

CAMPPI (DI SPEZZAMENTO)

Note Title

12/14/2017

Estensioni quadratiche

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

$$\left[\begin{array}{l} x^2 - a \\ ax^2 + bx + c = 0 \end{array} \right. \quad \left. \begin{array}{l} (x - \sqrt{a})^2 \\ \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{array} \right]$$

stiamo dividendo per 0!

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

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

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

➡ $\sqrt{\beta} \in K(\sqrt{\alpha})$ perché $\sqrt{\beta} = \pm y \sqrt{\alpha}$

$$\sqrt{\alpha} \in K(\sqrt{\beta}) \quad \text{---} \quad \sqrt{\alpha} = \pm y \sqrt{\beta}$$

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

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

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

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

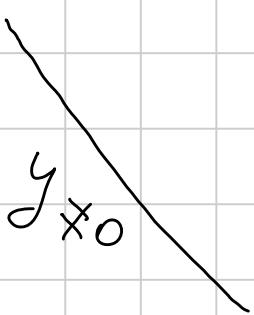
$$\sqrt{\beta} - y\sqrt{\alpha} = x \in K$$

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

$\text{char } K \neq 2$

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

$y=0 \quad \beta=x^2, \quad K(\sqrt{\beta})=K$
 $K(\sqrt{\alpha})=K(\sqrt{\beta})=K$
 $\alpha=z^2, \quad z \in K^\times$
 $\Rightarrow \beta/\alpha = (x/z)^2 = y^2$



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

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

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

$$\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{12})$$

$$12/3 = 4 = \square \in \mathbb{Q}$$

$$\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$$

$$3/2 \neq \square \in \mathbb{Q}$$

Campo di Spezzamento di $x^p - a$

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

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

Penso ricondursi al caso di $a \in \mathbb{Z}$.

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

Campo di spezz. $q(x)$
||

Campo di spezz. $q\left(\frac{x}{n}\right)$
||

Campo di spezz. $x^p/m^p - m/n$
||

Campo di spezz. $x^p - m \cdot m^{p-1}$

Diciamo $p \neq 2$. $x^p - a$ e' 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 $1 \in \mathbb{C}$

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

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

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

$$\prod_{j=1}^k \left(x - \zeta_p^{ij} \sqrt[p]{a} \right) \in \mathbb{Q}[x]$$

\Rightarrow termine noto è razionale, e in effetti

intero (lemma di Gauss)

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

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

e' possibile solo in due casi:

$$k=p \quad ①$$

$$a = \text{potenza} \quad ② \quad p\text{-esima}$$

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

$$② \Rightarrow a = b^p$$

Caso 2: $a = b^p$ C. spezz. $(x^p - b^p) =$ C. spezz. $(x^p - 1)$

$$x^p - 1 = (x-1)(1+x+\dots+x^{p-1})$$

irriducibile

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

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

= Campo di spezz. $(x^p - 1)$

DEF

$\mathbb{Q}(\zeta_m)$ è detto l'^o n -esimo campo

CICLOTOMICO

Caso 1: $x^p - a$ irriducibile

Radici: $\sqrt[p]{\alpha_0}, \zeta_p \sqrt[p]{\alpha_1}, \zeta_p^2 \sqrt[p]{\alpha_2}, \dots, \zeta_p^{p-1} \sqrt[p]{\alpha_{p-1}}$

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

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

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

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

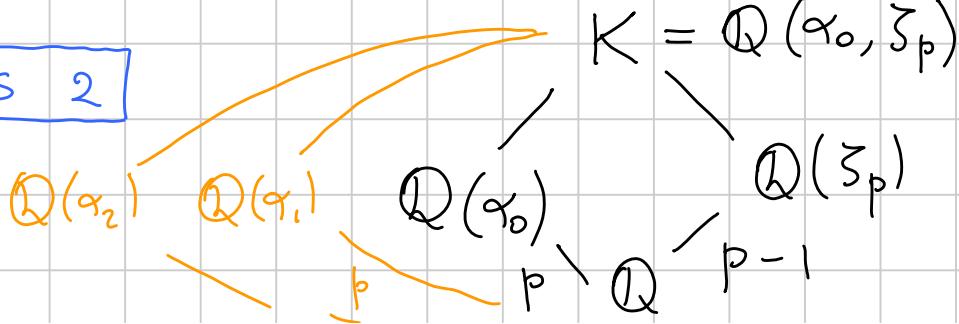
$$= \mathbb{Q}(\alpha_0, \zeta_p)$$

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

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

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

OSS 2



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

perché $(p, p-1) = 1$

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 $6 = 3!$

DIM

Chiamiamo α_0 la radice reale e

$\alpha_1, \bar{\alpha}_1$ le due complesse coniugate.

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_0) \subseteq \mathbb{Q}(\alpha_0, \alpha_1) \subseteq \mathbb{Q}(\alpha_0, \alpha_1, \bar{\alpha}_1)$$

grado 3

2

uguaglianza

(aggiungo rad. irrid. deg = 3)

Prodotto $\alpha_0 \cdot \alpha_1 \cdot \bar{\alpha}_1 = -$ termine noto di $f(x) \in \mathbb{Q}$

$$\Rightarrow \bar{\alpha}_1 = \frac{-f(0)}{\alpha_0 \cdot \alpha_1} \in \mathbb{Q}(\alpha_0, \alpha_1)$$

$$3! \geq [\mathbb{Q}(\alpha_0, \alpha_1) : \mathbb{Q}] = [\mathbb{Q}(\alpha_0, \alpha_1) : \mathbb{Q}(\alpha_0)] \underbrace{[\mathbb{Q}(\alpha_0) : \mathbb{Q}]}_3$$

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

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

\nexists I 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 "e"

2 e si conclude.

GRADO 4: ESEMPI

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

Campo di spezz: $\mathbb{Q} \stackrel{[2]}{\subseteq} \mathbb{Q}(\sqrt{5}) \stackrel{[2]}{\subseteq} \mathbb{Q}(\sqrt{5}, \sqrt{-5})$
ha grado 4

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

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

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

1° eserc.

$(\Rightarrow) \frac{5}{\sqrt{-5}}$ non è un \Box in \mathbb{Q} , che è vero

$$\begin{array}{ccc} & \mathbb{Q}(\sqrt{5}, \sqrt{-5}) & \\ \swarrow & & \searrow \\ \mathbb{Q}(\sqrt{5}) & & \mathbb{Q}(\sqrt{-5}) \\ \downarrow 2 & & \downarrow 2 \end{array}$$

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

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

* $g(x) = \text{pol. min. } \alpha$. Grado del

campo di spezz. di $g(x)$ su \mathbb{Q} ?

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

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

$$f(x) = (x^2 - 2)^2 - 7 \quad \text{e.c. } f(x) = 0$$

$$= x^4 - 4x^2 - 3 \quad \text{NON HA RADICI RAZIONALI}$$

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

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

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

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

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

$-\alpha_3$

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

$$[(x-\alpha)(x-\alpha_1)] \cdot [(x-\alpha_2)(x-\alpha_3)]$$

reali complesse coniugate

che non funziona, perché il primo fattore e'

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

CONCLUSIONE

$f(x)$ irrid \Rightarrow e' il polinomio minimo di $\alpha \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$

Campo di spez?

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \alpha_1) \subseteq \dots$$

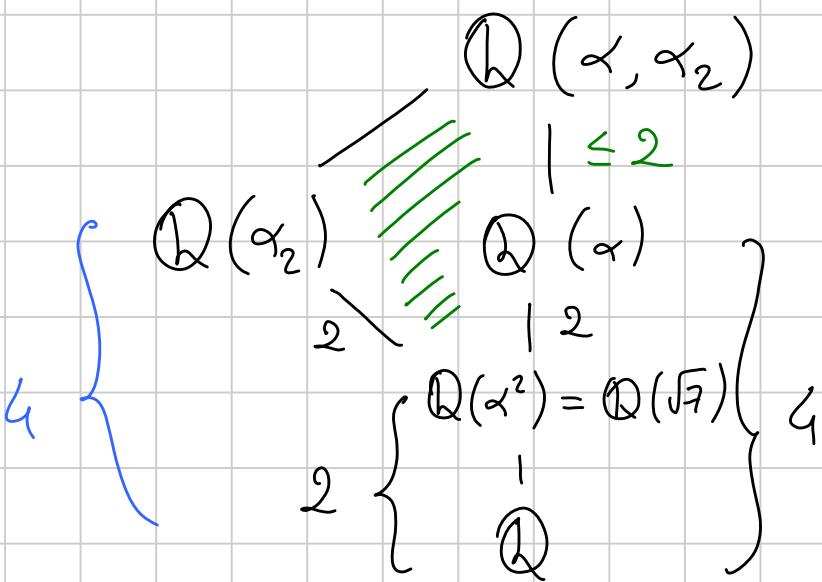
4 questi due ?

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

$$\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \alpha_1) = K$$

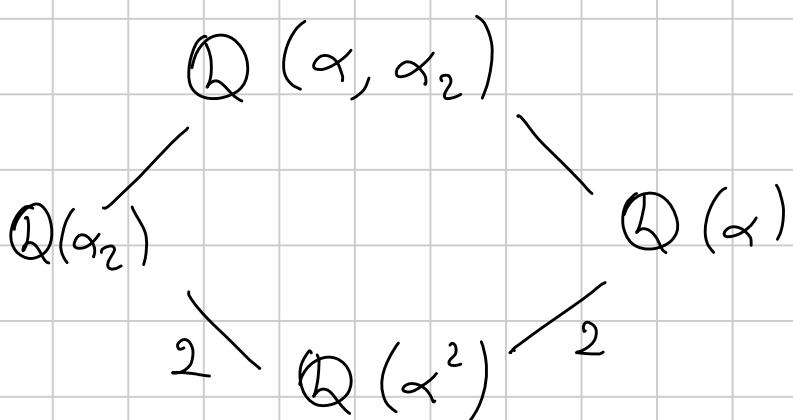
Siccome $[\mathbb{Q}(\alpha, \alpha_1) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4$

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



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

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



Resta da capire se $[Q(\alpha, \alpha_2) : Q(\alpha)]$ sia 1 oppure 2. In effetti è 2, perché

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

CONCLUSIONE

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

$$K = Q(\alpha, \alpha_2) \quad [K : Q] = [K : Q(\alpha)] [Q(\alpha) : Q]$$

$$= 2 \cdot 4 = 8$$

- determinare grado campo spezz. $x^4 + 3x^2 + 1$
(esercizio!)

Un calcolo di polinomi minimi

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

SOLUZIONE

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

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

e $q(x)$ è irriducibile ($\Delta \neq 0$ in \mathbb{Q})
Eisenstein
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 $\alpha+2$:

$$f(x-2) = (x-2)^4 + 2(x-2)^2 + 2$$

\Downarrow

$$g(x)$$

Troviamo polinomio che si annulli in $\frac{1}{\alpha+2}$:

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

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

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

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

in modo da renderlo monico