Lezione 7-12-20

Traslato di un'estensione

$$\begin{tikzcd}[column sep=small] & KL \arrow[dl, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash, "\text{Galois}"'] & & L \arrow[dl, dash, "\text{qualsiasi (finita)}"] \\ & F & \end{tikzcd}$$

Risultato: KL/L è di Galois

e $\mathrm{Gal}(KL/L) \simeq \mathrm{Gal}(K/L\cap K)$

che è un sottogruppo di $\mathrm{Gal}(K/F)$

Dim K/F è il c.d.s di un polinomio separabile a coeff. in F.

[Perché un polinomio? Perché siccome il grado dell'est è finito sicuramente mi basta un n° finito di polinomi $\Rightarrow$ mi basta il loro prodotto]

Sia $p \in F[x]$ tale pol. Se $\alpha_1, \dots, \alpha_n$ sono le radici (in $\bar{F}$) di p, allora $K = F(\alpha_1, \dots, \alpha_n)$.

Ma allora $KL = L(\alpha_1, \dots, \alpha_n)$ è il cds di p su L, e quindi KL/L è normale.

Consideriamo ora

$$\mathrm{Res}: \mathrm{Gal}(KL/L) \longrightarrow \mathrm{Gal}(K/F)$$
$$\sigma \longmapsto \sigma|_K$$

Tale mappa (*) ha senso poiché $\sigma \in \mathrm{Gal}(KL/L)$ è un automorfismo

$$\sigma : KL \hookrightarrow KL \subseteq \bar{L} = \bar{F}$$

dunque la sua restrizione a K è

$$\sigma|_K : K \hookrightarrow \bar{F}$$

Ma K/F è normale, dunque $\sigma|_K(K) \subseteq K$ e quindi è un automorfismo di K.

Inoltre $\sigma|_L = id \Rightarrow \sigma|_F = id$, e quindi

$$\sigma \in Gal(K/F)$$

(*) è un omomorfismo

$$Res(\sigma \circ \tau) = \sigma \circ \tau|_K = \sigma|_K \circ \tau|_K = Res\,\sigma \circ Res\,\tau$$

(*) è iniettivo

$$Res(\sigma) = id_K \Rightarrow \sigma|_K = id \quad e \quad \sigma|_L = id$$

Quindi F^σ è un campo che contiene K e L, quindi contiene almeno KL

Dunque $\sigma|_{KL} = \sigma = id$, cioè Res è iniettivo.

(*) Siccome σ fissa L, $\sigma|_K$ fissa $\underline{K \cap L}$

gli el. di L che sono ancora nel dominio di σ

$$\Rightarrow Im\,Res \subseteq \{\tau \in Gal(K/F) \text{ tale che } \tau|_{K\cap L} = id\}$$

$$= Gal(K/K\cap L)$$

Viceversa, dato $\tau \in Gal(K/K\cap L)$ voglio dire che $\exists\, \sigma \in Gal(KL/L)$ tale che $Res\,\sigma = \sigma|_K = \tau$.

$$\begin{tikzcd} KL \arrow[dr, hook, "\sigma"] & \\ K \arrow[u, phantom, "\cup" rotate=90] \arrow[r, hook, "\tau"] & \bar{F} \end{tikzcd}$$

Siccome KL/L è finita, esistono tante ext quanto il grado

CAVEAT: non è detto che ce ne sia una che sia l'identità su L

L'unica cosa che so è che sono l'id. su $K \cap L$

(*) A mano: $K = F(\alpha_1, \dots, \alpha_n) = F(\alpha)$

teorema dell'El Primitivo

e sia $f(t) := \prod_{\sigma \in Gal(KL/L)} (t - \sigma(\alpha))$

Questo pol. è invariante per l'azione di $Gal(KL/L)$, dunque i suoi coefficienti sono in

se applico un $\sigma' \in Gal$ al polinomio ottengo lo stesso polinomio

$$Fix(Gal(KL/L)) = L$$

D'altro canto $f \in K[t]$: infatti $\alpha \in K = F(\alpha)$ e essendo K/F normale segue che tutti i suoi coniugati $\sigma(\alpha)$ sono in K.

Segue che $f \in K \cap L[t]$. Dunque

$$\begin{tikzcd} & KL \arrow[dl, dash] \arrow[dr, dash, "\leq m"] & \\ K \arrow[dr, dash, "m"'] & & L \arrow[dl, dash] \\ & K \cap L \arrow[d, dash] & \\ & F & \end{tikzcd}$$

$$\deg f = \# Gal(KL/L) = [KL : L] \leq [K : K \cap L]$$

D'altro canto α è radice di $f(t)$, quindi f è divisibile per il pol. minimo di α su $K \cap L$

Ma $(K \cap L)(\alpha) = K$, dunque il pol. minimo di α su $K \cap L$ ha grado $[K : K \cap L]$. Segue che

$$[K : K \cap L] \leq \deg f \leq [K : K \cap L]$$

$$\implies \deg f = \# Gal(KL/L) = [K : K \cap L]$$

Ma dato che $\begin{tikzcd} K \arrow[d, dash, "\Rightarrow \text{Galois}"] \arrow[dd, dash, bend right, "\text{Galois}"'] \\ K \cap L \arrow[d, dash] \\ F \end{tikzcd}$ segue che $[K : K \cap L] = \# Gal(K / K \cap L)$

Dunque $\mathrm{Res}: \mathrm{Gal}(KL/L) \longrightarrow \mathrm{Gal}(K/K\cap L)$ è un omom. iniettivo tra insiemi della stessa cardinalità

$\Rightarrow$ Res è isom. $\Rightarrow$ $\mathrm{Gal}(KL/L) \simeq \mathrm{Gal}(K/K\cap L)$ $\square$

COR K/F di Gal, L/F qualsiasi.

$$\begin{tikzcd}[column sep=small] & KL \arrow[dl, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash, "\mathrm{Gal}"'] & & L \arrow[dl, dash, "\text{qualsiasi (finita)}"] \\ & F & \end{tikzcd}$$

Supponiamo che $K \cap L = F$. Allora

$$[KL:L] = [K:F]$$

DIM

$$[KL:L] = \#\mathrm{Gal}(KL/L) = \#\mathrm{Gal}(K/K\cap L) = \#\mathrm{Gal}(K/F) = [K:F]$$

CONTROES:

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt[3]{2}\zeta_3) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash, "3"] \\ & \mathbb{Q} & \end{tikzcd}$$

$\Rightarrow 2$ non 3

Gruppo di Galois del composto

$$\begin{tikzcd}[column sep=small] & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 \arrow[dr, dash, "\mathrm{Gal}"'] & & K_2 \arrow[dl, dash, "\mathrm{Gal}"] \\ & F & \end{tikzcd}$$

Supponiamo K_1/F, K_2/F Galois

(1) K_1K_2/F è di Galois

(DIM) Infatti se $K_1 = \text{cds di } (p_1, \dots)$

$K_2 = \text{cds di } (q_1, \dots)$

allora $K_1K_2 = \text{cds di } (p_1, \dots, q_1, \dots)$ $\square$

(2) $\mathrm{Gal}(K_1K_2/F)$?

Considero la restrizione (doppia)

$$\alpha: \mathrm{Gal}(K_1K_2/F) \longrightarrow \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$
$$\sigma \longmapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

(*) α è omom. e vablé

(*) α è iniettivo: se $\alpha(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2}) = (id_{K_1}, id_{K_2})$

allora $Fix(\sigma) \supseteq K_1, K_2 \Rightarrow Fix(\sigma) \supseteq K_1K_2$

$\Rightarrow \sigma = id_{K_1K_2}$.

(*) α è isomorfismo se e solo se $K_1 \cap K_2 = F$

$$\begin{tikzcd}[column sep=small] & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\ & K_1 \cap K_2 \arrow[d, dash] & \\ & F & \end{tikzcd}$$

$$[K_1K_2 : F] = \underbrace{[K_1K_2 : K_2]}_{\text{ris. di prima}}[K_2 : K_1 \cap K_2][K_1 \cap K_2 : F]$$

$$= \overbrace{[K_1 : K_1 \cap K_2]}[K_2 : K_1 \cap K_2][K_1 \cap K_2 : F]$$

OSS: α è isom. $\Leftrightarrow$ $[K_1K_2 : F] = [K_1 : F][K_2 : F]$

$$\begin{array}{ccc} [K_1K_2 : F] & = & [K_1 : F][K_2 : F] \\ \| & & \| \\ \#Gal(K_1K_2/F) & & \#Gal(K_1/F) \cdot \#Gal(K_2/F) \end{array}$$

Ma $[K_1K_2 : F] = [K_1 : K_1 \cap K_2][K_2 : F] = [K_1 : F][K_2 : F]$

$\Leftrightarrow [K_1 : K_1 \cap K_2] = [K_1 : F]$

$\Leftrightarrow [K_1 : K_1 \cap K_2] = [K_1 : K_1 \cap K_2][K_1 \cap K_2 : F]$

$\Leftrightarrow [K_1 \cap K_2 : F] = 1 \Leftrightarrow K_1 \cap K_2 = F$. $\square$

Ricapitolando:

TEOREMA K/F, L/F di Galois. Allora

$$\begin{tikzcd}[column sep=small] & KL \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "\overset{Gal}{\Uparrow}"] & \\ K \arrow[dr, dash, "Gal"'] & & L \arrow[dl, dash, "Gal"] \\ & F & \end{tikzcd}$$

(*) KL/F è di Galois

(*) $Gal(KL/F) \hookrightarrow Gal(K/F) \times Gal(L/F)$

$\sigma \longmapsto (\sigma|_K, \sigma|_L)$

(*) $Gal(KL/F) \simeq Gal(K/F) \times Gal(L/F) \Leftrightarrow K \cap L = F$.

$\mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$ ~ già fatto, vogliamo rifarlo meglio

$$\mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3}) = \mathbb{Q}(i, \sqrt{-3}, \sqrt[3]{3})$$

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{-3}, \sqrt[3]{3}) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$\mathbb{Q}(\sqrt{-3}, \sqrt[3]{3}) = \mathbb{Q}(\zeta_3, \sqrt[3]{3}) = \mathrm{cds}(x^3 - 3)$$

Vogliamo dire che $\underbrace{\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt{-3}, \sqrt[3]{3})} = \mathbb{Q}$

OSS: Questo est ha grado al max 2 su $\mathbb{Q}$.

Se ha grado 1 ho finito. Se ha grado 2 allora $\mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_3, \sqrt[3]{3})$.

DIAGRAMMI DI GALOIS!

$$\begin{tikzcd}
 & & L := \mathbb{Q}(\zeta_3, \sqrt[3]{3}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash, "3 = \#A_3"] & \\
\mathbb{Q}(\sqrt[3]{3}) \arrow[drr, dash, "3"'] & \mathbb{Q}(\sqrt[3]{3}\,\zeta_3) \arrow[dr, dash, "3"] & \mathbb{Q}(\sqrt[3]{3}\,\zeta_3^2) \arrow[d, dash, "3"] & L^{A_3} \arrow[dl, dash, "2 = {[S_3 : A_3]}"] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

$$\begin{tikzcd}
 & & \{id\} \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"] \arrow[d, dash, "2"] \arrow[dr, dash, "3 = \#A_3"] & \\
\langle (1,2) \rangle \arrow[drr, dash, "3"'] & \langle (1,3) \rangle \arrow[dr, dash, "3"] & \langle (2,3) \rangle \arrow[d, dash, "3"] & A_3 \arrow[dl, dash, "2 = {[S_3 : A_3]}"] \\
 & & S_3 &
\end{tikzcd}$$

Siccome c'è un unico sgrp. di indice 2 su S_3 c'è un unico sottocampo di $L/\mathbb{Q}$ t.c. $[L^{A_3} : \mathbb{Q}] = 2$

Ma $\mathbb{Q}(\zeta_3)$ è un tale campo! $\Rightarrow L^{A_3} = \mathbb{Q}(\zeta_3) \neq \mathbb{Q}(i)$

Dunque $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt{-3}, \sqrt[3]{3}) = \mathbb{Q}$. Per l'ultimo Teorema allora

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times S_3.$$

⊙ Descrivere le est. quadratiche di $\mathbb{Q}$ contenute in $K = \mathbb{Q}(i, \sqrt[3]{3}, \sqrt{-3})$.

A mano ci vengono ad esempio

$$\mathbb{Q}(i), \quad \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}), \quad \mathbb{Q}(\sqrt{3})$$

Sono tutte? Per teoria di Gal, basta trovare i sgrp. di indice 2 di $Gal(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times S_3$.

Oss: se $H < G$ ha indice 2, allora è normale e $\{g^2 : g \in G\} \subseteq H$.

Infatti sia $\pi : G \twoheadrightarrow G/H \simeq \mathbb{Z}/2\mathbb{Z}$

$$\pi(g^2) = \pi(g)^2 = id \Rightarrow g^2 \in Ker\,\pi = H. \quad \square$$

In particolare $G_2 := \langle g^2 : g \in G \rangle \subseteq H$.

Inoltre è normale in H: $\quad h g^2 h^{-1} = (h g h^{-1})^2$ [il coniugato di un quadrato è un quadrato]

Esiste quindi un teorema di corrisp. fra

$$\{\text{sgrp. di } G \text{ contenenti } G_2\} \longleftrightarrow \{\text{sgrp. di } G/G_2\}$$

Se vogliamo H di indice 2 allora H contiene $G_2 \Rightarrow$ siamo nelle HP del Teorema di corrisp.

Nel nostro caso: $G \simeq \mathbb{Z}/2\mathbb{Z} \times S_3$. Chi è G_2?

Dato $(n, \rho) \in G$, si ha che $(n,\rho)^2 = (2n, \rho^2) = (0, \rho^2)$

Ma $\rho \in S_3 \Rightarrow \rho^2$ è $\begin{cases} id & \text{se } \rho \text{ ha ordine 1 o 2} \\ \rho^{-1} & \text{se } \rho \text{ ha ordine 3} \end{cases} \Rightarrow$ prendo tutti i 3-cicli

$$\Rightarrow G_2 = \{(0, id)\} \cup \{(0, \text{3-cicli})\} = \{0\} \times A_3.$$

Dunque i sgrp di indice 2 in G corrispondono ai sgrp. di indice 2 in

$$\mathbb{Z}/2\mathbb{Z} \times S_3 \big/ \{0\} \times A_3 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$\Rightarrow$ ci sono 3 sgrp. di indice 2 in $(\mathbb{Z}/_2\mathbb{Z})^2$
(cioè $\langle(0,1)\rangle$, $\langle(1,0)\rangle$, $\langle(1,1)\rangle$)

$\Rightarrow$ ci sono 3 sotto ext quadratiche di $K/\mathbb{Q}$ e cioè

$$\mathbb{Q}(\sqrt{-3})\ ;\ \mathbb{Q}(\sqrt{3})\ ;\ \mathbb{Q}(i). \qquad \blacksquare$$

$$\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}) =: K$$

$p_1, \dots, p_n \in \mathbb{Z}$ primi distinti. Classificare le sottoext. quadratiche.

OSS: Dato un sottoinsieme non vuoto $I \subseteq \{1, \dots, n\}$ c'è l'estensione

$$\mathbb{Q}\left(\sqrt{\prod_{i \in I} p_i}\right)$$

ES: $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r}) \rightsquigarrow \sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{pq}, \sqrt{pr}, \sqrt{qr}$, $\sqrt{pqr}$

OSS: se $I \neq J \subseteq \{1, \dots, n\}$: sostengo che

$\mathbb{Q}\left(\sqrt{\prod_I p_i}\right) \neq \mathbb{Q}\left(\sqrt{\prod_J p_j}\right)$. Infatti sono uguali se

$\prod_I p_i \cdot \prod_J p_j$ è un quadrato in $\mathbb{Q}$ $\iff$ è un quadrato in $\mathbb{Z}$

Ma dato un certo $k \in \{1, \dots, n\}$ ho 3 possibilità
- $k \notin I, \notin J \Rightarrow \exp = 0$
- $k \in I, \notin J$ o viceversa $\Rightarrow \exp = 1$
- $k \in I \cap J \Rightarrow \exp = 2$

Dunque le ext sono uguali se e solo se ogni $k \in I$ è anche in J $\Rightarrow$ ma $I \neq J$, assurdo.

TESI INTERMEDIA: $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/_2\mathbb{Z})^2$

DIM Per induzione su n.

BASE: $n = 1$, $K = \mathbb{Q}(\sqrt{p}) \Rightarrow$ ok

IND: Vorrei dim che
$$K_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}$$

$$\begin{tikzcd}[column sep=small] & K_{n+1} \arrow[dl, dash] \arrow[dr, dash] & \\ K_n = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) \arrow[dr, dash, "(\mathbb{Z}/2\mathbb{Z})^n"'] & & \mathbb{Q}(\sqrt{p_{n+1}}) \arrow[dl, dash, "\mathbb{Z}/2\mathbb{Z}"] \\ & \mathbb{Q} & \end{tikzcd}$$

A quel punto per il corollario
$$\begin{aligned} \mathrm{Gal}(K_{n+1}/\mathbb{Q}) &\cong \mathrm{Gal}(K_n/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{p_{n+1}})/\mathbb{Q}) \\ &\cong (\mathbb{Z}/2\mathbb{Z})^n \times \mathbb{Z}/2\mathbb{Z} \\ &= (\mathbb{Z}/2\mathbb{Z})^{n+1} \end{aligned}$$

Certamente $K_n \cap \mathbb{Q}(\sqrt{p_{n+1}})$ ha grado 1 o 2 su $\mathbb{Q}$.
Se avesse grado 2 allora $\mathbb{Q}(\sqrt{p_{n+1}}) \subseteq K_n$. Ma le sottoest. quadratiche contenute in K_n

- sono $2^n - 1$: corrispondono ai sottogrp. di indice 2 in $(\mathbb{Z}/2\mathbb{Z})^n$, ovvero ai sottosp. vettoriali di dim $n-1$ in $\mathbb{F}_2^n$, ovvero alle eq. lineari in n variabili su $\mathbb{F}_2$
$$\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n = 0$$
$\Rightarrow$ ho 2^n scelte, ma escludendo la scelta $\lambda_1 = \dots = \lambda_n = 0$ me ne rimangono $2^n - 1$

- d'altro canto ne ho già contate $n-1$: sono $\mathbb{Q}(\sqrt{\prod_I p_i})$ al variare di I tra i sottoinsiemi non vuoti di $\{1, \dots, n\}$.

Se fosse $\mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}(\sqrt{\prod_I p_i})$ allora

$p_{n+1} \cdot \prod_I p_i$ non può essere un quadrato poiché

p_{n+1} ha esponente 1 in questo prodotto.

$\Rightarrow \mathbb{Q}(\sqrt{p_{n+1}}) \cap K_n = \mathbb{Q}$ e quindi la tesi. $\boxtimes$

Sottoest. di $\mathbb{Q}(\sqrt[4]{2})$

$$
\begin{tikzcd}
\mathbb{Q}(\sqrt[4]{2}) = F \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}
$$

è l'unica?

Non è Galois: ma $\sqrt[4]{2}$ ha come polinomio minimo $x^4 - 2 \rightsquigarrow \{\sqrt[4]{2};\ i\sqrt[4]{2};\ -\sqrt[4]{2};\ -i\sqrt[4]{2}\}$

Sia $K = \text{cds}(x^4 - 2)$

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt[4]{2}, i) \arrow[dl, dash] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(i) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[4]{2}) \arrow[dl, dash, "4"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Si vede anche a mano, ma con gli strumenti di oggi:

$$
\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i) \arrow[dr, dash, "2"', "\text{Galois}"] & & \mathbb{Q}(\sqrt[4]{2}) \arrow[dl, dash, "4"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Inoltre $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}$

e quindi $[K : \mathbb{Q}(\sqrt[4]{2})] = 4$

Segue quindi che

$$[K : \mathbb{Q}] = 8.$$

Vogliamo ora trovare $\text{Gal}(K/\mathbb{Q})$.

MODO 1: $\text{Gal}(K/\mathbb{Q}) \hookrightarrow S_4$, inoltre $\#\text{Gal}(K/\mathbb{Q}) = 8$

$\#S_4 = 24$. <u>OSS</u>: 8 è la max potenza di 2 che divide 24

$\Rightarrow \text{Gal}(K/\mathbb{Q}) \simeq$ un 2-Sylow di $S_4 \simeq D_4$

MODO 2: Sia $\sigma \in \text{Gal}(K/\mathbb{Q})$. σ è det. da

$$\sigma(\sqrt[4]{2}) = \sqrt[4]{2} \cdot i^n$$
$$\sigma(i) = \pm i$$

In totale ci sono al max 8 scelte $\Rightarrow$ ma $\#\text{Gal}(K/\mathbb{Q}) = 8$

$\Rightarrow$ tutte le scelte sono verificate

Siano $\sigma_1 = \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2}\, i \\ i \mapsto i \end{cases}$, $\sigma_2 = \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{cases}$

Si osserva che σ_1 ha ordine 4:

$$\sigma_1^4 = \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2}\, i^4 = \sqrt[4]{2} \\ i \mapsto i \end{cases} = id.$$

Inoltre $\sigma_2^2 = id$ e $\langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle = \{id\}$

Infine $\langle \sigma_1 \rangle \triangleleft \text{Gal}(K/\mathbb{Q})$ (ha indice 2)

Dunque $\text{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_4$

$$
\begin{tikzcd}
K \arrow[d, dash, "2"'] \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash] \arrow[dd, dash, bend right, "4"'] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
\{id\} \arrow[d, dash, "2"'] \\
\langle \sigma_2 \rangle \arrow[d, dash, bend right, "4"'] \\
D_4
\end{tikzcd}
$$

OSS: $\langle \sigma_2 \rangle$ fissa $\mathbb{Q}(\sqrt[4]{2}) \Rightarrow \mathbb{Q}(\sqrt[4]{2}) = K^{\langle \sigma_2 \rangle}$

Per Teorema di Galois per trovare le sottoest. di $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ devo trovare i sottogr. di D_4 contenenti $\langle \sigma_2 \rangle$.

$$H < \underset{\mathbb{Z}/4\mathbb{Z}}{\langle \sigma_1 \rangle} \rtimes \underset{\mathbb{Z}/2\mathbb{Z}}{\langle \sigma_2 \rangle} \quad \text{contenente} \quad \langle \sigma_2 \rangle$$