Bases de Groebner

4.2. Lema de Dickson

(4.2.1) Definición. Un ideal I de $k[x_1 \dots, x_n]$ se dice que es monomial si existe $E \subseteq \mathbb{N}^n$, $E \neq \emptyset$ tal que $I = (\mathbf{x}^\alpha; \alpha \in E)$.

(4.2.2) Lema. *Si $I = (\mathbf{x}^\alpha; \alpha \in E)$ es un ideal monomial de $k[x_1, \dots, x_n]$, entonces un monomio $\mathbf{x}^\beta$ pertenece a I si, y sólo si existe $\alpha \in E$ tal que $\beta = \alpha + \gamma$ para algún $\gamma \in \mathbb{N}$.*

Demostración. Si $\beta = \alpha + \gamma$, con $\gamma \in E$, entonces $\mathbf{x}^\beta \in I$.
Recíprocamente, si $\mathbf{x}^\beta \in I$, entonces existen

$$\alpha^1, \dots, \alpha^s \in E \quad \text{y} \quad h_1, \dots, h_s \in k[x_1, \dots, x_n]$$

tales que

$$\mathbf{x}^\beta = \sum_{i=1}^{s} \mathbf{x}^{\alpha^i} h_i.$$

Si $h_i = \sum_{j=1}^{r_i} \;_{ij}\mathbf{x}^{\;\;i}$, entonces

$$\mathbf{x}^\beta = \sum_{i=1}^{s} \sum_{j=1}^{r_i} \;_{ij}\mathbf{x}^{\alpha^i \;\;\; i},$$

de donde existe $\;, j$ tales que $\beta = \alpha^i + \gamma^{ij}$. $\square$

(4.2.3) Lema. *Sea $I = (\mathbf{x}^\alpha; \alpha \in E)$ un ideal monomial de $k[x_1, \dots, x_n]$ con $\emptyset \neq E \subseteq \mathbb{N}^n$. ntonces $\;\in I$ si, y sólo si los monomios de pertenecen a I. ec´procamente, si I es un ideal de $k[x_1, \dots, x_n]$ de manera que los monomios de cualquier elemento de pertenecen a I, entonces I es monomial.*

Demostración. Sea $I = (\mathbf{x}^\alpha)_{\alpha \in E}$ monomial y $\;\in I$. Si $\; = \sum_{j=1}^{r} a_j \mathbf{x}^{\beta}$, entonces existen $\alpha^1, \dots, \alpha^s \in E$ y $h_1, \dots, h_s \in k[x_1, \dots, x_n]$ tales que

$$= \sum_{l=1}^{s} h_l \mathbf{x}^{\alpha^l}.$$

Si $h_i = \sum_{j=1}^{r_i} \ _{ij}\mathbf{x}^{\ \ i}$, entonces

$$= \sum_{j=1}^{r} a_j \mathbf{x}^{\beta} \ = \sum_{i=1}^{s} \sum_{j=1}^{r_i} \ _{ij}\mathbf{x}^{\ \ i \ \ \alpha^i},$$

de donde $a_j\mathbf{x}^{\beta}$ es combinación lineal de potencias $\mathbf{x}^{\ \ i \ \ \alpha^i}$, y por lo tanto pertenece a I.

Recíprocamente, si los monomios que forman un polinomio pertenecen a I, entonces también pertenece a I por ser suma de elementos de I.

Sea ahora I un ideal tal que $\in I$ si, y sólo si los monomios de pertenecen a I. Si E es el conjunto de todos los exponentes de los monomios de los elementos de I, entonces

$$\{\mathbf{x}^{\alpha}\}_{\alpha\in E} \subseteq I \subseteq (\mathbf{x}^{\alpha})_{\alpha\in E},$$

y por lo tanto $I = (\mathbf{x}^{\alpha})_{\alpha\in E}$. □

(4.2.4) Lema. (de Dickson). *Si $I = (\mathbf{x}^{\alpha}; \alpha \in E)$ es un ideal monomial de $k[x_1, \ldots, x_n]$ con $\emptyset \neq E \subseteq \mathbb{N}^n$, entonces existen $\alpha^1, \ldots, \alpha^r \in E$ tales que $I = (\mathbf{x}^{\alpha^1}, \ldots, \mathbf{x}^{\alpha^r})$.*

Demostración. Inducción sobre n.

Si $n = 1$, entonces el ideal monomial $I = (x^{\alpha}; \alpha \in E)$ es principal y generado por x^{β}, donde $\beta = \min E$.

Supongamos que todo ideal monomial $I = (\mathbf{x}^{\alpha}; \alpha \in E)$ de $k[x_1, \ldots, x_{n-1}]$ es generado por un subconjunto finito de $\{\mathbf{x}^{\alpha}\}_{\alpha\in E}$, y sea $I = (\mathbf{x}^{\alpha}; \alpha \in E)$ un ideal monomial de $k[x_1, \ldots, x_n]$. Denotemos a x_n por y, y consideremos el ideal monomial J de $k[x_1, \ldots, x_{n-1}]$ generado por el conjunto

$$\{\mathbf{x}^{\alpha}; \exists r \in \mathbb{N}, \mathbf{x}^{\alpha} y^r \in I\}.$$

Por la hipótesis de inducción, existen $\alpha^1, \ldots, \alpha^s \in \mathbb{N}^{n-1}$ y $m_1, \ldots, m_s \in \mathbb{N}$ tales que $\mathbf{x}^{\alpha^i} y^{m_i} \in I$ y $\mathbf{x}^{\alpha^1}, \ldots, \mathbf{x}^{\alpha^s}$ genera J. Sea $m = \max\{m_1, \ldots, m_s\}$, y consideremos los monomios $\mathbf{x}^{\alpha^1} y^m, \ldots, \mathbf{x}^{\alpha^s} y^m \in I$.

Para cada $p \in \{0, \ldots, m-1\}$ sea J_p el ideal monomial de $k[x_1, \ldots, x_{n-1}]$ generado por los monomios $\mathbf{x}^{\alpha}$ tal que $\mathbf{x}^{\alpha} y^k \in I$. Por la hipótesis de inducción, existen $\alpha^{p1}, \ldots, \alpha^{ps_p}$ tales que $\mathbf{x}^{\alpha^{p1}}, \ldots, \mathbf{x}^{\alpha^{ps_p}}$ genera a J_p. El conjunto

$$S = \{\mathbf{x}^{\alpha^1} y^m, \ldots, \mathbf{x}^{\alpha^s} y^m\} \cup (\bigcup_{p=0}^{m-1} \{\mathbf{x}^{\alpha^{p1}} y^p, \ldots, \mathbf{x}^{\alpha^{ps_p}} y^p\})$$

es un sistema generador de I.

Además, si $\{\mathbf{x}^{\beta^1}, \ldots, \mathbf{x}^{\beta^s}\}$ es un sistema generador de $I = (\mathbf{x}^{\alpha^1})_{\alpha \in E}$, entonces cada $\mathbf{x}^{\beta^i}$ es múltiplo de un $\mathbf{x}^{\alpha^i}$ con $\alpha^i \in E$ y por lo tanto $\{\mathbf{x}^{\alpha^1}, \ldots, \mathbf{x}^{\alpha^s}\}$ es un sistema generador de I. $\square$

(4.2.5) Corolario. *Sea "$\leq$" una relación en $\mathbb{N}^n$ tal que*

(4.2.5.1) *"$\leq$" es un orden total;*

(4.2.5.2) *si $\alpha \leq \beta, \gamma \in \mathbb{N}^n$ entonces $\alpha + \gamma \leq \beta + \gamma$;*

(4.2.5.3) *$\alpha \geq (0, \ldots, 0)$ para todo $\alpha \in \mathbb{N}^n$.*

ntonces "$\leq$" es un orden monomial en $k[x_1, \ldots, x_n]$.