

Breaking extensions into pieces

$$F \subset K \quad \text{Galois}$$

\downarrow

$$\underbrace{F \subset L}_{\text{Galois}} \subset \underbrace{L \subset K}_{\text{Galois}}$$

$$G = \text{Aut}(K/F)$$

$$H = \text{Aut}(K/L).$$

- $$\left. \begin{array}{l} \textcircled{1} F \subset L \text{ Galois} \\ \textcircled{2} \sigma(L) = L \text{ for all } \sigma \in G \\ \textcircled{3} H \subseteq G \text{ normal.} \end{array} \right\} \text{Eqv.}$$

$\textcircled{1} \Rightarrow \textcircled{2}$: Take $\alpha \in L$ want: $\sigma(\alpha) \in L$

Let $p(x) \in F[x]$ be the min poly of α . Then $p(x)$ splits completely over L .
(because $F \subset L$ is Galois). & $\sigma(\alpha)$ also satisfies $p(x) = 0 \Rightarrow \sigma(\alpha) \in L$.

$\textcircled{2} \Rightarrow \textcircled{3}$ Take $h \in H$ and $\sigma \in G$. Want: $\sigma h \sigma^{-1} \in H$

Take $\alpha \in L$ Then $\sigma h \underbrace{\sigma^{-1}(\alpha)}_{\text{in } L} = \sigma \sigma^{-1}(\alpha) = \alpha.$

$\textcircled{3} \Rightarrow \textcircled{1}$ Take $\alpha \in L$. ~~Other~~ All roots of min poly of α are $\{\sigma\alpha \mid \sigma \in G\}$
Want: $\sigma\alpha \in L$. Take $h \in H$ want: $h(\sigma\alpha) = \sigma\alpha$
 $\underbrace{\sigma^{-1} h \sigma(\alpha)}_{\text{in } L} = \alpha$

□

$$\textcircled{2} \quad \sigma(L) = L$$

\Rightarrow Can Take $\sigma: K \rightarrow K$ & restrict it to L
 $\sigma: L \rightarrow L$

Gives

$$\text{Aut}(K/F) \rightarrow \text{Aut}(\cancel{K} L/F)$$

With kernel = $\text{Aut}(K/L)$

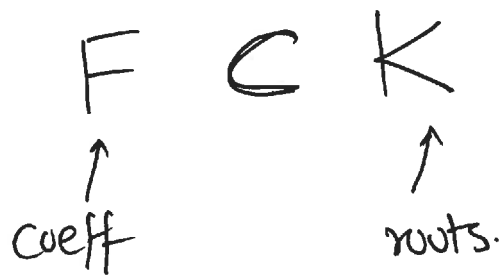
\Rightarrow Image has size $|\text{Aut}(K/F)| / |\text{Aut}(K/L)| = |\text{Aut}(L/F)|$

\Rightarrow Image is $\text{Aut}(L/F) \Rightarrow$ surj.

First iso thm $\Rightarrow \quad \text{Aut}(K/F) / \text{Aut}(K/L) \cong \text{Aut}(L/F).$

Quartic: Take $p(x) \in F[x]$

$K = \text{Splitting field.}$

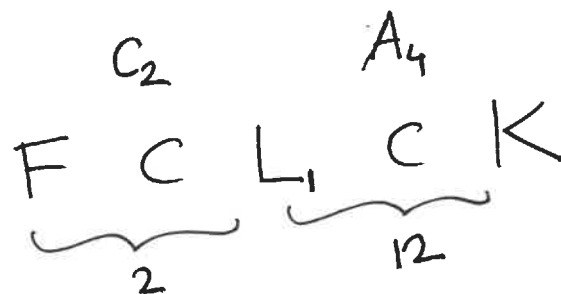


$$G = \text{Aut}(K/F) \hookrightarrow S_4$$

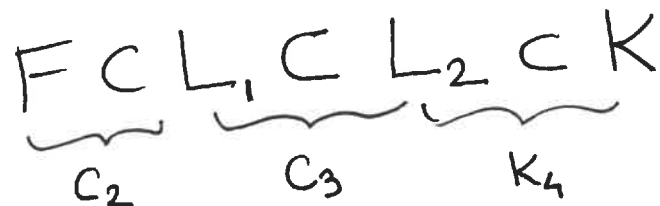
Assume $G = S_4$ (hardest case).

$$\zeta_2, \zeta_3 \in F.$$

Try $A_4 \subset S_4$

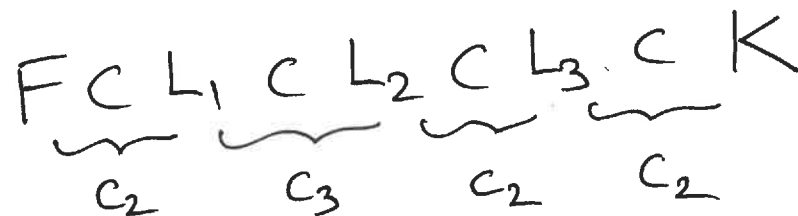


$$\begin{array}{c} \text{id} \\ (12)(34) \\ (13)(24) \\ (14)(23) \\ \hline K_4 \end{array} \triangleleft A_4$$



$$K_4 = C_2 \times C_2$$

$$C_2 \triangleleft K_4 \rightarrow C_2$$



✓

Suppose \underbrace{FCK} is Galois with Galois gp G .

$$\exists F \subset L_1 \subset L_2 \subset \dots \subset L_k = K$$

$$\begin{aligned} L_i \subset L_{i+1} \text{ is Galois of order } p_i \\ = \text{gp } \mathbb{Z}/p_i\mathbb{Z} \\ = C_{p_i} \end{aligned}$$

$$\Leftrightarrow \underbrace{G \triangleright H_1}_{C_{p_1}} \triangleright \underbrace{H_2}_{C_{p_2}} \triangleright \dots \triangleright 1$$

$$(S_4 \triangleright A_4 \triangleright K_4 \triangleright C_2 \triangleright 1)$$

A finite group G is solvable if \exists chain of subgroups

$$G \triangleright G_1 \triangleright G_2 \triangleright G_3 \triangleright \dots \triangleright 1$$

$$G_{i+1} \subset G_i \text{ is normal \& } G_{i+1}/G_i \cong \mathbb{Z}/p_i\mathbb{Z} \text{ prime } p_i$$

If $p(x) \in F[x]$ has a solvable Galois gp (& F contains enough roots of 1)
then the roots of $p(x)$ are expressible as iterated radicals of
elts in F .