Polinomi simmetrici

§1.1 Definizione e prime proprietà

Sia $\mathbb{K}$ un campo. Dati $\sigma \in S_n$ e un polinomio $f \in \mathbb{K}[x_1, \ldots, x_n]$, si definisce il seguente polinomio:

$$(\sigma \cdot f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

ossia il polinomio ottenuto permutando le variabili x_i secondo σ.

Definizione 1.1.1. Si definisce $\mathrm{Sym}[X_n]$ su K come il sottoanello di $\mathbb{K}[x_1, \ldots, x_n]$ dei **polinomi simmetrici**, ossia di quei polinomi tali che $\sigma \cdot f = f$, $\forall\, \sigma \in S_n$.

Definizione 1.1.2. Sia $d \in \mathbb{N}$ tale che $0 \leq d \leq n$. Si definisce **polinomio simmetrico elementare** su $\mathrm{Sym}[X_n]$ ogni polinomio della seguente forma:

$$e_d(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \cdots < i_d \leq n} \underbrace{x_{i_1} \cdots x_{i_n}}_{d \text{ volte}},$$

dove si pone $e_0(x_1, \ldots, x_n) := 1$

Osservazione. Qualora siano noti al contesto le variabili su cui è definito $\mathrm{Sym}[X_n]$ si può omettere la parentesi di e_d, scrivendo pertanto semplicemente e_d.

Osservazione. Sia $p(x) = a_n x^n + \ldots + a_0$ un polinomio in $\mathbb{K}[x]$. Siano λ_1, ..., λ_n le sue radici nel suo campo di spezzamento. Allora vale che:

$$a_{n-i} = (-1)^i\, a_n\, e_i(\lambda_1, \ldots, \lambda_n).$$

Definizione 1.1.3. Sia $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, si definisce:

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \quad |\alpha| = \sum_{i=1}^{n} \alpha_i.$$

Osservazione. Ogni monomio nelle variabili x_1, ..., x_n può essere rappresentato nella forma x^α, ponendo α_i uguale al numero di volte in cui la variabile x_i compare nel monomio.

Definizione 1.1.4. Si definisce *degree lexicographic order* (**deglex**) la seguente relazione di ordine sui monomi monici di un polinomio:

$$x^\alpha > x^\beta \overset{\text{def}}{\iff} |\alpha| > |\beta| \text{ oppure } |\alpha| = |\beta| \text{ e } \alpha > \beta \text{ secondo il LO},$$

dove con LO si indica il *lexicographic order*.

Osservazione 1.1.5. Il *deglex* è una relazione di ordine totale.

Proposizione 1.1.6

Vale la seguente equivalenza:

$$x^\alpha x^\gamma > x^\beta x^\gamma \iff x^\alpha > x^\beta.$$

Dimostrazione. Si dimostrano le due implicazioni separamente.

($\Longrightarrow$) Se $|\alpha| + |\gamma| > |\beta| + |\gamma|$, allora anche $|\alpha| > |\beta|$, e dunque $x^\alpha > x^\beta$. Altrimenti, esiste un $i \in \mathbb{N}$ tale per cui $\alpha_i + \gamma_i > \beta_i + \gamma_i$ e $\alpha_j + \gamma_j = \beta_j + \gamma_j \ \forall\, j < i$. Allora anche $\alpha_j = \beta_j \ \forall\, j < i$ e $\alpha_i > \beta_i$. Dunque, per il LO, $\alpha > \beta$, e quindi $x^\alpha > x^\beta$.

($\Longleftarrow$) Se $|\alpha| > |\beta|$, allora anche $|\alpha| + |\gamma| > |\beta| + |\gamma|$, e dunque $x^\alpha x^\gamma > x^\beta x^\gamma$. Altrimenti, esiste un $i \in \mathbb{N}$ tale per cui $\alpha_i > \beta_i$ e $\alpha_j = \beta_j \ \forall\, j < i$. Allora anche $\alpha_j + \gamma_j = \beta_j + \gamma_j$ $\forall\, j < i$ e $\alpha_i + \gamma_i > \beta_i + \gamma_i$. Dunque, per il LO, $\alpha + \gamma > \beta + \gamma$, e quindi $x^\alpha x^\gamma > x^\beta x^\gamma$. □

Proposizione 1.1.7

Sia $\alpha \in \mathbb{N}^n$. Allora esiste un numero finito di $\beta \in \mathbb{N}^n$ tale che $x^\alpha > x^\beta$.

Dimostrazione. Siano fissati gli α_i. Se $x^\alpha > x^\beta$, allora vale sicuramente l'equazione:

$$\alpha_1 + \ldots + \alpha_n > \beta_1 + \ldots + \beta_n,$$

che ammette un numero finito di soluzioni. □

Definizione 1.1.8. Si definisce **leading term** di un polinomio in x_1, ..., x_n il termine cx^α tale che $x^\alpha > x^\beta$, per ogni altro monomio x^β del polinomio.

Proposizione 1.1.9

Siano f e $g \in \mathbb{K}[x_1, \dots, x_n]$. Il *leading term* di fg è il prodotto dei *leading term* di f e di g.

Dimostrazione. Siano x^α e x^β i rispettivi *leading term* di f e di g. Sia inoltre x^γ il *leading term* di fg. Si assuma che $x^\gamma \neq x^\alpha x^\beta$.

Poiché ogni monomio del prodotto di fg è un prodotto di due monomi di f e di g, x^γ potrà scriversi come prodotto di $x^\delta x^\zeta$, dove x^δ è un monomio di f e x^ζ è un monomio di g.

Poiché x^α è il *leading term* di f, vale la seguente disuguaglianza:

$$x^\alpha > x^\delta,$$

da cui, dalla *Proposizione 1.1.6*, si ricava che:

$$x^\alpha x^\zeta > x^\delta x^\zeta.$$

Analogamente vale la seguente altra disuguaglianza:

$$x^\beta > x^\zeta,$$

da cui si ottiene che:

$$x^\alpha x^\beta > x^\alpha x^\zeta.$$

Combinando le due disuguaglianze si ottiene infine che:

$$x^\alpha x^\beta > x^\delta x^\zeta,$$

che è assurdo, dal momento che $x^\delta x^\zeta = x^\gamma$ è il *leading term* di fg, ↯. Quindi $x^\gamma = x^\alpha x^\beta$. □

Lemma 1.1.10

Sia cx^α il *leading term* di $f \in \mathrm{Sym}[X_n]$, con $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. Allora $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$.

Dimostrazione. Si dimostra la tesi contronominalmente.

Sia cx^β un monomio di f con $\beta = (\beta_1, \dots, \beta_n)$ tale che esistano $i < j \mid \beta_i < \beta_j$. Si consideri $\gamma \in \mathbb{N}^n$ come la tupla riordinata in modo decrescente di β e sia $\sigma \in S_n$ tale che $\gamma = (\beta_{\sigma(1)}, \dots, \beta_{\sigma(n)})$.

Poiché f è un polinomio simmetrico, $\sigma \cdot f = f$. Quindi f ammette un monomio della forma cx^γ. Dal momento che $\gamma > \beta$ per il LO, $x^\gamma > x^\beta$. Quindi cx^β non è il *leading term* di f. □

Teorema 1.1.11 (*Teorema fondamentale dei polinomi simmetrici*)
Sia $\mathbb{K}$ un campo. Vale il seguente isomorfismo:

$$\mathrm{Sym}[X_n] \cong \mathbb{K}[e_1, \dots, e_n].$$

Dimostrazione. Sia cx^α il *leading term* di f, con $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. Per il *Lemma 1.1.10*, $\alpha_i - \alpha_{i+1} \geq 0 \; \forall \, 1 \leq i < n$.

Si definisca dunque $\beta \in \mathbb{N}^n$ in modo tale che $\beta_i = \alpha_i - \alpha_{i+1} \geq 0 \; \forall \, 1 \leq i < n$ e $\beta_n = \alpha_n$.

Si consideri il monomio $e_1^{\beta_1} e_2^{\beta_2} \dots e_n^{\beta_n}$: il suo *leading term*, per la *Proposizione 1.1.9*, è il prodotto dei *leading term* dei suoi fattori, ossia $x_1^{\alpha_1} \cdots x_n^{\alpha_n} = x^\alpha$.

Si consideri adesso come polinomio $f - ce_1^{\beta_1} e_2^{\beta_2} \dots e_n^{\beta_n}$, e si reiteri l'algoritmo fino a quando il risultato non è zero. Che l'algoritmo termini è garantito dalla *Proposizione 1.1.7*, da cui si desume che vi è numero finito di *leading term* possibili una volta tolto ad ogni iterazione il termine $ce_1^{\beta_1} e_2^{\beta_2} \dots e_n^{\beta_n}$.

Infine si sarà ottenuto una rappresentazione di f come combinazione di e_1, ..., e_n. Questa rappresentazione è unica perché i termini $e_1^{\beta_1} e_2^{\beta_2} \dots e_n^{\beta_n}$ sono linearmente indipendenti, dal momento che i loro *leading term* sono distinti.

Si costruisca dunque l'omomorfismo $\Pi : \mathrm{Sym}[X_n] \to \mathbb{K}[e_1, \dots, e_n]$ che associa ad ogni polinomio simmetrico la sua rappresentazione in $\mathbb{K}[e_1, \dots, e_n]$.

Si verifica che Π è un omomorfismo. Poiché tale omomorfismo è iniettivo e surgettivo, è un isomorfismo, da cui la tesi. □