Lezione 13 Algebra I

Federico De Sisti

2025-04-28

0.1 Estensioni

Definizione 1
$\mathbb{F}$ campo, Un'estensione di $\mathbb{F}$ è una coppia $(\mathbb{K}, \varphi)$ dove $\mathbb{K}$ è un campo e $\varphi : \mathbb{F} \to \mathbb{K}$ è un omomorfismo iniettivo di anelli

Notazione 1
scriveremo $\mathbb{F} \subseteq \mathbb{K}$

Notazione 2
$p \in \mathbb{Z}_{>0}$ primo $\mathbb{F}_p$ è il campo $(\mathbb{Z}/(p), +, \cdot)$

Proposizione 1
$\mathbb{K}$ è un campo, Allora $\mathbb{Q} \subseteq \mathbb{K}$ oppure esiste $p \in \mathbb{Z}_{\geq 0}$ primo tale che $\mathbb{F}_p$

Dimostrazione
Ricordo che esiste un unico omomorfismo di anelli $\chi : \mathbb{Z} \to \mathbb{K}$ che è definito da

$$\chi(1_{\mathbb{Z}}) = 1_{\mathbb{K}}.$$

Ricordo che

$$\ker(\chi) = \begin{cases} 0 \\ p \quad \text{con } p \in \mathbb{Z}_{\geq 0} \text{ primo} \end{cases} .$$

perché $\mathbb{K}$ è dominio d'integrità.
Abbiamo $\mathbb{Z}/\ker(\phi) \cong im(\chi) \subseteq \mathbb{K}$ *(sottoanello)* ***2 casi:***

- *Se $\ker(\phi) = (p)$ allora*

  $$\mathbb{F}_p = \mathbb{Z}/(p) \cong im(\chi) \subseteq \mathbb{K}.$$

  quindi è un'estensione di campi

- $\ker(\phi) = (0)$ *allora*

  $$\mathbb{Z} \cong im(\chi) \subseteq \mathbb{K}.$$

  non è estensione di campi ma solo un sottoanello.
  Dalla proprietà universale del campo dei quozienti
  AGGIUNGI IMMAGINE 1 34
  Quindi $\mathbb{Q} \subseteq \mathbb{L}$ è un'estensione di campi

□

Esercizio
Se $\mathbb{F} \subseteq \mathbb{K}$ è estensione di campi, allora $\mathbb{K}$ è un $\mathbb{F}$-spazio vettoriale.

Definizione 2
Il grado di un'estensione $\mathbb{F} \subseteq \mathbb{K}$ *è*

$$[\mathbb{K} : \mathbb{F}] = \dim_{\mathbb{F}}(\mathbb{K}).$$

Esempio
$\mathbb{R} \subseteq \mathbb{C}$ estensione $[\mathbb{C} : \mathbb{R}] = 2$ infatti $\{1, i\}$ è una base di $\mathbb{C}$ come $\mathbb{R}$ spazio vettoriale.
esempio:
$\mathbb{F}$ campo, $\mathbb{K} = Frac(\mathbb{F}[x]) = \mathbb{F}(x)$
$\mathbb{F} \subseteq \mathbb{F}[x] \subseteq \mathbb{F}(x) = \mathbb{K}$
Dimostrare che
$[\mathbb{K} : \mathbb{F}] = +\infty$

Proposizione 2
Siano $\mathbb{F} \subseteq \mathbb{K}$ *e* $\mathbb{K} \subseteq \mathbb{L}$ *estensioni di campi. Allora*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}].$$

Dimostrazione
È sufficiente studiare il caso $\begin{cases} [\mathbb{L} : \mathbb{K}] = m \\ [\mathbb{K} : \mathbb{F}] = n \end{cases}$
dato che il caso in cui i gradi sono infiniti è banale.
Dobbiamo dimostrare che $[\mathbb{L} : \mathbb{F}] = m \cdot n$
$B_{\mathbb{L},\mathbb{K}} = \{v_1, \dots, v_m\}$ *base di* $\mathbb{L}$ *su* $\mathbb{K}$
$B_{\mathbb{K},\mathbb{F}} = \{w_1, \dots, w_n\}$ *base di* $\mathbb{K}$ *su* $\mathbb{F}$
Dimostriamo che una base di $\mathbb{L}$ *su* $\mathbb{F}$ *è*
$B_{\mathbb{L},\mathbb{F}} = \{w_j, v_i\}_{\substack{j=1,\dots,n \\ i=1,\dots,m}}$

- $B_{\mathbb{L},\mathbb{F}}$ *è un insieme di generatori.*
  Infatti $h \in \mathbb{L}$
  $\Rightarrow l = \sum_{i=1}^{m} b_i v_i$ *con* $b_i \in \mathbb{K} = \sum_{i=i}^{m} \sum_{j=1}^{n} a_{ij}(w_j v_i)$
- $B_{\mathbb{L},\mathbb{F}}$ *è un insieme di vettori lineramente indipendenti. Infatti:*

$$\sum_{i,j} a_{ij}(w_j v_i) = 0.$$

$$\Rightarrow \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} w_j \right) v_i = 0.$$

è una combinazione lineare in Ł *a coefficienti in* $\mathbb{K}$ *di* $v_1, \dots, v_m$
Quindi:

$$\sum_{j=1}^{n} a_{ij} w_j = 0 \quad \forall i \in \{1, \dots, m\}.$$

da cui $a_{ij} = 0 \quad i, j$ *poiché i* w_j *sono linearmente indipendenti su* $\mathbb{F}$

□

Notazione 3
$\mathbb{F} \subseteq \mathbb{K}$ *estensione,* $S \subseteq \mathbb{K}$ *sottoinsieme*
Denotiamo:

1. $\mathbb{F}[S]$ *il più piccolo sottoanello di* $\mathbb{K}$ *contenente* $\mathbb{F}$ *ed* S
2. $\mathbb{F}(S) = Frac(\mathbb{F}[S])$

Esercizio
Dimostrare che $\mathbb{F}(S)$ è il più piccolo sottocampo di $\mathbb{K}$ contenente $\mathbb{F}$ e S.
$\mathbb{F}(S)$ è l'intersezione di tutti i tali sottocampi (contenenti $\mathbb{F}$ e S).

Definizione 3
$\mathbb{F} \subseteq \mathbb{K}$ *estensione,* $s \in \mathbb{K}$ *si dice*

- *algebrico su* $\mathbb{F}$ *se esiste un polinomio* $\in \mathbb{F}[x]$ *tale che* $f(s) = 0$
- *trascendente su* $\mathbb{F}$ *se non è algebrico su* $\mathbb{F}$

Esempi: $\mathbb{Q} \subseteq \mathbb{C}$

- π è trascendente su $\mathbb{Q}$
- i è algebrico su $\mathbb{Q}$ poichè soddisfa $x^2 + 1$
- e^π è trascendente su $\mathbb{Q}$
- π^e non è noto se sia algebrico o trascendente su $\mathbb{Q}$

Definizione 4
$\mathbb{F} \subseteq \mathbb{K}$ *estensione* $s \in \mathbb{K}$ *definiamo*

$$\begin{aligned} \psi_s : &\mathbb{F}[x] \to \mathbb{K} \\ &f \to f(s) \end{aligned}.$$

ψ_s *si dice omomorfismo di valutazione su* s

Esercizio
Dimostrare che ψ_s è un omomorfismo di anelli.
Esercizio
Dimostrare che $(\psi_s) = \mathbb{F}[s]$ **Osservazione**
Se s è algebrico su $\mathbb{F}$ esiste un unico polinomio monico $p \in \mathbb{F}[x]$ tale che

$(\psi_s) = (p)$.
Infatti $\mathbb{F}[x]$ è un PID
quindi $\ker(\psi_s) \subseteq \mathbb{F}[x]$ è generato da un solo elemento
L'unicità segue dal fatto che lo scegliamo monico.

Definizione 5
$\mathbb{F} \subseteq \mathbb{K}$ *estensione se* $\mathbb{K}$ *algebrico su* $\mathbb{F}$.
Allora il polinomio dell'osservazione si dice polinomio minimo di s *su* $\mathbb{F}$

Osservazione
$\mathbb{F} \subseteq \mathbb{K}$ estensione, $s \in \mathbb{K}$ trascendente su $\mathbb{F}$. Allora $\ker(\psi_s) = \{0\}$

Proposizione 3
$\mathbb{F} \subseteq \mathbb{K}$ *estensione* $s \in \mathbb{K}$ *trascendente, Allora* $[\mathbb{K} : \mathbb{F}] = \infty$

Dimostrazione
$\psi_s : \mathbb{F}[x] \to \mathbb{K}$
è iniettivo
$\Rightarrow \mathbb{F}[x] \cong im(\psi_s) = \mathbb{F}[s]$
$\Rightarrow F(x) \cong Frac(\mathbb{F}[s]) = \mathbb{F}(s)$
$\Rightarrow [\mathbb{F}(s) : \mathbb{F}] = \infty$
Ma $\mathbb{F}_(s) \subseteq \mathbb{K}$ *quindi* $[\mathbb{K} : \mathbb{F}] = \infty$ □

Corollario 1
$\mathbb{F} \subseteq \mathbb{K}$ *estensione tale che* $[\mathbb{K} : \mathbb{F}] < -\infty$ *Allora tutti gli elementi di* $\mathbb{K}$ *sono algebrici su* $\mathbb{F}$

Esempio:

1. tutti gli elementi di $\mathbb{C}$ sono algebrici su $\mathbb{R}$ poiché $[\mathbb{C} : \mathbb{R}] = 2$

2. π trascendente su $\mathbb{Q} \Rightarrow [\mathbb{R} : \mathbb{Q}] = \infty$

Proposizione 4
$\mathbb{F} \subseteq \mathbb{K}$ *estensione* $s \in \mathbb{K}$ *algebrico su* $\mathbb{F}$.
Allora:

1. $\mathbb{F}(s) = \mathbb{F}[s] \cong \mathbb{F}[x]/(p)$ *dove* p *è il polinomio minimo di* s *su* $\mathbb{F}$
2. $[\mathbb{F}(s) : \mathbb{F}] = deg(p) < \infty$

Dimostrazione
1)$\psi_s : \mathbb{F}[x] \to \mathbb{K}$

$$\mathbb{F}[x]/(p) = \mathbb{F}[x]/\ker(\psi_s) \cong im(\psi_s) = \mathbb{F}[s].$$

Per verificare che $\mathbb{F}(s) = \mathbb{F}[s]$ *è sufficiente dimostrare che* $\mathbb{F}[s]$ *è un campo*
Ora $\mathbb{F}[s] \subseteq \mathbb{K} \Rightarrow \mathbb{F}[s]$ *dominio d'integrità.*
$\Rightarrow \mathbb{F}[s] \cong \mathbb{F}[x]/(p)$ *quindi* (p)
è un ideale primo in $\mathbb{F}[x]$
Ma in un PID un ideale è primo se e solo se è massimale
Quindi $\mathbb{F}[x]/(p)$ *è un campo. 2) Una base di* $\mathbb{F}[x](p)$ *come* $\mathbb{F}$*-spazio vettoriale è* $\{1, x, x^2, \ldots, x^{\deg(p)-1}\}$
$\Rightarrow [\mathbb{F}(s) : \mathbb{F}] = deg(p)$ □

Corollario 2
$\mathbb{F} \subseteq \mathbb{K}$ *estensione*

- $s \in \mathbb{K}$ *è algebrico* $\Leftrightarrow [\mathbb{F}(s) : \mathbb{F}] < \infty$
- $s \in \mathbb{K}$ *è trascendente* $\Leftrightarrow [\mathbb{F}(s) : \mathbb{F}] = \infty$

Esercizi

1. $\mathbb{F} \subseteq \mathbb{K}$ estensione, $s \in \mathbb{K}$ algebrico su $\mathbb{F}$ Allora il suo polinomio minimo è irriducibile in $\mathbb{F}[x]$

Sol: Abbiamo visto che $(p) \subseteq \mathbb{F}[x]$ è massimale $\Rightarrow p$ è irriducibile.

2. $\mathbb{F} \subseteq \mathbb{K}$ estensione, $f \in \mathbb{F}[x]$ irriducibile e monico, se $s \in \mathbb{K}$ soddisfa $f(s) = 0$ allora f è il polinomio minimo di s su $\mathbb{F}$

Sol: Sia $p \in \mathbb{F}[x]$ il polinomio minimo di s su $\mathbb{F}$. Allora: $f \in (p)$
$\Rightarrow p \mid f$ in $\mathbb{F}[x]$
Ma l'ipotesi di irriducibilità di f implica che p, f associati ed essendo entrambi monici $\Rightarrow f = p$

3. Dimostrare che se $\mathbb{K}$ è campo finito allora $|\mathbb{K}| = p^n$ dove $p, n \in \mathbb{Z}_{\geq 0}$ e p primo.