Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 19-05-2020

Campo fisso di un gruppo di automorfismi

G gruppo, X G-insieme $\implies$

$$X^G := \{x \in X \,:\, gx = x \;\forall\, g \in G\} \subseteq X.$$

L campo, $G < \mathrm{G}(L) \implies$

$$L^G = \{\alpha \in L \,:\, \sigma(\alpha) = \alpha \;\forall\, \sigma \in G\} \subseteq L$$

sottocampo (detto campo fisso di G).

Teorema (Artin)

L campo, $G < \mathrm{G}(L)$ finito $\implies [L : L^G] \leq \#G$.

Dimostrazione (inizio).

$\#G = m$, $G = \{\sigma_1 = \mathrm{id}_L, \ldots, \sigma_m\}$.

Dati $\alpha_1, \ldots, \alpha_n \in L$ distinti con $n > m$, basta dimostrare che $\{\alpha_1, \ldots, \alpha_n\}$ è linearmente dipendente su L^G.

$v_j := (\sigma_1(\alpha_j), \ldots, \sigma_m(\alpha_j)) \in L^m$ (per $j = 1, \ldots, n$) distinti.

Dimostrazione (fine)

$\{v_1, \ldots, v_n\}$ linearmente dipendente su L (perché $n > m$) $\implies$

$$W := \{(\beta_1, \ldots, \beta_n) \in L^n : \sum_{j=1}^{n} \beta_j v_j = 0\}$$

L-sottospazio vettoriale non nullo di L^n.

$\sigma \in G$, $(\beta_1, \ldots, \beta_n) \in W \implies (\sigma(\beta_1), \ldots, \sigma(\beta_n)) \in W$:
$(\beta_1, \ldots, \beta_n) \in W \iff \sum_{j=1}^{n} \beta_j \sigma_i(\alpha_j) = 0 \ \forall\, i = 1, \ldots, m \implies$
$\sum_{j=1}^{n} \sigma(\beta_j)(\sigma \circ \sigma_i)(\alpha_j) = 0 \ \forall\, i = 1, \ldots, m \iff$
$(\sigma(\beta_1), \ldots, \sigma(\beta_n)) \in W$ perché $\{\sigma \circ \sigma_1, \ldots, \sigma \circ \sigma_m\} = G$.

$(\gamma_1, \ldots, \gamma_n) \in W \setminus \{0\}$ ($\implies \exists j_0 \in \{1, \ldots, n\}$ tale che $\gamma_{j_0} \neq 0$ e posso supporre $\gamma_{j_0} = 1$) con il minimo numero di componenti $\neq 0$.

$\sigma \in G \implies \delta_j := \gamma_j - \sigma(\gamma_j)$ tali che $(\delta_1, \ldots, \delta_n) \in W$ e $\delta_j = 0$ se $\gamma_j = 0$ o $j = j_0 \implies (\delta_1, \ldots, \delta_n) = 0$ per l'ipotesi su $(\gamma_1, \ldots, \gamma_n)$
$\implies \gamma_j = \sigma(\gamma_j) \in L^G$ (per $j = 1, \ldots, n$) tali che $\sum_{j=1}^{n} \gamma_j \alpha_j = 0$
perché $\sum_{j=1}^{n} \gamma_j \sigma_i(\alpha_j) = 0 \ \forall\, i = 1, \ldots, m$ e $\sigma_1 = \mathrm{id}_L$.

Corrispondenza tra sottocampi e sottogruppi

L campo $\implies$ le funzioni

$$\phi\colon \{K : K \subseteq L \text{ sottocampo}\} \to \{G : G < \mathrm{G}(L)\} \quad K \mapsto \mathrm{G}_K(L)$$
$$\psi\colon \{G : G < \mathrm{G}(L)\} \to \{K : K \subseteq L \text{ sottocampo}\} \quad G \mapsto L^G$$

soddifano le seguenti proprietà:

i $K' \subseteq K \subseteq L$ sottocampi $\implies$ $\phi(K) \subseteq \phi(K')$ (cioè $\mathrm{G}_K(L) < \mathrm{G}_{K'}(L)$);

ii $G' < G < \mathrm{G}(L) \implies \psi(G) \subseteq \psi(G')$ (cioè $L^G \subseteq L^{G'}$);

iii $K \subseteq L$ sottocampo $\implies$ $K \subseteq \psi(\phi(K))$ (cioè $K \subseteq L^{\mathrm{G}_K(L)}$);

iv $G < \mathrm{G}(L) \implies G \subseteq \phi(\psi(G))$ (cioè $G < \mathrm{G}_{L^G}(L)$).

Segue formalmente che valgono queste ulteriori proprietà:

v $K \subseteq L$ sottocampo $\implies$ $\phi(K) = \phi(\psi(\phi(K)))$ (cioè $\mathrm{G}_K(L) = \mathrm{G}_{L^{\mathrm{G}_K(L)}}(L)$) perché $\phi(K) \subseteq \phi(\psi(\phi(K)))$ per iv e $K \subseteq \psi(\phi(K))$ per iii, quindi $\phi(\psi(\phi(K))) \subseteq \phi(K)$ per i;

vi $G < \mathrm{G}(L) \implies \psi(G) = \psi(\phi(\psi(G)))$ (cioè $L^G = L^{\mathrm{G}_{L^G}(L)}$).

Corrispondenza nel caso finito

Da v e vi segue anche che $\phi|_{\mathrm{im}(\psi)}\colon \mathrm{im}(\psi) \to \mathrm{im}(\phi)$ è biunivoca con inversa $\psi|_{\mathrm{im}(\phi)}\colon \mathrm{im}(\phi) \to \mathrm{im}(\psi)$, dove $\mathrm{im}(\psi) = \{L^G : G < \mathrm{G}(L)\}$ e $\mathrm{im}(\phi) = \{\mathrm{G}_K(L) : K \subseteq L \text{ sottocampo}\}$.

Teorema

1. $G < \mathrm{G}(L)$ *finito* $\implies$ $[L : L^G] = \#G$, $L^G \subseteq L$ *di Galois e* $G = \mathrm{G}_{L^G}(L)$.
2. $K \subseteq L$ *estensione finita* $\implies$ $\#\mathrm{G}_K(L) \leq [L : K]$ *e vale l'uguaglianza* $\iff$ $K \subseteq L$ *di Galois* $\iff$ $K = L^{\mathrm{G}_K(L)}$.

Corollario

$$\{K : K \subseteq L \text{ di Galois}\} \to \{G : G < \mathrm{G}(L) \text{ finito}\} \quad K \mapsto \mathrm{G}_K(L)$$

$$\{G : G < \mathrm{G}(L) \text{ finito}\} \to \{K : K \subseteq L \text{ di Galois}\} \quad G \mapsto L^G$$

sono funzioni biunivoche una l'inversa dell'altra e che invertono le inclusioni. Inoltre $K \subseteq L$ *di Galois* $\implies$ $\#\mathrm{G}_K(L) = [L : K]$.

Dimostrazione del Teorema

Sappiamo già che:

1' $G < \mathrm{G}(L)$ finito $\implies [L : L^G] \leq \#G$;

2' $K \subseteq L$ estensione finita $\implies \#\mathrm{G}_K(L) \leq [L : K]$ e vale l'uguaglianza $\iff K \subseteq L$ di Galois.

1. Per 1' $[L : L^G] \leq \#G < \infty$.
   Per iv $G < \mathrm{G}_{L^G}(L)$, e quindi $\#G \leq \#\mathrm{G}_{L^G}(L)$.
   Per 2' $\#\mathrm{G}_{L^G}(L) \leq [L : L^G]$.
   Dunque $[L : L^G] = \#G = \#\mathrm{G}_{L^G}(L)$ (per cui $G = \mathrm{G}_{L^G}(L)$) e, ancora per 2', $L^G \subseteq L$ di Galois.
2. Per iii $K \subseteq L^{\mathrm{G}_K(L)}$.
   Per 2' $\#\mathrm{G}_K(L) \leq [L : K] < \infty$.
   Per 1 $L^{\mathrm{G}_K(L)} \subseteq L$ di Galois e $[L : L^{\mathrm{G}_K(L)}] = \#\mathrm{G}_K(L)$.
   Dunque, se $K = L^{\mathrm{G}_K(L)}$, allora $K \subseteq L$ è di Galois.
   Viceversa, se $K \subseteq L$ è di Galois, allora, sempre per 2', $[L : K] = \#\mathrm{G}_K(L) = [L : L^{\mathrm{G}_K(L)}]$, da cui segue $K = L^{\mathrm{G}_K(L)}$.