CAMPI (DI SPEZZAMENTO)

Note Title 12/14/2017

Estensioni quadratiche

K campo $(\mathrm{char}(K) \neq 2)$

$$x^2 - a \qquad (x-\sqrt{a})^2$$

$$ax^2+bx+c=0 \qquad \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

stiamo dividendo per 0!

$$K(\sqrt{\alpha}) = K(\sqrt{\beta}) \iff \exists\, \gamma \in K \text{ t.c. } \beta = \alpha \cdot \gamma^2$$

$\alpha, \beta \in K^\times$

$$\Updownarrow$$

$$\sqrt{\beta} = \pm\gamma\sqrt{\alpha}$$

$\boxed{\Leftarrow}$ $\sqrt{\beta} \in K(\sqrt{\alpha})$ perché $\sqrt{\beta} = \pm\gamma\sqrt{\alpha}$

$\sqrt{\alpha} \in K(\sqrt{\beta})$ —— $\sqrt{\alpha} = \pm \frac{1}{\gamma}\sqrt{\beta}$

$$\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(2\sqrt{2}) = \mathbb{Q}(\sqrt{2})$$

$\boxed{\Rightarrow}$ $K(\sqrt{\alpha}) = K(\sqrt{\beta}) \Rightarrow \sqrt{\beta} \in K(\sqrt{\alpha})$

$$K(\sqrt{\alpha}) = \{x + y\sqrt{\alpha} \mid x, y \in K\}$$

Quindi $\sqrt{\beta} = x + y\sqrt{\alpha}$ per qualche $x, y \in K$

$$\sqrt{\beta} - y\sqrt{\alpha} = x \in K$$

$$\underbrace{\beta + \alpha y^2}_{\in K} - 2y\sqrt{\alpha\beta} = \underbrace{x^2}_{\in K} \Rightarrow 2y\sqrt{\alpha\beta} \in K$$

char $K \neq 2$

$\Longrightarrow y\sqrt{\alpha\beta} \in K$

$y=0$: $\beta = x^2$, $K(\sqrt{\beta}) = K$

$K(\sqrt{\alpha}) = K(\sqrt{\beta}) = K$

$\alpha = z^2$, $z \in K^\times$

$\Rightarrow \beta/\alpha = (x/z)^2 = \gamma^2$

$y \neq 0$: $\sqrt{\alpha\beta} \in K$

$\Rightarrow \exists\, \delta \in K^\times$ t.c. $\alpha\beta = \delta^2$

$$\Rightarrow \beta/\alpha = \frac{\alpha\beta}{\alpha^2} = \frac{\delta^2}{\alpha^2}$$

e' il quad. di $\gamma = \delta/\alpha$

$\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{12})$ $\quad 12/3 = 4 = \square \in \mathbb{Q}$

$\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$ $\quad 3/2 \neq \square \in \mathbb{Q}$

Campo di spezzamento di $x^p - a$

Sia $a \in \mathbb{Q}^\times$, p primo $\quad x^p - a \in \mathbb{Q}[x]$

Sia K il campo di spezz. su $\mathbb{Q}$.

Posso ricondurmi al caso di $a \in \mathbb{Z}$.

$q(x) = x^p - \frac{m}{n}$

$$\begin{aligned} &\text{Campo di spezz. } q(x) \\ &\qquad \| \\ &\text{Campo di spezz. } q\left(\frac{x}{n}\right) \\ &\qquad \| \\ &\text{campo di spezz. } x^p/n^p - m/n \\ &\qquad \| \\ &\text{campo di spezz } x^p - m \cdot n^{p-1} \end{aligned}$$

Diciamo $p \neq 2$. $x^p - a$ è irriducibile, a meno che $a = b^p$ per un certo $b \in \mathbb{Z}$

Se $a = b^p$ il pol. ha una radice

Viceversa: sia ζ_p radice p-esima primitiva di $1 \in \mathbb{C}$

$$(x - \sqrt[p]{a})(x - \zeta_p \sqrt[p]{a})(x - \zeta_p^2 \sqrt[p]{a}) \cdots (x - \zeta_p^{p-1} \sqrt[p]{a})$$

Un fattore irrid. di $x^p - a$ in $\mathbb{Q}[x]$ è prodotto di un po' di questi termini lineari

Quindi: prendiamo un fattore irrid in $\mathbb{Q}[x]$,

$$\prod_j \left(x - \zeta_p^{i_j} \sqrt[p]{a}\right) \in \mathbb{Q}[x]$$

$\Rightarrow$ termine noto è razionale, e in effetti intero (lemma di Gauss)

$$\Rightarrow |\text{termine noto}| = \left(\sqrt[p]{a}\right)^{\overbrace{\#\text{ fattori nel prodotto}}^{k}} \in \mathbb{Z}$$

$$\Rightarrow a^{k/p} \in \mathbb{Z} \Rightarrow a^{k/p} = b \Rightarrow a = b^{p/k}$$

è possibile solo in due casi: $k = p$ ① ; $a =$ potenza ② p-esima

① $\Rightarrow$ $x^p - a$ irrid. (perché i suoi fattori irrid. su $\mathbb{Q}$ hanno grado $k = p$)

② $\Rightarrow$ $a = b^p$

$\boxed{\text{Caso 2: } a = b^p}$ C. spezz $(x^p - b^p)$ = C. spezz. $(x^p - 1)$

$$x^p - 1 = (x-1)\underbrace{(1 + x + \dots + x^{p-1})}_{\text{irriducibile}}$$

Radici: $\zeta_p, \zeta_p^2, \zeta_p^3, \dots, \zeta_p^{p-1}$

$$\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p, \zeta_p^2, \zeta_p^3, \dots, \zeta_p^{p-1})$$

$$= \text{Campo di spezz. } (x^p - 1)$$

DEF $\mathbb{Q}(\zeta_n)$ è detto l'*n-esimo campo* **CICLOTOMICO**

Caso 1: $x^p - a$ irriducibile

Radici: $\underset{\alpha_0}{\sqrt[p]{a}},\ \underset{\alpha_1}{\zeta_p \sqrt[p]{a}},\ \zeta_p^2 \sqrt[p]{a},\ \dots,\ \underset{\alpha_{p-1}}{\zeta_p^{p-1} \sqrt[p]{a}}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_0) \subseteq \mathbb{Q}(\alpha_0, \alpha_1) \subseteq \dots \subseteq \mathbb{Q}(\alpha_0, \dots, \alpha_{p-1})$$

$$[\mathbb{Q}(\alpha_0) : \mathbb{Q}] = p$$

$$\mathbb{Q}(\alpha_0) \simeq \mathbb{Q}[x]/(x^p - a)$$

OSS CHIAVE $\mathbb{Q}(\alpha_0, \alpha_1) = \mathbb{Q}(\alpha_0, \alpha_1/\alpha_0)$

$$= \mathbb{Q}(\alpha_0, \zeta_p)$$

$$= \mathbb{Q}(\alpha_0, \zeta_p, \zeta_p\alpha_0, \zeta_p^2\alpha_0, \zeta_p^3\alpha_0, \dots, \zeta_p^{p-1}\alpha_0)$$

$$= \mathbb{Q}(\alpha_0, \zeta_p\alpha_0, \dots, \zeta_p^{p-1}\alpha_0)$$

$=$ campo di spezzamento di $x^p - a = K$

OSS 2

$$\begin{tikzcd}
 & & K = \mathbb{Q}(\alpha_0, \zeta_p) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha_2) & \mathbb{Q}(\alpha_1) & \mathbb{Q}(\alpha_0) & \mathbb{Q}(\zeta_p) \\
 & & \mathbb{Q} \arrow[ull, dash] \arrow[ul, dash, "p"] \arrow[u, dash, "p"] \arrow[ur, dash, "p-1"'] &
\end{tikzcd}$$

$[K : \mathbb{Q}] \leq p(p-1)$, ma c'è uguaglianza

perché $(p, p-1) = 1$

$\boxed{\text{GRADO 3}}$ Sia $f(x) \in \mathbb{Q}[x]$ un polinomio irrid. di grado 3. Supponiamo che $f(x)=0$ abbia esattamente 1 radice reale.

Dim. che il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ ha grado $6 = 3!$

$\boxed{\text{DIM}}$ Chiamiamo α_0 la radice reale e $\alpha_1, \overline{\alpha_1}$ le due complesse coniugate.

$$\mathbb{Q} \underset{\substack{\text{grado } 3 \\ (\text{aggiungo rad. irrid. deg}=3)}}{\boxed{\subseteq}} \mathbb{Q}(\alpha_0) \underset{2}{\boxed{\subseteq}} \mathbb{Q}(\alpha_0, \alpha_1) \underset{\text{uguaglianza}}{\boxed{\subseteq}} \mathbb{Q}(\alpha_0, \alpha_1, \overline{\alpha_1})$$

Prodotto $\alpha_0 \cdot \alpha_1 \cdot \overline{\alpha_1} = -$ termine noto di $f(x) \in \mathbb{Q}$

$$\Rightarrow \overline{\alpha_1} = \frac{-f(0)}{\alpha_0 \cdot \alpha_1} \in \mathbb{Q}(\alpha_0, \alpha_1)$$

$$3! \geq [\mathbb{Q}(\alpha_0, \alpha_1) : \mathbb{Q}] = [\mathbb{Q}(\alpha_0, \alpha_1) : \mathbb{Q}(\alpha_0)] \underbrace{[\mathbb{Q}(\alpha_0) : \mathbb{Q}]}_{3}$$

Basta escludere $[\mathbb{Q}(\alpha_0,\alpha_1):\mathbb{Q}(\alpha_0)]=1$

$$\iff \mathbb{Q}(\alpha_0,\alpha_1)=\mathbb{Q}(\alpha_0)\subseteq\mathbb{R}$$

$$\mathbb{Q}(\alpha_0,\alpha_1)\not\subseteq\mathbb{R}$$

↳ sono diversi: uno è contenuto in $\mathbb{R}$, l'altro no

Quindi $[\mathbb{Q}(\alpha_0,\alpha_1):\mathbb{Q}(\alpha_0)]>1$, e dunque è

2 e si conclude.

GRADO 4: ESEMPI

- $p(x)=x^4-25=(x^2-5)(x^2+5)$

campo di spezz: $\mathbb{Q}\underset{2}{\boxed{\subseteq}}\mathbb{Q}(\sqrt{5})\underset{2}{\boxed{\subseteq}}\mathbb{Q}(\sqrt{5},\sqrt{-5})$.

ha grado 4

Domanda: $\mathbb{Q}(\sqrt{5})\subseteq\mathbb{Q}(\sqrt{5},\sqrt{-5})$ è di grado 2?

$$\iff \sqrt{-5}\notin\mathbb{Q}(\sqrt{5})$$

$$\iff \mathbb{Q}(\sqrt{-5})\neq\mathbb{Q}(\sqrt{5})$$

1° eserc.

$\iff$ $5/-5$ NON è un $\square$ in $\mathbb{Q}$, che è vero

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{5},\sqrt{-5}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{-5}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

- Sia $\alpha = \sqrt{2+\sqrt{7}} \in \mathbb{R} \subseteq \mathbb{C}$.

  * $[\mathbb{Q}(\alpha) : \mathbb{Q}]$

  * $g(x)$ = pol. min. α. Grado del campo di spezz. di $g(x)$ su $\mathbb{Q}$?

$$\alpha^2 - 2 = \sqrt{7}$$

$$(\alpha^2-2)^2 - 7 = 0$$

$$f(x) = (x^2-2)^2 - 7 \quad \text{e' t.c. } f(\alpha) = 0$$

$$= x^4 - 4x^2 - 3$$

NON HA RADICI RAZIONALI

$$y^2 - 4y - 3 = 0$$

$$y_{1,2} = \frac{4 \pm \sqrt{28}}{2} = 2 \pm \sqrt{7}$$

$$x_{1,2,3,4} = \pm \sqrt{2 \pm \sqrt{7}}$$

$$f(x) = \Big(x - \underbrace{\sqrt{2+\sqrt{7}}}_{\alpha}\Big)\Big(x + \underbrace{\sqrt{2+\sqrt{7}}}_{-\alpha_1}\Big)\Big(x - \overbrace{\sqrt{2-\sqrt{7}}}^{\alpha_2}\Big)\Big(x + \underbrace{\sqrt{2-\sqrt{7}}}_{-\alpha_3}\Big)$$

Radici: α, $\alpha_1 = -\alpha$, α_2, $\alpha_3 = -\alpha_2$

Se $f(x)$ si fattorizzasse su $\mathbb{Q}$, sarebbe prodotto di 2 fattori di grado 2

Guardando le radici in $\mathbb{C} \setminus \mathbb{R}$, l'unica fatt. possibile è

posso ottenere coeff. $\in \mathbb{R}$ solo accoppiando le radici complesse coniugate

$$\left[(x - \underset{\text{reali}}{\alpha})(x - \alpha_1) \right] \cdot \left[(x - \alpha_2)(x - \alpha_3) \right]$$

reali — complesse coniugate

che non funziona, perché il primo fattore è

$$x^2 - (2 + \sqrt{7}) \notin \mathbb{Q}[x]$$

$\boxed{\text{CONCLUSIONE}}$ $f(x)$ irrid $\Rightarrow$ è il polinomio minimo di $\alpha \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$

$\boxed{\text{Campo di spez?}}$

$$\mathbb{Q} \underset{4}{\subseteq} \mathbb{Q}(\alpha) \boxed{\subseteq} \mathbb{Q}(\alpha, \alpha_1) \boxed{\subseteq} \ldots$$

?

questi due campi sono uguali perché $\alpha_1 = -\alpha$

$$\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \alpha_2) = K$$

Siccome $[\mathbb{Q}(\alpha, \alpha_2) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\alpha_2) : \mathbb{Q}] = 4$

Sappiamo se non altro che $[K : \mathbb{Q}(\alpha)] \leq 4$

$$\alpha_2 = \sqrt{2-\sqrt{7}}$$

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha, \alpha_2) \arrow[dl, dash] \arrow[d, dash, "\leq 2"] \\
\mathbb{Q}(\alpha_2) \arrow[dr, dash, "2"'] & \mathbb{Q}(\alpha) \arrow[d, dash, "2"] \\
 & \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{7}) \arrow[d, dash] \\
 & \mathbb{Q}
\end{tikzcd}$$

$$4 \qquad 2 \qquad 4$$

$$[\mathbb{Q}(\alpha, \alpha_2) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\alpha_2) : \mathbb{Q}(\alpha^2)] = 2$$

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha, \alpha_2) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha_2) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash, "2"] \\
 & \mathbb{Q}(\alpha^2) &
\end{tikzcd}$$

Resta da capire se $[\mathbb{Q}(\alpha, \alpha_2) : \mathbb{Q}(\alpha)]$ sia 1 oppure 2. In effetti e' 2, perché

$$\mathbb{Q}(\alpha) \subseteq \mathbb{R} \quad \text{ma} \quad \mathbb{Q}(\alpha, \alpha_2) \not\subseteq \mathbb{R}$$

$\boxed{\text{CONCLUSIONE}}$ $K =$ campo di spezz. di $g(x)$

$$K = \mathbb{Q}(\alpha, \alpha_2) \qquad [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}]$$

$$= 2 \cdot 4 = 8$$

• determinare grado campo spezz. X^4+3X^2+1
(esercizio!)

Un calcolo di polinomi minimi

$\alpha \in \mathbb{C}$ radice di $\overbrace{X^4+2X^2+2}^{f(x)}$. Determinare polinomio min di α^2 e di $(\alpha+2)^{-1}$

$\boxed{\text{SOLUZIONE}}$ $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$ perché il polinomio è di Eisenstein per $p=2$

$$q(x) = X^2+2X+2 \qquad q(\alpha^2) = \alpha^4+2\alpha^2+2=0$$

e $q(x)$ è irriducibile $\left(\underset{\text{Eisenstein}}{\Delta \neq \square} \text{ in } \mathbb{Q}\right)$
e monico

Troviamo polinomio che si annulli in $1/\alpha$:

$$X^4 f\left(\frac{1}{X}\right) = \left[\left(\frac{1}{X}\right)^4 + 2\cdot\left(\frac{1}{X}\right)^2+2\right]\cdot X^4$$

$$= 2X^4+2X^2+1$$

POLINOMIO RECIPROCO

Troviamo polinomio che si annulli in $\alpha+2$:

$$\underset{\substack{\parallel \\ g(x)}}{f(X-2)} = (x-2)^4+2(x-2)^2+2$$

Troviamo polinomio che si annulli in $1/\alpha+2$:

$$x^4 g\left(\frac{1}{x}\right) = (1-2x)^4 + 2x^2(1-2x)^2 + 2x^4$$

$\boxed{\text{OSS}}$ $\mathbb{Q}\left(\frac{1}{\alpha+2}\right) = \mathbb{Q}(\alpha+2) = \mathbb{Q}(\alpha)$

$$\left[\mathbb{Q}\left(\frac{1}{\alpha+2}\right) : \mathbb{Q}\right] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$$

$\Rightarrow$ polinomio minimo di $\frac{1}{\alpha+2}$ ha grado 4

$\Rightarrow$ è $\frac{1}{26}\left[2x^4 + 2x^2(1-2x)^2 + (1-2x)^4\right]$,

ovvero $x^4 g\left(\frac{1}{x}\right)$ diviso per il coefficiente di x^4

in modo da renderlo monico