

Tema 4

Bases de Groebner

Las bases de Groebner se introducen para resolver, entre otros, los siguientes problemas relativos a los ideales del anillo de polinomios $k[x_1, \dots, x_n]$ algorítmicamente:

1. **Problema de pertenencia a un ideal.** Dado un ideal

$$I = (f_1, \dots, f_s)$$

del anillo de polinomios y un polinomio f , ¿se puede determinar cuando $f \in I$ y cuando no?

2. **Problema de calcular los puntos de un conjunto algebraico afín.** Si

$$V = V(f_1, \dots, f_s),$$

determinar si V es o no finito y calcular todos los puntos $p \in V$.

3. **Problema de implícitación.** Si V es un subconjunto de $\mathbb{A}^n k$ tal que sus puntos están dados de forma paramétrica por

$$a_1 = f_1(t_1, \dots, t_s), \dots, a_n = f_n(t_1, \dots, t_s),$$

entonces V es un conjunto algebraico afín. Calcular las ecuaciones que lo definen.

Para $n = 1$, el problema de pertenencia a un ideal se resuelve con el algoritmo de división euclídea: Si $I = (g)$, entonces para todo polinomio $f \in k[x]$ existen $h, r \in k[x]$, donde el grado de r es estrictamente menor que el de g , tales que $f = gh + r$. Entonces $f \in I$ si, y sólo si $r = 0$.

Para $n \geq 0$, si el conjunto algebraico afín V está definido por polinomios $f_1, \dots, f_s$ de grado 1, entonces el problema de calcular los puntos de V está resuelto por el algoritmo de Gauss para resolver sistemas de ecuaciones lineales. En efecto, $(a_1, \dots, a_n) \in V$ si, y sólo si, $(a_1, \dots, a_n)$ es una solución del sistema de ecuaciones lineales $f_1 = \dots = f_s = 0$.

Además, si V es un conjunto de $\mathbb{A}^n k$ parametrizado por los polinomios de grado uno $f_1, \dots, f_n \in k[t_1, \dots, t_s]$, donde

$$f_i = a_{i1}t_1 + \dots + a_{is}t_s + b_i$$

entonces el sistema de ecuaciones

$$\left. \begin{array}{l} a_{11}t_1 + \dots + a_{1s}t_s - x_1 = -b_1 \\ a_{21}t_1 + \dots + a_{2s}t_s - x_2 = -b_2 \\ \vdots \\ a_{n1}t_1 + \dots + a_{ns}t_s - x_n = -b_n \end{array} \right\}$$

se puede convertir en un sistema en el que el número de ecuaciones que no dependen de $t_1, \dots, t_s$ sea máximo, y en las que dependen de alguno de ellos sólo esté uno de los t_i . Entonces V es el conjunto algebraico afín definido por las ecuaciones en las que no están $t_1, \dots, t_s$.

4.1. Órdenes monomiales

Al igual que en el conjunto de las potencias de x del anillo de polinomios $k[x]$ hay definido un orden total, dado por el grado, nos plantearemos dotar al conjunto de elementos $x_1^{s_1} \dots x_n^{s_n}$ de $k[x_1, \dots, x_n]$ de un orden total, que además verifique determinadas propiedades.

Dado que dicho conjunto se corresponde biyectivamente con $\mathbb{N} \times \dots \times \mathbb{N}$, podemos asumir el problema de dotar a este producto cartesiano de un orden total.

(4.1.1) Definición. Un orden monomial en $k[x_1, \dots, x_n]$ es una relación binaria “ $\leq$ ” en $\mathbb{N}^n = \mathbb{N} \times \dots \times \mathbb{N}$ tal que:

(4.1.1.1) “ $\leq$ ” es una relación de orden total;

(4.1.1.2) si $\alpha, \beta, \gamma \in \mathbb{N}^n$ y $\alpha < \beta$, entonces $\alpha + \gamma < \beta + \gamma$;

(4.1.1.3) “ $\leq$ ” es un buen orden, es decir, todo subconjunto no vacío de $\mathbb{N}^n$ tiene un elemento minimal para “ $\leq$ ”.

(4.1.2) Ejemplo. El orden usual en $\mathbb{N}$ es un orden monomial en $k[x]$.

(4.1.3) Lema. Una relación de orden “ $\leq$ ” en $\mathbb{N}^n$ es un buen orden si, y sólo si para toda cadena decreciente $\alpha_1 \geq \alpha_2 \geq \dots$ de $\mathbb{N}^n$ existe un n tal que $\alpha_i = \alpha_n$ para todo $i \geq n$.

Demostración. Supongamos que “ $\leq$ ” no es un buen orden, esto es, que hay un conjunto $\emptyset \neq S \subseteq \mathbb{N}^n$ tal que S no tiene un elemento minimal. Sea $\alpha \in S$. Entoces existe $\alpha \geq \alpha_2 \in S$, $\alpha_2 \neq \alpha$ y también $\alpha_2 \geq \alpha_3 \in S$, $\alpha_2 \neq \alpha_3$, y así sucesivamente se construye una sucesión estrictamente decreciente en $\mathbb{N}^n$.

Recíprocamente, si $\alpha_1 \geq \alpha_2 \geq \dots$ es una sucesión estrictamente decreciente en $\mathbb{N}^n$, entonces $S = \{\alpha_i\}_{i=1}^\infty$ es un conjunto no vacío que no tiene elemento minimal. $\square$

(4.1.4) Ejemplo. Orden lexicográfico. Definamos en $\mathbb{N}^n$

$$(\alpha_1, \dots, \alpha_n) <_{lex} (\beta_1, \dots, \beta_n) \Leftrightarrow \exists i \in \{1, \dots, n\} \begin{cases} \alpha_j = \beta_j \text{ si } 1 \leq j \leq i-1, \\ \alpha_i < \beta_i \end{cases}.$$

(o equivalentemente, definamos en el conjunto de monomios

$$\{x_1^{\alpha_1} \cdots x_n^{\alpha_n}\}_{\alpha_1, \dots, \alpha_n \in \mathbb{N}}$$

la relación

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} <_{lex} x_1^{\beta_1} \cdots x_n^{\beta_n} \Leftrightarrow \exists i \in \{1, \dots, n\}; \begin{cases} \alpha_j = \beta_j \text{ si } 1 \leq j \leq i-1, \\ \alpha_i < \beta_i \end{cases}.$$

La relación

$$\alpha \leq_{lex} \beta \Leftrightarrow \alpha = \beta \text{ o } \alpha <_{lex} \beta$$

es un orden monomial en $k[x_1, \dots, x_n]$.

La reflexividad es consecuencia de la definición de $\leq_{lex}$.

Si

$$\alpha = (\alpha_1, \dots, \alpha_n) \neq (\beta_1, \dots, \beta_n) = \beta \in \mathbb{N}^n$$

entonces existe $i \in \{1, \dots, n\}$ tal que $\alpha_j = \beta_j$ para $1 \leq j < i$ y $\alpha_i \neq \beta_i$. Luego o bien $\alpha_i < \beta_i$, con lo que $\alpha <_{lex} \beta$ pero $\beta \not<_{lex} \alpha$, o bien $\alpha_i > \beta_i$, con lo que $\beta <_{lex} \alpha$ pero $\alpha \not<_{lex} \beta$.

Si

$$\alpha \leq_{lex} \beta \leq_{lex} \gamma \in \mathbb{N}^n,$$

entonces existen $i, j \in \{1, \dots, n+1\}$ tales que $\alpha_k = \beta_k$ para $1 \leq k < i$, $\beta_k = \gamma_k$ para $1 \leq k < j$ y $\alpha_i < \beta_i$ (resp. $\beta_j < \gamma_j$) si $i \neq n+1$ (resp. si $j \neq n+1$). Sea $l = \min\{i, j\}$, entonces $\alpha_k = \beta_k = \gamma_k$ para $1 \leq k < l$ y $\alpha_l < \gamma_l$ si $l \neq n+1$. Luego “ $\leq_{lex}$ ” es transitiva.

Además, si $\alpha, \beta \in \mathbb{N}^n$, entonces o bien $\alpha = \beta$ o bien $\alpha \neq \beta$, en cuyo caso, tal como hemos visto en el párrafo anterior, o bien $\alpha \leq_{lex} \beta$, o bien $\beta \leq_{lex} \alpha$. Luego “ $\leq_{lex}$ ” es un orden total.

Si $\alpha \leq_{lex} \beta, \gamma \in \mathbb{N}^n$, entonces existe $i \in \{1, \dots, n+1\}$ tal que $\alpha_j = \beta_j$ para $1 \leq j < i$ y $\alpha_i < \beta_i$ si $i \neq n+1$. Luego $\alpha_j + \gamma_j = \beta_j + \gamma_j$ para $1 \leq j < i$ y $\alpha_i + \gamma_i < \beta_i + \gamma_i$ si $i \neq n+1$, con lo que $\alpha + \gamma \leq_{lex} \beta + \gamma$.

Sea ahora $\alpha^1 \geq_{lex} \alpha^2 \geq_{lex} \alpha^3 \geq_{lex} \dots$ una sucesión en $\mathbb{N}^n$. Como el orden usual en $\mathbb{N}$ es un buen orden, para cada $i \in \{1, \dots, n\}$ existe $p_i \in \mathbb{N}$ tal que $\alpha_i^j = \alpha_i^{p_i}$ para todo $j \geq p_i$. Sea $p = \sup\{p_1, \dots, p_n\}$. Entonces $\alpha^j = \alpha^p$ para todo $j \geq p$. Por (4.1.3), esto implica que “ $\leq_{lex}$ ” es un buen orden.

(4.1.5) El orden lexicográfico depende de la ordenación con que tomemos las variables. En efecto, para el orden “ $\leq_{lex}$ ” del ejemplo anterior,

$$x_1 >_{lex} x_2 >_{lex} \dots >_{lex} x_n.$$

Si σ es una permutación de orden n , el orden lexicográfico con

$$x_{\sigma(1)} \geq \dots \geq x_{\sigma(n)}$$

viene dado por

$$\alpha <_{lex}^{\sigma} \beta \Leftrightarrow \exists i \in \{1, \dots, n\}, \begin{cases} \alpha_{\sigma(j)} = \beta_{\sigma(j)} \text{ si } 1 \leq j < i, \\ \alpha_{\sigma(i)} < \beta_{\sigma(i)} \end{cases}.$$

La relación “ $\leq_{lex}^{\sigma}$ ” es un orden monomial en $k[x_1, \dots, x_n]$.

(4.1.6) Definición. Si $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, denotemos por $|\alpha|$ a la suma $\sum_{i=1}^n \alpha_i$. Se dice que un orden “ $\leq$ ” en $\mathbb{N}^n$ es graduado si siempre que $|\alpha| < |\beta|$ entonces $\alpha < \beta$.

El orden lexicográfico (con $x_1 > x_2 > \dots > x_n$, por ejemplo) no es un orden graduado, porque por ejemplo $|(2, 0)| < |(1, 5)|$, mientras que $x_1^2 > x_1 x_2^5$.

(4.1.7) Ejemplo. Orden lexicográfico graduado. Definamos en $\mathbb{N}^n$

$$\alpha <_{glex} \beta \Leftrightarrow \begin{cases} |\alpha| < |\beta|, \\ \text{o } |\alpha| = |\beta| \text{ y } \alpha <_{lex} \beta \end{cases}.$$

La relación “ $\leq_{glex}$ ” es un orden monomial graduado en $k[x_1, \dots, x_n]$ y $x_1 >_{glex} x_2 >_{glex} \dots >_{glex} x_n$.

De nuevo, para cada permutación σ de orden n ,

$$\alpha <_{glex}^{\sigma} \beta \Leftrightarrow \begin{cases} |\alpha| < |\beta|, \\ \text{o } |\alpha| = |\beta| \text{ y } \alpha <_{lex}^{\sigma} \beta \end{cases}$$

define un orden monomial graduado en $k[x_1, \dots, x_n]$ con

$$x_{\sigma(1)} >_{\text{glex}}^{\sigma} x_{\sigma(2)} >_{\text{glex}}^{\sigma} \cdots >_{\text{glex}}^{\sigma} x_{\sigma(n)}.$$

(4.1.8) Ejemplo. Orden lexicográfico inverso. Definamos en $\mathbb{N}^n$

$$\alpha <_{\text{grevlex}} \beta \Leftrightarrow \begin{cases} |\alpha| < |\beta|, \\ \text{o } |\alpha| = |\beta| \text{ y } \exists i \in \{1, \dots, n\}, \begin{cases} \alpha_j = \beta_j \text{ si } i < j \leq n, \\ \alpha_i \geq \beta_i \end{cases} \end{cases}.$$

La relación “ $\leq_{\text{grevlex}}$ ” es un orden monomial graduado en $k[x_1, \dots, x_n]$ en el que $x_1 >_{\text{grevlex}} x_2 >_{\text{grevlex}} \cdots >_{\text{grevlex}} x_n$.

Si σ es una permutación de orden n , entonces

$$\alpha \leq_{\text{grevlex}}^{\sigma} \beta \Leftrightarrow (\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) \leq_{\text{grevlex}} (\beta_{\sigma(1)}, \dots, \beta_{\sigma(n)})$$

es un orden monomial graduado para el que

$$x_{\sigma(1)} >_{\text{grevlex}}^{\sigma} \cdots >_{\text{grevlex}}^{\sigma} x_n.$$

(4.1.9) Si $n = 1$, entonces $\leq_{\text{lex}} \equiv \leq_{\text{glex}} \equiv \leq_{\text{grevlex}}$ y coincide con el orden usual en $\mathbb{N}$.

Si $n = 2$, entonces $\leq_{\text{glex}} \equiv \leq_{\text{grevlex}} \not\equiv \leq_{\text{lex}}$.

Si $n = 3$, entonces $\leq_{\text{lex}} \not\equiv \leq_{\text{glex}} \not\equiv \leq_{\text{grevlex}}$. Por ejemplo, $x^2 y z^3 \leq_{\text{grevlex}} x y^3 z^2$ pero $x^2 y z^3 \geq_{\text{glex}} x y^3 z^2$.

En general, si $n \geq 2$ y $\alpha \in \mathbb{N}^n$ con $\alpha_i \geq 1$ para algún $i \in \{1, \dots, n-1\}$, entonces $\{\beta \in \mathbb{N}^n; \beta \leq_{\text{lex}} \alpha\}$ es no finito.

Sin embargo, si $\leq$ es un orden graduado, entonces $\{\beta \in \mathbb{N}^n; \beta \leq \alpha\}$ es finito para todo $\alpha \in \mathbb{N}^n$.

(4.1.10) Definición. Sea “ $\leq$ ” un orden monomial en $k[x_1, \dots, x_n]$. Si

$$f = \sum_{\alpha \in \mathbb{N}^n} c_{\alpha} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in k[x_1, \dots, x_n],$$

entonces

(4.1.10.1) se llama exponente inicial de f respecto de “ $\leq$ ”, y se denota $\exp_{\leq} f$, a $\max\{\beta \in \mathbb{N}; c_{\beta} \neq 0\}$ (usando el orden total “ $\leq$ ”);

(4.1.10.2) se llama monomio inicial de f respecto de “ $\leq$ ”, y se denota $lm_{\leq} f$, a $\mathbf{x}^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ donde $\alpha = \exp_{\leq} f$;

(4.1.10.3) se llama coeficiente director de f respecto de “ $\leq$ ”, y se denota por $lc_{\leq} f$, a c_{α} tal que $\alpha = \exp_{\leq} f$;

(4.1.10.4) se llama forma inicial de f respecto de “ $\leq$ ”, y se denota $in_{\leq} f$, a $c_{\alpha} \mathbf{x}^{\alpha} = c_{\alpha} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ donde $\alpha = \exp_{\leq} f$.

(4.1.11) Ejemplo. Sea

$$u = (u_1, \dots, u_n) \in \mathbb{N}^n \setminus \{(0, \dots, 0)\}$$

y “ $\leq_\sigma$ ” un orden monomial en $k[x_1, \dots, x_n]$. Definamos

$$(\alpha_1, \dots, \alpha_n) <_{\sigma, u} (\beta_1, \dots, \beta_n) \Leftrightarrow \begin{cases} \alpha \cdot u < \beta \cdot u \\ \text{o } \alpha \cdot u = \beta \cdot u, \alpha <_\sigma \beta \end{cases}.$$

La relación $\leq_{u, \sigma}$ es un orden monomial en $k[x_1, \dots, x_n]$ que se denomina orden pesado determinado por u y el orden $\leq_\sigma$.

Si $u = (1, \dots, \overset{i}{1}, 0, \dots, 0)$ y “ $\leq_\sigma$ ” = “ $\leq_{\text{grevlex}}$ ”, al orden pesado $\leq_{u, \text{grevlex}}$ se le denomina i -ésimo orden de eliminación porque verifica la siguiente propiedad:

(4.1.11.1) i -ésima propiedad de eliminación: Si $f \in k[x_1, \dots, x_n]$ e

$$\text{in}_{\leq_{u, \text{grevlex}}} f \in k[x_{i+1}, \dots, x_n],$$

entonces $f \in k[x_{i+1}, \dots, x_n]$.

El orden “ $\leq_{\text{lex}}$ ” también verifica esta propiedad.

(4.1.12) Ejemplo. Sea “ $\leq_1$ ” un orden monomial en $k[x_1, \dots, x_n]$ y “ $\leq_2$ ” un orden monomial en $k[y_1, \dots, y_m]$. La relación $\leq$, donde

$$\begin{aligned} & (\alpha_1, \dots, \alpha_n, \alpha_{n+1}, \dots, \alpha_{n+m}) < (\beta_1, \dots, \beta_n, \beta_{n+1}, \dots, \beta_{n+m}) \\ \Leftrightarrow & \begin{cases} (\alpha_1, \dots, \alpha_n) <_1 (\beta_1, \dots, \beta_n) \\ \text{o } (\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n), (\alpha_{n+1}, \dots, \alpha_{n+m}) <_2 (\beta_{n+1}, \dots, \beta_{n+m}), \end{cases} \end{aligned}$$

es un orden monomial en $k[x_1, \dots, x_n, y_1, \dots, y_m]$ que se denomina orden producto de $\leq_1$ y $\leq_2$.

(4.1.13) Proposición. Sea “ $\leq$ ” un orden monomial en $k[x_1, \dots, x_n]$ y $f, g \in k[x_1, \dots, x_n]$. Entonces

$$(4.1.13.1) \quad \exp(fg) = \exp f + \exp g;$$

$$(4.1.13.2) \quad \text{in}(fg) = \text{in} f + \text{in} g;$$

$$(4.1.13.3) \quad \exp(f+g) \leq \max\{\exp f, \exp g\}.$$