Lezione N+3 Algebra I

Federico De Sisti

2025-05-22

0.1 Ordine lessicografico sui monomi

$\mathbb{F}$ campo
Definiamo l'ordinamento lessicografico sull'insieme dei monomi monici in $\mathbb{F}[x_1, \ldots, x_n]$
Diremo che
$x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \quad k_1, \ldots, k_n \in \mathbb{Z}_{\geq 0}$
è maggiore di $x_1^{h_1} \cdot \ldots \cdot x_n^{h_n} \quad h_1, \ldots, h_n \in \mathbb{Z}_{\geq 0}$
se esiste $s \in \{1, \ldots, n-1\}$ tale che:

1. $k_j = h_j \quad \forall j \in \{1, \ldots, s\}$
2. $k_{s+1} > h_{s+1}$

Esempio
$n = 2$

- $x_1^2 > x_1$
- $x_1 > x_2$
- $x_1 > x_2^{69}$

0.2 Polinomi simmetrici

Definizione 1
$\mathbb{F}$ campo

1. *$p \in \mathbb{F}[x_1, \ldots, x_n]$ si dice polinomio simmetrico*
   $s \in p(x_1, \ldots, x_n) = p(x_{\tau(1)}, \ldots, x_{\tau(n)})$
   per ogni $\tau \in S_n$
2. *I polinomi simmetrici elementari sono*

$$\varepsilon_s(x_1, \ldots, x_n) = \sum_{1 \leq j_1 < \ldots < j_s \leq n} x_{j_1} \cdot \ldots \cdot x_{j_s}.$$

   con $s \in \{1, \ldots, n\}$
3. *L'insieme dei polinomi simmetrici si denota $\mathbb{F}[x_1, , x_n]^{S_n}$*

Obiettivo
Ogni polinomio simmetrico si scrive in modo unico come polinomio nei polinomi simmetrici elementari

Teorema 1
$\mathbb{F}[x_1, \ldots, x_n]^{S_n} \cong F[\varepsilon_1, \ldots, \varepsilon_n]$

Dimostrazione
Sia $p \in \mathbb{F}[x_1, \ldots, x_n]^{S_n}$
Sia $\alpha x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ il monomio massimo fra quelli che appaiono in p.

- *dimostriamo che* $k_1 \geq k_2 \geq \ldots \geq k_n$
  Se per assurdo $k_1 < k_2$ *allora potremmo applicare* $\tau = (12) \in S_n$*per ottenere il monomio*

$$\alpha x_2^{k_1} \cdot x_1^{k_2} \cdot x_3^{k_3} \cdot \ldots \cdot x_n^{k_n} \quad \textit{in } p.$$

  Ma questo monomio è

$$\alpha \cdot x_1^{k_2} \cdot x_2^{k_1} \cdot x_3^{k_3} \cdot \ldots \cdot x_n^{k_n} > \alpha x_1^{k_1} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n}.$$

  da cui l'assurdo per l'ipotesi di massimalità

- $\phi_1(x_1, \ldots, x_n) := \varepsilon_1^{k_1-k_2} \cdot \ldots \cdot \varepsilon_s^{k_s-k_{s+1}} \cdot \ldots \cdot \varepsilon_n^{k_n}$
  $\Rightarrow \phi_1 \in \mathbb{F}[x_1, \ldots, x_n]^{S_n}$
  Il monomio massimo di ϕ_1 *è*

$$(x_1)^{k_1-k_2} \cdot (x_1 x_2)^{k_2-k_3} \cdot \ldots \cdot (x_1 \ldots x_n)^{k_n}.$$

  ovvero

$$x_1^{k_1} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n}.$$

- $p - \alpha \cdot \phi_1 \in \mathbb{F}[x_1, \ldots, x_n]^{S_n}$
  ha monomio massimo minore rispetto a p

- *Iterando il procedimento un numero finito di volte avremo*

$$p = \alpha_1 \phi_1 + \ldots + \alpha_r \phi_r \in \mathbb{F}[\varepsilon_1, \ldots, \varepsilon_n].$$

Unicità
"basta" verificare che se $\exists g \in \mathbb{F}[z_1, \ldots, z_n]$ *tale che*

$$g(\varepsilon_1, \ldots, \varepsilon_n) = 0.$$

allora $g(z_1, \ldots, z_n) = 0$
Dimostriamo che se

$$g(z_1, \ldots, z_n) \neq 0.$$

allora

$$g(\varepsilon_1, \ldots, \varepsilon_n) \neq 0.$$

Dato $g \in \mathbb{F}[z_1, \ldots, x_n] \setminus \{0\}$
consideriamo il monomio massimo in g

$$\beta \cdot z_1^{h_1} \cdot \ldots \cdot x_n^{h_n}.$$

Allora il monomio massimo in $g(\varepsilon_1, \ldots, \varepsilon_n)$ *rispetto alle variabili* $x_1, \ldots, x_n$

$$\beta \cdot x_1^{h_1} \cdot (x_1 x_2)^{h_2} \cdot \ldots \cdot (x_1 \ldots x_n)^{h_n}.$$

ovvero

$$\beta \cdot x^{h_1+\ldots+h_n} \cdot x_2^{h_2+\ldots+h_n} \cdot \ldots \cdot x_n^{h_n}.$$

In particolare

$$g(\varepsilon_1, \ldots, \varepsilon_n) \neq 0.$$

□

0.3 Estensioni radicali e gruppi risolubili

Definizione 2 (Estesione radicale)
$\mathbb{F}$ *campo con* $char(F) = 0$, *Un'estensione* $\mathbb{F} \subseteq \mathbb{K}$ *si dice radicale se* $\exists m, n_1, \ldots, n_m \in \mathbb{Z}_{\geq 1}$ *e* $\exists \alpha_1, \ldots, \alpha_m \in \mathbb{K}$ *tali che*

1. $\mathbb{F} \subseteq \mathbb{F}(\alpha_1, \ldots, \alpha_m) = \mathbb{K}$
2. $\alpha_1^{n_1} \in \mathbb{F}$
3. $\alpha_j^{n_j} \in \mathbb{F}(\alpha_1, \ldots, \alpha_{j-1})$ $\;j \in \{2, \ldots, m\}$

Definizione 3
$f \in \mathbb{F}[x]$ *risolubile per radicali se un suo campo di spezzamento* $\mathbb{F} \subseteq \mathbb{K}$ *esiste un'estensione* $\mathbb{K} \subseteq \mathbb{L}$ *tale che* $\mathbb{F} \subseteq \mathbb{L}$ *è un'estensione radicale.*

Proposizione 1
Sia $\mathbb{F}$ *campo,* $char(\mathbb{F}) = 0$ $\mathbb{F} \subseteq \mathbb{K}$ *estensione radicale, allora esiste un'estensione* $\mathbb{K} \subseteq \mathbb{L}$ *tale che la composizione* $\mathbb{F} \subseteq \mathbb{L}$ *sia Galoisiana radicale (di grado finito)*

Dimostrazione
Sia $\alpha_1, \ldots, \alpha_m$ *successione radicale per* $\mathbb{F} \subseteq \mathbb{K}$ *Siano* $p_j \in \mathbb{F}[x]$ *polinomi minimi di* d_j *per* $j \in \{1, \ldots, m\}$
$f = p_1 \cdot \ldots \cdot p_m \in \mathbb{F}[x]$
Sia $\mathbb{F} \subseteq \mathbb{L}$ *campo di spezzamento di* $f \Rightarrow \mathbb{F} \subseteq \mathbb{L}$ *Galoisiano di grado finito*

- *Dimostriamo che* $\mathbb{F} \subseteq \mathbb{L}$ *è la composizione dell'estensione* $\mathbb{F} \subseteq \mathbb{K}$ *con un'estensione* $\mathbb{K} \subseteq \mathbb{L}$
  Siano $\beta_1, \ldots \beta_m \in \mathbb{L}$ *radici (qualsiasi) di* $p_1, \ldots p_m$ *rispettivamente*
  INSERISCI IMMAGINE 5 31 22 maggio
  Quindi abbiamo l'estensione $\mathbb{K} \hookrightarrow \mathbb{L}$ *che rende commutativo il diagramma*
  INSERISCI IMMAGINE 5 33 22 maggio

- *Resta da verificare che* $\mathbb{F} \subseteq \mathbb{L}$ *sia radicale.*
  Abbiamo dimostrato che $\beta_1, \ldots, \beta_m$ *è una successione radicale per* $\mathbb{F} \subseteq \mathbb{F}(\beta_1, \ldots, \beta_n)$
  Siano $\{\beta_{j,r}\}_{k \in \{1, \ldots, deg(p_j)\}}$ *le radici di* p_j *in* $\mathbb{L}$
  $\Rightarrow F \subseteq F(\beta_{1,1}, \ldots, \beta_{1,\deg(p_1)}, \beta_{2,1}, \ldots, \beta_{2,\deg(p_1)}, \ldots, \beta_{n,1}, \ldots, \beta_{n,\deg(p_1)})$

$\square$

Lemma 1
$\mathbb{F}$ campo, $char(\mathbb{F}) = 0, a \in \mathbb{F} \setminus \{0\}$ supponiam oche $\mathbb{F}$ contega tutte le radiii $n-$ e

PARTE CHE MANCA RECUPERALA DA LEONARDO

Proposizione 2
$\mathbb{F}$ campo, $char(\mathbb{F}) = 0$ $\mathbb{F} \subseteq \mathbb{K}$ estensione Galoisiana e radicale. Allora $G(\mathbb{K}, \mathbb{F})$ è risolubile

Dimostrazione
$\alpha_1, \dots, \alpha_k$ successione radicale di esponenti $n_1, \dots n_m$ per $\mathbb{F} \subseteq \mathbb{K}$
$n = mcm(n_1, \dots, n_m) \in \mathbb{Z}_{\geq 1}$ Abbiamo $\alpha_j^n \in \mathbb{F}(\alpha_1, \dots, \alpha_{j-1})$
Sia $\omega \in \mathbb{A}$ radice n-esima primitiva dell'unità .

$$\mathbb{F} = \mathbb{L}_0 \subseteq \mathbb{L}_1 = \mathbb{L}_0(\omega) \subseteq \mathbb{L}_2 = \mathbb{L}_1(\alpha_1 \subseteq \ldots \subseteq \mathbb{L}_j = \mathbb{L}_{j-1}(\alpha_j) \subseteq \ldots \subseteq \mathbb{L} = \mathbb{K}(\omega).$$

dimostriamo che $G(\mathbb{L}, \mathbb{F})$ è risolubile.
$\mathbb{F} \subseteq \mathbb{L}$ è un'estensione Galoisiana perché composizione

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

la prima giustificata perché Galoisiana per ipotesi e la seconda per cambio di sp. di $x^n - 1 \in \mathbb{K}[x]$
Quindi per il teorema di Galois abbiamo catena di sottogruppi

$$G(\mathbb{L}, \mathbb{F}) = G(\mathbb{L}, \mathbb{L}_0) \geq G(\mathbb{L}, \mathbb{L}_1) \geq \ldots \geq G(\mathbb{L}, \mathbb{L}) = \{id\}.$$

Verifichiamo che

1. *$G(\mathbb{L}, \mathbb{L}_j) \trianglerighteq G(\mathbb{L}, \mathbb{L}_{j+1})$ infatti l'estensione $\mathbb{L}_j \subseteq \mathbb{L}_{j+1}$ è normale, perché è campo di spezzamento del polinomio $x^n - \alpha_{j+1}^n \in \mathbb{L}_j[x]$*
2. *$\dfrac{G(\mathbb{L}, \mathbb{L}_j)}{G(\mathbb{L}, \mathbb{L}_{j+1})} \cong G(\mathbb{L}_{j+1}, \mathbb{L}_j)$ che è abeliano (lemma)*

Quindi $G(\mathbb{L}, \mathbb{F})$ è risolubile

- *Resta da verificare che $G(\mathbb{L}, \mathbb{F})$ è risolubile*
  Abbiamo $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{K}(\omega) = \mathbb{L}$
  dove $\mathbb{F} \subseteq \mathbb{K}$ normale per ipotesi Dal teorema di Galois:

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

  quoziente di un gruppo risolubile $\Rightarrow$ risolubile

$\square$

Teorema 2
$\mathbb{F}$ campo, char$(\mathbb{F}) = 0$ $f \in \mathbb{F}[x]$ risolubile per radicali.
Allora il suo campo di spezzamento $\mathbb{F} \subseteq \mathbb{K}$ ha gruppo di Galois $G(\mathbb{K}, \mathbb{F})$ risolubile.

Dimostrazione
Sappiamo che esiste estensione $\mathbb{K} \subseteq \mathbb{L}$ tale che $\mathbb{F} \subseteq \mathbb{L}$ sia radicale e Galoisiana
Dalla proposizione segue che $G(\mathbb{L}, \mathbb{F})$ risolubile
Ora, $\mathbb{F} \subseteq \mathbb{K}$ normale (poiché campo di spezzamento) quindi per teorema di Galois

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

che è risolubile poiché quoziente di risolubile. □

0.4 Teorema di Abel-Ruffini

Definizione 4
$\mathbb{F} = \mathbb{Q}(a_1, \ldots, a_n)$ dove $a_1, \ldots, a_n$ variabili trascendenti.

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} a + a_n \in \mathbb{F}[x].$$

si dice polinomio generico di grado n.

Teorema 3 (Abel-Ruffini (1799) - Galois (1846))
Il polinomio generico di grado $n \geq 5$ non è risolubile per radicali

Dimostrazione
Dato $\mathbb{F} \subseteq \mathbb{K}$ campo di spezzamento di f, dimostriamo che

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

e dunque non risolubile per $n \geq 5$

- *$\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ radici di $f \in \mathbb{F}[x]$*
  $f(x) = \prod_{j=1}^{n} (x - \alpha_j) = x^n + \sum_{s=1}^{n} (-1)^n \left(\sum_{1 \leq j_1 < \ldots < j_s \leq n} a_{j_1} \cdot \ldots \cdot a_{j_s} \right) x^{n-s}$
  quindi $a_s \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ $\quad s \in \{1, \ldots, n\}$
  Quindi il campo di spezzamento di f è

  $$\mathbb{F} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n).$$

- *Esiste un omomorfismo di gruppi (iniettivo!)*

  $$\begin{array}{c} i : S_n \to G(\mathbb{K}, \mathbb{F}) \\ \tau \to i_\tau \end{array}.$$

dove $i_\tau(\alpha_j) = \alpha_{\tau(j)}$
$H := im(i) \leq G(\mathbb{K}, \mathbb{F})$ *con* $H \cong S_n$

- *Dal teorema di Galois*

$$S_n \cong H = G(\mathbb{K}, \mathbb{K}_H) = G(\mathbb{K}, \mathbb{F}).$$

dove l'ultima uguaglianza segue dal fatto che $\mathbb{Q}[x_1, \ldots, x_n]^{S_n} = \mathbb{Q}[\varepsilon_1, \ldots, \varepsilon_n]$

$\square$