

Polinomi simmetrici e omogenei

In sottogruppi finiti di un campo (\mathbb{K}, \cdot)

Andrea Marino

September 4, 2014

Trattazione

Polinomi simmetrici, campi e gruppi. Sia \mathbb{K} un campo, e sia G un sottogruppo finito di (\mathbb{K}, \cdot) . Detto $t = |G| = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, sia $p \in \mathbb{K}[x_1, \dots, x_t]$ un polinomio simmetrico e omogeneo di grado n , e sia $\ell(t) = \text{lcm}(\varphi(p_1^{\alpha_1}), \dots, \varphi(p_k^{\alpha_k}))$. Se $\ell(t) \nmid n$, allora $p(x_1, \dots, x_t) = 0$, dove $\{x_1, \dots, x_t\}$ sono gli elementi di G .

Dimostrazione

Step 1

Sia r un intero positivo. Se $\ell(t) \nmid r$, allora esiste un $a \in G$ tale che $a^r \neq 1$.

Per il teorema dei gruppi abeliani finitamente generati, esistono dei gruppi ciclici C_{q_1}, \dots, C_{q_m} tali che

$$G = C_{q_1} \otimes \dots \otimes C_{q_m}$$

con q_1, \dots, q_m potenze di primi tali che $q_1 \cdot \dots \cdot q_m = t$. Visto che $\ell(t) \nmid r$, esisterà almeno un primo $s \mid \ell(t)$ tale che $s \nmid r$. Inoltre, dal fatto che

$$\varphi(q_1) \cdot \dots \cdot \varphi(q_m) = \varphi(q_1 \cdot \dots \cdot q_m) = \varphi(t) = \varphi(p_1^{\alpha_1}) \cdot \dots \cdot \varphi(p_k^{\alpha_k})$$

e che l'ultimo membro ha gli stessi fattori primi di $\ell(t)$, esisterà anche un q_i tale che $s \mid \varphi(q_i)$. Sia g un generatore di C_{q_i} . Allora $g^r \neq 1$, perchè $s \mid \varphi(q_i)$, $s \nmid r \Rightarrow \varphi(q_i) \nmid r$. D'altronde $g \in C_{q_i} \Rightarrow g \in G$, e dunque abbiamo trovato l'elemento che cercavamo.

Step 2

Sia r un intero positivo, e sia

$$\sigma_r(X) = \sum_{X_r \subseteq X} \prod_{x \in X_r} x$$

dove si intende che $|X_r| = r \leq |X|$ (e che le operazioni sono tutte in \mathbb{K}).

Allora se $\ell(t) \nmid r$ si ha $\sigma_r(G) = 0$.

Richiamiamo il fatto che se $a \in G$ allora la classe laterale aG coincide con G .

Consideriamo un elemento $g \in G$ tale che $g^r \neq 1$ (esiste per lo step precedente).

Allora, usando la commutatività G , la simmetria e l'omogeneità di σ_r :

$$g^r \sigma_r(G) = g^r \sum_{X_r \subseteq G} \prod_{x \in X_r} x = \sum_{X_r \subseteq G} \prod_{x \in X_r} gx = \sigma_r(gG) = \sigma_r(G)$$

da cui, per la commutatività di \mathbb{K} rispetto a $+$:

$$(g^r - 1)\sigma_r(G) = 0$$

D'altronde per ipotesi $g^r \neq 1$, perciò $\sigma_r(G) = 0$ per la legge di annullamento del prodotto.

Conclusione. Per il teorema fondamentale dei polinomi simmetrici, il polinomio simmetrico $p(x_1, \dots, x_t)$ può essere scritto come $q(\sigma_1(G), \dots, \sigma_t(G))$ per qualche $q \in \mathbb{K}[x_1, \dots, x_t]$, dove $G = \{x_1, \dots, x_t\}$. Consideriamo un monomio M di $q(\cdot)$, della forma $c \cdot \sigma_{a_1}^{b_1}(G) \cdot \dots \cdot \sigma_{a_m}^{b_m}(G)$ per alcuni $c, m, a_1, b_1, \dots, a_m, b_m$ interi. Visto che p è omogeneo, tutti i monomi di q devono avere grado n in termini di x_1, \dots, x_t . Perciò

$$b_1 a_1 + \dots + b_m a_m = \deg(M) = n$$

Supponiamo per assurdo che $\ell(t) \mid a_i$ per ogni $i = 1, \dots, m$. Allora $\ell(t) \mid b_1 a_1 + \dots + b_m a_m = n$, assurdo per ipotesi. Dunque esiste un a_i tale che $\ell(t) \nmid a_i$. Ma allora, per quanto detto allo step 2, abbiamo che $\sigma_{a_i}(G) = 0$. Perciò $M = 0$.

Ogni monomio in $q(\cdot)$ vale 0, e dunque

$$p(x_1, \dots, x_t) = q(\sigma_1(G), \dots, \sigma_t(G)) = 0$$

che è la tesi.