Lezione N+1 Algebra 1

Federico De Sisti

2025-05-15

0.1 Teorema dell'elemento primitivo

Ricordo: Abbiamo dimostrato

Teorema 1
$\mathbb{F}$ campo infinito, allora ogni estensione separabile di grado finito è semplice

Teorema 2 (elemento primitivo)
$\mathbb{F}$ campo. Ogni estensione separabile di grado finito di $\mathbb{F}$ è semplice

Dimostrazione
si tratta di studiare il caso $|\mathbb{F}| < +\infty$. Sappiamo che il gruppo moltiplicativo $U_{\mathbb{F}} = \mathbb{F} \setminus \{0\}$ è ciclico.
Sia ora $\mathbb{F} \in \mathbb{K}$ estensione finita
$\Rightarrow \exists \alpha \in \mathbb{K}$ *tale che* $U_{\mathbb{K}} =< \alpha > \Rightarrow \mathbb{F} \subseteq \mathbb{F}(\alpha) = \mathbb{K}$ □
Osservazione
Nel caso finito non abbiamo usato l'ipotesi di estensione separabile
Il prossimo risultato è dimostrato da Galois(1831) di Steinitz(1910)

1 Teoria di Galois

Definizione 1
$\varphi : \mathbb{F} \to \mathbb{K}$ estensione di campi
$\overline{\varphi}_{\mathbb{K}} : \mathbb{K} \to \overline{\mathbb{K}}$ chiusura algebrica
Un $\mathbb{F}$-omomorfismo di $\mathbb{K}$ è un estensione $\psi : \mathbb{K} \to \overline{\mathbb{K}}$ tale che il diagramma (INSERISCI IMMAGINE 4 30), sia commutativo.

Esercizio:
L'insieme $I(\mathbb{K}, \mathbb{F})$ degli $\mathbb{F}$-omomorfismi di $\mathbb{K}$ non dipende dalla scelta di $\varphi_{\mathbb{K}}$
Esempio:
$\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{A}$
dove la prima freccia è φ e la seconda è $\overline{\phi}_k$
il polinomio minimo di $\sqrt[3]{2}$ è $x^3 - 2 \in \mathbb{Q}[x]$
$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega^2)$
dove $\omega = \frac{-1+i\sqrt{3}}{2} \in \mathbb{A}$
L'estensione

$$\begin{aligned} \psi : &\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{A} \\ &\sqrt[3]{2} \to \sqrt[3]{2}\omega \end{aligned}.$$

Proposizione 1
Sia $\mathbb{F} \subseteq \mathbb{K}$ estensione separabile e di grado finito, allora

$$|I(\mathbb{K}, \mathbb{F})| = [\mathbb{K} : \mathbb{F}].$$

Dimostrazione
Dal teorema dell'elemento primitivo $\exists \alpha \in \mathbb{K}$ *tale che* $\mathbb{F} \subseteq \mathbb{F}(\alpha) = \mathbb{K}$
Sia $\psi \in I(\mathbb{K}, \mathbb{F})$
ψ *è univocamente determinato da* $\psi(\alpha)$

- *dimostriamo che* $\alpha, \psi(\alpha)$ *sono coniugati*
  sia $f \in \mathbb{F}[x]$ *il polinomio minimo di* α, *allora* $0 = \psi(0) = \psi(f(\alpha)) = f(\psi(\alpha))$
  $\Rightarrow f$ *è il polinomio minimo di* $\psi(\alpha)$
- *per ogni radice* β *di* f *l'applicazione*

$$\begin{aligned} \psi_\beta : \mathbb{K} \setminus \mathbb{F}(\alpha) &\to \overline{\mathbb{K}} \\ \alpha \to \psi_(\alpha) &= \beta \end{aligned} .$$

  è un omomorfismo di anelli (con $im(\psi_\beta) = \mathbb{F}(\beta)$*)*
- *Dato che* $\mathbb{F} \subseteq \mathbb{K}$ *è estensione separabile* $\Rightarrow f$ *ammette* $\deg(f)$ *radici distinte, quindi*

$$|I(\mathbb{K}, \mathbb{F})| = deg(f) = [\mathbb{K} : \mathbb{F}].$$

□

Definizione 2 (Gruppo di Galois)
$\mathbb{F} \subseteq K$ *estensione. Il suo gruppo di Galoi s è* $(G(\mathbb{K}, \mathbb{F}), \circ)$ *dove*

$$G(\mathbb{K}, \mathbb{F}) = \{\sigma : \mathbb{K} \to \mathbb{K} \mid \sigma \text{ è isomorfismo di anelli e } \sigma|_{\mathbb{F}} = id_{\mathbb{F}}\}.$$

$e \circ$ *è la composizione*

Osservazione:
Data l'estensione $\varphi : \mathbb{F} \to \mathbb{K}$ e dato $\omega : \mathbb{K} \to \mathbb{K}$ scriveremo $\omega|_{\mathbb{F}} = id_{\mathbb{F}}$intendendo che, inserisci diagramma, è un diagramma commutativo.

Proposizione 2
$\mathbb{F} \subseteq Ł$ *estensione*

$$|G(\mathbb{K}, \mathbb{F})| \leq |I(\mathbb{K}, \mathbb{F})|.$$

Dimostrazione
Costruiamo un'applicazione iniettiva fra insiemi
G(K,F) $\to I(\mathbb{K}, \mathbb{F})$

inserisciimmagine

dove $\overline{\varphi}_{\mathbb{K}} : \mathbb{K} \to \overline{\mathbb{K}}$ *è una chiusura algebrica fissata*

- X *è ben definita poiché* $\sigma \in G(\mathbb{K}, \mathbb{F})$ *allora*
  INSERISCI IMMAGINE 4 58
  è un diagramma commutativo

- *Inoltre X è iniettiva poiché.*
  $X(\sigma_1) = X(\sigma_2)$
  $\Rightarrow \overline{\phi}_{\mathbb{K}} = \sigma_1 = \overline{\sigma}_{\mathbb{K}} = \sigma_2 \Rightarrow \sigma_1 = \sigma_2$

□

Corollario 1
$\mathbb{F} \subseteq \mathbb{K}$ *estensione separabile di grado finito, allora*

$$|G(\mathbb{K}, \mathbb{F})| \leq [\mathbb{K} : \mathbb{F}].$$

Dimostrazione
questo segue dalle proposizioni precedenti. □

Definizione 3
$\mathbb{K}$ *campo* $H \leq Aut(\mathbb{K})$
Poniamo

$$\mathbb{K}_H := \{k \in \mathbb{K} \mid \omega(k) = k \forall \sigma \in H\}.$$

si dice campo fissato da H.

Esercizio:
Dimostrare che è un campo.

Definizione 4 (Galois)
$\mathbb{F} \subseteq \mathbb{K}$ *estensione*

$$\mathcal{F}_{\mathbb{K},\mathbb{F}} = \{\textit{estensioni intermedie } \mathbb{F} \subset \mathbb{L} \subset \mathbb{K}\}.$$

$$\mathcal{G}_{\mathbb{K},\mathbb{F}} = \{\textit{sottogruppi di } G(\mathbb{K}, \mathbb{F}).$$

$$\begin{aligned} \psi :& \mathcal{F}_{\mathbb{K},\mathbb{F}} \to \mathcal{G}_{\mathbb{K},\mathbb{F}} \\ & (\mathcal{F} \subseteq \mathbb{L} \subseteq \mathbb{K}) \to G(\mathbb{K}, \mathbb{L}) \leq G(\mathbb{K}, \mathbb{F}) \end{aligned}.$$

$$\begin{aligned} \Phi :& \mathcal{G}_{\mathbb{K},\mathbb{F}} \to \mathcal{F}_{\mathbb{K},\mathbb{F}} \\ & H \leq G(\mathbb{K}, \mathbb{F}) \to \mathbb{F} \subseteq \mathbb{K}_H \subseteq \mathbb{K} \end{aligned}.$$

ψ e ϕ si dicono corrispondenze di Galois

Domande:

1. $\Phi(\psi(\text{Ł})) = \text{Ł}$? per ogni estensione $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$
2. $\psi(\Phi(H)) = H$? per ogni $H \leq G(\mathbb{K}, \mathbb{F})$

Esercizi:
$\mathbb{F} \subseteq \mathbb{K}$ estensione, dimostrare

1. $G(\mathbb{K}, \mathbb{K}) = \{id\}$
2. $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{L}_2 \subseteq \mathbb{K}$
   $\Rightarrow \psi(\mathbb{L}_2) = G(\mathbb{K}, \mathbb{L}_2) \leq G(\mathbb{K}, \mathbb{L}_1) = \psi(\mathbb{L}_1)$
3. $\mathbb{K}_{\{id\}} = \mathbb{K}$
4. $H_1 \leq H_2 \leq G(\mathbb{K}, \mathbb{F})$
   $\Rightarrow F \subseteq \mathbb{K}_{H_2} = \Phi(H_2) \subseteq \mathbb{K}_{H_1} = \Phi(H_1) \subseteq \mathbb{K}$
5. $H \leq G(\mathbb{K}, \mathbb{F}) \Rightarrow H \leq G(\mathbb{K}, \mathbb{K}_H) = \psi(\mathbb{K}_H) = \psi(\Phi(H))$
6. $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K} \Rightarrow \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}_{G(\mathbb{K},\mathbb{L})} \subseteq \mathbb{K}$

$$\begin{aligned} \psi : &\mathcal{F}_{\mathbb{K},\mathbb{F}} \to \mathcal{G}_{\mathbb{K},\mathbb{F}} \\ &(\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}) \to \mathcal{G}(\mathbb{K}, \mathbb{L})^{\cdot} \end{aligned}$$

$$\psi : \mathcal{G}_{\mathbb{K},\mathbb{F}} \to \mathcal{F}_{\mathbb{K},\mathbb{F}} \quad H \leq G(\mathbb{K}, \mathbb{F}) \to F \subseteq \mathbb{K}_G \subseteq \mathbb{K}.$$

Osservazione

- $H \leq \psi(\Phi(H))$
- $\mathbb{L} \subseteq \Phi(\psi(\mathbb{L}))$

Obiettivo
Esibire condizioni su $\mathbb{F} \subseteq \mathbb{K}$ affinché Φ, ψ siano una l'inversa dell'altra

Teorema 3
$\mathbb{F} \subseteq \mathbb{K}$ separabile di grado finito. Allora dato $H \leq G(\mathbb{K}, \mathbb{F})$ abbiamo

- $|H| = [\mathbb{K}, \mathbb{K}_H]$
- $\psi(\Phi(H)) = H$

Dimostrazione
Abbiamo $H \leq G(\mathbb{K}, \mathbb{K}_H)$

$$\Rightarrow |H| \leq |G(\mathbb{K}, \mathbb{K}_H)| \leq [\mathbb{K}, \mathbb{K}_H].$$

basta verificare che

$$|H| \geq [\mathbb{K}, \mathbb{K}_H].$$

per dedurre entrambi gli enunciati.
Dal teorema dell'elemento primitivo esiste $\alpha \in \mathbb{K}$ tale che

$$\mathbb{F} \subseteq \mathbb{F}(\alpha) = \mathbb{K}.$$

Vogliamo costruire un polinomio $f \in \mathbb{K}_H$ di cui α sia radice.

$$H = \{\sigma_1 = Id, \sigma_2, \ldots, \sigma_h\}.$$

Definiamo:

$$\alpha_s := \sum_{1 \le j_1 < \ldots < j_s \le h} \sigma_{j_1}(\alpha) \cdot \ldots \cdot \sigma_{j_s}(\alpha) \in \mathbb{K}$$

Poniamo

$$f(x) = \prod_{j=1}^{h} (x - \sigma_j(\alpha)) = x^h - \alpha_1^{h-1} + \ldots + (-1)^h \alpha_h \in \mathbb{K}[x].$$

Chiaramente $f(\delta) = 0$. Verifichiamo $\alpha_s \in \mathbb{K}_H$ ovvero $\sigma_t(\alpha_s) = \alpha_s \ \forall t, s \in \{1, \ldots, h\}$
Abbiamo

$$\sigma_t(\alpha_s) = \sum_{1 \le j_1 < \ldots < j_s \le h} \sigma_{j_1}(\alpha) \cdot \ldots \cdot \sigma_{j_s}(\alpha) = \sigma_s.$$

Dove l'ultima uguaglianza segue dal fatto che

$$\begin{aligned} H &\to H \\ \sigma_j &\to \sigma_t \cdot \sigma_j \end{aligned}.$$

è un isomorfismo $\forall t \in \{1, \ldots, h\}$
$\Rightarrow f \in \mathbb{K}_H[x]$
$\Rightarrow |H| = h = deg(f) \ge deg($ *polinomio minimo di α su* $\mathbb{K}_H) = [\mathbb{K}_H(\alpha) : \mathbb{K}_H] = [\mathbb{K} : \mathbb{K}_H]$

□

Teorema 4
$\mathbb{F} \subseteq \mathbb{K}$ estensione separabile di grado finito.
Allora sono equivalenti:

1. *$\mathbb{F} \subseteq \mathbb{K}$ estensione normale*
2. *$\Phi(\psi(\mathbb{L})) = \mathbb{L}$ per ogni $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$*

Dimostrazione
2) $\Rightarrow$ 1) *per ipotesi abbiamo $\mathbb{F} = \mathbb{K}_{G(\mathbb{K},\mathbb{F})}$*
Per dimostrare che $\mathbb{F} \subseteq \mathbb{K}$ è normale, basta verificare che sia un campo di spezzamento di un polinomio $f \in \mathbb{F}[x]$.
Per il teorema dell'elemento primitivo
$\exists \alpha \in \mathbb{K}$ *tale che* $\mathbb{F} \subseteq \mathbb{F}(\alpha) = \mathbb{K}$
Inoltre $|G(\mathbb{K}, \mathbb{F})| < +\infty$
$G(\mathbb{K}, \mathbb{F}) = \{\sigma_1, \ldots, \sigma_h\}$

$f(x) = \prod_{j=1}^{h}(x - \sigma_j(\alpha)) = x^h - \alpha_1 x^{h-1} + \ldots + (-1)^h \alpha_h$
dove

$$\alpha_s = \sum_{i \leq j_1 < \ldots < j_s \leq h} \sigma_{j_1}(\alpha) \cdot \ldots \cdot \sigma_{j_s}(\alpha).$$

$f(x) \in \mathbb{K}[x]$
Osserviamo che $s, t \in \{1, \ldots, h\}$

$$\sigma_t(\alpha_s) = \sum_{1 \leq j_1 < \ldots < j_s \leq h} (\sigma_t \sigma_{j_1})(\alpha) \cdot \ldots \cdot (\sigma_t \sigma_{j_s})(\alpha).$$

$\Rightarrow \alpha_s \in \mathbb{K}_{G(\mathbb{K},\mathbb{F})} = \mathbb{F} \Rightarrow f(x) \in \mathbb{F}[x]$

- f *si decompone in fattori lineari in* $\mathbb{K}[x]$
- $f(\alpha) = 0$ *quindi data un'estensione* $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ *abbiamo* $\alpha \in \mathbb{L}$
  $\Rightarrow \mathbb{K} = \mathbb{F}(\alpha) \subseteq \mathbb{L} \subseteq \mathbb{K}$
  $\Rightarrow \mathbb{L} = \mathbb{K}$
  $\Rightarrow \mathbb{F} \subseteq \mathbb{K}$ *è campo di spezzamento di* f.

1) $\Rightarrow$ 2) *Dobbiamo verificare che se* $\mathbb{F} \subseteq \mathbb{K}$ *è separabile, di grado finito e normale, allora*

$$\Phi(\psi(\mathbb{L})) = \mathbb{L} \quad \text{per ogni } \mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}.$$

$\mathbb{L} \subseteq \Phi(\psi(\mathbb{L})) = \mathbb{K}_{G(\mathbb{K},\mathbb{L})}$
Verificare che $\mathbb{K}_{G(\mathbb{K},\mathbb{L})} \subseteq \mathbb{L}$
Sappiamo che $\mathbb{L} \subseteq \mathbb{K}$
è estensione normale di grado finito.
Quindi esiste polinomio $f \in \mathbb{L}[x]$ *tale che* $\mathbb{L} \subseteq \mathbb{K}$ *sia campo di spezzamento di* f.
Procedo per induzione su $[\mathbb{L} : \mathbb{K}]$
se $[\mathbb{L} : \mathbb{K}] = 1 \Rightarrow \mathbb{L} = \mathbb{K}$
$\Rightarrow \mathbb{K}_{G(\mathbb{K},\mathbb{L})} = \mathbb{K} = \mathbb{L}$
Se $[\mathbb{K} : \mathbb{L}] > 1$ *allora*
$f : p_1 \cdot \ldots \cdot_r$ *fattorizzazione in irriducibili*
Possiamo assumere che $deg(p_1) > 1$.
Siano $\alpha_1, \alpha_2, \ldots, \alpha_h \in \mathbb{K}$ *le radici di* p_1 $(deg(p_1) = h > 1)$

$$[\mathbb{K} : \mathbb{L}] = [\mathbb{K} : \mathbb{L}(\alpha_1)][\mathbb{L}(x) : \mathbb{L}].$$

con $[\mathbb{L}(x) : \mathbb{L}] = h$
Quindi

$$[\mathbb{K} : \mathbb{L}(\alpha_1)] < [\mathbb{K} : \mathbb{L}].$$

e per ipotesi induttiva

$$\mathbb{K}_{G(\mathbb{K},\mathbb{L}(\alpha_1)} = \mathbb{L}(\alpha_1).$$

Definiamo

$$\sigma_1, \dots, \sigma_h \in G(\mathbb{K}, \mathbb{L}).$$

$$\begin{aligned} \sigma_s : &\mathbb{K} \to \mathbb{K} \\ &\alpha_1 \to \alpha_s \end{aligned}.$$

(si può estendere a tutto $\mathbb{K}$*)*
Dobbiamo verificare $\mathbb{K}_{G(\mathbb{K},\mathbb{L})} \subseteq \mathbb{L}$
Sia $k \in_{G(\mathbb{K},\mathbb{L})} \subseteq \mathbb{K}_{G(\mathbb{K},\mathbb{L}(\alpha))} = \mathbb{L}(\alpha_1)$
$\Rightarrow k = c_0 + c_1\alpha_1 + \dots + c_{h-1}\alpha_1^{h-1} \in \mathbb{L}(\alpha_1)$
$\Rightarrow \sigma_s(k) = k \quad \forall s \in \{1, \dots, h\}$.
poiché $\sigma_s \in G(\mathbb{K}, \mathbb{L})$
Ora $f(x) = (c_0 - k) + c_1 x + \dots, c_h x^{h-1} \in \mathbb{L}(\alpha_1)[x]$
$\alpha_s = \sigma_s(\alpha_1)$ *è radice di* $f(x) \ \ \forall s \in \{1, \dots, h\}$ *che sono tutte distinte.*
Quindi ho h *radici ma* $deg(f) = h - 1 \Rightarrow f(x) = 0 \Rightarrow k = c_0 \in \mathbb{L}$

□

Definizione 5
$\mathbb{F} \subseteq \mathbb{K}$ *si dice estensione Galoisiana se è separabile e normale*

Corollario 2
$\mathbb{F} \subseteq \mathbb{K}$ *estensione Galoisiana di grado finito, allora* Φ, ψ *sono una l'inversa dell'altra*