \ldots, X_n]$, son equivalentes:

(a) G es una reducción simétrica iterada de F.
(b) Existe un polinomio $H \in K[X_1, \ldots, X_n]$ tal que $G = F - H(E_1, \ldots, E_n)$

Teorema. 67.8. (Teorema fundamental de los polinomios simétricos)
Dado $F \in K[X_1, \ldots, X_n]$, son equivalentes:

(a) F is simétrico.
(b) 0 es una reducción simétrica iterada de F.
(c) Existe $H \in K[X_1, \ldots, X_n]$ tal que $F = H(E_1, \ldots, E_n)$.