

Def $K \geq F$ ^{finita} si dice radicale se $\exists a \in K$

i) $K = F[a]$

ii) $\exists n \in \mathbb{N}$ tale che $a^n = b \in F$

ossia (in modo ambiguo) $K = F[\sqrt[n]{b}]$

Def $F = K_0 \leq K_1 \leq \dots \leq K_m = K$ $K \geq F$ si dice radicale iterata se $\forall i$ $K_i \leq K_{i+1}$ est. rad.

Def Data $f(x) \in F[x]$ si dice risolvibile per radicali se $\exists L \geq F$ radicale iterata tale $L \geq Sp_F(f(x))$

Es: $f(x) = x^2 + ax + b \in F[x]$ con $F \neq 2$

$$K = F[\sqrt{\Delta}] \quad \Delta = a^2 - 4b$$

$$r_{1,2} = \frac{-a \pm \sqrt{\Delta}}{2}$$

$m \in \mathbb{N}$ $x^m - 1 \in \mathbb{Q}[x]$ $\Phi_m(x) = \prod_{j \in \mathbb{Z}/m^*} (x - \omega^j)$ $\text{ord}(\omega) = m$

$K = \mathbb{Q}(\omega) \geq \mathbb{Q}$ è Galois $|K : \mathbb{Q}| = \varphi(m)$

$\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/m^*$ è abeliano (caso particolare

di gruppi risolubile).

Es: $m=3$ $\text{ord}(\omega) = 3$ $K = \mathbb{Q}(\omega)$ $|K : \mathbb{Q}| = 2$

$\text{min}_{\mathbb{Q}}(\omega) = x^2 + x + 1 = \phi_3(x)$ $\omega = \sqrt[3]{1}$ $1 \neq \omega$

$\omega \in \mathbb{C}$ $\text{Re}(\omega), \text{Im}(\omega)$? $K \geq \mathbb{Q}$ estensione radicale

$\exists m \in \mathbb{N}$ $a \in K$: i) $K = \mathbb{Q}[a]$ $K = \mathbb{Q}[\omega]$
ii) $a^m = b \in \mathbb{Q}$ $\omega^3 = 1$

$m = \varphi(m) = 2$ a si ottiene modificando ω .

$\lambda = -1$ $\text{ord}(\lambda) = \varphi(m) = 2$

$a = \omega + \lambda \sigma(\omega)$ dove $\langle \sigma \rangle = \text{Gal}(K/\mathbb{Q})$

$\mathbb{Z}/3^* = \langle 2 \rangle$ $\sigma(\omega) = \omega^2$

$$\sigma(a) = \omega^2 + \lambda\omega = \lambda a, \text{ infatti } \lambda a = \lambda\omega + \omega^2$$

Algebra Lineare $\sigma \in C_A(F')$ σ è F-lineare

$$\sigma(a) = \lambda a \quad a \in K \text{ autovettore di autovalore } \lambda \text{ rispetto a } \sigma$$

$$\sigma(a^2) = \sigma(a)^2 = (\lambda a)^2 = \lambda^2 a^2 = a^2 \in C_K(\langle \sigma \rangle) = \mathbb{Q}$$

$$a^2 = b \in \mathbb{Q} \quad a \notin \mathbb{Q} \quad K = \mathbb{Q}[a], \quad a^2 = b$$

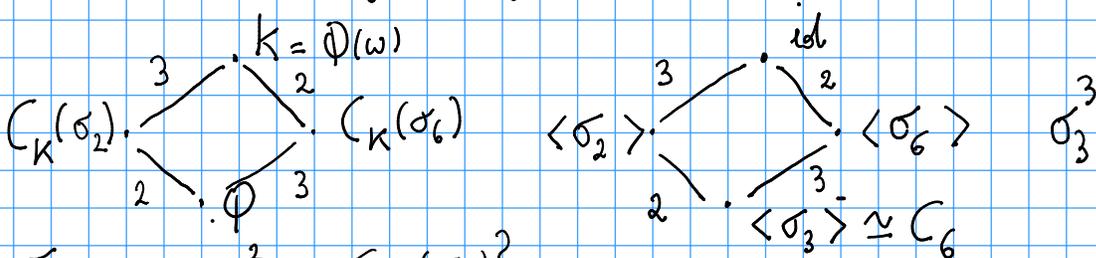
$$\omega^2 + \omega + 1 = 0; \quad a = \omega - \omega^2 \quad a^2 = \omega^2 + \omega^4 - 2\omega^3 = \omega^2 + \omega - 2$$

$$\text{ossia } a^2 = \underbrace{\omega^2 + \omega + 1}_{-3} = -3 \quad a = \sqrt{-3}$$

$$a = \omega + \omega + 1 \quad \omega = \frac{-1 \pm \sqrt{-3}}{2} = -\frac{1}{2} \pm i \frac{\sqrt{3}}{2} \quad \omega \leftrightarrow \omega^2$$

$$m=7 \quad \text{ord}(\omega) = 7 \quad \phi_7(x) = \sum_{i=0}^6 x^i \quad G = \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \simeq \mathbb{Z}/7^*$$

$$\langle 3 \rangle \quad G = \langle \sigma_3 \rangle \quad \sigma_3: \omega \mapsto \omega^3$$



$$\sigma_2: \omega \mapsto \omega^2 \quad C_K(\sigma_2)?$$

$$\eta = \omega + \omega^2 + \omega^4 \in C_K(\sigma_2) \quad \sigma_3(\eta) = \omega^3 + \omega^6 + \omega^5 \neq \eta$$

$$\text{altri menti: } 1 + \omega + \omega^3 - \omega^2 - \omega^5 - \omega^4 = 0 \text{ ossia}$$

ω annullerebbe polinomio di grado 5

$$\text{min}_{\mathbb{Q}}(\eta)? \quad \text{min}_{\mathbb{Q}}(\eta) = \prod_{\beta \in \eta^G} (x - \beta)$$

$$\text{dove } \eta^G = \{ \gamma(\eta) : \gamma \in G \} \quad |\eta^G| = |G : C_G(\eta)| = 2$$

$$(x - \eta)(x - \sigma_3(\eta)) = x^2 - (\eta + \sigma_3(\eta))x + \eta\sigma_3(\eta)$$

$$\eta + \sigma_3(\eta) = \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = -1$$

$$2 = \eta\sigma_3(\eta) \xrightarrow{\text{exp}} \underline{4}, \underline{0}, \underline{6}, \underline{5}, \underline{1}, \underline{0}, \underline{0}, \underline{3}, \underline{2}$$

$$x^2 + x + 2 \quad \frac{-1 \pm \sqrt{-7}}{2} \quad C_K(\sigma_2) = \mathbb{Q}[\sqrt{-7}] = \mathbb{Q}[\eta]$$

Ex

$$K \quad \exists a \in K$$

$$L = \mathbb{Q}[\sqrt{-7}]$$

$$i) K = L[a]$$

L

$$ii) a^3 \in L$$

$$\text{Se } a^3 = b \in L \quad \min_L(a) = x^3 - b$$

Sia a' altra radice di $x^3 - b$ $a' \in K$ K/\mathbb{Q} normale

$$a'/a = \lambda? \quad (a'/a)^3 = \frac{(a')^3}{a^3} = \frac{b}{b} = 1 = \lambda^3 \quad \lambda \neq 1 \quad \text{ord}(\lambda) = 3$$

quindi $\lambda \in K$ Assomb Infatti se $\lambda \in K$

$$\text{ord}(\omega) = 7, \text{ord}(\lambda) = 3 \quad \omega, \lambda \in K \quad \omega\lambda \in K$$

e ha ordine 21 $\mathbb{Q}(\omega\lambda) \subseteq K$

$$12 = \varphi(21) \quad | \quad | 6 \text{ Assomb}$$

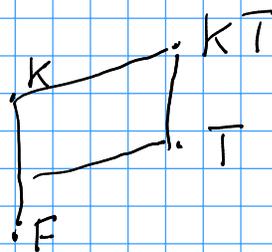
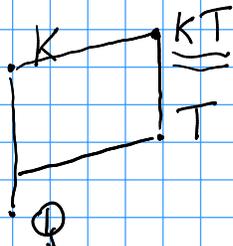
$$\mathbb{Q} \quad \mathbb{Q}$$

Il motivo per cui non ottengo a ; $a \in L$

è la mancanza di radici di ordine $|K:L|$

Aggiungo a K le radici cubiche unità $T = \mathbb{Q}(\lambda)$

$$\text{ord}(\lambda) = 3$$



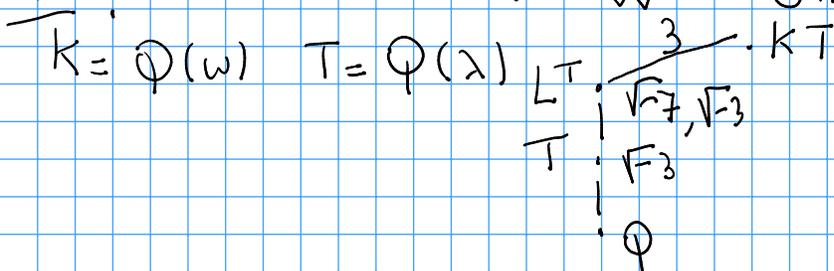
Teor: (Aggiunzione delle razionalità)

$$K \supseteq F \text{ finita Galois}, F \subseteq T$$

$$i) KT \supseteq T \text{ è di Galois}$$

$$ii) \text{Gal}(KT/T) \cong \text{Gal}(K/K \cap T) \subseteq \text{Gal}(K/F)$$

$$\left(KT/T \cong K/K \cap T \right) \quad \left(\frac{U+W}{W} \cong \frac{U}{U \cap W} \right)$$



KT/T Galois KT/LT Galois ha grado 3 K/L

$KT \ni a$ tale che $i) KT = LT[a]$

ii) $a^3 = b \in LT$

$\beta \in C_K(\sigma_6)$ $\beta = \omega + \omega^6$ ha grado 3 su \mathbb{Q} .

Notate che β^G ha 3 coniugati $\beta, \sigma_2(\beta), \sigma_3(\beta)$

$\tau = \sigma_3$ $\beta, \tau(\beta), \tau^2(\beta)$ τ si estende a KT

$\tau(\lambda) = \lambda$

$a = \beta + \lambda \tau(\beta) + \lambda^2 \tau^2(\beta)$

$\tau(a) = \tau(\beta) + \lambda \tau^2(\beta) + \lambda^2 \beta = \lambda^2 a$

$\tau(a^3) = a^3 \in C_{KT}(\tau) = LT$

M_{AGMA} $a^3 = 21\lambda + 14$ $a = \sqrt[3]{21\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) + 14}$

$\mathbb{Q}(a, \sqrt{-7}, \sqrt{-3}) \ni \omega$