Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione dell'08-05-2020

Esercizio sulle estensioni di $\mathbb{Q}$

Osservazione

$K \subseteq L$ estensione, $\alpha \in L$, $f \in K[X]$ monico e irriducibile, $f(\alpha) = 0$
$\Longrightarrow$ $f = \mathrm{m}_{\alpha,K}$ ($\mathrm{m}_{\alpha,K} \mid f$ e sono entrambi monici e irriducibili).

1. $\forall\, n > 0\ \exists\, \alpha \in \mathbb{C}$ tale che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
2. $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.
3. $[\mathbb{R} : \mathbb{Q}] = [\mathbb{C} : \mathbb{Q}] = \infty$.
4. L'estensione $\mathbb{Q} \subseteq \overline{Q}$ non è finitamente generata.

Esercizio sulle estensioni di $\mathbb{Q}$

Osservazione

$K \subseteq L$ estensione, $\alpha \in L$, $f \in K[X]$ monico e irriducibile, $f(\alpha) = 0$ $\implies$ $f = \mathrm{m}_{\alpha,K}$ ($\mathrm{m}_{\alpha,K} \mid f$ e sono entrambi monici e irriducibili).

1. $\forall\, n > 0\ \exists\, \alpha \in \mathbb{C}$ tale che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
2. $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.
3. $[\mathbb{R} : \mathbb{Q}] = [\mathbb{C} : \mathbb{Q}] = \infty$.
4. L'estensione $\mathbb{Q} \subseteq \overline{Q}$ non è finitamente generata.

1. $\alpha := \sqrt[n]{2} \in \mathbb{R}$ è radice di $X^n - 2 \in \mathbb{Q}[X]$ monico e irriducibile (per il criterio di Eisenstein relativo al primo 2) $\implies$ $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(X^n - 2) = n$.
2. $\forall\, n > 0$, dato α come nel punto 1, $\alpha \in \overline{\mathbb{Q}}^{\mathbb{C}} = \overline{\mathbb{Q}}$ $\implies$ $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \overline{\mathbb{Q}}$ estensioni $\implies$ $[\overline{Q} : \mathbb{Q}] \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
3. $\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$ estensioni $\implies$ $[\mathbb{C} : \mathbb{Q}] \geq [\overline{Q} : \mathbb{Q}] = \infty$.
   $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ estensioni, $[\mathbb{C} : \mathbb{R}] = 2$, per assurdo $[\mathbb{R} : \mathbb{Q}] = n < \infty$ $\implies$ $[\mathbb{C} : \mathbb{Q}] = 2n < \infty$, assurdo.
4. È algebrica ma non finita (per il punto 2).

Esercizio sugli elementi trascendenti

$K \subseteq L$ estensione, $\alpha \in L$ trascendente su K, $\beta \in K(\alpha) \setminus K \implies$

1. α algebrico su $K(\beta)$;
2. β trascendente su K.

Esercizio sugli elementi trascendenti

$K \subseteq L$ estensione, $\alpha \in L$ trascendente su K, $\beta \in K(\alpha) \setminus K \implies$

1. α algebrico su $K(\beta)$;
2. β trascendente su K.

1. $\beta \in K(\alpha) \implies \exists f, g \in K[X]$ con $g \neq 0$ ($\implies g(\alpha) \neq 0$) tali che $\beta = f(\alpha)g(\alpha)^{-1} \implies 0 = f(\alpha) - \beta g(\alpha) = h(\alpha)$ con $h := f - \beta g \in K(\beta)[X] \implies \alpha$ algebrico su $K(\beta)$ perché $h \neq 0$: per assurdo $h = 0 \implies$ (se $f = \sum_{i \geq 0} a_i X^i$ e $g = \sum_{i \geq 0} b_i X^i$ con $a_i, b_i \in K$ e $b_n \neq 0$ per qualche $n \in \mathbb{N}$) $0 = f - \beta g = \sum_{i \geq 0}(a_i - \beta b_i)X^i \implies a_n - \beta b_n = 0 \implies \beta = a_n b_n^{-1} \in K$, assurdo.
2. $K \subseteq K(\beta) \subseteq K(\alpha)$ estensioni tali che $[K(\alpha) : K] = \infty$ (perché α trascendente su K) e $[K(\alpha) = K(\beta)(\alpha) : K(\beta)] < \infty$ (perché α algebrico su $K(\beta)$) $\implies [K(\beta) : K] = \infty \implies \beta$ trascendente su K.

Esercizio sulle estensioni finite

$K \subseteq K' \subseteq L$ estensioni, $\alpha \in L$ con $[K' : K] = n$ e $[K(\alpha) : K] = m$.

1. $\mathrm{mcm}(m, n) \mid [K'(\alpha) : K] \leq mn$ (dunque $[K'(\alpha) : K] = mn$ se $\mathrm{mcd}(m, n) = 1$).
2. $[K'(\alpha) : K] \nmid mn$ se $K = \mathbb{Q}$, $L = \mathbb{C}$, $K' = \mathbb{Q}(\beta)$ con α e β radici distinte di $X^3 - 2$.

Esercizio sulle estensioni finite

$K \subseteq K' \subseteq L$ estensioni, $\alpha \in L$ con $[K' : K] = n$ e $[K(\alpha) : K] = m$.

1. $\mathrm{mcm}(m, n) \mid [K'(\alpha) : K] \leq mn$ (dunque $[K'(\alpha) : K] = mn$ se $\mathrm{mcd}(m, n) = 1$).
2. $[K'(\alpha) : K] \nmid mn$ se $K = \mathbb{Q}$, $L = \mathbb{C}$, $K' = \mathbb{Q}(\beta)$ con α e β radici distinte di $X^3 - 2$.

1. $m' := [K'(\alpha) : K'] \leq m$, $K \subseteq K' \subseteq K'(\alpha)$ estensioni $\implies$ $l := [K'(\alpha) : K] = [K'(\alpha) : K'][K' : K] = m'n \leq mn$.
   $K \subseteq K(\alpha) \subseteq K'(\alpha)$ estensioni $\implies$ $m \mid l$; $n \mid l = m'n$ $\implies$ $\mathrm{mcm}(m, n) \mid l$.
2. $\mathrm{m}_\alpha = \mathrm{m}_\beta = X^3 - 2$ (perché monico e irriducibile in $\mathbb{Q}[X]$) $\implies$ $m = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\mathrm{m}_\alpha) = 3$ e analogamente $n = 3$.
   $\omega := \alpha\beta^{-1} \in \mathbb{C}$ tale che $K'(\alpha) = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta, \omega)$.
   $\omega^3 = \alpha^3\beta^{-3} = 1$ $\implies$ ω radice di $X^3 - 1 = (X - 1)f$ con $f := (X^2 + X + 1)$ monico e irriducibile in $\mathbb{Q}[X]$; $\omega \neq 1$ $\implies$ ω radice di f $\implies$ $\mathrm{m}_\omega = f$ $\implies$ $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\mathrm{m}_\omega) = 2$.
   $[K'(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta, \omega) : \mathbb{Q}] = 3 \cdot 2 = 6 \nmid mn = 9$.

Esercizio

1. $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.
2. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
3. $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
4. Determinare $\mathrm{m}_{\sqrt{2}+\sqrt{3},\mathbb{Q}}$.

Esercizio

1. $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.
2. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
3. $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
4. Determinare $\mathrm{m}_{\sqrt{2}+\sqrt{3},\mathbb{Q}}$.

1. $\mathrm{m}_{\sqrt{2}} = X^2 - 2 \implies [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $\mathrm{m}_i = X^2 + 1 \implies [\mathbb{Q}(i) : \mathbb{Q}] = 2$. Dunque $l := [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$ tale che $2 = \mathrm{mcm}(2, 2) \mid l \mid 2 \cdot 2 = 4 \implies l = 2$ o 4. Per assurdo $l = 2 \implies [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 1 \implies \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}) \implies i \in \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, assurdo.
2. Analogamente al punto 1, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2$ o 4. Per assurdo sia $2 \implies \sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Poiché $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[X]/(X^2 - 2)$, che ha come $\mathbb{Q}$-base $\{\overline{1}, \overline{X}\}$, $\mathbb{Q}(\sqrt{2})$ ha come $\mathbb{Q}$-base $\{1, \sqrt{2}\} \implies \exists!\, a, b \in \mathbb{Q}$ tali che $\sqrt{3} = a + b\sqrt{2} \implies 3 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2} \implies a^2 + 2b^2 = 3$ e $2ab = 0 \implies a = 0$ e $2b^2 = 3$ o $b = 0$ e $a^2 = 3$, assurdo.

Dimostrazione di 3 e 4

3. $\alpha := \sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3}) \implies \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$, e per dimostrare che $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$ (e quindi concludere che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{3})$) basta verificare che $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\alpha)$.
$\alpha^2 = 5+2\sqrt{6} \in \mathbb{Q}(\alpha) \implies \sqrt{6} = (\alpha^2-5)/2 \in \mathbb{Q}(\alpha) \implies$
$\alpha\sqrt{6} = 2\sqrt{3}+3\sqrt{2} \in \mathbb{Q}(\alpha) \implies$
$2\sqrt{3}+3\sqrt{2}-2\alpha = \sqrt{2} \in \mathbb{Q}(\alpha) \implies \alpha-\sqrt{2} = \sqrt{3} \in \mathbb{Q}(\alpha)$.
4. Come visto nel punto 3, $2\sqrt{6} = \alpha^2-5 \implies$

$$24 = (\alpha^2-5)^2 = \alpha^4-10\alpha^2+25$$

$\implies \alpha^4-10\alpha^2+1 = 0 \implies \alpha$ è radice di $f := X^4-10X^2+1 \in \mathbb{Q}[X] \implies \mathrm{m}_\alpha \mid f$. Per i punti 3 e 2

$$\deg(\mathrm{m}_\alpha) = [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4 = \deg(f)$$

$\implies \mathrm{m}_\alpha$ e f sono associati $\implies \mathrm{m}_\alpha = f$ perché sono entrambi monici.

Costruzioni con riga e compasso

- $C_0 := \{(0,0),(1,0)\} \subset \mathbb{R}^2$ e $\forall\, n > 0$ $C_n := \{(\alpha,\beta) \in T \cap T'\}$, dove T e T' (con $T \neq T'$) sono rette passanti per due punti di C_{n-1} o circonferenze con centro un punto di C_{n-1} e raggio la distanza tra due punti di C_{n-1}.
- $\alpha \in \mathbb{R}$ è costruibile (con riga e compasso) se $(\alpha, 0) \in C_n$ per qualche $n \in \mathbb{N}$.
- Non è difficile dimostrare che $\alpha \in \mathbb{R}$ costruibile $\implies$ $\exists\, \mathbb{Q} = F_0 \subseteq \cdots \subseteq F_n \subset \mathbb{R}$ estensioni con $\alpha \in F_n$ e $[F_i : F_{i-1}] = 2$ per $i = 1, \ldots, n$ $\implies$

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [F_n : \mathbb{Q}] = 2^n$$

$\implies$ $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ per qualche $m \leq n$.

- Dunque $\alpha \in \mathbb{R}$ non è costruibile se $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ non è una potenza di 2. Per esempio $\sqrt[3]{2}$ non è costruibile (è impossibile "duplicare il cubo").

Radice di un polinomio in un'estensione

Dato $f \in K[X]$ (che posso supporre irriducibile e monico), esiste un'estensione $K \subseteq L$ tale che f abbia una radice $\alpha \in L$?
Se la risposta è sì, $f = \mathrm{m}_{\alpha,K}$; inoltre posso supporre $L = K(\alpha)$, e in questo caso $L \cong K[X]/(f)$.

Radice di un polinomio in un'estensione

Dato $f \in K[X]$ (che posso supporre irriducibile e monico), esiste un'estensione $K \subseteq L$ tale che f abbia una radice $\alpha \in L$?
Se la risposta è sì, $f = \mathrm{m}_{\alpha,K}$; inoltre posso supporre $L = K(\alpha)$, e in questo caso $L \cong K[X]/(f)$.

Proposizione

$f \in K[X]$ irriducibile e monico, $\pi\colon K[X] \to L := K[X]/(f)$ proiezione al quoziente, $\alpha := \pi(X) \in L \implies \pi|_K\colon K \to L$ estensione, $L = K(\alpha)$ e $f = \mathrm{m}_{\alpha,K}$ (quindi f ha una radice in L).

Dimostrazione.

f irriducibile $\implies$ (f) ideale massimale $\implies$ L campo.
$\pi|_K$ estensione perché omomorfismo di anelli con K e L campi.
π omomorfismo di K algebre tale che $\pi(X) = \alpha \implies \pi(g) = g(\alpha)$
$\forall\, g \in K[X] \implies L = \{g(\alpha) : g \in K[X]\} = K[\alpha] = K(\alpha)$.
f irriducibile e monico, $f(\alpha) = \pi(f) = 0 \implies f = \mathrm{m}_{\alpha,K}$. □

Campo di spezzamento di un polinomio

Definizione

Un campo di spezzamento di $f \in K[X] \setminus \{0\}$ è un'estensione $K \subseteq L$ tale che:

- f si spezza su L, cioè $\exists\, c \in K^*$ e $\alpha_1, \ldots, \alpha_n \in L$ tali che $f = c\prod_{i=1}^{n}(X - \alpha_i)$;
- $K \subseteq L' \subseteq L$ estensione tale che f si spezza su $L' \implies L' = L$.

Se $K \subseteq L$ è un campo di spezzamento di f, si dice anche che L è un campo di spezzamento di f su K.

Osservazione

$K \subseteq L$ estensione tale che $f = c\prod_{i=1}^{n}(X - \alpha_i) \in K[X]$ si spezza su $L \implies \exists!\, K \subseteq L_0 \subseteq L$ estensione tale che $K \subseteq L_0$ è un campo di spezzamento di f; inoltre $L_0 = K(\alpha_1, \ldots, \alpha_n)$.
Infatti f si spezza su $K(\alpha_1, \ldots, \alpha_n)$, e se $K \subseteq L' \subseteq L$ è un'estensione tale che f si spezza su L', allora $\alpha_1, \ldots, \alpha_n \in L'$ (per l'unicità della fattorizzazione in $L[X]$), per cui $K(\alpha_1, \ldots, \alpha_n) \subseteq L'$.

Esistenza del campo di spezzamento

Teorema

K campo, $0 \neq f \in K[X]$.

1. *Esiste un campo di spezzamento di f.*
2. *$n := \deg(f)$, $K \subseteq L$ campo di spezzamento di f $\implies$ $[L : K] \mid n!$. Inoltre $n \mid [L : K]$ se f è irriducibile in $K[X]$.*

Dimostrazione.

1. Per l'Osservazione basta dimostrare che esiste un'estensione $K \subseteq L$ tale che f si spezza su L.
   Per induzione su n: se $n = 0$, basta prendere $L = K$.
   Se $n > 0$, allora $\exists\, g \in K[X]$ irriducibile tale che $g \mid f$.
   Per la Proposizione $\exists\, K \subseteq K'$ estensione e $\exists\, \alpha \in K'$ tale che $g(\alpha) = 0 \implies f(\alpha) = 0 \implies f = (X - \alpha) f_1$ con $f_1 \in K'[X]$ e $\deg(f_1) = n - 1$.
   Per induzione $\exists\, K' \subseteq L$ estensione tale che f_1 si spezza su L $\implies$ f si spezza su L.

Dimostrazione di 2

Per definizione $\exists\, c \in K^*$ e $\alpha_1, \ldots, \alpha_n \in L$ tali che $f = c\prod_{i=1}^{n}(X - \alpha_i)$, e per l'Osservazione $L = K(\alpha_1, \ldots, \alpha_n)$.
Per induzione su n: se $n = 0$, allora $f = c \in K^*$ (non irriducibile in $K[X]$) $\implies$ $L = K$ $\implies$ $[L : K] = 1 \mid n! = 1$.
Se $n > 0$ e f è irriducibile in $K[X]$, allora $\mathrm{m}_{\alpha_1,K} = c^{-1}f$ $\implies$ $[K(\alpha_1) : K] = \deg(\mathrm{m}_{\alpha_1,K}) = n$. Posto $n' := [L : K(\alpha_1)]$, $[L : K] = [L : K(\alpha_1)][K(\alpha_1) : K] = n'n$, per cui $n \mid [L : K]$.
$f = (X - \alpha_1)f_1$ in $K(\alpha_1)[X]$ con $f_1 := c\prod_{i=2}^{n}(X - \alpha_i)$ tale che $K(\alpha_1) \subseteq L$ campo di spezzamento di f_1 (perché f_1 si spezza su L e $L = K(\alpha_1)(\alpha_2, \ldots, \alpha_n)$). Poiché $\deg(f_1) = n - 1$, per induzione $n' = [L : K(\alpha_1)] \mid (n-1)!$ $\implies$ $[L : K] = n'n \mid (n-1)!n = n!$.
Se $n > 0$ e $f = gh$ non è irriducibile in $K[X]$ (con $0 < m := \deg(g) < n$), posso supporre $g = c\prod_{i=1}^{m}(X - \alpha_i)$ e $h = \prod_{i=m+1}^{n}(X - \alpha_i)$ $\implies$ $K' := K(\alpha_1, \ldots, \alpha_m)$ campo di spezzamento di g su K e L campo di spezzamento di h su K'.
Per induzione $[K' : K] \mid m!$ e $[L : K'] \mid (n-m)!$ $\implies$ $[L : K] = [L : K'][K' : K] \mid (n-m)!m! \mid n!$.