Álgebra Conmutativa Computacional

F. J. Lobillo

2019/2020

Capítulo 3

Bases de Gröbner y Algoritmos Básicos

3.1 Ideales en $\mathbb{N}^n$

Definición 3.1. Un subconjunto $\varnothing \neq M \subseteq \mathbb{N}^n$ se dice ideal si $M = M + \mathbb{N}^n$. Se dice que un ideal $M \subseteq \mathbb{N}^n$ está generado por $F \subseteq M$ si $M = F + \mathbb{N}^n$.

Teorema 3.2 (Lema de Dickson)**.** *Todo ideal en $\mathbb{N}^n$ está finitamente generado.*

Demostración. Consecuencia directa del Teorema 2.6. □

En realidad es sencillo comprobar que los Teoremas 2.6 y 3.2 son equivalentes.
Dado $F \subseteq \mathbb{F}[x_1, \ldots, x_n]$, definimos

$$\exp(F) = \{\exp(f) \mid f \in F \setminus \{0\}\}.$$

Proposición 3.3. *Si $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ es un ideal no nulo, entonces* $\exp(I)$ *es un ideal en $\mathbb{N}^n$.*

Demostración. Sea $\alpha \in \exp(I)$ y $\beta \in \mathbb{N}^n$. Existe $f \in I$ tal que $\exp(f) = \alpha$. Dado que $X^\beta f \in I$ y $\exp(X^\beta f) = \exp(X^\beta)\exp(f) = \beta+\alpha$, tenemos que $\beta + \alpha \in \exp(I)$, lo que demuestra el resultado. □

3.2 División en $\mathbb{F}[x_1, \ldots, x_n]$

Teorema 3.4. *Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y sea $F = \{f_1, \ldots, f_s\}$ un subconjunto en $\mathbb{F}[x_1, \ldots, x_n]$. Todo elemento $f \in \mathbb{F}[x_1, \ldots, x_n]$ puede escribirse como*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

para ciertos $q_1, \ldots, q_s, r \in \mathbb{F}[x_1, \ldots, x_n]$, donde

- $\operatorname{supp}(r) \cap (\exp(F) + \mathbb{N}^n) = \varnothing$,
- $r = 0$ *o* $\exp(r) \leq \exp(f)$,
- *para cada* $1 \leq i \leq s$, $q_i f_i = 0$ *o* $\exp(f) \geq \exp(q_i f_i)$.

Demostración. Vamos a demostrar que la salida del Algoritmo 1 satisface las propiedades del teorema. Diremos que $p, q_1, \ldots, q_s, r$ es una etapa correcta de la división si

- $p = 0$ o $\exp(p) \leq \exp(f)$,
- $f = p + q_1 f_1 + \cdots + q_s f_s + r$,
- $\operatorname{supp}(r) \cap (\exp(F) + \mathbb{N}^n) = \varnothing$,
- $r = 0$ o $\exp(r) \leq \exp(f)$,

Algorithm 1 Algoritmo de división multivariable

procedure DIVISION($f, f_1, \ldots, f_s$)
  $p \leftarrow f$
  $r \leftarrow 0$
  for $1 \leq i \leq s$ **do**
    $q_i \leftarrow 0$
  while $p \neq 0$ **do**
    $i \leftarrow 1$
    $step \leftarrow 0$
    while $i \leq s$ **and** $step = 0$ **do**
      if $\exp(p) = \exp(f_i) + \gamma$ **then**
        $q_i \leftarrow q_i + \frac{lc(p)}{lc(f_i)} X^\gamma$
        $p \leftarrow p - \frac{lc(p)}{lc(f_i)} X^\gamma f_i$
        $step \leftarrow 1$
      else
        $i \leftarrow i + 1$
    if $step = 0$ **then**
      $r \leftarrow r + lt(p)$
      $p \leftarrow p - lt(p)$
  return $q_1, \ldots, q_s, r$

- para cada $1 \leq i \leq s$, $q_i f_i = 0$ o $\exp(f) \geq \exp(q_i f_i)$.

Observemos primeramente que los valores iniciales $(p, q_1, \ldots, q_s, r) = (f, 0, \ldots, 0, 0)$ son una etapa correcta de la división. Supongamos por tanto que $p, q_1, \ldots, q_s, r$ son una etapa correcta de la división y sean $p', q_1', \ldots, q_s', r'$ los valores de dichas variables después de una ejecución del bucle **while** principal. Vamos a demostrar que se $\exp(p') < \exp(p)$ y $p', q_1', \ldots, q_s', r'$ también son una etapa correcta de la división.

Supongamos en primer lugar que $\exp(p) \in \exp(F) + \mathbb{N}^n$. Sea $i_0 = \min\{1 \leq i \leq s \mid \exp(p) \in \exp(f_i) + \mathbb{N}^n\}$ y sea $\exp(p) = \exp(f_{i_0}) + \gamma$. En este caso el bucle termina con los siguientes nuevos valores:

$$\begin{aligned} p' &= p - \tfrac{lc(p)}{lc(f_{i_0})} X^\gamma f_{i_0}, \\ q_{i_0}' &= q_{i_0} + \tfrac{lc(p)}{lc(f_{i_0})} X^\gamma, \\ q_j' &= q_j \quad \text{si } j \neq i_0, \\ r' &= r. \end{aligned}$$

Por una parte,

$$\exp(X^\gamma f_{i_0}) = \gamma + \exp(f_{i_0}) = \exp(p)$$

y

$$lc\left(\tfrac{lc(p)}{lc(f_{i_0})} X^\gamma f_{i_0}\right) = \tfrac{lc(p)}{lc(f_{i_0})}\, lc(f_{i_0}) = lc(p),$$

por lo que $\exp(p') < \exp(p)$. Por otra parte,

$$\begin{aligned}\exp(q'_{i_0} f_{i_0}) &= \exp\left(q_{i_0} f_{i_0} + \tfrac{\mathrm{lc}(p)}{\mathrm{lc}(f_{i_0})} X^\gamma f_{i_0}\right)\\ &\leq \max\left\{\exp(q_{i_0} f_{i_0}), \exp\left(\tfrac{\mathrm{lc}(p)}{\mathrm{lc}(f_{i_0})} X^\gamma f_{i_0}\right)\right\}\\ &\leq \max\{\exp(f), \exp(p)\}\\ &= \exp(f).\end{aligned}$$

Finalmente,

$$\begin{aligned}f &= p + q_1 f_1 + \cdots + q_s f_s + r\\ &= p - \tfrac{\mathrm{lc}(p)}{\mathrm{lc}(f_{i_0})} X^\gamma f_{i_0} + q_1 f_1 + \cdots + q_s f_s + \tfrac{\mathrm{lc}(p)}{\mathrm{lc}(f_{i_0})} X^\gamma f_{i_0} + r\\ &= p' + q'_1 f_1 + \cdots + q'_s f_s + r',\end{aligned}$$

por lo que hemos demostrado que $p', q'_1, \ldots, q'_s, r'$ son una etapa correcta de la división.
Supongamos por el contrario que $\exp(p) \notin \exp(F) + \mathbb{N}^n$. En este segundo caso el bucle termina con los siguientes nuevos valores:

$$\begin{aligned}p' &= p - \mathrm{lt}(p)\\ q'_j &= q_j \quad \text{para } 1 \leq j \leq s,\\ r' &= r + \mathrm{lt}(p).\end{aligned}$$

Es inmediato que $p' = 0$ o $\exp(p') < \exp(p) \leq \exp(f)$. Además, $\mathrm{supp}(r') \subseteq \mathrm{supp}(r) \cup \{\exp(p)\}$, por lo que $\mathrm{supp}(r') \cap (\exp(F) + \mathbb{N}^n) = \varnothing$. Finalmente

$$\begin{aligned}f &= p + q_1 f_1 + \cdots + q_s f_s + r\\ &= p - \mathrm{lt}(p) + q_1 f_1 + \cdots + q_s f_s + r + \mathrm{lt}(p)\\ &= p' + q'_1 f_1 + \cdots + q'_s f_s + r',\end{aligned}$$

por lo que en este segundo caso $p', q'_1, \ldots, q'_s, r'$ son también una etapa correcta de la división.
Consecuentemente, si el algoritmo termina la salida satisface las condiciones del teorema. Queda verificar que el algoritmo termina. Sean $p_0, p_1, \ldots$ los diferentes valores que va tomando p en cada bucle del algoritmo. Tal y como hemos observado antes, $\exp(p_i) > \exp(p_{i+1})$, por lo que la cadena debe terminar, es decir, debe existir i_0 tal que $p_{i_0} = 0$. □

El polinomio r que obtenemos como salida del Algoritmo 1 recibe el nombre de resto de la división de f por $[f_1, \ldots, f_s]$, y se denota $r = \mathrm{rem}(f, [f_1, \ldots, f_s])$. Debemos observar que en la división el modo en que están ordenados los elementos de F es esencial como el siguiente ejemplo muestra. Por tanto, el resto se obtiene al dividir un polinomio entre una lista ordenada, no entre un subconjunto. Si $F = \{f_1, \ldots, f_s\}$, denotamos $[F] = [f_1, \ldots, f_s]$.

Ejemplo 3.5. Sean $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ y $f_2 = y^2 - 1$ polinomios en $\mathbb{Q}[x, y]$. En $\mathbb{N}^2$ consideramos el orden lexicográfico con $(1, 0) > (0, 1)$. Vamos a dividir f entre $F = \{f_1, f_2\} = \{f_2, f_1\}$ considerando las dos posibles ordenaciones.

3.3 Bases de Gröbner y Teorema de la base de Hilbert

Definición 3.6. Sea I un ideal en $\mathbb{F}[x_1, \ldots, x_n]$ y sea $\leq$ un orden admisible en $\mathbb{N}^n$. Un subconjunto $G = \{g_1, \ldots, g_t\} \subseteq I$ se dice que es una base de Gröbner para I si $\exp(I) = \exp(G) + \mathbb{N}^n$.

Teorema 3.7. *Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y sea I un ideal en $\mathbb{F}[x_1,\ldots,x_n]$ no nulo tiene una base de Gröbner. Si $G=\{g_1,\ldots,g_t\}$ una base de Gröbner para I entonces $I=\langle G\rangle$.*

Demostración. Por la Proposición 3.3 y el Teorema 3.2, I tiene una base de Gröbner, es decir existe $G=\{g_1,\ldots,g_t\}\subseteq I$ tal que

$$\exp(I)=\exp(G)+\mathbb{N}^n.$$

Veamos que $I=\langle G\rangle$. Para ello sea $f\in I$. Por el Teorema 3.4 existen $q_1,\ldots,q_t,r\in\mathbb{F}[x_1,\ldots,x_n]$ tales que

$$f=q_1g_1+\cdots+q_tg_t+r$$

y

$$\operatorname{supp}(r)\cap(\{\exp(g_1),\ldots,\exp(g_t)\}+\mathbb{N}^n)=\varnothing.$$

Como $r=f-q_1g_1-\cdots-q_tg_t\in I$, si $r\neq 0$ tenemos que

$$\exp(r)\in\operatorname{supp}(r)\cap(\{\exp(g_1),\ldots,\exp(g_t)\}+\mathbb{N}^n)=\varnothing,$$

lo que es contradictorio. Por tanto $r=0$, es decir, $f=q_1g_1+\cdots+q_tg_t$. Con esta identidad demostramos que $I=\langle g_1,\ldots,g_t\rangle$. □

Corolario 3.8 (Teorema de la base de Hilbert)**.** *Todo ideal en el anillo de polinomios $\mathbb{F}[x_1,\ldots,x_n]$ está finitamente generado, es decir, $\mathbb{F}[x_1,\ldots,x_n]$ es un anillo Noetheriano.*

Demostración. Dado que $\{0\}=\langle 0\rangle$, podemos suponer que $I\neq\{0\}$. El resultado es entonces consecuencia del Teorema 3.7. □

Recordemos que un anillo R es Noetheriano si satisface las siguientes condiciones equivalentes.

1. R satisface la Condición de Cadena Ascendente, es decir, dada una cadena de ideales $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_k \subseteq \cdots$, existe n tal que $I_n = I_m$ para todo $m \geq n$.
2. Todo ideal de R es finitamente generado.

Lema 3.9. *Sea $\leq$ un orden admisible en $\mathbb{N}^n$. Sea $I \leq \mathbb{F}[x_1, \ldots, x_n]$ un ideal distinto de cero. Para cualquier polinomio $f \in \mathbb{F}[x_1, \ldots, x_n]$, existe un único $r \in \mathbb{F}[x_1, \ldots, x_n]$ tal que*

(1) $\operatorname{supp}(r) \cap \exp(I) = \varnothing$,

(2) $f - r \in I$.

Demostración. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I. Por el Teorema 3.4, $r = \operatorname{rem}(f, [G])$ satisface las propiedades del Lema, ya que $\exp(I) = \exp(G) + \mathbb{N}^n$. Tenemos, por tanto, que demostrar la unicidad. Supongamos que r, r' satisfacen las condiciones del lema. Sean $g, g' \in I$ tales que $f = g + r = g' + r'$. Entonces

$$r - r' = r - f + f - r' = -g + g' \in I.$$

Si $r \neq r'$, $\exp(r - r') \in \exp(I)$ y

$$\exp(r - r') \in \operatorname{supp}(r - r') \subseteq \operatorname{supp}(r) \cup \operatorname{supp}(r'),$$

por lo que

$$\begin{aligned} \varnothing &\neq (\operatorname{supp}(r) \cup \operatorname{supp}(r')) \cap \exp(I) \\ &= (\operatorname{supp}(r) \cap \exp(I)) \cup (\operatorname{supp}(r') \cap \exp(I)) \\ &= \varnothing \cup \varnothing, \end{aligned}$$

una contradicción. Por tanto $r = r'$ y tenemos la unicidad. □

Al elemento r que proporciona el Lema 3.9 lo denotamos $r = \mathrm{rem}(f, I)$. Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para I. En la demostración hemos visto que $\mathrm{rem}(f, I) = \mathrm{rem}(f, [G])$. En particular, el resto obtenido al dividir por polinomios que constituyen una base de Gröbner es único, y podemos, en este caso, denotarlo por $\mathrm{rem}(f, G)$.

Corolario 3.10. *Sean $\leq$ un orden admisible en $\mathbb{N}^n$, $I \leq \mathbb{F}[x_1, \ldots, x_n]$ un ideal no nulo, y G una base de Gröbner para I. Entonces $f \in I$ si y solo si* $\mathrm{rem}(f, G) = 0$.

Demostración. Si $\mathrm{rem}(f, G) = 0$ es inmediato que $f \in I$. Por otra parte, si $f \in I$, 0 y $\mathrm{rem}(f, G)$ satisfacen las propiedades del Lema 3.9, por lo que son iguales por la unicidad. □

3.4 Algoritmo de Buchberger

Dados $\alpha, \beta \in \mathbb{N}^n$, definimos

$$\mathrm{lcm}(\alpha, \beta) = (\mathrm{máx}\{\alpha_1, \beta_1\}, \ldots, \mathrm{máx}\{\alpha_n, \beta_n\}).$$

Proposición 3.11. $(\alpha + \mathbb{N}^n) \cap (\beta + \mathbb{N}^n) = \mathrm{lcm}(\alpha, \beta) + \mathbb{N}^n$.

Demostración. Sea $\gamma = \mathrm{lcm}(\alpha, \beta)$. Dado que $\gamma_i = \alpha_i + \delta_i$ para cualquier $1 \leq i \leq s$, tenemos que $\gamma = \alpha + \delta$, por lo que $\gamma + \mathbb{N}^n \subseteq \alpha + \mathbb{N}^n$. Análogamente $\gamma + \mathbb{N}^n \subseteq \beta + \mathbb{N}^n$, por lo que

$$\mathrm{lcm}(\alpha, \beta) + \mathbb{N}^n \subseteq (\alpha + \mathbb{N}^n) \cap (\beta + \mathbb{N}^n).$$

Supongamos que $\lambda \in (\alpha + \mathbb{N}^n) \cap (\beta + \mathbb{N}^n)$. Existen ρ, η tales que $\lambda = \alpha + \rho = \beta + \eta$. Como consecuencia $\lambda_i \geq \alpha_i$ y $\lambda_i \geq \beta_i$ para cualquier $1 \leq i \leq s$, es decir, $\lambda_i \geq \text{máx}\{\alpha_i, \beta_i\}$ para cada $1 \leq i \leq s$. Por tanto $\lambda \in \text{lcm}(\alpha, \beta) + \mathbb{N}^n$, lo que demuestra la segunda inclusión y el resultado. □

Cuando $\gamma \in \alpha + \mathbb{N}^n$, emplearemos la notación $\gamma - \alpha$ para referirnos al elemento δ tal que $\gamma = \alpha + \delta$.

Definición 3.12. Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ no nulos. Sean $\alpha = \exp(f)$, $\beta = \exp(g)$ y $\gamma = \text{lcm}(\alpha, \beta)$. Se define el S-polinomio de f y g como

$$S(f, g) = \text{lc}(g)X^{\gamma-\alpha}f - \text{lc}(f)X^{\gamma-\beta}g.$$

Lema 3.13. $\exp(S(f, g)) < \text{lcm}(\exp(f), \exp(g))$.

Demostración. Sean $\alpha = \exp(f)$, $\beta = \exp(g)$ y $\gamma = \text{lcm}(\alpha, \beta)$. Por las Proposición 2.13, observemos que

$$\exp(\text{lc}(g)X^{\gamma-\alpha}f) = \exp(\text{lc}(f)X^{\gamma-\beta}g) = \gamma$$

y

$$\text{lc}\left(\text{lc}(g)X^{\gamma-\alpha}f\right) = \text{lc}\left(\text{lc}(f)X^{\gamma-\beta}g\right) = \text{lc}(f)\,\text{lc}(g),$$

luego la Proposición 2.12 demuestra el resultado. □

Lema 3.14. *Sean* $p_1, \ldots, p_s \in \mathbb{F}[x_1, \ldots, x_n]$ *tales que* $\exp(p_i) = \delta$ *para todo* $1 \leq i \leq s$. *Si* $\exp\left(\sum_{i=1}^{s} p_i\right) < \delta$, *existen* $c_{ij} \in \mathbb{F}$ *para cada* $1 \leq i < j \leq s$ *tales que*

$$\sum_{i=1}^{s} p_i = \sum_{i<j} c_{ij} S(p_i, p_j).$$

Demostración. Sea $d_i = \mathrm{lc}(p_i)$. Dado que $\exp\left(\sum_{i=1}^{s} p_i\right) < \delta$, la Proposición 2.12 implica que $\sum_{i=1}^{s} d_i = 0$. Si $i < j$, como $\exp(p_i) = \exp(p_j) = \delta$, tenemos que

$$S(p_i, p_j) = d_j p_i - d_i p_j.$$

Se sigue que

$$\begin{aligned}\textstyle\sum_{i=1}^{s-1} \frac{1}{d_s} S(p_i, p_s) &= \textstyle\frac{1}{d_s} \sum_{i=1}^{s-1} (d_s p_i - d_i p_s) \\ &= \textstyle\sum_{i=1}^{s-1} p_i + \frac{-d_1 - \cdots - d_{s-1}}{d_s} p_s \\ &= \textstyle\sum_{i=1}^{s-1} p_i + \frac{d_s}{d_s} p_s \\ &= \textstyle\sum_{i=1}^{s} p_i,\end{aligned}$$

lo que demuestra el resultado. □

Teorema 3.15 (Criterio de Buchberger)**.** *Sea $\leq$ un orden admisible en $\mathbb{N}^n$ y sea $I \leq \mathbb{F}[x_1, \ldots, x_n]$ un ideal no nulo. Sea $G = \{g_1, \ldots, g_t\}$ un conjunto de generadores de I. G es una base de Gröbner para I si y solo si para cualesquiera $1 \leq i < j \leq t$, $\mathrm{rem}(S(g_i, g_j), [G]) = 0$.*

Demostración. Si G es una base de Gröbner, dado que $S(g_i, g_j) \in \langle G \rangle = I$, tenemos que $\mathrm{rem}(S(g_i, g_j), G) = 0$ por el Corolario 3.10. Supongamos por tanto que para cada pareja $1 \leq i < j \leq t$, tenemos que $\mathrm{rem}(S(g_i, g_j), [G]) = 0$. Sea $f \in I$ no nulo. Queremos demostrar que $\exp(f) \in \exp(G) + \mathbb{N}^n$. Sea

$$\delta = \text{mín}\left\{\text{máx}\{\exp(h_1 g_1), \ldots, \exp(h_t g_t)\} \mid f = \textstyle\sum_{i=1}^{t} h_i g_i\right\},$$

que existe por ser $\leq$ un buen orden. Por la Proposición 2.12, tenemos que $\exp(f) \leq \delta$. Si $\exp(f) = \delta$, existe $1 \leq i \leq t$ tal que $\exp(f) =$

$\exp(h_i g_i) = \exp(h_i) + \exp(g_i) \in \exp(G) + \mathbb{N}^n$, luego nos queda analizar el caso $\exp(f) < \delta$. Fijemos una expresión $f = \sum_{i=1}^{t} h_i g_i$ con δ mínimo. Sea $\mathbf{i} = \{i_1, \ldots, i_s\} = \{1 \leq i \leq t \mid \exp(h_i g_i) = \delta\}$. Tenemos que

$$\begin{aligned} f &= \sum_{j=1}^{s} h_{i_j} g_{i_j} + \sum_{i \notin \mathbf{i}} h_i g_i \\ &= \sum_{j=1}^{s} \mathrm{lt}(h_{i_j}) g_{i_j} + \sum_{j=1}^{s} (h_{i_j} - \mathrm{lt}(h_{i_j})) g_{i_j} + \sum_{i \notin \mathbf{i}} h_i g_i. \end{aligned}$$

Dado que

$$\exp\left(\sum_{j=1}^{s} (h_{i_j} - \mathrm{lt}(h_{i_j})) g_{i_j} + \sum_{i \notin \mathbf{i}} h_i g_i\right) < \delta,$$

tenemos que $\sum_{j=1}^{s} \mathrm{lt}(h_{i_j}) g_{i_j}$ satisface las condiciones del Lema 3.14, y por tanto

$$\sum_{j=1}^{s} \mathrm{lt}(h_{i_j}) g_{i_j} = \sum_{1 \leq j < k \leq s} c_{jk} S(\mathrm{lt}(h_{i_j}) g_{i_j}, \mathrm{lt}(h_{i_k}) g_{i_k}) \qquad (3.1)$$

para ciertos $c_{jk} \in \mathbb{F}$.

Sean $1 \leq j < k \leq s$ y sea

$$\gamma_{jk} = \mathrm{lcm}(\exp(g_{i_j}), \exp(g_{i_k})).$$

Por la Proposición 3.11, $\delta = \gamma_{jk} + \gamma$ para un cierto $\gamma \in \mathbb{N}^n$. Tenemos

que

$$\begin{aligned}
&S\left(\mathrm{lt}(h_{i_j})g_{i_j}, \mathrm{lt}(h_{i_k})g_{i_k}\right) = \\
&= \mathrm{lc}(\mathrm{lt}(h_{i_k})g_{i_k})\,\mathrm{lt}(h_{i_j})g_{i_j} - \mathrm{lc}(\mathrm{lt}(h_{i_j})g_{i_j})\,\mathrm{lt}(h_{i_k})g_{i_k} \\
&= \mathrm{lc}(h_{i_j})\,\mathrm{lc}(h_{i_k})\left(\mathrm{lc}(g_{i_k})X^{\delta-\exp(g_{i_j})}g_{i_j} - \mathrm{lc}(g_{i_j})X^{\delta-\exp(g_{i_k})}g_{i_k}\right) \\
&= \mathrm{lc}(h_{i_j})\,\mathrm{lc}(h_{i_k})X^{\gamma} \\
&\quad \cdot \left(\mathrm{lc}(g_{i_k})X^{\gamma_{jk}-\exp(g_{i_j})}g_{i_j} - \mathrm{lc}(g_{i_j})X^{\gamma_{jk}-\exp(g_{i_k})}g_{i_k}\right) \\
&= \mathrm{lc}(h_{i_j})\,\mathrm{lc}(h_{i_k})X^{\delta-\gamma_{jk}}S(g_{i_j}, g_{i_k}) \\
&= \mathrm{lc}(h_i)\,\mathrm{lc}(h_{i_k})X^{\delta-\gamma_{jk}}\textstyle\sum_{l=1}^{t} q_l g_l \\
&= \textstyle\sum_{l=1}^{t} b_l g_l,
\end{aligned} \tag{3.2}$$

donde $b_l = \mathrm{lc}(h_{i_j})\,\mathrm{lc}(h_{i_k})X^{\delta-\gamma_{jk}}q_l$ y $q_1, \ldots, q_t, 0$ son la salida del Algoritmo 1. Dado que $q_1, \ldots, q_t$ son la salida del Algoritmo 1, si $q_l g_l \neq 0$ tenemos que $\exp(q_l g_l) \leq \exp(S(g_{i_j}, g_{i_k}))$, por lo que si $b_l q_l \neq 0$,

$$\exp(b_l g_l) \leq X^{\delta-\gamma_{jk}}\exp(S(g_{i_j}, g_{i_k})) < \delta$$

por el Lema 3.13. Juntando las ecuaciones (3.1) y (3.2), tenemos que

$$\textstyle\sum_{j=1}^{s} \mathrm{lt}(h_{i_j})g_{i_j} = \sum_{l=1}^{t} f_l g_l,$$

donde $\exp(f_l g_l) < \delta$. De esta forma

$$f = \textstyle\sum_{l=1}^{t} f_l g_l + \sum_{j=1}^{s}(h_{i_j} - \mathrm{lt}(h_{i_j}))g_{i_j} + \sum_{i\notin \mathbf{i}} h_i g_i$$

es una expresión de f en la que el exponente de todos los sumandos es menor que δ, lo que contradice su minimalidad de δ. Por tanto $\exp(f) = \delta$ y $\exp(f) \in \exp(G) + \mathbb{N}^n$. □

Algorithm 2 Algoritmo de Buchberger

```
procedure GROEBNER(F)
    G ← F.
    repeat
        G' ← G
        for each pair {f, g} ⊆ G' do
            r ← rem(S(f, g), [G'])
            if r ≠ 0 then
                G ← G ∪ {r}
    until G = G'
    return G
```

Teorema 3.16. *El Algoritmo 2 calcula correctamente una base de Gröbner para* $\langle F \rangle$.

Demostración. Si el algoritmo termina la salida es una base de Gröbner para el ideal que genera por el Teorema 3.15. Sean $f, g \in G'$ y $r = \mathrm{rem}(S(f,g), [G'])$. Como

$$r = S(f,g) + \textstyle\sum_{g \in G'} h_g g \in \langle G' \rangle ,$$

tenemos que $\langle G' \rangle = \langle G' \cup \{r\} \rangle$, por lo que $\langle G \rangle = \langle G' \rangle$ al final del blucle **repeat-until**. Por tanto si el algoritmo termina su salida es una

base de Gröbner para $\langle F\rangle$. Queda ver que el algoritmo termina. Sea $r = \mathrm{rem}(S(f,g),[G'])$ con $f,g \in G'$. Como $\mathrm{supp}(r)\cap(\exp(G')+\mathbb{N}^n) = \varnothing$, tenemos que si $r \neq 0$, $\exp(r) \notin \exp(G') + \mathbb{N}^n$, luego

$$\exp(G') + \mathbb{N}^n \subset \exp(G) + \mathbb{N}^n.$$

Esto nos da una cadena ascendente

$$\exp(G_0) + \mathbb{N}^n \subset \exp(G_1) + \mathbb{N}^n \subset \cdots \subset \exp(G_i) + \mathbb{N}^n \subset \cdots,$$

donde G_i son las sucesivas salidas del bucle **repeat-until**, que por el Lema de Dickson (Teorema 3.2) debe estabilizar. Por tanto el algoritmo termina. □

Ejemplo 3.17. Sea $I = \langle f_1, f_2\rangle$ donde f_1, f_2 son los dados en el Ejemplo 3.5. Calculemos una base de Gröbner para I.

Sea M un ideal en $\mathbb{N}^n$. Decimos que A es un conjunto generador minimal de M si $M = A + \mathbb{N}^n$ pero $M \neq (A \setminus \{\alpha\}) + \mathbb{N}^n$ para cualquier $\alpha \in A$.

Lema 3.18. *Sea $A \subseteq \mathbb{N}^n$ y $\alpha \in A$. Si $\alpha \in (A \setminus \{\alpha\}) + \mathbb{N}^n$, entonces $A + \mathbb{N}^n = (A \setminus \{\alpha\}) + \mathbb{N}^n$.*

Demostración. Como $A \subseteq (A \setminus \{\alpha\}) + \mathbb{N}^n$, tenemos que $A + \mathbb{N}^n \subseteq (A \setminus \{\alpha\}) + \mathbb{N}^n$. La inclusión contraria es inmediata. □

Lema 3.19. *Todo ideal $M \subseteq \mathbb{N}^n$ tiene un único conjunto generador minimal.*

Demostración. Supongamos que tenemos dos conjuntos generadores minimales $A = \{\alpha(1),\ldots,\alpha(s)\}$ y $B = \{\beta(1),\ldots,\beta(t)\}$, finitos por

el Lema de Dickson (Teorema 2.6). Como $\alpha(1) \in M$, existen $\beta(i), \gamma$ tales que $\alpha(1) = \beta(i_1) + \gamma$. Como $\beta(i_1) \in M$, $\beta(i_1) = \alpha(j) + \gamma'$, por lo que $\alpha(1) = \alpha(j) + \gamma + \gamma'$. Como A es minimal, el Lema 3.18 implica que $\alpha(j) = \alpha(1)$, por lo que $\alpha(1) = \beta_{i_1}$. Supongamos que $\alpha(l) = \beta_{i_l}$ para $1 \leq l \leq k-1$. El mismo argumento anterior implica que $\alpha(k) = \beta_{i_k}$ para cierto i_k. Reiterando la construcción, $A \subseteq B$. Por simetría, $B \subseteq A$, de donde tenemos la igualdad. □

El Lema 3.19 nos dice que existe un conjunto generador minimal y el Lema 3.18 nos dice como calcularlo. Una base de Gröbner G de I se dice minimal si $\exp(G)$ es un conjunto generador minimal de $\exp(I)$. Si bien los conjuntos generadores minimales son únicos, las bases de Gröbner minimales no lo son.

Ejemplo 3.20. $\{y^2 - 1, x - y\}$ y $\{y^2 - x + y - 1, x - y\}$ son ambas bases de Gröbner minimales para $I = \langle f_1, f_2 \rangle$ con respecto al orden DEGREVLEX, donde f_1, f_2 son los dados en el Ejemplo 3.5

Definición 3.21. Una base de Gröbner reducida para un ideal I es una base de Gröbner G tal que

(1) para todo $g \in G$, $\mathrm{lc}(g) = 1$,

(2) para todo $g \in G$, $\mathrm{supp}(g) \cap (\exp(G \setminus \{g\}) + \mathbb{N}^n) = \varnothing$.

Teorema 3.22. *Todo ideal tiene una única base de Gröbner reducida para un orden admisible dado.*

Demostración. Dado un ideal I, sea $G \subseteq I$ tal que $\exp(G)$ es un conjunto generador minimal de $\exp(I)$. Sea $g \in G$ y sea $r = \mathrm{rem}(g, [G \setminus \{g\}])$. Como $\exp(g) \notin \exp(G \setminus \{g\}) + \mathbb{N}^n$, podemos observar del Algoritmo

1 que $\exp(g) = \exp(r)$, y dado que $g - r \in \langle G \setminus \{g\}\rangle \subseteq I$, tenemos que $r \in I$. Como $\exp(G) = \exp((G \setminus \{g\}) \cup \{r\})$, concluimos que $G' = (G \setminus \{g\}) \cup \{r\}$ es una nueva base de Gröbner en la que $\operatorname{supp}(r) \cap (\exp(G' \setminus \{r\}) + \mathbb{N}^n) = \varnothing$. Reiterando el proceso en cada elemento de G, y dividiendo cada elemento de g por su coeficiente líder, obtenemos una base de Gröbner reducida para I.
Queda demostrar la unicidad. Sean G_1, G_2 dos bases de Gröbner reducidas. Como $\exp(G_1) = \exp(G_2)$ por el Lema 3.19, dado $g_1 \in G_1$ existe un único $g_2 \in G_2$ tal que $\exp(g_1) = \exp(g_2)$. Como $g_1 - g_2 \in I$, $\operatorname{rem}(g_1 - g_2, G_1) = 0$ por el Corolario 3.10. Observemos que

$$\operatorname{supp}(g_1 - g_2) \subseteq (\operatorname{supp}(g_1) \cup \operatorname{supp}(g_2)) \setminus \{\exp(g_1)\}$$

y que para $i \in \{1, 2\}$,

$$\operatorname{supp}(g_i) \setminus \{\exp(g_i)\} \cap (\exp(G_i) + \mathbb{N}^n) = \varnothing,$$

por lo que

$$\operatorname{supp}(g_1 - g_2) \cap (\exp(G_1) + \mathbb{N}^n) = \varnothing,$$

y por el Lema 3.9, $\operatorname{rem}(g_1 - g_2, G_1) = g_1 - g_2$. En consecuencia $g_1 = g_2$, de lo que deducimos que $G_1 = G_2$. □

Corolario 3.23. *Dos ideales en un anillo de polinomios son iguales si y solo si sus bases de Gröbner reducidas son iguales.*

3.5 Aplicación: Sistema de Posicionamiento Global (GPS)

El sistema de posicionamiento global conocido como GPS consta de los siguientes elementos.

- 24 satélites (y 6 de refuerzo) en órbita estable, conocida y transmitida.
- Todos *perfectamente* sincronizados con relojes atómicos.
- Cada uno de ellos emite una señal pseudoaleatoria única junto con información referente a su posición.
- El receptor GPS mide el momento en que recibe las señales de los satélites.
- Como el receptor sabe en qué instante se ha enviado la señal, el retardo en el tiempo que tarda la señal en llegar multiplicado por la velocidad de la luz nos da la distancia *exacta* a la que están los satélites.

Si (x_i, y_i, z_i) es la posición del satélite, t_i el tiempo que tarda en llegar la señal y (x, y, z) la posición del receptor, entonces

$$(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 - (ct_i)^2 = 0$$

donde c es la velocidad de la luz. Si tomamos (x, y, z) como variable tenemos la ecuación de una esfera centrada en (x_i, y_i, z_i) y de radio ct_i.
Si disponemos de los datos de tres satélites, la posición viene determinada por los puntos de la variedad

$$\mathbf{V}\left(\left\langle (x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 - (ct_i)^2 \mid 1 \leq i \leq 3 \right\rangle\right).$$

Una base de Gröbner del ideal está compuesta de un polinomio cuadrático en z junto con dos polinomios lineales en x, y e y, z, por lo que es

sencillo calcular los dos puntos de la variedad. Uno de ellos nos dice la posición.
La sincronización de los relojes (atómicos) de los satélites es extrema, pero el receptor no dispone de un reloj atómico y por tanto su sincronización no es perfecta. Eso quiere decir que hay un retraso o adelanto d del reloj del receptor con respecto de los relojes de los satélites. Si t_i es el tiempo medido por el receptor, la ecuación se convierte en

$$(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 = (c(t_i + d))^2$$

Con al menos cuatro satélites podemos considerar d como variable, por tanto tenemos averiguar la variedad asociada al ideal

$$\left\langle (x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 - (c(t_i + d))^2 \mid 1 \leq i \leq 4 \right\rangle$$

Una base de Gröbner consiste en un polinomio cuadrático en d junto con tres polinomios lineales en x, d, y, d y z, d, por lo que tenemos dos posiciones posibles, una de ellas correctas. Una vez calculado el valor correcto de d, podemos sincronizar el reloj del receptor con los satélites. A partir de ese momento podemos trabajar con ideales de la forma

$$\left\langle (x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 - (ct_i)^2 \mid 1 \leq i \leq 3 \right\rangle$$

como en el primer caso.

Ejercicios sobre Bases de Gröbner y Algoritmos Básicos

Ejercicio 3.1. Demuestra que un anillo satisface la condición de cadena ascendente si y sólo si todo ideal del mismo es finitamente generado.

Ejercicio 3.2. Dados $f = x^7y^2 + x^3y^2 - y + 1$, $f_1 = xy^2 - x$ y $f_2 = x - y^3$ en $\mathbb{Q}[x, y, z]$, calcula la división de f entre $[f_1, f_2]$ con respecto al orden DEGLEX. Realiza más divisiones cambiando la ordenación de los divisores y el orden admisible. Realiza el ejercicio cambiando $\mathbb{Q}$ por $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$ y $\mathbb{F}_5$.

Ejercicio 3.3. Dados $f = xy^2z^2 + xy - yz$, $f_1 = x - y^2$, $f_2 = y - z^3$ y $f_3 = z^2 - 1$ en $\mathbb{Q}[x, y, z]$, calcula la división de f entre $[f_1, f_2, f_3]$ con respecto al orden DEGLEX. Realiza más divisiones cambiando la ordenación de los divisores y el orden admisible.

Ejercicio 3.4. Sean $f = x^3 - x^2y - x^2z + x$, $f_1 = x^2y - z$ y $f_2 = xy - 1$ en $\mathbb{Q}[x, y, z]$, en el que consideramos el orden DEGREVLEX.

(1) Calcula $r_1 = \text{rem}(f, [f_1, f_2])$ y $r_2 = \text{rem}(f, [f_2, f_1])$.

(2) Sea $r = r_1 - r_2$, ¿$r \in \langle f_1, f_2 \rangle$? Si la respuesta es afirmativa escribe $r = p_1f_1 + p_2f_2$.

(3) Calcula $\text{rem}(r, [f_1, f_2])$.

Ejercicio 3.5. Dados $f_1 = x^4y^4 - z$, $f_2 = x^3y^3 - 1$ y $f_3 = x^2y^4 - 2x$ en $\mathbb{Q}[x, y, z]$ con el orden DEGLEX, encuentra, si es posible, $g \in \langle f_1, f_2, f_3 \rangle$ tal que $\text{rem}(g, [f_1, f_2, f_3]) \neq 0$.

Ejercicio 3.6. Demuestra que el cálculo del resto en el Algoritmo 1 es lineal.

Ejercicio 3.7. Si G es una base de Gröbner para I y $G \subseteq G' \subseteq I$, demuestra que G' es también una base de Gröbner para I.

Ejercicio 3.8. Calcula una base de Gröbner para el ideal

$$\langle x^4y^2 - z, x^3y^3 - 1, x^2y^4 - 2z\rangle \subseteq \mathbb{Q}[x, y, z]$$

con respecto al orden DEGLEX. Realiza el ejercicio cambiando $\mathbb{Q}$ por $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$ y $\mathbb{F}_5$.

Ejercicio 3.9. Si $f \in \mathbb{F}[x_1, \ldots, x_n]$ y $f \notin \langle x_1, \ldots, x_n\rangle$, demuestra que $\langle x_1, \ldots, x_n, f\rangle = \mathbb{F}[x_1, \ldots, x_n]$.

Ejercicio 3.10. Demuestra que las variedades afines satisfacen la condición de cadena descendente, es decir, si tenemos una cadena

$$V_1 \supseteq V_2 \supseteq \cdots \supseteq V_i \supseteq \cdots,$$

demuestra que existe $n \in \mathbb{N}$ tal que $V_n = V_{n+k}$ para todo $k \in \mathbb{N}$.

Ejercicio 3.11. Sea $V = \mathbf{V}(x^2 - y, y + x^2 - 4) \subseteq \mathbb{C}^2$. Calcula los puntos de la variedad.

Ejercicio 3.12. Sea $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ un ideal y sea $G = \{g_1, \ldots, g_t\}$ una base de I, es decir, $I = \langle G\rangle$. Demuestra que G es una base de Gröbner para I si y solo si para cualquier $f \in \mathbb{F}[x_1, \ldots, x_n]$,

$$f \in I \iff \operatorname{rem}(f, [G]) = 0.$$

Ejercicio 3.13. Calcula $S(f, g)$ es los siguientes casos,

(1) $f = 4x^2z - 7y^2$, $g = xyz^2 + 3xz^4$

(2) $f = x^4y - z^2$, $g = 3xz^2 - y$

(3) $f = x^7y^2z + 2ixyz$, $g = 2x^7y^2z + 4$

Ejercicio 3.14. ¿Depende $S(f, g)$ del orden admisible empleado?

Ejercicio 3.15. Sea G una base de Gröbner para I. Demuestra que $\text{rem}(f, G) = \text{rem}(g, G)$ si y solo si $f - g \in I$. Demuestra además que

$$\text{rem}(f + g, G) = \text{rem}(f, G) + \text{rem}(g, G)$$

y que

$$\text{rem}(fg, G) = \text{rem}(\text{rem}(f, G)\,\text{rem}(g, G), G).$$

Ejercicio 3.16. Calcula una base de Gröbner para los siguientes ideales.

(1) $I = \langle x^2y - 1, xy^2 - x\rangle$

(2) $I = \langle x^2 + y, x^4 + 2x^2y + y^2 + 3\rangle$

(3) $I = \langle x - z^4, y - z^5\rangle$

Calcula también la base de Gröbner reducida con respecto al orden LEX.

Ejercicio 3.17. Sea

$$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w\rangle \subseteq \mathbb{Q}[x, y, z, t]$$

Calcula una base de Gröbner reducida para I.

Ejercicio 3.18. Sea $A = (a_{ij}) \in \mathbb{F}^{m\times n}$ y sea $f_i = \sum_{j=1}^{n} a_{ij}x_j$. Consideremos en $\mathbb{N}^n$ el orden LEX. Sea $I = \langle f_1, \ldots, f_m\rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$. Sean $g_1, \ldots, g_t$ los polinomios asociados a las filas no nulas de la forma escalonada reducida de A.

(1) Comprueba que $I = \langle g_1, \ldots, g_t\rangle$.

(2) Calcula $\operatorname{rem}(S(g_i, g_l), [g_1, \ldots, g_t])$. Consejo: obsérvese que solo se emplean g_i y g_l en la división.

(3) Concluye que $\{g_1, \ldots, g_t\}$ es una base de Gröbner reducida para I.

Bibliografía

[1] David A. Cox, John Little, and Donald O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Text in Mathematics. Springer, fourth edition, 2015.

[2] Serge Lang. *Undergraduate Algebra*. Undergraduate Text in Mathematics. Springer, second edition, 1990.