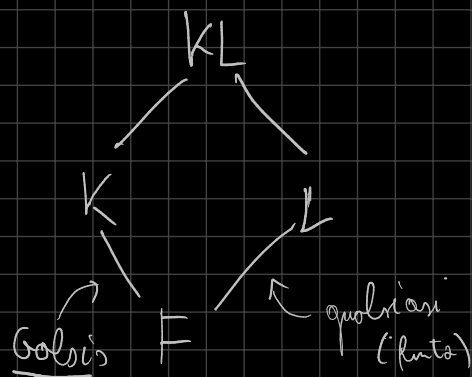


## TRASLATO DI UN' ESTENSIONE



RISULTATO:  $KL/L$  è di Galois

$$\text{e } \text{Gal}(KL/L) \cong \text{Gal}(K/L \cap K)$$

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

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

**T** Perché un polinomio? Perché ricorre al 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 c.d.s di  $p$  su  $L$ ,  
e quindi  $KL/L$  è normale.

Consideriamo ora

$$\text{Res: } \begin{array}{ccc} \text{Gal}(KL/L) & \longrightarrow & \text{Gal}(K/F) \\ \sigma & \longmapsto & \sigma|_K \end{array}$$

Tale mappa

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

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

sempre la sua restrizione a  $K$  è

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

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

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

$$\sigma \in \text{Gal}(K/F)$$

(\*) è un omomorfismo

$$\text{Res}(\sigma \circ \tau) = \sigma \circ \tau|_K = \sigma|_K \circ \tau|_K = \text{Res} \sigma \circ \text{Res} \tau$$

(\*) è iniettivo

$$\text{Res}(\sigma) = \text{id}_K \Rightarrow \sigma|_K = \text{id} \text{ e } \sigma|_L = \text{id}$$

Quindi  $F^\sigma$  è un campo che contiene  $K$  e  $L$ , quindi  
contiene almeno  $KL$

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

(\*) Siccome  $\sigma$  fissa  $L$ ,  $\sigma|_K$  fissa  $K \cap L$

quell. di  $L$  che sono ancora  
nel dominio di  $\sigma$

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

$$= \text{Gal}(K/K \cap L)$$

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

$$\begin{array}{ccc} KL & \xrightarrow{\sigma} & \\ \cup & \searrow & \\ \tau: K & \hookrightarrow & \bar{F} \end{array}$$

Siccome  $KL/L$  è finita, esistono tante est. 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

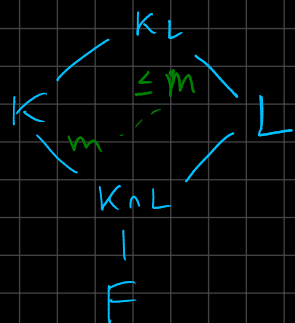
e sia  $f(t) := \prod_{\sigma \in \text{Gal}(KL/L)} (t - \sigma(\alpha))$

Questo pol. è invariante per l'azione di  $\text{Gal}(KL/L)$ , ↗ ne applico un  $\sigma' \in \text{Gal}$  al polinomio ottengo lo stesso polinomio  
 dunque i suoi coefficienti sono in

$$\text{Fix}(\text{Gal}(KL/L)) = L$$

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



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

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

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

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

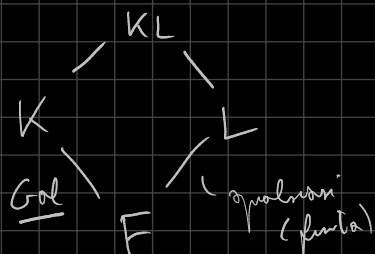
$$\Rightarrow \deg f = \# \text{Gal}(KL/L) = [K:K \cap L]$$

Ma dato che  $\text{Gal}is \left( \begin{matrix} K \\ \text{---} \\ K \cap L \\ \text{---} \\ F \end{matrix} \right) \xrightarrow{\text{Gal}is} K \cap L$  segue che  $[K:K \cap L] = \# \text{Gal}(K/K \cap L)$

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

COR

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



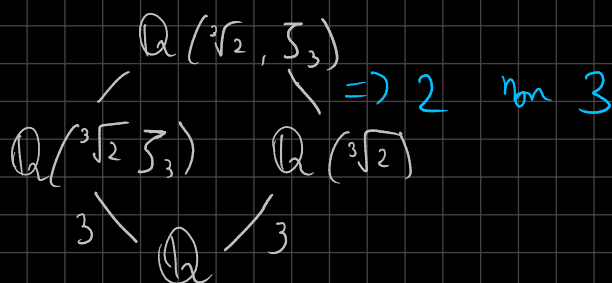
Supponiamo che  $K \cap L = F$ . Allora

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

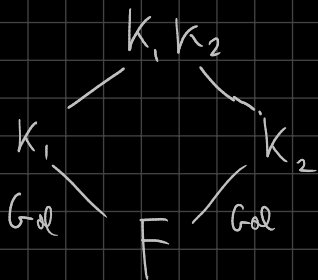
DIM

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

CONTROES:



## GRUPPO DI GALOIS DEL COMPOSTO



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)  $\text{Gal}(K_1K_2/F)$ ?

Considero la restrizione (doppia)

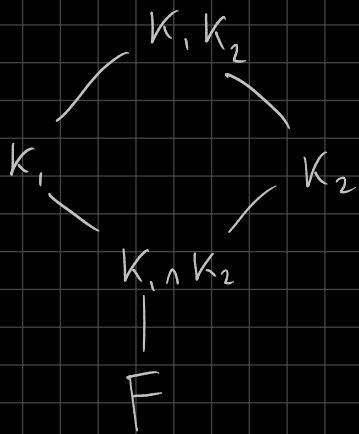
$$\begin{aligned} \alpha: \text{Gal}(K_1K_2/F) &\longrightarrow \text{Gal}(K_1/F) \times \text{Gal}(K_2/F) \\ \sigma &\longmapsto (\sigma|_{K_1}, \sigma|_{K_2}) \end{aligned}$$

(\*)  $\alpha$  è omom. e valloè

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

allora  $Fix(\sigma) \supseteq K_1, K_2 \Rightarrow Fix(\sigma) \supseteq K_1 K_2$   
 $\Rightarrow \sigma = id_{K_1 K_2}$ .

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



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

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

Oss:  $\alpha$  è isom.  $\Leftrightarrow [K_1 K_2 : F] = [K_1 : F] [K_2 : F]$

$\#Gal(K_1 K_2 / F) = \#Gal(K_1 / F) \cdot \#Gal(K_2 / F)$

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

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

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

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

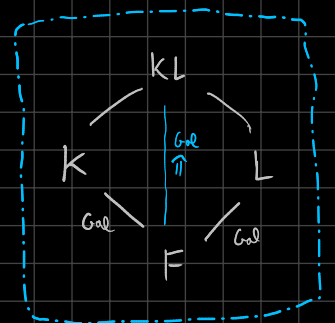
Ricapitolando:

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

(\*)  $KL/F$  è di Galois

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

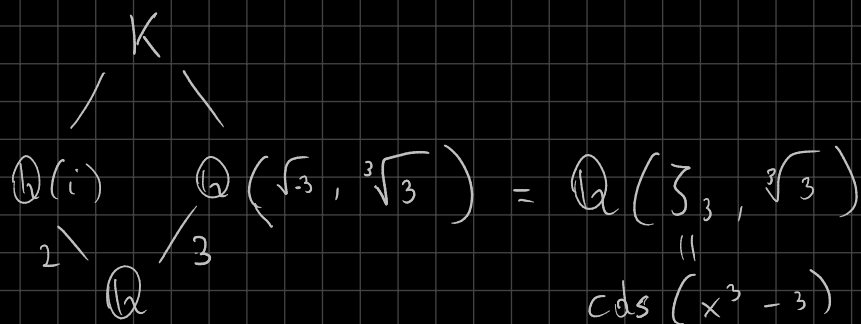
$\sigma \mapsto (\sigma|_K, \sigma|_L)$



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

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

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

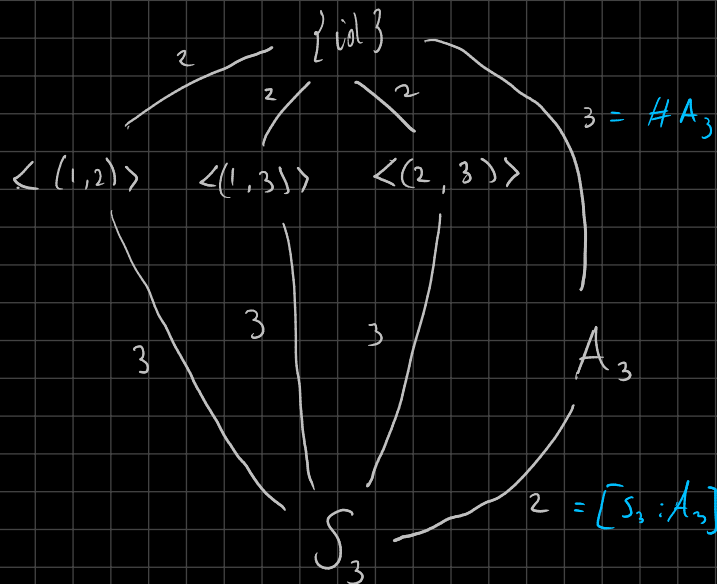
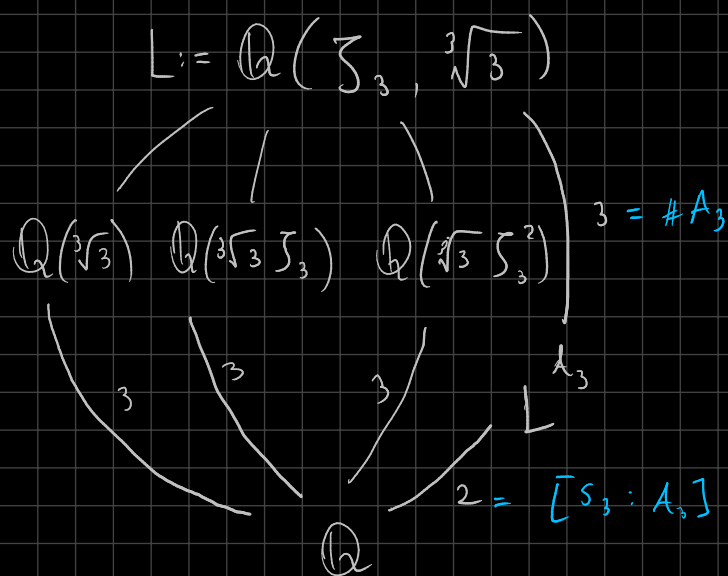


Vogliamo dire che  $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) = \mathbb{Q}$

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

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

DIAGRAMMI DI GALOIS!



Siccome c'è un unico sottogrup. 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'ultima tesi allora

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

① Descrivere le est. quadratiche di  $\mathbb{Q}$  contenute in  $K = \mathbb{Q}(i, \sqrt[3]{3}, \sqrt{-3})$ .

A nous ci vengono ad esempio

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

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

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

Infatti sia  $\pi : G \rightarrow G/H \cong \mathbb{Z}/2\mathbb{Z}$

$$\pi(g^2) = \pi(g)^2 = \text{id} \Rightarrow g^2 \in \ker \pi = H. \quad \square$$

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

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

Esiste quindi un teorema di corrisp. fra

$$\{\text{sottogr. di } G \text{ contenenti } G_2\} \leftrightarrow \{\text{sottogr. di } G/G_2\}$$

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

Nel nostro caso:  $G \cong \mathbb{Z}/2\mathbb{Z} \times S_3$ . 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 id se  $\rho$  ha ordine 1 o 2

↙  $\rho^{-1}$  se  $\rho$  ha ordine 3  $\Rightarrow$  prende tutti i 3-adi

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

Dunque i sottogr. di indice 2 in  $G$  corrispondono ai sottogr. di indice 2 in  $\mathbb{Z}/2\mathbb{Z} \times S_3 / \{0\} \times A_3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow$  ci sono 3 sottogr. 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 sottoest. quadratiche di  $K/\mathbb{Q}$  e cioè

$$\mathbb{Q}(\sqrt{3}) ; \mathbb{Q}(\sqrt{2}) ; \mathbb{Q}(i).$$

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

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

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

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

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

$$\mathbb{Q}(\sqrt{\prod_{i \in I} p_i}) \neq \mathbb{Q}(\sqrt{\prod_{j \in J} p_j}).$$
 Infatti sono uguali se

$$\prod_{i \in I} p_i \cdot \prod_{j \in J} p_j \text{ è un quadrato in } \mathbb{Q} \Leftrightarrow \text{è un quadrato in } \mathbb{Z}$$

Ma dato un certo  $K \in \{1, \dots, n\}$  ho 3 possibilità  $\begin{cases} K \notin I, \notin J \Rightarrow \text{exp. } 0 \\ K \in I, \notin J \Rightarrow \text{exp. } 1 \\ \text{viceversa} \\ K \in I \cap J \Rightarrow \text{exp. } 2 \end{cases}$

Dunque le est. sono uguali se e solo se

ogni  $K \in I$  è anche in  $J \Rightarrow$  se  $I \neq J$ , assurdo.

TESI INTERMEDIA:  $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$

DIM Per induzione su  $n$ .

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



IND: Vorrei dim che

$$K_n \cap \mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}$$

A quel punto per il corollario

$$K_{n+1} = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}, \sqrt{p_{n+1}})$$

$(\mathbb{Z}/2\mathbb{Z})^*$        $\mathbb{Q}$        $\mathbb{Z}/2\mathbb{Z}$

$$\text{Gal}(K_{n+1}/\mathbb{Q})$$

$$\cong \text{Gal}(K_n/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\sqrt{p_{n+1}})/\mathbb{Q})$$

$$\cong (\mathbb{Z}/2\mathbb{Z})^n \times \mathbb{Z}/2\mathbb{Z}$$

$$= (\mathbb{Z}/2\mathbb{Z})^{n+1}$$

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 sottost. quadratiche contenute in  $K_n$

- sono  $2^n - 1$ , corrispondono ai sottogruppi 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  $\lambda_1 = \dots = \lambda_n = 0$

ne restano  $2^n - 1$

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

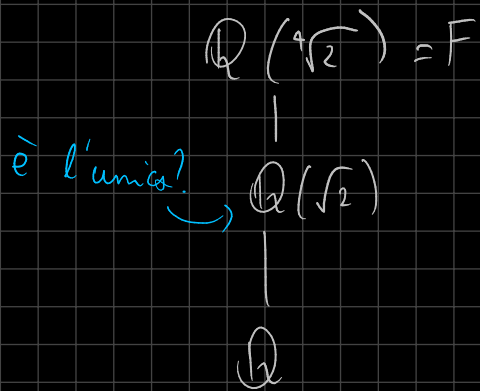
Se fosse  $\mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}(\sqrt{\prod_{i \in I} p_i})$  allora

$p_{n+1} \cdot \prod_{i \in I} p_i$  non può essere un quadrato poiché

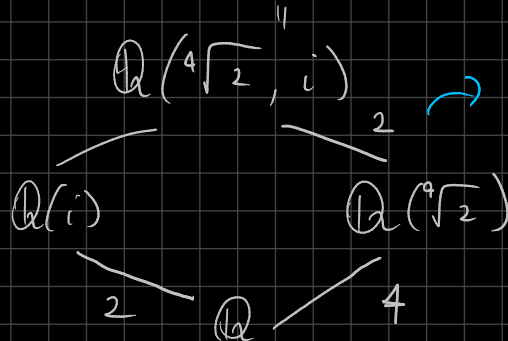
$p_{n+1}$  ha esponente 1 in questo prodotto.

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

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



Non è Galois: ma  $\sqrt[4]{2}$  ha come  
polinomio minimo  $x^4 - 2$   
Sia  $K = \text{cds}(x^4 - 2)$



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

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

$\mathbb{Q}$

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

Segue quindi che

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

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

Modo 1:  $\text{Gal}(K/\mathbb{Q}) \hookrightarrow S_4$ , inoltre  $\# \text{Gal}(K/\mathbb{Q}) = 8$   
 $\# S_4 = 24$ . Oss: 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  $\sigma \in \text{Gal}(K/\mathbb{Q})$ .  $\sigma$  è det. da

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

$$\sigma(i) = \pm i$$

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

$\Rightarrow$  tutte le scelte sono verificate

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

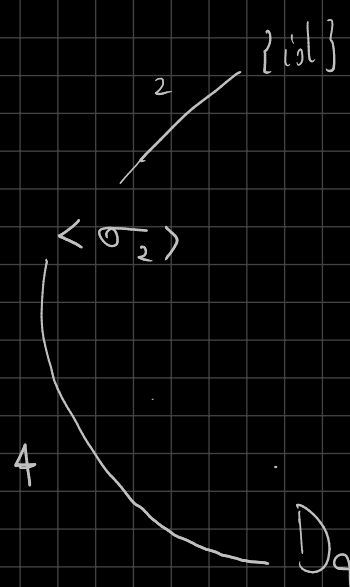
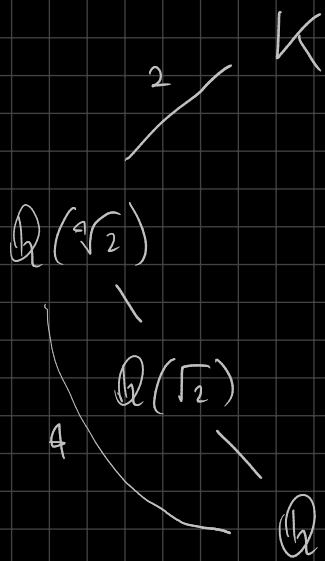
Si osserva che  $\sigma_1$  ha ordine 4:

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

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

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

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



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

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

$$H < \langle \sigma_1 \rangle \rtimes \langle \sigma_2 \rangle \quad \text{contenente } \langle \sigma_2 \rangle$$

$$\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$



