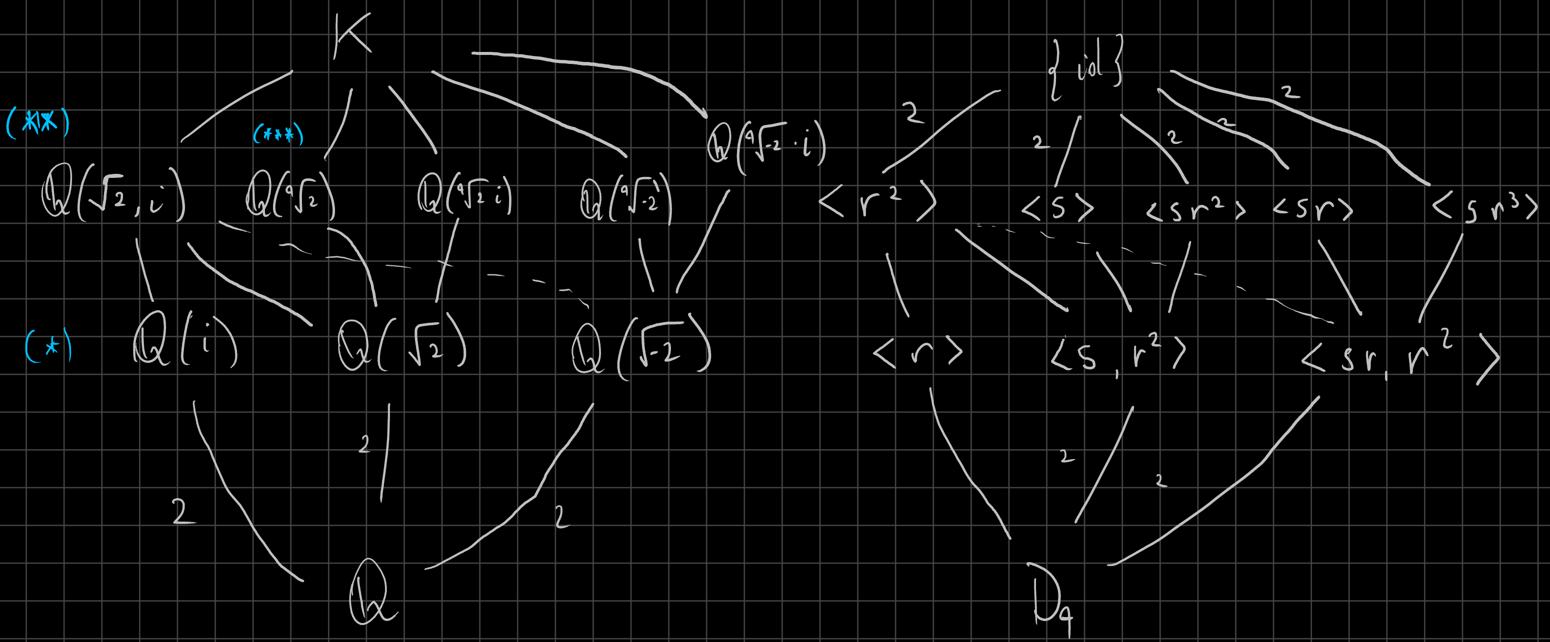
LEZIONE 9 - 12 - 20

$$K = \mathbb{Q}(\sqrt[4]{2}, i) \rightsquigarrow Gal(K/\mathbb{Q}) \simeq D_4$$

$$r = \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2}\, i \\ i \mapsto i \end{cases} \qquad s := \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{cases} \sim \text{coniugio complesso}$$



OSS: se $H < D_4$ con $|H| = 4 \iff [D_4 : H] = 2 \iff H$ contiene l'insieme dei quadrati $\{g^2 : g \in D_4\} = \{e, r^2\} = \langle r^2 \rangle$

Allora

$$\{\text{sgp. di } D_4 \text{ di indice } 2\} \longleftrightarrow \{\text{sgp. di } \tfrac{D_4}{\langle r^2 \rangle} \text{ di indice } 2\}$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$\{\text{sgp di } D_4 \text{ contenenti i quadrati} = \langle r^2 \rangle\} \qquad \{\text{sgp di } (\mathbb{Z}/2\mathbb{Z})^2 \text{ di indice } 2\}$$

↳ stesso ragion. per i quadrati $\Rightarrow$ ogni quadrato fa l'id. ed è un gruppo con 4 el $\Rightarrow (\mathbb{Z}/2\mathbb{Z})^2$

(*) gruppi / est. di indice/grado 2

$$\{\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{-2})\}$$

$$\updownarrow \qquad \updownarrow \qquad \updownarrow$$

$$\{\langle r \rangle,\ \langle s, r^2 \rangle,\ \langle sr, r^2 \rangle\}$$

Siccome r fissa i si ha che $\mathbb{Q}(i) \longleftrightarrow \langle r \rangle$

Consideriamo ora $\langle s, r^2 \rangle$: s NON fissa i $\Rightarrow$ non fissa $\underset{i\sqrt{2}}{\overset{\|}{\sqrt{-2}}}$

$\Rightarrow \langle s, r^2 \rangle \longleftrightarrow \mathbb{Q}(\sqrt{2})$

Infine $\langle sr, r^2 \rangle \longleftrightarrow \mathbb{Q}(\sqrt{-2})$

ALTRO MODO : $\langle s, r^2 \rangle$:

$$r^2 = \begin{cases} \sqrt[4]{2} \overset{r}{\longmapsto} \sqrt[4]{2}\, i \overset{r}{\longmapsto} -\sqrt[4]{2} \\ i \longmapsto i \end{cases}$$

Ma allora $r^2(\sqrt{2}) = r^2((\sqrt[4]{2})^2) = r^2(\sqrt[4]{2})^2 = (-\sqrt[4]{2})^2 = \sqrt{2}$

Però allo stesso modo $r^2(\sqrt{-2}) = \sqrt{-2}$:(

$s(\sqrt{2}) = s(\sqrt[4]{2})^2 = \sqrt{2}$ ✓

$s(\sqrt{-2}) = s(i) \cdot s(\sqrt{2}) = -i\sqrt{2} = -\sqrt{-2}$ NO PE

$\langle r^2, s \rangle \longleftrightarrow \mathbb{Q}(\sqrt{2})$, $\langle r^2, sr \rangle \longleftrightarrow \mathbb{Q}(\sqrt{-2})$

(**) Oss. che $\langle r^2 \rangle \subseteq \langle r \rangle, \langle s, r^2 \rangle, \langle sr, r^2 \rangle$

Per la corr. di Galois segue che

$$K^{\langle r^2 \rangle} \supseteq \underset{\mathbb{Q}(i)}{\overset{\|}{K^{\langle r \rangle}}}, \underset{\mathbb{Q}(\sqrt{2})}{\overset{\|}{K^{\langle s, r^2 \rangle}}}, \underset{\mathbb{Q}(\sqrt{-2})}{\overset{\|}{K^{\langle sr, r^2 \rangle}}}$$

$$\Rightarrow K^{\langle r^2 \rangle} = \mathbb{Q}(i, \sqrt{2})$$

ALTRO MODO: r^2 fissa $\sqrt{2}$ (visto sopra) e i (perché r fissa i)

(***) $\mathbb{Q}(\sqrt[4]{2}) \subseteq K^{\langle s \rangle}$ poiché s fissa $\sqrt[4]{2}$

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[4]{2}) & & K^{\langle s \rangle} \\ \Big|\, 4 & & \Big|\, 4 = [D_4 : \langle s \rangle] \\ \mathbb{Q} & & \mathbb{Q} \end{array} \Rightarrow \mathbb{Q}(\sqrt[4]{2}) = K^{\langle s \rangle}$$

OSS : la domanda originaria era scoprire le sottoest. di $\mathbb{Q}(\sqrt[4]{2}) = K^{\langle s \rangle}$

Ma l'unico sgrp. di D_4 contenente $\langle s \rangle$ è $\langle s, r^2 \rangle$

$\Rightarrow$ l'unica sottoest. è $K^{\langle s, r^2 \rangle} = \mathbb{Q}(\sqrt{2})$ ∎

Mancano $K^{\langle sr \rangle}$, $K^{\langle sr^2 \rangle}$, $K^{\langle sr^3 \rangle}$

$$sr = \begin{cases} \sqrt[4]{2} \xmapsto{r} \sqrt[4]{2}\, i \xmapsto{s} -\sqrt[4]{2} \cdot i \\ i \xmapsto{r} i \xmapsto{s} -i \end{cases}$$

Come costruisco un el. fissato da sr?

OSS UTILE IN GENERALE

Dato $\alpha \in K$, $\beta := \alpha + (sr)(\alpha)$ è fissato da sr

$\Rightarrow (sr)(\beta) = (sr)(\alpha) + (sr)^2(\alpha) = (sr)(\alpha) + \alpha$ ✓

Scegliendo $\alpha = i$ mi va male: $i + sr(i) = i - i = 0$ e vabbè

$\alpha = \sqrt[4]{2}$: $\sqrt[4]{2} + sr(\sqrt[4]{2}) = \sqrt[4]{2} - i\sqrt[4]{2}$

$= \sqrt[4]{2}(1-i) =: \beta$

Allora $\beta^4 = 2 \cdot (1-i)^4 = 2 \cdot (\cancel{1} + \cancel{(-1)} - 2i)^2 = -8$

$\Rightarrow \beta^4 + 8 = 0 \Rightarrow \beta$ è radice di $x^4 + 8 = 0$

È irriducibile? Siamo su $\mathbb{Q}$: $\left(\frac{x}{2}\right)^4 + \frac{1}{2} = 0$

$\Rightarrow$ il campo ottenuto aggiungendo β è come aggiungere $\sqrt[4]{-\frac{1}{2}}$

$$\mathbb{Q}(\sqrt[4]{-8}) = \mathbb{Q}\left(\sqrt[4]{-\tfrac{1}{2}}\right) = \mathbb{Q}(\sqrt[4]{-2})$$

$x^4 + 2 \Rightarrow$ irr. per Eisenstein

$\Rightarrow K^{\langle sr \rangle} = \mathbb{Q}(\sqrt[4]{-2})$

Ora $K^{\langle sr^2 \rangle}$:

$$sr^2 = \begin{cases} \sqrt[4]{2} \xmapsto{r} \sqrt[4]{2}\, i \xmapsto{r} -\sqrt[4]{2} \xmapsto{s} -\sqrt[4]{2} \\ i \xmapsto{r^2} i \xmapsto{s} -i \end{cases}$$

Evidentemente $\sqrt[4]{2}\,i \xmapsto{sr^2} \sqrt[4]{2}\,i \Rightarrow K^{\langle sr^2\rangle} = \mathbb{Q}(\sqrt[4]{2}\,i)$

Ora $K^{\langle sr^3\rangle}$:

Prendo $\gamma := sr^3(\sqrt[4]{2}) + \sqrt[4]{2} = \sqrt[4]{2}\cdot i + \sqrt[4]{2} = \sqrt[4]{2}\,(i+1)$

$$\sqrt[4]{2} \xmapsto{r^2} -\sqrt[4]{2} \xmapsto{r} -\sqrt[4]{2}\cdot i \xmapsto{s} \sqrt[4]{2}\,i$$

Oss: $\gamma^4 = 2\,(i+1)^4 = 2\cdot\left((\cancel{-1}) + \cancel{1} + 2i\right)^2 = -8$

$\Rightarrow$ ha grado 4 su $\mathbb{Q}$! ???

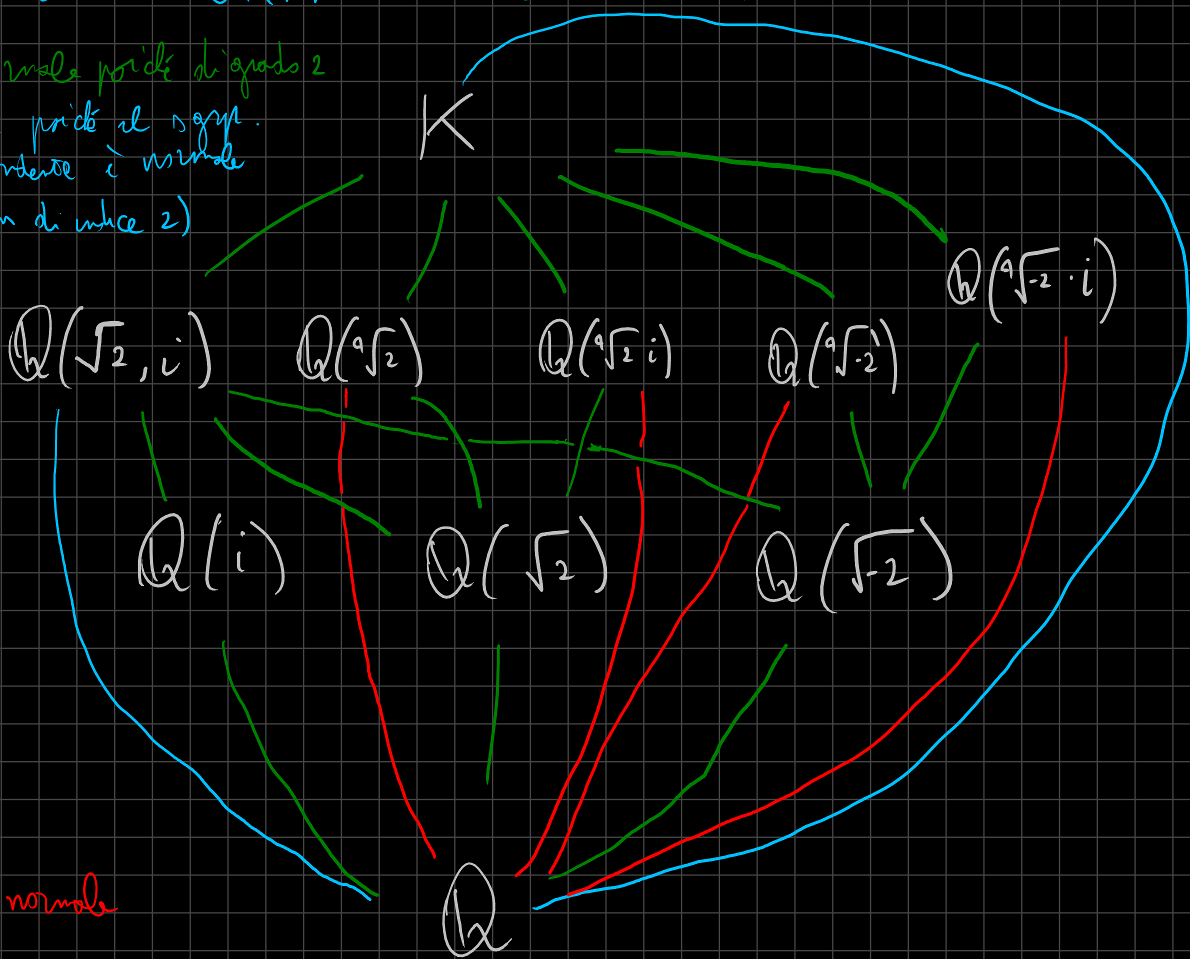
OSS: $\sqrt[4]{2}, \sqrt[4]{-2} \in K \Rightarrow \sqrt[4]{\frac{2}{-2}} = \sqrt[4]{-1} \in K$

Infatti una radice 4ª di -1 è una radice 8ª dell'unità, e una tale radice è $\frac{1+i}{\sqrt{2}}$

SOTTOEST NORMALI NEL DIAGRAMMA

VERDE: normale poiché di grado 2

BLU: normale poiché il sottogr. corrispondente è normale (ma non di indice 2)



ROSSO: non normale

$\mathbb{C}(t^7 + t^{-7}) \subseteq \mathbb{C}(t)$

$u := t^7 + t^{-7}$. Polinomio minimo di t su $\mathbb{C}(u)$ è

$$u t^7 = t^{14} + 1 \rightsquigarrow x^{14} - u x^7 + 1$$

È minimo poiché è irriducibile, poiché nella variabile u ha grado 1

$$u(-x^7) + (x^{14}+1) = a(x) \cdot \big(b(x) \cdot u + c(x) \big)$$

$\hookrightarrow$ unica fatt. possibile
pol. in x $\cdot$ pol di grado 1 in u

$\Rightarrow a(x) \mid x^7 \wedge a(x) \mid x^{14}+1$

$\Rightarrow a(x) \mid (x^7, x^{14}+1) = 1 \Rightarrow a$ è invertibile

$\Rightarrow$ è irriducibile $\Rightarrow \mathbb{C}(t) / \mathbb{C}(u)$ ha grado 14.

(*) È Galois: vediamo che è il CDS su $\mathbb{C}(u)$ di

$$\mu(x) := x^{14} - u x^7 + 1$$

Una è t. Altre sei sono $t\zeta_7^i$ per $i=1, \dots, 6$

Infatti:

$$(t\zeta_7^i)^{14} - u(t\zeta_7^i)^7 + 1 = t^{14} - u t^7 + 1 = 0$$

L'altra metà? Questo polinomio è SIMMETRICO: quindi se α è radice lo è anche α^{-1}

$$\mu\left(\tfrac{1}{t}\right) = \frac{1}{t^{14}} - \frac{u}{t^7} + 1 = \frac{1}{t^{14}}\left(t^{14} - u t^7 + 1\right) = 0$$

$\Rightarrow$ Radici di $\mu(x) = \{ t \cdot \zeta_7^i, \ t^{-1} \zeta_7^i, \ i = 0, \dots, 6 \} \subseteq \mathbb{C}(t)$

$\Rightarrow \mathbb{C}(t)$ è cds di $\mu(x)$ su $\mathbb{C}(u) \Rightarrow$ Galois

$G := \mathrm{Gal}(\mathbb{C}(t) / \mathbb{C}(t))$, $\# G = 14$.

$\Rightarrow G \simeq \mathbb{Z}/_{14}\mathbb{Z}$ oppure D_7

Automorfismi ovvi:

① $\sigma_1 = t \longmapsto t\zeta_7$

$$\begin{tikzcd}
\mathbb{C}(t) = \mathbb{C}(u)(t) \arrow[rr, "\sim"] \arrow[dr, dash] & & \mathbb{C}(u)(\zeta_7 t) = \mathbb{C}(t) \arrow[dl, dash] \\
& \mathbb{C}(u) &
\end{tikzcd}$$

$\sigma_1 : \mathbb{C}(t) \longrightarrow \mathbb{C}(t)$ fissa $u = t^7 + t^{-7}$

$f(t) \longmapsto f(t\zeta_7)$ $\Rightarrow u(t\zeta_7) = (t\zeta_7)^7 + (t\zeta_7)^{-7}$

$= t^7 + t^{-7}$ ✓

$\mathrm{ord}\, \sigma_1 = 7$

② $\sigma_2 : \mathbb{C}(t) \longrightarrow \mathbb{C}(t)$

$t \longmapsto t^{-1}$

In effetti $\sigma_2 \in \mathrm{Gal}(\mathbb{C}(t) / \mathbb{C}(u))$ perché

$$\sigma_2(u) = \sigma_2(t^7 + t^{-7}) = t^{-7} + t^7 \quad ✓$$

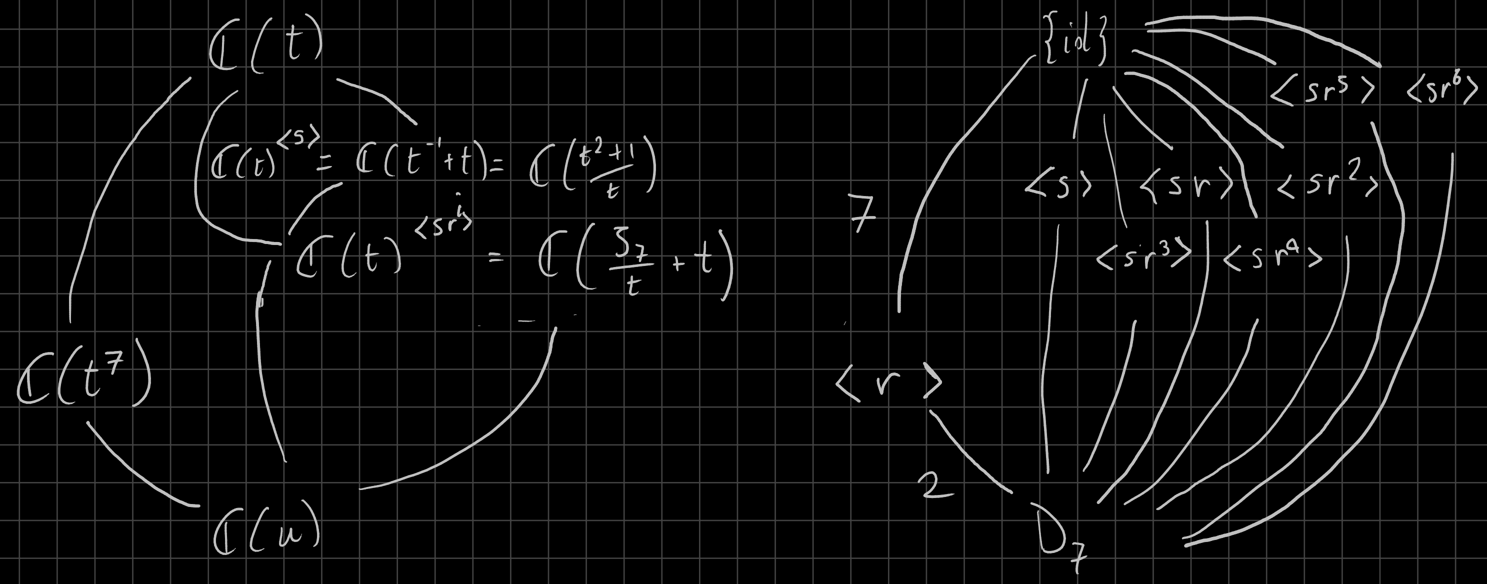
$\mathrm{ord}\, \sigma_2 = 2$

Osserviamo inoltre che $\sigma_2 \sigma_1 (t) = \sigma_2(t\zeta_7) = \zeta_7 t^{-1}$

$\sigma_1 \sigma_2 (t) = \sigma_1(t^{-1}) = (t\zeta_7)^{-1} = \zeta_7^{-1} t^{-1}$

$\Rightarrow$ Il gruppo $G \simeq D_7$

Studiamo il reticolo di sottoestensioni di $\mathbb{C}(t)/\mathbb{C}(u)$



dove $r := \sigma_1$, $s := \sigma_2$

$r = t \mapsto t\zeta_7$, dunque $r(t^7) = (t\zeta_7)^7 = t^7$

Sicuramente quindi $\mathbb{C}(t^7) \subseteq \mathbb{C}(t)^{\langle r\rangle}$

Sostengo che $\mathbb{C}(t^7) = \mathbb{C}(t)^{\langle r\rangle}$: per un OSS vista nella lezione del 25-11-20 il grado di

$$\begin{array}{c}\mathbb{C}(t)\\ |\\ \mathbb{C}\left(\frac{p(t)}{q(t)}\right)\end{array} \quad \text{è} \quad \left[\mathbb{C}(t) : \mathbb{C}\left(\frac{p(t)}{q(t)}\right)\right] = \max\{\deg p, \deg q\}$$

Dunque $[\mathbb{C}(t) : \mathbb{C}(t^7)] = 7$, ma per Corrispondenza c'è una sola sottoest. di $\mathbb{C}(t)/\mathbb{C}(u)$ il cui grado è 7 e quindi deve essere questa

- Ora, $\mathbb{C}(t)^{\langle s\rangle}$? Strategia di prima :

$$\beta := s(t) + t = t + t^{-1} \quad (\text{ha grado } 2 \text{ ! YEE})$$

- Ultimo : $\mathbb{C}(t)^{\langle sr^i\rangle}$?

$$\gamma := sr^i(t) + t = s(t\zeta_7^i) + t = \frac{\zeta_7^i}{t} + t$$

Estensione di $\mathbb{Q}$ con gruppo $\mathbb{Z}/3\mathbb{Z}$

Consideriamo

$$\begin{tikzcd}[column sep=small]
& \mathbb{Q}(\zeta_7) \arrow[dl, dash, "2"'] \arrow[dd, dash] \\
\mathbb{Q}(\zeta_7)^H = F \arrow[dr, dash, "3"'] & \\
& \mathbb{Q}
\end{tikzcd}$$

$\mathrm{Gal} \simeq (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z} \Rightarrow$ contiene un'ext di grado 2 e una di grado 2

$j \mapsto (\zeta_7 \mapsto \zeta_7^j)$

dove $H < (\mathbb{Z}/7\mathbb{Z})^\times$ di ordine 2

$H = \langle -1 \rangle \longrightarrow$ meglio: $H = \langle (\zeta_7 \mapsto \zeta_7^{-1}) \rangle < \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$

OSS: $\zeta_7 \mapsto \zeta_7^{-1}$ coincide con (la restrizione del coniugio complesso)

$\Rightarrow$ il campo fisso è $\subseteq \mathbb{R}$ $\Rightarrow$ $\mathbb{Q}(\zeta_7)^H = \mathbb{Q}(\zeta_7) \cap \mathbb{R}$

Un el. fisso è $(\zeta_7 \mapsto \zeta_7^{-1})(\zeta_7) + \zeta_7 = \zeta_7^{-1} + \zeta_7 =: \alpha$.

Sicuramente

$$\begin{tikzcd}
\mathbb{Q}(\zeta_7) \arrow[d, dash, "2"'] \\
\mathbb{Q}(\zeta_7)^H \arrow[d, dash] \\
\mathbb{Q}(\alpha) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

2? $\Rightarrow$ Sì: cerco il pol. minimo di ζ_7 su $\mathbb{Q}(\alpha)$.

$$\alpha = \zeta_7 + \zeta_7^{-1} \iff \zeta_7 \alpha = \zeta_7^2 + 1$$

$$\iff \mu(x) := x^2 - \alpha x + 1$$

si annulla in ζ_7

dunque il grado del pol. minimo ≤ 2!

Segue quindi che $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(\alpha)] \leq 2$

Ma $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(\alpha)] \geq [\mathbb{Q}(\zeta_7) : \mathbb{Q}(\zeta_7)^H] = 2$

dunque il grado è eff. 2 e $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_7)$.

(*) $\mathbb{Q}(\alpha)/\mathbb{Q}$ è normale? sì: $Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ è abeliano $\Rightarrow$ ogni sottogr. è normale

$$\Rightarrow Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq \frac{Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})}{H} \simeq \mathbb{Z}/_{3}\mathbb{Z}$$

(*) Pol minimo di α su $\mathbb{Q}$?

$$\deg \text{pol minimo} = [\mathbb{Q}(\alpha):\mathbb{Q}] = 3$$

Come lo troviamo?

$$\zeta_7^6 + \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2 + \zeta_7 + 1 = 0$$

$$\zeta_7^3 + \zeta_7^2 + \zeta_7 + 1 + \frac{1}{\zeta_7} + \frac{1}{\zeta_7^2} + \frac{1}{\zeta_7^3} = 0 \quad ; \quad \alpha = \zeta_7 + \zeta_7^{-1}$$

$$\Rightarrow \alpha^3 = \zeta_7^3 + \zeta_7^{-3} + 3(\zeta_7 + \zeta_7^{-1})$$

$$\alpha^2 = \zeta_7^2 + \zeta_7^{-2} + 2$$

$$\Rightarrow \alpha^3 + \alpha^2 - 2\alpha - 1 = 0$$

$\Rightarrow q = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ ha α come radice, è monico ed è del grado giusto $\Rightarrow$ YEE

Metodo più sistematico

Le altre radici di α stanno in $\mathbb{Q}(\zeta_7)$ e le posso ottenere tramite azioni di gruppi di Galois

Infatti: esiste sicuramente un'isom. di campi

$$\mathbb{Q}(\alpha) \xrightarrow{\sim} \mathbb{Q}(\alpha')$$

che porta $\alpha \mapsto \alpha'$ (radici del pol. minimo di α). Dato che $\mathbb{Q}(\alpha)/\mathbb{Q}$ è normale tale im. è un automorfismo $(\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha'))$

Ma $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \twoheadleftarrow Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})$

quindi le altre radici sono della forma $\sigma(\alpha)$ con $\sigma \in Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})$

⌈ Equiv: è la proprietà di estensione delle immersioni di campo ⌋

$$\sigma_2 \doteq \zeta_7 \longmapsto \zeta_7^2 \Rightarrow \sigma_2(\alpha) = \zeta_7^2 + \zeta_7^{-2}$$

$$\sigma_3 = \zeta_7 \longmapsto \zeta_7^3 \Rightarrow \sigma_3(\alpha) = \zeta_7^3 + \zeta_7^{-3}$$

$$\sigma_4(\alpha) = \zeta_7^4 + \zeta_7^{-4} = \zeta_7^{-3} + \zeta_7^{+3}$$

$$\sigma_5(\alpha) = \zeta_7^5 + \zeta_7^{-5} = \zeta_7^{-2} + \zeta_7^{+3}$$

$$\sigma_6(\alpha) = \sigma_{-1}(\alpha) = \zeta_7^{-1} + \zeta_7^{1}$$

OSS: $$Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q}) / \underset{\langle \sigma_{-1} \rangle}{\overset{\shortparallel}{H}} \simeq Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$$

Siccome ad es. $\sigma_5 = (\zeta_7 \mapsto \zeta_7^5 = \zeta_7^{-2}) = \sigma_{-1}\sigma_2$

segue che questi due elementi sono uguali nel quoziente

$Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \Rightarrow$ mandano α nello stesso coniugato

Stessa cosa $\sigma_4 \sim \sigma_3$

Quindi $$\mu_\alpha(x) = \left(x - (\zeta_7^{-1} + \zeta_7)\right)\left(x - (\zeta_7^{-2} + \zeta_7^{2})\right)\left(x - (\zeta_7^{-3} + \zeta_7^{3})\right)$$

Facendo i calcoli si arriva al polinomio (che mia però)

ES CON I CAMPI FINITI

$$\begin{array}{cc} & \mathbb{F}_8 \\ Gal & | \\ \shortparallel & \\ \mathbb{Z}/3\mathbb{Z} & \mathbb{F}_2 \\ \shortparallel & \\ \langle x \mapsto x^2 \rangle & \\ \text{Frobenius} & \end{array}$$

$f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ e sia $\alpha \in \mathbb{F}_{2^3}$ una radice di $f(x)$. Chi sono le altre?

La fattorizzazione di f in $\mathbb{F}_2[x]$ è

$$f(x) = (x - \alpha)(x - \underset{(x\mapsto x^2)(\alpha)}{\overset{\shortparallel}{\alpha^2}})(x - \underset{(x\mapsto x^2)^2(\alpha)}{\overset{\shortparallel}{\alpha^4}})$$

$f \in \mathbb{Q}[x]$ di grado p primo, $p-2$ radici reali

Supponiamo f irriducibile. Det. il Gal di $f(x)$. $=: G$

Sia $K = \mathrm{cds}(f)$.

$$\begin{array}{l} K = \mathbb{Q}(\alpha_1, \dots, \alpha_n) \\ \Big| \qquad \mathbb{Q}(\alpha_1) \\ \mathbb{Q} \diagup p \quad (f \text{ irriducibile}) \end{array}$$

(*) $G \hookrightarrow S_p$

(*) $\# G = [K:\mathbb{Q}] \mid p$

Dal teorema di Cauchy, G contiene un el. di ordine $p \Rightarrow$ un p-ciclo. σ

Sia $\tau : \mathbb{C} \to \mathbb{C}$ il coniugio complesso. $\tau|_K$ ha senso, poiché $\{\alpha_1, \dots, \alpha_p\}$ è stabile per l'azione di τ, e inoltre fissa $\mathbb{Q}$

$\Rightarrow \tau|_K \in \mathrm{Gal}(K/\mathbb{Q})$

Se WLOG α_1 e α_2 sono le due radici complesse coniugate allora $\tau|_K$ (come el. di S_p) è $(1,2)$

$\Rightarrow \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_p$ e $(1,2), \underbrace{\sigma}_{p\text{-ciclo}} \in \mathrm{Gal}(K/\mathbb{Q})$

Ma $\langle 2\text{-ciclo}, p\text{-ciclo} \rangle = S_p$

$\Rightarrow \mathrm{Gal}(K/\mathbb{Q}) \cong S_p$ ∎