DEPARTAMENTO DE MATEMÁTICA
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CONCEPCIÓN

Bases de Grobner

Natalia García
27 de febrero de 2009

1. Introducción

En este trabajo construiremos un algoritmo para la división en el anillo $k[x_1, \ldots, x_n]$, que será una generalización del algoritmo para la división en $k[x]$. Este tiene el problema que no es conmutativo ya que al dividir un polinomio f por otros $g_1, \ldots, g_s$ se obtienen distintos restos al cambiar el orden de los g_i. Las bases de Grobner tienen la propiedad que al dividir un polinomio por los elementos de esta se obtiene un resto único, sin importar el orden de división. Esto nos da variadas aplicaciones entre las que se encuentran decidir la pertenencia de un polinomio a un ideal y decidir igualdad de ideales.

2. Bases de Grobner

2.1. Órdenes monomiales

En el algoritmo de la división en $k[x]$ hay una noción de orden en los términos de los polinomios, dada por el grado. Si queremos extender este método para $k[x_1, \ldots, x_n]$, debemos encontrar una forma de ordenar unívocamente los términos de polinomios de más variables, que además sea compatible con su estructura.

Definición 2.1 *Un **monomio** sobre $k[x_1, \ldots, x_n]$ está definido por $x_1^{a_1} \cdot x_2^{a_2} \cdots x_n^{a_n}$, donde cada a_i es un entero no negativo. Representaremos a este monomio por medio del vector $(a_1, \ldots, a_n) \in \mathbb{N}^n$.*

Definición 2.2 *Un **orden** sobre un conjunto A es una relación reflexiva, antisimétrica y transitiva. Un orden $<$ sobre un conjunto A es un **orden total** si dados $a, b \in A$, entonces $a < b$, $b < a$ o $a = b$.*

Definición 2.3 *Un **orden monomial** $\prec$ sobre $k[x_1, \ldots x_n]$ es un orden total sobre los vectores $(a_1, \ldots, a_n) \in \mathbb{N}^n$, el cual satisface las siguientes condiciones:*

i) Para todo $a, b, c \in \mathbb{N}^n$, si $a \prec b$ entonces $a + c \prec b + c$.

ii) Es un buen orden sobre $\mathbb{N}^n$, es decir, todo conjunto no vacío de elementos de $\mathbb{N}^n$ tiene un elemento minimal.

Si $p = x_1^{a_1} \cdots x_n^{a_n}$, $q = x_1^{b_1} \cdots x_n^{b_n}$, algunos tipos de órdenes monomiales son:

- **Orden Lexicográfico (lex):** Aquí $q \prec p$ si en la resta $(a_1, \ldots, a_n) - (b_1, \ldots, b_n)$ la primera coordenada distinta de cero de izquierda a derecha es positiva.
- **Orden Lexicográfico Graduado (grlex):** Los monomios se ordenan por grado total, y las igualdades se resuelven usando el orden lexicográfico. Es decir, $q \prec p$ si $\sum a_i > \sum b_i$, o $\sum a_i = \sum b_i$ y en $(a_1, \ldots, a_n) - (b_1, \ldots, b_n)$ el primer término distinto de cero de izquierda a derecha es positivo.
- **Orden Lexicográfico Graduado Inverso (grevlex):** Los monomios se ordenan por grado total, y las igualdades se resuelven usando el orden lexicográfico inverso. Es decir, $q \prec p$ si $\sum a_i > \sum b_i$, o $\sum a_i = \sum b_i$ y en $(a_1, \ldots, a_n) - (b_1, \ldots, b_n)$ el primer término distinto de cero de derecha a izquierda es negativo.

Ejemplo 2.1 Ordenar los siguientes monomios en $k[x_1, x_2, x_3]$ con respecto a los órdenes monomiales Lexicográfico y Lexicográfico Graduado Inverso:

$$a = x_1^3 x_2 x_3^2 \quad b = x_2^5 x_3$$

Representando estos monomios como vectores de $\mathbb{N}^3$, vemos que en la resta $(3,1,2) - (0,5,1) = (3,-4,1)$ la primera coordenada distinta de cero de izquierda a derecha es positiva, así que con el orden lexicográfico tenemos que $b \prec a$. Ordenando con respecto al orden lexicográfico graduado inverso tenemos que $\sum a_i = 6 = \sum b_i$ por lo que debemos comparar a y b usando el orden lexicográfico inverso. Calculamos $a - b$, $(3,1,2) - (0,5,1) = (3,-4,1)$. La primera coordenada de derecha a izquierda es positiva, así que $a \prec b$.

Definición 2.4 *Sea $f = \sum c_a x_1^{a_1} \cdots x_n^{a_n}$ un polinomio distinto de cero, con $a = (a_1, \ldots, a_n)$. Usando un orden monomial fijo, definimos:*

- ***Multigrado:*** $mdeg(f) := \max(a \in \mathbb{N}^n | c_a \neq 0)$
- ***Coeficiente líder:*** $Lc(f) := c_{mdeg(f)}$
- ***Monomio líder:*** $Lm(f) := x^{mdeg(f)}$
- ***Término líder:*** $Lt(f) := Lc(f)Lm(f)$

Notar que lo definido varía al cambiar el orden monomial usado.

Definición 2.5 *Sea $I \subset k[x_1, \ldots, x_n]$ un ideal distinto del $\{0\}$.*

(i) Denotamos por $Lt(I)$ al conjunto de términos lider de elementos de I. Entonces,

$$Lt(I) = \{cx^a | existe\ f \in I\ con\ Lt(f) = cx^a\}$$

*(ii) $\langle LT(I) \rangle$ es el **ideal inicial de I**.*

2.2. Algoritmo de la división

Para encontrar un algoritmo de la división para $k[x_1, \ldots, x_n]$ probaremos utilizar una generalización del algoritmo de la división para $k[x]$.

Teorema 2.1 (Algoritmo de la división en $k[x_1, \ldots, x_n]$) *Sea $F = (f_1, \ldots, f_s)$ una s-upla ordenada de polinomios de $k[x_1, \ldots, x_n]$. Entonces cada $f \in k[x_1, \ldots, x_n]$ puede ser escrito como:*

$$f = a_1 f_1 + \ldots + a_s f_s + r$$

donde $a_i, r \in k[x_1, \ldots, x_n]$ y, o bien $r = 0$ o bien r es una combinación lineal de monomios con coeficientes en k, tal que ninguno de ellos es divisible por algun $Lt(f_1), \ldots, Lt(f_s)$. Llamaremos a r el resto de f dividido por F. Además, si $a_i f_i \neq 0$, se tiene $mdeg(f) \geq mdeg(a_i f_i)$

`Demostración:` Construimos un algoritmo para la división en $k[x_1, \ldots, x_n]$.
Con un orden monomial fijo, dividimos f en $(f_1, \ldots, f_s)$
Si $Lt(f_1)$ divide a $Lt(f)$, definimos $\bar{a}_1 = \frac{Lt(f)}{Lt(f_1)}$ y escribimos $f = \bar{a}_1 f_1 + h_1$
Si $Lt(f_1)$ divide a $Lt(h_1)$, $\bar{a}_2 = \frac{Lt(h_1)}{Lt(f_1)}$, $f = \bar{a}_1 f_1 + \bar{a}_2 f_1 + h_2$
Repetimos hasta $f = a_1 f_1 + r_1$ con $Lt(f_1)$ que no divide a $Lt(r_1)$.
Se repite lo anterior con r_1 y f_2. $r_1 = a_2 f_2 + r_2$ con $Lt(f_2)$ que no divide a $Lt(r_2)$.

$$\Rightarrow f = a_1 f_1 + a_2 f_2 + r_2$$

Continuamos con $f_3, \ldots, f_s$ y al resto r_s obtenido le aplicamos los pasos anteriores con $f_1, \ldots, f_s, f_1, \ldots$[†] hasta $f = a_1 f_1 + \ldots + a_s f_s + r^{(1)}$ (con distintos $a_1,\ a_2$), obteniendo $r^{(1)}$ tal que $Lt(f_i)$ no divide a $Lt(r^{(1)})$ para cualquier i.
Separamos $r^{(1)} = Lt(r^{(1)}) + r^{(2)}$
Se repite todo lo anterior para $r^{(2)}$. Si $r^{(3)}$ es el nuevo resto, $r^{(3)} = Lt(r^{(3)}) + r^{(4)}$, entonces

$$f = a_1 f_1 + \cdots + a_s f_s + Lt(r^{(1)}) + Lt(r^{(3)}) + r^{(4)}, \quad Lt(f_i) \nmid Lt(r^{(3)})\ \forall i$$

(con distintos a_i) Continuamos y obtenemos $f = a_1 f_1 + \cdots + a_s f_s + Lt(r^{(1)}) + Lt(r^{(3)}) + \cdots + Lt(r^{(m-1)}) + r^{(m)}$ (con distintos a_i), con $Lt(f_i) \nmid r^{(m+1)},\ \forall i$.
$r = Lt(r^{(1)}) + \cdots + Lt(r^{(m-1)}) + r^{(m)}$. Cuando no es cero, es combinación lineal de monomios a coeficientes en k tales que ninguno de ellos es divisible por $Lt(f_i)$ para todo i.
El algoritmo termina porque el orden en los monomios es un buen orden, y en cada división $h_i = \frac{Lt(h_i)}{Lt(g)} g + h_{i+1}$, tenemos que $h_{i+1} = h_i - \frac{Lt(h_i)}{Lt(g)} g$ donde los $Lt(h_i)$ se cancelan, por lo que $mdeg(h_{i+1}) < mdeg(h_i)$.
Para probar la relación entre $mdeg(f)$ y $mdeg(a_i f_i)$, vemos que cada término en a_i es de la forma $Lt(p)/Lt(f_i)$, para algún $p \in k[x_1, \ldots, x_n]$. El algoritmo comienza con $p = f$ y en la parte anterior probamos que en cada paso de la división el multigrado disminuye. Esto significa que todo monomio de a_i es menor o igual que $Lm(f)/Lm(f_i)$ con el orden monomial utilizado, en particular $Lm(a_i) \prec Lm(f)/Lm(f_i)$. Usando el hecho que $Lm(ab) \prec Lm(a)Lm(b)$, tenemos $Lm(a_i f_i) \prec Lm(f)$, lo que implica $mdeg(a_i f_i) \leq mdeg(f)$. □

† Debemos repetirlo con $f_1, \ldots, f_s$ porque al obtener r_i nos aseguramos que $Lt(r_i)$ no es divisible por $Lt(f_i)$, pero puede darse que sea divisible por $Lt(f_j)$, con $j < i$.

Ejemplo 2.2 Sean $f_1 = xy + 1$, $f_2 = y^2 - 1 \in k[x, y]$ con el orden lexicográfico. Dividiendo $f = xy^2 - x$ por $F_1 = \langle f_1, f_2 \rangle$

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$$

tenemos que el resto es $(-x - y)$. Dividiendo ahora por $F_2 = \langle f_2, f_1 \rangle$

$$xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$$

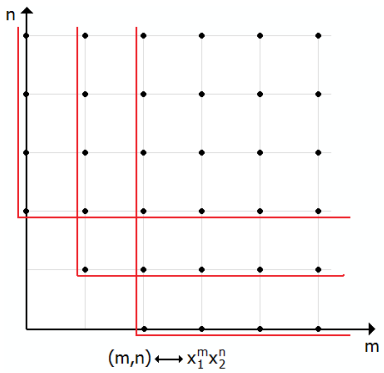
se obtiene que el resto es cero. El segundo cálculo nos dice que $f \in \langle f_1, f_2 \rangle$, pero del primer cálculo nos damos cuenta que un f puede pertenecer a un ideal y aun así su resto al ser dividido por los generadores de este puede ser no nulo. Para arreglar esta situación daremos a conocer un sistema de generadores del ideal para los cuales la condición necesaria y suficiente para que f pertenezca al ideal es que el resto al ser dividido por los elementos del sistema de generadores sea cero. Estos sistemas de generadores especiales se llaman las *Bases de Grobner.*

2.3. Bases de Grobner

Definición 2.6 *Un ideal $I \subset k[x_1, \ldots, x_n]$ es un* ***ideal monomial*** *si existe $A \subset \mathbb{N}^n$ (posiblemente infinito) de manera que I consiste de todos los polinomios que son sumas finitas de la forma $\sum_{a \in A} h_a x^a$, donde $h_a \in k[x_1, \ldots, x_n]$. En este caso, escribimos $I = \langle x^a | a \in A \rangle$.*

Lema 2.1 (de Dickson) (Teorema 5, §4, [1]) *Un ideal monomial $I = \langle x^a : a \in A \subset \mathbb{N}^n \rangle \subset k[x_1, \ldots, x_n]$ puede ser escrito de la forma $I = \langle x^{a_1}, \ldots, x^{a_s} \rangle$, donde $a_1, \ldots, a_s \in A$. En particular, I posee una base finita.*

`Demostración (en` $k[x, y]$`):` Monomios del ideal monomial se ven como copias del primer cuadrante trasladados. Por ejemplo, con $I = \left\{ x^a y^b | a + b \geq 2 \right\}$, cuyos generadores son x^2, xy, y^2, el esquema es:



Hablaremos de los vectores representantes y los monomios del ideal sin distinción. Sea I un ideal monomial. Podemos suponer que I no es vacío. Recorremos cada columna del retículo desde el eje m en forma creciente, comenzando con el eje n, borrando la columna si no encontramos monomios del ideal en ella. Cuando encontramos un monomio del ideal, lo

marcamos y dejamos de recorrerlas. Hacemos lo mismo con las filas, recorremos cada una desde el eje n comenzando con la de abajo y marcamos el primer monomio que encontremos. Siempre vamos a encontrar estos monomios porque $I \neq \phi$. Suponemos que los monomios marcados son $x^a y^b$, $x^c y^d$ respectivamente. Entonces todos los monomios de la forma $x^m y^n$ con $m \geq a$ y $n \geq b$, o $m \geq c$ y $n \geq d$ están en el ideal y son generados por alguno de los 2 monomios marcados. Los monomios con $m < a$ o $n < d$ no están en el ideal. Por lo tanto, si hay otro generador que no pueda ser generado por los dos anteriores, éste estará en el rectángulo de monomios que cumplen $a \leq m < c$ y $d \leq n < b$, el cual contiene una cantidad finita de posibilidades. □

Lema 2.2 *Sea $I \subset k[x_1, \ldots, x_n]$ un ideal. Entonces:*

- *$\langle Lt(I) \rangle$ es un ideal monomial.*
- *Existen $g_1, \ldots, g_s \in I$ tales que $\langle Lt(I) \rangle = \langle Lt(g_1), \ldots, Lt(g_s) \rangle$*

`Demostración:` $\langle Lm(g) : g \in I - \{0\} \rangle$ es un ideal monomial. Como cada $Lm(g)$ difiere sólo en una constante de $Lt(g)$, tenemos que $\langle Lm(g) : g \in I - \{0\} \rangle = \langle Lt(g) : g \in I - \{0\} \rangle = \langle Lt(I) \rangle$, luego $\langle Lt(I) \rangle$ es ideal monomial. Para la segunda parte, sabemos que $\langle Lt(I) \rangle = \langle Lm(I) \rangle$. Por el lema de Dickson, $\langle Lm(I) \rangle$ posee una base finita: $\langle Lm(g_1), \ldots, Lm(g_s) \rangle$. Como $Lm(g_i)$ difiere sólo por una constante de $Lt(g_i)$, se tiene que $\langle Lm(g_1), \ldots, Lm(g_s) \rangle = \langle Lt(g_1), \ldots, Lt(g_s) \rangle = \langle Lt(I) \rangle$. □

Definición 2.7 *Un subconjunto finito $S = \{g_1, \ldots, g_s\}$ de un ideal $I \subset k[x_1, \ldots, x_n]$ es una* ***base de Grobner*** *para I si $\langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle$*

Teorema 2.2 *Cada ideal $I \subset k[x_1, \ldots, x_n]$ distinto del $\{0\}$ posee una base de Grobner. Además, una base de Grobner para un ideal I es una base de I.*

`Demostración:` Dado el ideal I, por el Lema 2.2 existen $g_1, \ldots, g_s \in I$ tales que $\langle Lt(I) \rangle = \langle Lt(g_1), \ldots, Lt(g_s) \rangle$ que por definición es base de Grobner. Nos queda probar que $\langle g_1, \ldots, g_s \rangle$ e I son iguales. $\langle g_1, \ldots, g_s \rangle \subset I$ porque todos los $g_i \in I$. Sea $f \in I$ un polinomio. Si usamos el algoritmo de la división para dividir f por $\langle g_1, \ldots, g_s \rangle$, obtenemos una expresión de la forma

$$f = h_1 g_1 + \ldots + h_s g_s + r$$

con $h_i \in k[x_1, \ldots, x_n]$. Si $r \neq 0$, tenemos que $r = f - h_1 g_1 - \ldots - h_s g_s \in I$, esto implica que $Lt(r) \in \langle Lt(I) \rangle = \langle Lt(g_1), \ldots, Lt(g_s) \rangle$, luego $Lt(r)$ sería divisible por algún $Lt(g_i)$ lo que contradice el algoritmo de la división. Así, r debe valer cero y $f \in \langle g_1, \ldots, g_s \rangle$. Por lo tanto, $I = \langle g_1, \ldots, g_s \rangle$. □

Ejemplo 2.3 En $\mathbb{C}[x, y]$, $I = \langle x^2 - 1, y^2 - 1, x^2 - y \rangle$, $\mathcal{G} = \{g_1, g_2\}$, con $g_1 = x^2 - y$, $g_2 = y - 1$. Usaremos el orden lexicográfico. Probaremos que $\mathcal{G}$ es base de Grobner de I. Tenemos que $Lt(g_1) = x^2$, $Lt(g_2) = y$. $Lt(I) \supseteq \{x^2, y\}$, porque $x^2 - y \in I$ e $y - 1 = (x^2 - 1) - (x^2 - y) \in I$. Esto implica que $\langle Lt(I) \rangle \supseteq \langle x^2, y \rangle = \langle Lt(g_1), Lt(g_2) \rangle$.
Necesitamos probar $\langle Lt(I) \rangle \subseteq \langle Lt(g_1), Lt(g_2) \rangle$, que es equivalente a probar $\langle Lm(I) \rangle = \langle Lm(g_1), Lm(g_2) \rangle = \langle x^2, y \rangle$. Para probar esto último nos basta verificar que $Lm(I) \subseteq \langle Lm(g_1), Lm(g_2) \rangle$

Los únicos monomios que no están en $\langle Lm(g_1), Lm(g_2)\rangle$ son 1 y x. Como $\mathbb{V}(I) \supset \{(1,1),(-1,1)\}$ deducimos que $\mathbb{V}(I) \neq \phi$, lo que implica que $1 \notin I$.
Probaremos ahora que $x \notin Lm(I)$. Si no ocurre esto, $\exists p = x + q(y) \in I$.
Como $\mathbb{V}(I) \supset \{(1,1),(-1,1)\}$, $p(1,1) = 1 + q(1) = 0$ y $p(-1,1) = -1 + q(1) = 0$, entonces $1 + q(1) = 0 = -1 + q(1)$ lo que implica que $1 = -1$. Contradicción. Por lo tanto $x \notin Lm(I)$.
Como probamos que $\langle Lt(I)\rangle = \langle Lt(g_1), Lt(g_2)\rangle$ tenemos que $\mathcal{G}$ es base de Grobner de I.

3. Aplicaciones

3.1. Pertenencia de un f a un ideal

Teorema 3.1 *Sea $\mathcal{G} = \{f_1, \ldots, f_s\}$ una base de Grobner de un ideal I de $k[x_1, \ldots, x_n]$ y $f \in k[x_1, \ldots, x_n]$. Entonces, existe un único $r \in k[x_1, \ldots, x_n]$ con las dos propiedades siguientes:*

i) Si $r \neq 0$, entonces ningún término de r está en $\langle Lt(f_1), \ldots, Lt(f_s)\rangle$

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

En particular, r es el resto que produce el algoritmo de división de f entre $\mathcal{G}$ sin importar como se ordenen los elementos de $\mathcal{G}$

`Demostración:` Para demostrar la existencia de r usamos el algoritmo de la división en $k[x_1, \ldots, x_n]$. Tenemos que $f = g_1 f_1 + \ldots + g_s f_s + r$, para ciertos $g_i \in k[x_1, \ldots, x_n]$, con $i \in \{1, \ldots, s\}$, y $r \in k[x_1, \ldots, x_n]$ que verifican la primera condición.
Para la unicidad, sean $r, r' \in k[x_1, \ldots, x_n]$ tales que $f = g + r$, $f = g' + r'$, verificando i) y ii). Entonces $r - r' = g - g' \in I$. Si $r \neq r'$, se tiene que $Lt(r - r') \in \langle Lt(I)\rangle = \langle Lt(f_1), \ldots, Lt(f_s)\rangle$. Esto implica que algún término de r o de r' es divisible por algún $Lt(f_i)$, con $i \in \{1, \ldots, s\}$, lo cual contradice i). Luego, $r = r'$, y de aquí se deduce también la última parte del teorema. □

A partir del teorema anterior se deduce una condición para la pertenencia de un polinomio de $k[x_1, \ldots, x_n]$ en un ideal.

Corolario 3.1 *Sean $\mathcal{G} = \{f_1, \ldots, f_s\}$ una base de Grobner de un ideal $I \subset k[x_1, \ldots, x_n]$ y $f \in k[x_1, \ldots, x_n]$. Entonces, $f \in I$ si y sólo si el resto de la división de f entre $\mathcal{G}$ es cero.*

3.2. Igualdad de ideales

Sabemos que todo ideal I posee una base de Grobner, y además esa base genera I. Ahora queremos mostrar una forma de construirla. Para eso se utiliza el *Algoritmo de Buchberger.*

Definición 3.1 *Sean $f, g \in k[x_1, \ldots, x_n]$ polinomios no nulos.*

- *Si $mdeg(f) = (\alpha_1, \ldots, \alpha_n)$, $mdeg(g) = (\beta_1, \ldots, \beta_n)$ entonces $\gamma = (\gamma_1, \cdots, \gamma_n)$, donde $\gamma_i = \max(\alpha_i, \beta_i)$ para todo i. Llamamos a x^γ el **mínimo común múltiplo** de $Lm(f)$ y $Lm(g)$ y escribiremos $x^\gamma = mcm(Lm(f), Lm(g))$.*

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

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

Teorema 3.2 (Algoritmo de Buchberger) (Teorema 2, §7, [1]) *Sea $I = \langle f_1, \ldots, f_s \rangle \neq \langle 0 \rangle$ un ideal polinomial. Entonces una base de Grobner para I puede ser construida en un número finito de pasos a través del siguiente algoritmo, donde denotamos por $\bar{f}^F$ al resto de la división de f por F:*

Input: $F = (f_1, \ldots, f_s)$
Output: a Groebner basis $G = (g_1, \ldots, g_t)$ para I, con $F \subset G$

$G := F$
REPEAT
    G':=G
    FOR each pair $\{p, q\}$, $p \neq q$ in G' DO
        $S := \overline{S(p,q)}^{G'}$
        IF $S \neq 0$ THEN $G := G \cup \{S\}$
UNTIL $G = G'$

Ejemplo 3.1 *Buscaremos una base de Grobner para $I = \langle x^2 - 1, y^2 - 1, x^2 - y \rangle$ en $\mathbb{C}[x, y]$ con el orden lexicográfico. Tomamos $G' = (x^2 - 1, y^2 - 1, x^2 - y)$. Calculamos:*

$S(x^2 - 1, y^2 - 1) = \frac{x^2y^2}{x^2}(x^2 - 1) - \frac{x^2y^2}{y^2}(y^2 - 1) = x^2 - y^2$
$\overline{S(x^2 - 1, y^2 - 1)}^{G'} = 0$
$S(x^2 - 1, x^2 - y) = \frac{x^2}{x^2}(x^2 - 1) - \frac{x^2}{x^2}(x^2 - y) = y - 1$
$\overline{S(x^2 - 1, x^2 - y)}^{G'} = y - 1$
$S(y^2 - 1, x^2 - y) = \frac{x^2y^2}{y^2}(y^2 - 1) - \frac{x^2y^2}{x^2}(x^2 - y) = -x^2 + y^3$
$\overline{S(y^2 - 1, x^2 - y)}^{G'} = y - 1$

Como algunos S nos dieron distintos de 0, debemos agregarlos a G'. Entonces $G' = (x^2 - 1, y^2 - 1, x^2 - y, y - 1)$. De aquí tenemos $\overline{S(x^2 - 1, y^2 - 1)}^{G'} = 0$, $\overline{S(x^2 - 1, x^2 - y)}^{G'} = 0$ y $\overline{S(y^2 - 1, x^2 - y)}^{G'} = 0$. Los dos últimos dan cero porque ahora podemos dividir por $y - 1$. Nos falta calcular $\overline{S(x^2 - 1, y - 1)}^{G'}$, $\overline{S(y^2 - 1, y - 1)}^{G'}$ y $\overline{S(x^2 - y, y - 1)}^{G'}$:

$S(x^2 - 1, y - 1) = \frac{x^2y}{x^2}(x^2 - 1) - \frac{x^2y}{y}(y - 1) = x^2 - y$
$\overline{S(x^2 - 1, y - 1)}^{G'} = 0$
$S(y^2 - 1, y - 1) = \frac{y^2}{y^2}(y^2 - 1) - \frac{y^2}{y}(y - 1) = y - 1$
$\overline{S(y^2 - 1, y - 1)}^{G'} = 0$
$S(x^2 - y, y - 1) = \frac{x^2y}{x^2}(x^2 - y) - \frac{x^2y}{y}(y - 1) = x^2 - y^2$
$\overline{S(x^2 - y, y - 1)}^{G'} = 0$

Ahora que todos los S dan cero, podemos decir que $\{x^2-1, y^2-1, x^2-y, y-1\}$ es base de Grobner para I.

Lema 3.1 *Sea G una base de Grobner para el ideal polinomial I. Sea $p \in G$ un polinomio tal que $Lt(p) \in \langle Lt(G-\{p\})\rangle$. Entonces $G-\{p\}$ es también una base de Grobner para I.*

`Demostración:` Sabemos por definición de Base de Grobner que $\langle Lt(G)\rangle = \langle Lt(I)\rangle$. Si $\langle Lt(p)\rangle \in \langle Lt(G-\{p\})\rangle$, entonces $Lt(G-\{p\}) = Lt(G)$. Por definición, se deduce que $G-\{p\}$ es también una base de Grobner para I. $\square$

El algoritmo de Buchberger construye una base de Grobner, pero algunos de los generadores creados son innecesarios (comparar ejemplos 2.3 y 3.1). Para poder eliminar algunos de estos utilizamos el lema anterior, y si además multiplicamos por constantes de manera que los términos lider posean constante igual a 1, obtenemos lo que se llama una base de Grobner minimal.

Definición 3.2 *Una **base de Grobner minimal** para un ideal polinomial I es una base de Grobner G tal que:*

i) $Lc(p) = 1$, para todo $p \in G$.

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

Definición 3.3 *Una **base de Grobner reducida** para un ideal polinomial I es una base de Grobner G para I tal que:*

i) $Lc(p) = 1$, para todo $p \in G$.

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

Las bases de Grobner reducidas tienen la propiedad que queríamos:

Proposición 3.1 (Proposición 6, §7, [1]) *Sea $I \neq 0$ un ideal polinomial. Entonces I tiene una única base de Grobner reducida.*

A partir de esto, es fácil ver cuando dos ideales de $k[x_1, \ldots, x_n]$ son iguales. Sólo basta calcular sus bases de Grobner reducidas que serán iguales si y sólo si los ideales son iguales.

Referencias

[1] D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms*, Springer, 37-92 (1997).