Curso: Degeneraciones Tóricas

Lara Bossinger

Universidad Nacional Autónoma de México, Unidad Oaxaca

Septiembre 6 2022

§1 Bases de Gröbner

Contenido

Ordenes parciales y totales

Definición (§2.1.2 HH)

Para un conjunto P un orden parcial es una relación $\leq$ en P tal que para todos $x, y, z \in P$ tenemos

1. $x \leq x$ *(reflexividad);*
2. $x \leq y$ *y* $y \leq x$ *implica* $x = y$ *(antisimetría);*
3. $x \leq y$ *y* $y \leq z$ *implica* $x \leq z$ *(transitividad).*

Un orden total en P es un orden parcial tal que para todos $x, y \in P$ tenemos $x \leq y$ o $y \leq x$.

Monomios y ordenes monomiales

Sea k un campo y $S = k[x_1, \ldots, x_n]$ el anillo de polinomios en las variables $x_1, \ldots, x_n$. Los monomios en S son elementos de la forma

$$x^a := x_1^{a_1} \cdots x_n^{a_n}, \quad \text{con} \quad a = (a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0}.$$

Sea $\mathrm{Mon}(S) \subset S$ el conjunto de monomios.

Monomios y ordenes monomiales

Sea k un campo y $S = k[x_1, \dots, x_n]$ el anillo de polinomios en las variables $x_1, \dots, x_n$. Los monomios en S son elementos de la forma

$$x^a := x_1^{a_1} \cdots x_n^{a_n}, \quad \text{con} \quad a = (a_1, \dots, a_n) \in \mathbb{Z}^n_{\geq 0}.$$

Sea $\mathrm{Mon}(S) \subset S$ el conjunto de monomios.

Definición

Un orden parcial en $Mon(S)$ se llama un buen orden si cumple

1. $1 \leq x^a$ *para todos* $1 \neq x^a \in Mon$;
2. *si* $x^a, x^b \in Mon$ *y* $x^a < x^b$ *también* $x^a x^c < x^b x^c \ \ \forall \ \ x^c \in Mon$.

Un orden monomial (o también orden de términos/monomios) es un orden total que es un buen orden.

El orden lexicografico y lexicografico reverso

El orden lexicografico $<_{lex}$ es el orden monomial definido como $x^a <_{lex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.

El orden lexicografico y lexicografico reverso

El orden lexicografico $<_{lex}$ es el orden monomial definido como $x^a <_{lex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.
El orden lexicografico graduado $<_{deglex}$ es el orden monomial definido como $x^a <_{deglex} x^b$ si y solo si

1. $\sum_{i=1}^{n} a_i < \sum_{i=1}^{n} b_i$, o
2. $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ y $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.

El orden lexicografico y lexicografico reverso

El orden lexicografico $<_{lex}$ es el orden monomial definido como $x^a <_{lex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.

El orden lexicografico graduado $<_{deglex}$ es el orden monomial definido como $x^a <_{deglex} x^b$ si y solo si

1. $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$, o
2. $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ y $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.

El orden lexicografico reverso $<_{revlex}$ es el orden monomial definido como $x^a <_{revlex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \max\{i : a_i - b_i \neq 0\}$.

Ejercicio 1

1. *¿Puedes dar una definición del orden lexicografico reverso graduado* $<_{degrevlex}$*?*

El orden lexicografico y lexicografico reverso

El orden lexicografico $<_{lex}$ es el orden monomial definido como $x^a <_{lex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.

El orden lexicografico graduado $<_{deglex}$ es el orden monomial definido como $x^a <_{deglex} x^b$ si y solo si

1. $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$, o
2. $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ y $a_j - b_j < 0$ para $j = \min\{i : a_i - b_i \neq 0\}$.

El orden lexicografico reverso $<_{revlex}$ es el orden monomial definido como $x^a <_{revlex} x^b$ si y solo si $a_j - b_j < 0$ para $j = \max\{i : a_i - b_i \neq 0\}$.

Ejercicio 1

1. *¿Puedes dar una definición del orden lexicografico reverso graduado $<_{degrevlex}$?*
2. *Ordena todos los monomios de $k[x_1, x_2, x_3]$ con grado menos o igual a 3 con respeto a los ordenes $<_{lex}, <_{deglex}$ y $<_{revlex}, <_{degrevlex}$.*

Formas y ideales iniciales

Sea $<$ un orden de monomios y $f = \sum_{i=1}^{m} c_i x^{a_i} \in S$. Definimos el monomio inicial de f con respeto a $<$ como

$$in_<(f) := x^{a_j} \text{ con } x^{a_j} = \max_{<}\{x^{a_i} : c_i \neq 0\}.$$

El coeficiente principal es c_j y $c_j x^{a_j}$ es la forma inicia. Para un ideal $I \subset S$ definimos $in_<(I) := \langle in_<(f) : 0 \neq f \in I \rangle$, su ideal inicial con respeto a $<$.

Formas y ideales iniciales

Sea $<$ un orden de monomios y $f = \sum_{i=1}^{m} c_i x^{a_i} \in S$. Definimos el monomio inicial de f con respeto a $<$ como

$$in_<(f) := x^{a_j} \text{ con } x^{a_j} = \max_<\{x^{a_i} : c_i \neq 0\}.$$

El coeficiente principal es c_j y $c_j x^{a_j}$ es la forma inicia. Para un ideal $I \subset S$ definimos $in_<(I) := \langle in_<(f) : 0 \neq f \in I \rangle$, su ideal inicial con respeto a $<$.

Lema (Lema 2.1.4 HH)

Verifica lo siguiente para $x^a, x^b \in Mon$ y $f, g \in S$:

1. *si x^a divide x^b, entonces $x^a \leq x^b$;*
2. *$in_<(x^a f) = x^a in_<(f)$;*
3. *$in_<(fg) = in_<(f) in_<(g)$;*
4. *$in_<(f+g) \leq \max\{in_<(f), in_<(f)\}$ con igualdad si $in_<(f) \neq in_<(g)$.*

Prueba: Tarea.

Base de Gröbner

Definición (Definición 2.1.5 en HH)

Sea $I \subset S$ un ideal y $<$ un orden monomial. Un conjunto finito $\{g_1, \ldots, g_s\}$ de elementos en I se llama una base de Gröbner de I con respeto a $<$ si

$$in_<(I) = (in_<(g_1), \ldots, in_<(g_s)).$$

Base de Gröbner

Definición (Definición 2.1.5 en HH)

Sea $I \subset S$ un ideal y $<$ un orden monomial. Un conjunto finito $\{g_1, \ldots, g_s\}$ de elementos en I se llama una base de Gröbner de I con respeto a $<$ si

$$in_<(I) = (in_<(g_1), \ldots, in_<(g_s)).$$

Ejemplo

Sea $<=<_{lex}$ el orden lexicografico en $S = k[x_1, \ldots, x_7]$ con respeto a $x_1 > \cdots > x_7$ y sean $f = x_1x_4 - x_2x_3$ y $g = x_4x_7 - x_5x_6$. Entonces, $in_<(f) = x_1x_4$ y $in_<(g) = x_4x_7$. El conjunto $\{f, g\}$ no es una base de Gröbner para el ideal $I = (f, g)$:

Base de Gröbner

Definición (Definición 2.1.5 en HH)

Sea $I \subset S$ un ideal y $<$ un orden monomial. Un conjunto finito $\{g_1, \ldots, g_s\}$ de elementos en I se llama una base de Gröbner *de I con respeto a $<$ si*

$$in_<(I) = (in_<(g_1), \ldots, in_<(g_s)).$$

Ejemplo

Sea $< = <_{lex}$ el orden lexicografico en $S = k[x_1, \ldots, x_7]$ con respeto a $x_1 > \cdots > x_7$ y sean $f = x_1x_4 - x_2x_3$ y $g = x_4x_7 - x_5x_6$. Entonces, $in_<(f) = x_1x_4$ y $in_<(g) = x_4x_7$. El conjunto $\{f, g\}$ no es una base de Gröbner para el ideal $I = (f, g)$:

Toma $h = x_7f - x_1g$, pues $in_<(h) = x_1x_5x_6 \notin (in_<(f), in_<(g))$.

Ejercicios y Tareas

Ejercicio 2

Sea J un ideal generado de monomios $\{x^{a_1}, \dots, x^{a_t}\}$. Muestra que un monomio x^b pertenece a J si y solo si existe un monomio x^c tal que $x^b = x^c x^{a_i}$ para algún $1 \leq i \leq t$.

Ejercicios y Tareas

Ejercicio 2

Sea J un ideal generado de monomios $\{x^{a_1}, \ldots, x^{a_t}\}$. *Muestra que un monomio* x^b *pertenece a J si y solo si existe un monomio* x^c *tal que* $x^b = x^c x^{a_i}$ *para algún* $1 \leq i \leq t$.

Prueba: Proposición 1.1.5, HH.

Tarea 1 (Lema 2.1.7, HH)

Sea $<$ *un orden monomial. Prueba que para ningún* $x^a \in Mon$ *existe una secuencia infinita descendiente de la forma* $x^a = x^{a_0} > x^{a_1} > x^{a_2} > \ldots$.

Bases de Gröbner son conjuntos de generadores

Teorema (Teorema 2.1.8, HH)

Sea I un ideal en S y $G = \{g_1, \ldots, g_s\}$ una base de Gröbner de I con respeto a un orden monomial $<$. Entonces G es un conjunto de generadores para I.

Bases de Gröbner son conjuntos de generadores

Teorema (Teorema 2.1.8, HH)

Sea I un ideal en S y $G = \{g_1, \ldots, g_s\}$ una base de Gröbner de I con respeto a un orden monomial $<$. Entonces G es un conjunto de generadores para I.

Prueba: Vamos a mostrar que cada $f \in I$ es un elemento en el ideal (G) de manera algoritmica. El **Lema 2.1.7** asegura que nuestro algoritmo termina.

Bases de Gröbner son conjuntos de generadores

Teorema (Teorema 2.1.8, HH)

Sea I un ideal en S y $G = \{g_1, \ldots, g_s\}$ una base de Gröbner de I con respeto a un orden monomial $<$. Entonces G es un conjunto de generadores para I.

Prueba: Vamos a mostrar que cada $f \in I$ es un elemento en el ideal (G) de manera algoritmica. El **Lema 2.1.7** asegura que nuestro algoritmo termina.

Sea $0 \neq f \in I$, entonces $in_<(f) \in in_<(I) = (in_<(g_1), \ldots, in_<(g_s))$. En particular, existe un $g_{i_0} \in G$ tal que $in_<(g_{i_0})$ divide $in_<(f)$.
Sea $x^{a_0} \in \text{Mon}(S)$ tal que $in_<(f) = x^{a_0} in_<(g_{i_0})$.

Continuación: Definimos

$$h_0 = f - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0} \in I$$

donde c_0 y c_{i_0} son los coeficientes principales de f y de g_{i_0}. Nota que el monomio inicial de f ya no es presente en h_0. Con **Lema 2.1.4(2)** concluimos $in_<(x^{a_0} g_{i_0}) = x^{a_0} in_<(g_{i_0})$ que implica $in_<(h_0) < in_<(f)$. Si $h_0 = 0$ tenemos $f \in (g_1, \ldots, g_s)$.

Continuación: Definimos

$$h_0 = f - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0} \in I$$

donde c_0 y c_{i_0} son los coeficientes principales de f y de g_{i_0}. Nota que el monomio inicial de f ya no es presente en h_0. Con **Lema 2.1.4(2)** concluimos $in_<(x^{a_0} g_{i_0}) = x^{a_0} in_<(g_{i_0})$ que implica $in_<(h_0) < in_<(f)$. Si $h_0 = 0$ tenemos $f \in (g_1, \dots, g_s)$.Si $h_0 \neq 0$ continuamos con h_0 en el lugar de f. Obtenemos

$$h_1 = f - c_{i_1}^{-1} c_1 x^{a_1} g_{i_1} - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0},$$

donde $g_{i_1} \in G$ tal que $in_<(g_{i_1})$ divide $in_<(h_0) = c' x^{a_1} in_<(g_{i_1})$, con $c' \in k$. Además c_{i_1} y c_1 son los coeficientes principales de g_{i_1} y h_0. Como antes, $in_<(h_1) < in_<(h_0)$. Si $h_1 = 0$ tenemos $f \in (g_1, \dots, g_s)$. Si $h_1 \neq 0$ continuamos.

Continuación: Definimos

$$h_0 = f - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0} \in I$$

donde c_0 y c_{i_0} son los coeficientes principales de f y de g_{i_0}. Nota que el monomio inicial de f ya no es presente en h_0. Con **Lema 2.1.4(2)** concluimos $in_<(x^{a_0} g_{i_0}) = x^{a_0} in_<(g_{i_0})$ que implica $in_<(h_0) < in_<(f)$. Si $h_0 = 0$ tenemos $f \in (g_1, \dots, g_s)$.Si $h_0 \neq 0$ continuamos con h_0 en el lugar de f. Obtenemos

$$h_1 = f - c_{i_1}^{-1} c_1 x^{a_1} g_{i_1} - c_{i_0}^{-1} c_0 x^{a_0} g_{i_0},$$

donde $g_{i_1} \in G$ tal que $in_<(g_{i_1})$ divide $in_<(h_0) = c' x^{a_1} in_<(g_{i_1})$, con $c' \in k$. Además c_{i_1} y c_1 son los coeficientes principales de g_{i_1} y h_0. Como antes, $in_<(h_1) < in_<(h_0)$. Si $h_1 = 0$ tenemos $f \in (g_1, \dots, g_s)$. Si $h_1 \neq 0$ continuamos.

Como no existen secuencias descendentes infinitas este procedimiento termina después de $N >> 0$ pasos y nos da una expresión

$$f = \sum_{q=0}^{N} c_{i_q}^{-1} c_q x^{a_q} g_{i_q} \in (g_1, \dots, g_s). \qquad \blacksquare$$

El teorema de la base de Hilbert

Como corolario inmediatamente obtenemos el famoso resultado de Hilbert:

Teorema de la base de Hilbert (Corolario 2.1.9, HH)

Cada ideal en el anillo de polinomios tiene un conjunto de generadores finito.

§2 Algoritmos

Contenido

El Algoritmo de división

Algoritmo de división (Teorema 2.2.1, HH)

Sean $<$ *un orden de monomios en* S *y* $g_1, \ldots, g_s \in S$ *no cero. Para cada polinomio* $f \in S$ *existen polinomios* $f_1, \ldots, f_s, f' \in S$ *con*

$$f = f_1 g_1 + f_2 g_2 + \cdots + f_s g_s + f', \quad \textit{tal que}$$

El Algoritmo de división

Algoritmo de división (Teorema 2.2.1, HH)

Sean $<$ *un orden de monomios en* S *y* $g_1, \ldots, g_s \in S$ *no cero. Para cada polinomio* $f \in S$ *existen polinomios* $f_1, \ldots, f_s, f' \in S$ *con*

$$f = f_1 g_1 + f_2 g_2 + \cdots + f_s g_s + f', \quad \textit{tal que}$$

1. *si* $f' \neq 0$ *tenemos para cada* x^a *monomio de* f' *que* $x^a \notin (in_<(g_1), \ldots, in_<(g_s))$*;*
2. *si* $f_i \neq 0$ *tenemos* $in_<(f) \geq in_<(f_i g_i)$.

El Algoritmo de división

Algoritmo de división (Teorema 2.2.1, HH)

Sean $<$ un orden de monomios en S y $g_1, \ldots, g_s \in S$ no cero. Para cada polinomio $f \in S$ existen polinomios $f_1, \ldots, f_s, f' \in S$ con

$$f = f_1 g_1 + f_2 g_2 + \cdots + f_s g_s + f', \quad \textit{tal que}$$

1. *si $f' \neq 0$ tenemos para cada x^a monomio de f' que $x^a \notin (in_<(g_1), \ldots, in_<(g_s))$;*
2. *si $f_i \neq 0$ tenemos $in_<(f) \geq in_<(f_i g_i)$.*

La expresión $f_1 g_1 + f_2 g_2 + \cdots + f_s g_s + f'$ de f se llama expresión estándar de f con respeto a $g_1, \ldots, g_s$. El polinomio f' se llama el resto de f con respeto a $g_1, \ldots, g_s$. Si $f' = 0$ digamos que f se reduce a cero con respeto a $\{g_1, \ldots, g_s\}$.

Prueba del Teorema 2.2.1

Como en la prueba del Teorema 1 vamos a usar el **Lema 2.1.7** y proceder de manera algorítmica.

Sea $I := (in_<(g_1), \ldots, in_<(g_s))$. Si ningún monomio de f esta en I toma $f' = f$ y $f_1 = \cdots = f_s = 0$.

Prueba del Teorema 2.2.1

Como en la prueba del Teorema 1 vamos a usar el **Lema 2.1.7** y proceder de manera algorítmica.

Sea $I := (in_<(g_1), \ldots, in_<(g_s))$. Si ningún monomio de f esta en I toma $f' = f$ y $f_1 = \cdots = f_s = 0$.

Supongamos que existe un monomio $x^a \in \text{supp}(f) \cap I$ y sea x^{a_0} el monomio más grande (con respeto a $<$) en $\text{supp}(f) \cap I$. Entonces, existe un g_{i_0} y un monomio x^{b_0} tal que $in_<(g_{i_0})x^{b_0} = x^{a_0}$. Escribimos

$$f = c_0' c_{i_0}^{-1} x^{b_0} g_{i_0} + h_1$$

donde c_0' es el coeficiente de x^{a_0} en f y c_{i_0} es el coeficiente principal de g_{i_0}.

Prueba del Teorema 2.2.1

Como en la prueba del Teorema 1 vamos a usar el **Lema 2.1.7** y proceder de manera algorítmica.

Sea $I := (in_<(g_1), \dots, in_<(g_s))$. Si ningún monomio de f esta en I toma $f' = f$ y $f_1 = \cdots = f_s = 0$.
Supongamos que existe un monomio $x^a \in \mathrm{supp}(f) \cap I$ y sea x^{a_0} el monomio más grande (con respeto a $<$) en $\mathrm{supp}(f) \cap I$. Entonces, existe un g_{i_0} y un monomio x^{b_0} tal que $in_<(g_{i_0})x^{b_0} = x^{a_0}$. Escribimos

$$f = c_0' c_{i_0}^{-1} x^{b_0} g_{i_0} + h_1$$

donde c_0' es el coeficiente de x^{a_0} en f y c_{i_0} es el coeficiente principal de g_{i_0}.
Entonces,

$$in_<(x^{b_0} g_{i_0}) = x^{b_0} in_<(g_{i_0}) = x^{a_0} \leq in_<(f).$$

Si $h_1 = 0$, o $h_1 \neq 0$ y $\mathrm{supp}(h_1) \cap I = \varnothing$, entonces $f = c_0' c_{i_0}^{-1} x^{b_0} g_{i_0} + h_1$ es una expresión estándar de f con respeto a $g_1, \dots, g_s$.

Continuación de la Prueba del Teorema 2.2.1

Falta el caso: $h_1 \neq 0$ y existe un monomio de h_1 que esta en I.

Sea x^{a_1} el monomio más grande en $\mathrm{supp}(h_1) \cap I$. Tenemos $x^{a_0} > x^{a_1}$.
Ningún monomio en $\mathrm{supp}(h_1) \cap I$ puede ser más grande que x^{a_0}; además $x^{a_0} \notin \mathrm{supp}(h_1)$.
Seguimos como antes y obtenemos una expresión

$$f = c_0' c_{i_0}^{-1} x^{b_0} g_{i_0} + c_1' c_{i_1}^{-1} x^{b_1} g_{i_1} + h_2$$

donde $x^{a_0} = x^{b_0} in_<(g_{i_1})$ para algún $g_{i_1} \in \{g_1, \ldots, g_s\}$, c_1' es el coeficiente de x^{a_1} en f y c_{i_1} es el coeficiente principal de g_{i_1}. Tenemos

$$in_<(x^{b_1} g_{i_1}) < in_<(x^{b_0} g_{i_0}) \leq in_<(f).$$

Continuando obtenemos una secuencia *finita* (**Lema 2.1.7**)
$x^{a_0} > x^{a_1} > x^{a_2} > \cdots > x^{a_N}$.

Tarea 2

Verifica que la secuencia nos da una expresión estándar de f con respeto a $g_1, \ldots, g_s$.

Ejemplo: (no) unicidad del resto

Ejercicio 3

Sean $g_1 = x^2 - z, g_2 = xy - 1 \in k[x, y, z]$ *con orden* $<_{lex}$ *inducida por* $x > y > z$*. Verifica que para* $f = x^3 - x^2y - x^2 - 1$ *las siguientes dos expresiones son estándar con respecto a* $\{g_1, g_2\}$ *y* $<$*:*

1. $f = (x - 1)g_1 - xg_2 + (xz - x - z - 1)$,
2. $f = (x - y - 1)g_1 + (xz - yz - z - 1)$.

Ejemplo: (no) unicidad del resto

Ejercicio 3

Sean $g_1 = x^2 - z, g_2 = xy - 1 \in k[x, y, z]$ *con orden* $<_{lex}$ *inducida por* $x > y > z$. *Verifica que para* $f = x^3 - x^2y - x^2 - 1$ *las siguientes dos expresiones son estándar con respecto a* $\{g_1, g_2\}$ *y* $<$*:*

1. $f = (x-1)g_1 - xg_2 + (xz - x - z - 1)$,
2. $f = (x-y-1)g_1 + (xz - yz - z - 1)$.

- $f = f_1g_1 + f_2g_2 + \cdots + f_sg_s + f'$
- si $f' \neq 0$ tenemos para cada x^a monomio de f' que $x^a \notin (in_<(g_1), \ldots, in_<(g_s))$
- si $f_i \neq 0$ tenemos $in_<(f) \geq in_<(f_ig_i)$.

Bases de Gröbner y unicidad del resto

Lema (Lema 2.2.3 en HH)

Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ *es una base de Gröbner para* $I = (g_1, \ldots, g_s)$ *con respeto a* $<$*. En este caso cada polinomio* $f \in S$ *tiene un resto único con respeto a* $\mathcal{G}$*.*

Bases de Gröbner y unicidad del resto

Lema (Lema 2.2.3 en HH)

Sea $\mathcal{G} = \{g_1, \dots, g_s\}$ es una base de Gröbner para $I = (g_1, \dots, g_s)$ con respeto a $<$. En este caso cada polinomio $f \in S$ tiene un resto único con respeto a $\mathcal{G}$.

Prueba: Supongamos que existen dos restos $f' \neq f''$ de f con respeto a $\mathcal{G}$. Una consecuencia del Teorema 2 es que $f' - f'' \in I$. Entonces, $h := in_<(f' - f'') \in in_<(I)$. El monomio h es un monomio no cero en f' o f''. Pero f' y f'' son restos de f con respeto a $\mathcal{G}$. En particular, eso implica que ninguno de los monomios $in_<(g_1), \dots, in_<(g_s)$ divide h. Entonces, $h \notin (in_<(g_1), \dots, in_<(g_s))$, que es una contradicción. ■

Aplicación: Pertenencia a un ideal

El siguiente Corolario muestra la utilidad de bases de Gröbner para resolver el problema de la pertenencia a un ideal:

Corolario (Corolario 2.2.4, HH)

Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ *es una base de Gröbner para* $I = (g_1, \ldots, g_s)$ *con respeto a* $<$. *Entonces,* $f \in I$ *si y solo si el resto único de* f *con respeto a* $\mathcal{G}$ *es cero.*

Aplicación: Pertenencia a un ideal

El siguiente Corolario muestra la utilidad de bases de Gröbner para resolver el problema de la pertenencia a un ideal:

Corolario (Corolario 2.2.4, HH)

Sea $\mathcal{G} = \{g_1, \ldots, g_s\}$ es una base de Gröbner para $I = (g_1, \ldots, g_s)$ con respeto a $<$. Entonces, $f \in I$ si y solo si el resto único de f con respeto a $\mathcal{G}$ es cero.

Tarea 3

Muestra el Corolario 2.2.4.

Ejercicio 4

¿Conoces algún problema que se puede reformular como el problema de la pertenencia a un ideal? Si no, da le una búsqueda en google.

Referencias

1. Herzog, Jürgen; Hibi, Takayuki: Monomial ideals. Graduate Texts in Mathematics, 260. Springer-Verlag London, Ltd., London, 2011. xvi+305 pp. ISBN: 978-0-85729-105-9
2. Bernd Sturmfels: Gröbner bases and convex polytopes, Volume 8 of American Mathematical Soc.1996