Lezione N + 2 Algebra I

Federico De Sisti

2025-05-19

0.1 Applicazioni dell'altra volta

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

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

0.2 Il teorema di Galois

Esercizio:
$\mathbb{F} \subseteq \mathbb{K}$ un campo di spezzamento di $f \in \mathbb{F}[x]$.
Siano $\alpha, \beta \in \mathbb{K}$ radici di un polinomio irriducibile $p \in \mathbb{F}[x]$.
Allora $\exists \sigma \in G(\mathbb{K}, \mathbb{F})$, tale che $\sigma(\alpha) = \beta$ **Soluzione**
Sappiamo che $\exists \psi : \mathbb{F}(\alpha) \to \mathbb{F}(\beta)$ isomorfismo di anelli tale che:

$$\psi|_{\mathbb{F}} = Id \quad e \quad \psi(\alpha) = \beta.$$

AGGIUNGI FOTO 19 MARZO 1 20
Ora:

- $\mathbb{F}(\alpha) \subseteq \mathbb{K}$ è campo di spezzamento di $f \in \mathbb{F}(\alpha)[x]$
- $\mathbb{F}(\alpha) \underset{\phi}{\cong} \mathbb{F}(\beta) \subseteq \mathbb{K}$ campo di spezzamento di $f \in \mathbb{F}(\alpha)[x]$

Quindi dall'unicità (non canonica) dei campi di spezzamento esiste l'isomorfismo σ cercato.

Esercizio:
$\mathbb{F} \subseteq \mathbb{K}$ estensione Galoisiana di grado finito. Allora

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

Soluzione
$|G(\mathbb{K}, |F)| = [\mathbb{K} : \mathbb{K}_{G(\mathbb{K},\mathbb{F})}] = [\mathbb{K} : \mathbb{F}]$ □

Esercizio:
$\mathbb{F} \subseteq \mathbb{K}$ estensione normale e di grado finito.
Data un'estensione $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$

1. dimostrare che da $\mathbb{L} \subseteq \mathbb{K}$ è estensione normale
2. esibire un esempio in cui $\mathbb{F} \subseteq \mathbb{L}$ <u>non</u> è normale

Soluzione:

1. $\mathbb{F} \subseteq \mathbb{K}$ è campo di spezzamento per $f \in F[x]$.
   Allora $\mathbb{L} \subseteq \mathbb{K}$ è campo di spezzamento di $f \in \mathbb{L}[x]$

2. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ dove $\omega = \frac{-1+i\sqrt{3}}{2} \in \mathbb{A}$ tale estensione è campo di spezzamento di $x^3 - 2 \in \mathbb{Q}[x]$
Scegliamo $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2})$ $\mathbb{Q} \subseteq \mathbb{L}$ non è normale, infatti, $\sqrt[3]{2}, \sqrt[3]{2} \cdot \omega$ sono coniugati su $\mathbb{Q}$, eppure $\sqrt[3]{2} \cdot \omega \notin \mathbb{Q}(\sqrt[3]{2})$

Lemma 1
$\mathbb{F} \subseteq \mathbb{K}$ estensione Galoisiana di grado finito. $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ estensione intermedia.
Allora sono equivalenti due condizioni:

1. *$\mathbb{F} \subseteq \mathbb{L}$ estensione normale*
2. *$\sigma|_{\mathbb{L}} \in G(\mathbb{L}, \mathbb{F}) \quad \forall \sigma \in G(\mathbb{K}, \mathbb{F})$*
   (ovvero $\sigma(l) \subseteq \mathbb{L} \quad \forall \sigma \in G(\mathbb{K}, \mathbb{F})$)

Dimostrazione
1) $\Rightarrow$ 2)
Siano $\sigma \in F(\mathbb{K}, \mathbb{F}), \quad l \in \mathbb{L}$
Allora $l, \sigma(l)$ sono coniugati $\Rightarrow \sigma(l) \in \mathbb{L}$ poiché $\mathbb{F} \subseteq \mathbb{L}$ è normale
2) $\Rightarrow$ 1) *siano $k \in \mathbb{K}, l \in \mathbb{L}$ due elementi coniugati su $\mathbb{F}$*
$\Rightarrow \exists \sigma \in G(\mathbb{K}, \mathbb{F})$ tale che $k = \sigma(l) \in \mathbb{L}$ *(esercizio 1)*
Quindi $\mathbb{F} \subseteq \mathbb{L}$ normale □

Teorema 1 (Galois, 1846)
$\mathbb{F} \subseteq \mathbb{K}$ estensione Galoisiana di grado finito. $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ estensione intermedia. Allora:

1. *ψ e Φ sono una l'inversa dell'altra*
2. *$|G(\mathbb{K}, \mathbb{L})| = [\mathbb{K} : \mathbb{L}]$*
3. *$[G(\mathbb{K}, \mathbb{F}) : H] = [\mathbb{K}_H : \mathbb{F}]$*
4. *$G(\mathbb{K}, \mathbb{L}) \leq G(\mathbb{K}, \mathbb{F})$ è normale se e solo se $\mathbb{F} \subseteq \mathbb{L}$ è normale*
5. *Se $\mathbb{F} \subseteq \mathbb{L}$ è normale allora*

$$\frac{G(\mathbb{K}, \mathbb{F})}{G(\mathbb{K}, \mathbb{L})} \cong G(\mathbb{L}, \mathbb{F}).$$

Dimostrazione
1) *Già visto*
2) *Basta applicare uno degli esercizi di oggi all'estensione Galoisiana di grado finito $L \subseteq \mathbb{K}$*
3) $[G(\mathbb{K}, \mathbb{F}) : H] = \frac{|G(\mathbb{K}, \mathbb{F})|}{|H|} = \frac{|G(\mathbb{K}, \mathbb{F})|}{|G(\mathbb{K}, \mathbb{K}_H)|} \overset{(2)}{=} \frac{[\mathbb{K}:\mathbb{F}]}{[\mathbb{K}:\mathbb{K}_H]} = [\mathbb{K}_H : \mathbb{F}]$ 4) *dal lemma $\mathbb{F} \subseteq \mathbb{L}$ normale se e solo se $\sigma|_{\mathbb{L}} \in G(\mathbb{L}, \mathbb{F}) \quad \forall \sigma \in G(\mathbb{K}, \mathbb{F})$*

$\Leftrightarrow \forall \tau \in G(\mathbb{K}, \mathbb{L})$ *e* $\forall \sigma \in G(\mathbb{K}, \mathbb{F})$ *si ha* $\tau \circ \sigma|_{\mathbb{L}} = \sigma|_{\mathbb{L}}$
$\Leftrightarrow (\sigma^{-1} \circ \tau \circ \sigma)|_{\mathbb{L}} = Id_{\mathbb{L}}$
$\Leftrightarrow \sigma^{-1} G(\mathbb{K}, \mathbb{L}) \sigma \subseteq G(\mathbb{K}, \mathbb{L}) \quad \forall \sigma \in G(\mathbb{K}, \mathbb{F})$
5) *Definiamo l'omomorfismo*

$$\begin{aligned} g : G(\mathbb{K}, \mathbb{F}) &\to G(\mathbb{L}, \mathbb{F}) \\ \sigma &\to \sigma|)\mathbb{L} \end{aligned}.$$

g è ben definito per il lemma

- $\ker(g) = \{\sigma \in G(\mathbb{K}, \mathbb{F}) \mid \sigma|_{\mathbb{L}} = id_{\mathbb{L}}\} = G(\mathbb{K}, \mathbb{L})$
- *verifichiamo che g suriettiva dato* $\psi \in G(\mathbb{L}, \mathbb{F})$ *abbiamo*
  INSERISCI IMMAGINE 2 05 19 MAGGIO
  $F \subseteq \mathbb{K}$ *campo di spezzamento di* $f \in \mathbb{F}[x]$. *Allora*
  - $\mathbb{L} \subseteq \mathbb{K}$ *campo di spezzamento di* $f \in \mathbb{L}[x]$
  - $\mathbb{L} \underset{\psi}{\cong} \mathbb{L} \subseteq \mathbb{K}$ *campo di spezzamento per* $f \in \mathbb{L}[x]$

  $\Rightarrow \omega \in G(\mathbb{K}, \mathbb{F})$ *tale che* $g(\sigma) = \psi$

Dal teorema di isomorfismo tra anelli segue la tesi □

Esercizio
G gruppo, $|G| = 2^n$ $n \in \mathbb{Z}_{\geq 1}$. Allora $\exists G \leq G$ tale che $[G : H] = 2$
Esempio:
$f(x) = x^3 - 2 \in \mathbb{Q}[x]$
$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{K}$, $\omega = \frac{-1+i\sqrt{3}}{2} \in \mathbb{A}$
è estensione Galoisiana di grado finito,
Elenchiamo tutti gli elementi di $G(\mathbb{K}, \mathbb{Q})$

$$\rho : \begin{cases} \omega \to \omega \\ \sqrt[3]{2} \to \sqrt[3]{2}\omega \end{cases} \qquad \omega : \begin{cases} \omega \to \omega^2 \\ \sqrt[3]{2} \to \sqrt[3]{2} \end{cases}$$

$$\rho^2 = \begin{cases} \omega \to \omega \\ \sqrt[3]{2} \to \sqrt[3]{2}\omega^2 \end{cases} \qquad \sigma^2 = \rho^3 = Id$$

$$\sigma\rho^2 = \rho\sigma : \begin{cases} \omega \to \omega^2 \\ \sqrt[3]{2} \to \sqrt[3]{2}\omega \end{cases}$$

$$\rho^2\sigma = \sigma\rho : \begin{cases} \omega \to \omega^2 \\ \sqrt[3]{2} \to \sqrt[3]{2}\omega^2 \end{cases}$$

$G(\mathbb{K} : \mathbb{Q}) =< \rho, \sigma >\cong S_3 \cong D_3$
AGGIUNGI IMMAGINE 2 33
Elenchiamo tutte le estensioni intermedie

$$\mathbb{K}_{<\rho,\sigma>} = \mathbb{Q}.$$

$$\mathbb{K}_{<\rho>} = \mathbb{Q}(\omega).$$

AGGIUNGI IMMAGINE 2 38

0.3 Teorema fondamentale dell'algebra

Teorema 2
$\mathbb{C}$ *è algebricamente chiuso*

Dimostrazione
Procediamo per passi.

1. $\mathbb{R} \subseteq \mathbb{K}$ *estensione Galoisiana finita allora* $2 \mid [\mathbb{K} : \mathbb{R}]$
   Infatti un polinomio $f \in \mathbb{R}[x]$ *di grado dispari soddisfa*
   $$\lim_{x \to \pm\infty} f(x) = \pm\infty.$$
   $\Rightarrow$ *esiste una radice di* f *(Bolzano)*
   $\Rightarrow f$ *non è irriducibile.*
   L'estensione $\mathbb{R} \subseteq \mathbb{K}$ *è semplice* *(teorema elemento primitivo)*
   $\Rightarrow [\mathbb{K} : \mathbb{R}]$ *è il grado di un polinomio irriducibile in* $\mathbb{R}[x]$

2. $\mathbb{R} \subseteq \mathbb{K}$ *estensione Galoisiana finita.*
   Allora $[\mathbb{K} : \mathbb{R}] = 2^n$ *con* $n \in \mathbb{Z}_{\geq 0}$
   Infatti:
   $$2 \mid [\mathbb{K} : \mathbb{R}] = |G(\mathbb{K}, \mathbb{R})|.$$
   $\Rightarrow \exists H \in Syl_2(G(\mathbb{K}, \mathbb{R}))$ *(Sylow)*
   $\Rightarrow [\mathbb{K}_H : \mathbb{R}] = \dfrac{[\mathbb{K} : \mathbb{R}]}{[\mathbb{K} : \mathbb{K}_H]} = \dfrac{|G(\mathbb{K}, \mathbb{R})|}{|G(\mathbb{K}, \mathbb{K}_H)|} = \dfrac{|G(\mathbb{K}, \mathbb{R})|}{|H|}$
   <u>non</u> è divisibile per 2!
   $\Rightarrow \mathbb{K}_H = \mathbb{R}.$
   $\Rightarrow H = G(\mathbb{K}, \mathbb{K}_H) = G(\mathbb{K}, \mathbb{R})$
   $\Rightarrow |G(\mathbb{K}, \mathbb{R})| = |H| = 2^n$

3. $\mathbb{C} \subseteq \mathbb{K}$ *campo di spezzamento di* $f \in \mathbb{C}[x]$. *Allora* $\mathbb{C} = \mathbb{K}$.
   Infatti:
   $2^n = [\mathbb{K} : \mathbb{R}] = [\mathbb{K} : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = [\mathbb{K} : \mathbb{C}] \cdot 2$
   $\Rightarrow [\mathbb{K} : \mathbb{C}] = 2^{n-1}$
   Dobbiamo dimostrare che $n = 1$
   Se $n > 1$
   $$|G(\mathbb{K}, \mathbb{C})| = 2^{n-1}.$$
   $\Rightarrow \exists H \leq G(\mathbb{K}, \mathbb{C})$ *di indice 2.*
   $\Rightarrow [\mathbb{K}_H : \mathbb{C}] = \dfrac{[\mathbb{K} : \mathbb{C}]}{[\mathbb{K} : \mathbb{K}_H]} = \dfrac{|G(\mathbb{K}, \mathbb{C})|}{|G(\mathbb{K}, \mathbb{K}_H)|} = \dfrac{|G(\mathbb{K}, \mathbb{C})|}{|H|} = [G(\mathbb{K}, \mathbb{C}) : H] = 2$
   $C \subseteq \mathbb{K}_H$ *è estensione semplice*
   $\Rightarrow \exists \alpha \in \mathbb{K}_H$:
   $$\mathbb{C} \subseteq \mathbb{C}[\alpha] = \mathbb{K}_H.$$
   e il polinomio minimo p *di* α *su* $\mathbb{C}$ *ha grado* $[\mathbb{K}_h : \mathbb{C}] = 2$
   Quindi $p \in \mathbb{C}[x]$ *è irriducibile e di grado 2, assurdo.*
   $\Rightarrow n = 1 \Rightarrow \mathbb{K} = \mathbb{C}$

$\square$