Bases de Groebner

4.3. Algoritmo de división

(4.3.1) Proposición. (Algoritmo de división de Hironaka). *Sea "$\leq$" un orden monomial en $k[x_1, \ldots, x_n]$ y $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Sea*

$$\Delta_1 = expf_1 + \mathbb{N}^n \quad , \quad \Delta_i = (expf_i + \mathbb{N}^n) \backslash \bigcup_{j=1}^{i-1} \Delta_j$$

para cada $i \in \{2, \ldots, s\}$ y

$$\overline{\Delta} = \mathbb{N}^n \backslash \bigcup_{i=1}^{s} \Delta_i.$$

Entonces para todo $f \in k[x_1, \ldots, x_n]$ existen unos únicos

$$q_1, \ldots, q_s, r \in k[x_1, \ldots, x_n]$$

tales que

(4.3.1.1) $f = q_1 f_1 + \cdots + q_s f_s + r$;

(4.3.1.2) *si $q_i \neq 0$, $q_i = \sum_\alpha c_\alpha \mathbf{x}^\alpha$, entonces $\alpha + expf_i \in \Delta_i$ para cada $\alpha \in \mathbb{N}^n$ tal que $c_\alpha \neq 0$;*

(4.3.1.3) *si $r = \sum_\alpha c_\alpha \mathbf{x}^\alpha$, entonces $\alpha \in \overline{\Delta}$ para cada α tal que $c_{\alpha \neq 0}$.*

Demostración. Veamos primero la unicidad. Supongamos que $q_1, \ldots, q_s, r$ y $q_1', \ldots, q_s', r' \in k[x_1, \ldots, x_n]$ satisfacen (1),(2) y (3). Entonces

$$0 = f - f = (q_1 - q_1')f_1 + \cdots + (q_s - q_s')f_s + (r - r').$$

Supongamos que $r \neq r'$. Luego

$$(q_1 - q_1')f_1 + \cdots + (q_s - q_s')f_s = -(r - r') \neq 0.$$

Pero esto contradice el hecho de que $\Delta_1, \ldots, \Delta_s, \overline{\Delta}$ es una partición de $\mathbb{N}^n$, ya que $in(r - r') \in \overline{\Delta}$ e

$$in((q_1 - q_1')f_1 + \cdots + (q_s - q_s')f_s) \in \cup_{i=1}^s \Delta_i.$$

Por lo tanto $r = r'$.
Sea $i \in 1, \ldots, s$ y supongamos que $q_i \neq q_i'$. Dado que

$$(q_i' - q_i)f_i = (q_1 - q_1')f_1 + \cdots + (q_{i-1} - q_{i-1}')f_{i-1} + (q_{i+1} - q_{i+1}')f_{i+1} + \cdots + (q_s - q_s')f_s,$$

esto contradice que $\Delta_i \cap \bigcup_{j \neq i} \Delta_j = \emptyset$, ya que

$$in(q_i' - q_i)f_i \in \Delta_i$$

e

$$in((q_1 - q_1')f_1 + \cdots + (q_{i-1} - q_{i-1}')f_{i-1}$$
$$+(q_{i+1} - q_{i+1}')f_{i+1} + \cdots + (q_s - q_s')f_s) \in \bigcup_{j \neq i} \Delta_j.$$

Luego $q_i = q_i'$ para cada i.
Para probar la existencia, describiremos el algoritmo.
Comencemos con $q_1 = \cdots = q_s = r = 0$ y sea $f = f^{(0)}, f^{(1)}, f^{(2)}, \ldots$ la sucesión de polinomios construida recursivamente por

$$f^{(i+1)} = \begin{cases} f^{(i)} - inf^{(i)}, & \text{si } inf \in \overline{\Delta}, \text{y en ese caso sumamos } inf^{(i)} \text{ a } r \\ f^{(i)} - inf^{(i)}/inf_j f_j, & \text{si } inf \in \Delta_j, \text{ y sumamos } inf^{(i)}/inf_j \text{ a } q_j \end{cases}$$

De esta manera obtenemos una sucesión decreciente para el orden monomial "$\leq$"

$$expf^{(0)} \geq expf^{(1)} \geq expf^{(2)} \geq \cdots,$$

y dado que "$\leq$" es un buen orden, existe p tal que $f^{(i)} = f^{(p)}$ para todo $i \geq p$. Esto significa que $f^{(p)} = 0$, y por lo tanto $q_1, \ldots, q_s, r$, que por construcción satisfacen (2) y (3), verifican que

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

□