Lezione N Algebra 1

Federico De Sisti

2025-05-12

0.1 Campi Finiti

PARTE CHE MANCA

Teorema 1
Siano $p, n \in \mathbb{Z}_{\geq 1}$ con p primo. Allora esiste un campo $\mathbb{F}$ tale che $|\mathbb{F}| = p^n$ inoltre $\mathbb{F}$ è unico a meno di isomorfismo

Dimostrazione
L'unicità segue dalla proposizione e dall'unicità (non canonica) dei campi di spezzamento
Esistenza: *Sia $\mathbb{F}_p \subseteq \mathbb{L}$ un campo di spezzamento del polinomio $f(x) = x^p - x \in \mathbb{F}_p[x]$*
Definiamo:

$$\mathbb{F} = \{l \in \mathbb{L} \mid l^p = l\} \subseteq \mathbb{L} \text{ sottoinsieme.}$$

- $f'(x) = -1 \in \mathbb{F}_p[x]$
  f e f' sono coprimi
  $\Rightarrow$ *f è primo di radici multiple*
- *Allora $|\mathbb{F}| = deg(f) = p^n$.*
- *$\mathbb{F}$ è un campo. Infatti $\forall l_1, l_2 \in \mathbb{L}$ $(l_1 + l_2)^{p^n} = l_1^{p^n} + l_2^{p^n} = l_1 + l_2$*
  $(l_1 \cdot l_2)^{p^n} = l_1^{p^n} \cdot l_2^{p^n} = l_1 \cdot l_2$
  $(l_1^{-1})^{p^n} = (l_1^{p^n})^{-1} = l_1^{-1}$

Quindi $\mathbb{F} = \mathbb{L}$ □

Teorema 2
$|\mathbb{F}| = p^n$
Allora $U_{\mathbb{F}}$ è un gruppo ciclico

Dimostrazione
$U_{\mathbb{F}} = \mathbb{F} \setminus \{0\}$ con il prodotto con operazione
È un gruppo abeliano finito
$\Rightarrow$ *per teorema di struttura $\exists\ d_1, \dots, d_r \in \mathbb{Z}_{\geq 1}$ non nulli e non necessariamente distinti tali che.*

$$U_{\mathbb{F}} = C_{d_1} \times \ldots \times C_{d_r}.$$

dove ogni C_{d_i} sono gruppi ciclici generato da p_i di ordine d_i
Inoltre $d_j \mid d_{j+1} \quad \forall j \in \{1, \dots, r-1\}$
Quindi $(p_k^k)^{d_r} = id$
ovvero tutti gli elementi di $U_{\mathbb{F}}$ soddisfano il polinomio $x^{d_r} - 1 \in \mathbb{F}[x]$
Quindi $|U_{\mathbb{F}}| \leq deg(x^{d_r} - 1) = d_r$
Deduciamo $r = 1$
$\Rightarrow$ *$U_{\mathbb{F}} = C_{d_1}$ che è ciclico* □

0.2 Estensioni normali

Definizione 1
$\mathbb{F} \subseteq \mathbb{K}$ estensione di campi.

1. *Due elementi $\alpha, \beta \in \mathbb{K}$ algebrici su $\mathbb{F}$, si dicono coniugati se hanno lo stesso polinomio minimo.*
2. *$\mathbb{F} \subseteq \mathbb{K}$ si dice estensione normale se è chiusa rispetto ai coniugati.*

Osservazione:
Un'estensione $\mathbb{F} \subseteq \mathbb{K}$ è normale se e solo se ogni polinomio irriducibile in $\mathbb{F}[x]$ che ammette una radice in $\mathbb{K}$. Si decompone come prodotto di fattori lineari in $\mathbb{K}[x]$

Teorema 3
$\mathbb{F} \subseteq \mathbb{K}$ estensione. Allora sono equivalenti:

1. *$\mathbb{F} \subseteq \mathbb{K}$ normale $[\mathbb{K} : \mathbb{F}] < +\infty$*
2. *$\exists f \in \mathbb{F}[x]$ tale che $\mathbb{F} \subseteq \mathbb{K}$ sia un campo di spezzamento di f*

Dimostrazione
1) $\Rightarrow$ 2)
$[\mathbb{K} : \mathbb{F}] = n < +\infty \Rightarrow \exists\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{K}$ *base di* $\mathbb{K}$ *come* $\mathbb{F}$*-spazio vettoriale*
$\Rightarrow \mathbb{F} \subseteq \mathbb{F}(\alpha_1, \ldots, \alpha_k) = \mathbb{K}$
Essendo finita, l'estensione è algebrica.
Poniamo $p_j \in \mathbb{F}[x]$ *polinomio minimo di* $\alpha_j, \quad \forall j \in \{1, \ldots, n\}$ *Per l'ipotesi di normalità* p_j *si decompone in fattori lineari in* $\mathbb{K}[x], \quad \forall j \in \{1, \ldots, n\}$
Definiamo:

$$f(x) = p_1(x) \cdot \ldots p_k(x) \subseteq \mathbb{F}[x].$$

f *si decompone in fattori lineari in* $\mathbb{K}[x]$
Inoltre ogni estensione intermedia $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{K}$ *tale che* f *si decomponga come prodotto di fattori lineari in* $\mathbb{L}[x]$ *soddisfa* $a_j \in \mathbb{L} \quad \forall j \in \{1, \ldots, n\} \quad \Rightarrow \quad \mathbb{L} = \mathbb{K}$
2) $\Rightarrow$ 1)
dalle ipotesi $\Rightarrow [\mathbb{K} : \mathbb{F}] < +\infty$
Consideriamo $g \in \mathbb{F}[x]$ *irriducibile con* $\alpha \in \mathbb{K}$ *radice di* g
Consideriamo un campo di spezzamento $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *del polinomio* $f \cdot g$ *Sia* $\beta \in \mathbb{L}$ *radice di* g *dobbiamo dimostrare che* $\beta \in \mathbb{K}$
Abbiamo $\mathbb{F}(\alpha) \cong \mathbb{F}(\beta)$
quindi $[\mathbb{F}(\alpha) : \mathbb{F}] = [\mathbb{F}(\beta) : \mathbb{F}]$
Inoltre $\mathbb{F}(\alpha) \subseteq \mathbb{K}(\alpha)$ *e* $\mathbb{F}(\beta) \subseteq \mathbb{K}(\beta)$
Sono entrambi campi di spezzamento di f*.*
pensando $f \in \mathbb{F}_(\alpha)[x]$ *e* $f \in \mathbb{F}(\beta)[x]$ *rispettivamente.*
Dall'unicità dei campi di spezzamento:
IMMAGINE 14 30
In particolare $[\mathbb{K}(\alpha) : \mathbb{F}(\alpha)] = [\mathbb{K}(\beta) : \mathbb{F}(\beta)]$

$[\mathbb{K}(\alpha):\mathbb{K}][\mathbb{K}:\mathbb{F}] = [\mathbb{K}(\alpha):\mathbb{F}]$
$= [\mathbb{K}(\beta):\mathbb{F}(\beta)][\mathbb{F}(\beta):\mathbb{F}] = [\mathbb{K}(\beta):\mathbb{F}] = [\mathbb{K}(\beta):\mathbb{K}][\mathbb{K}:\mathbb{F}]$
da cui:

$$[\mathbb{K}(\beta):\mathbb{K}] = [\mathbb{K}(\alpha):\mathbb{K}] = 1.$$

$\Rightarrow \beta \in \mathbb{K}$ $\square$

0.3 Estensioni semplici e separabili

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

1. $k \in \mathbb{K}$ *si dice separabile su* $\mathbb{F}$ *se è algebrico e il suo polinomio minimo è separabile.*
2. $\mathbb{F} \subseteq \mathbb{K}$ *si dice estensione separabile se ogni elemento di* $\mathbb{K}$ *è separabile in* $\mathbb{F}$
3. $\mathbb{F} \subseteq \mathbb{K}$ *si dice estensione semplice se* $\exists \alpha \in \mathbb{K}$ *tale che* $\mathbb{F} \subseteq \mathbb{F}(\alpha) = \mathbb{K}$

Osservazione

- se $char(\mathbb{F}) = 0$ allora ogni estensione algebrica è separabile
- $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{2})$ è semplice (scegliere $\alpha = \sqrt{i} \in \mathbb{Q}(i, \sqrt{2})$

Proposizione 1
$\mathbb{F}$ *campo infinito.* $\mathbb{F} \subseteq \mathbb{K}$ *estensione.*
$a, b \in \mathbb{K}$ *separabili su* $\mathbb{F}$
Allora esiste $\alpha \in \mathbb{K}$ *tale che*

$$\mathbb{F}(\alpha) = \mathbb{F}(a, b).$$

Dimostrazione
Sia f, g *i polinomi minimi in* $\mathbb{F}[x]$ *di* a *e* b.
Per ipotesi sono entrambi privi di radici multiple.
Siano:

$$a_1, \ldots, a_n \quad e \quad b_1, \ldots, b_m.$$

le radici di f *e* g *in* $\mathbb{L}$
dove $\mathbb{F} \subseteq \mathbb{K} \subset \mathbb{L}$
un'ulteriore estensione dove f *e* g *si spezzano in fattori lineari.*
Supponiamo $a_1 = a$, $b_1 = b$
Studiamo l'equazione $a + \lambda b = a_i + \lambda b_j$
nella variabile λ *al variare di* $i \in \{1, \ldots, n\}$, $j \in \{2, \ldots, m\}$
Ogniuna di tali equazioni ammette l'unica soluzione

$$\lambda = \frac{a_i - a}{b - b_j} \in \mathbb{L}.$$

Essendo $|\mathbb{F}| = +\infty$ *esiste* $\gamma \in \mathbb{F}$ *che non sia soluzione di alcune delle precedenti* $n \cdot (m-1)$ *equazioni.*
Definiamo

$$\alpha = a + \gamma b \in \mathbb{F}(a, b).$$

Quindi $\mathbb{F}(\alpha) \subseteq \mathbb{F}(a, b)$
Resta da verificare che $\mathbb{F}(a, b) \subseteq \mathbb{F}(\alpha)$ *è sufficiente mostrare che* $b \in \mathbb{F}(\alpha)$
$(a = \alpha - \gamma b)$
Consideriamo

$$h(x) = f(\alpha - \gamma x) \in \mathbb{F}(\alpha)[x].$$

$h(\alpha - \gamma b) = f(a) = 0$
$h(b_j) = f(\alpha - \gamma b_j) = f(a + \gamma n - \gamma b_j) \neq 0$ *dato che l'argomento della funzione non è un* a_i
Deduciamo

$$MCD(h(x), g(x)) = (x - b) \quad in \quad \mathbb{L}[x].$$

Se per assurdo $MCD(h(x), g(x)) = 1$ *in* $\mathbb{F}(\alpha)[x]$ *avremmo un'identità di Bezout a coefficienti in* $\mathbb{F}(\alpha) \subseteq Ł$
$\Rightarrow$ *sarebbero coprimi anche in* $\mathbb{L}[x]$
Quindi

$$(x, b) \in \mathbb{F}(\alpha)[x] \Rightarrow b \in \mathbb{F}(\alpha).$$

$\square$

Corollario 1
$\mathbb{F}$ *campo infinito. Allora ogni estensione di* $\mathbb{F}$ *separabile e finita è semplice*

Dimostrazione
segue iterando la proposizione $\square$