Finally....

§16.7 The MAIN THEOREM OF GALOIS THEORY:

(16.7.1, 16.7.2, 16.7.3, 16.7.5)

Let $\mathbb{K} \supset \mathbb{F}$ be a Galois extension (with $[\mathbb{K}:\mathbb{F}]$ finite) and $\mathrm{char}(\mathbb{F})=0$, and $G := G(\mathbb{K}/\mathbb{F})$ the Galois group.

Then (a) one has a bijection,

$$\left\{ \begin{array}{l} \text{intermediate fields } \mathbb{L} \\ \text{with } \mathbb{F} \subset \mathbb{L} \subset \mathbb{K} \end{array} \right\} \underset{g}{\overset{f}{\rightleftarrows}} \left\{ \begin{array}{l} \text{subgroups } H \text{ with} \\ \{1\} \leq H \leq G \end{array} \right\}$$

sending $\mathbb{L} \longmapsto H := G(\mathbb{K}/\mathbb{L})$

$\mathbb{L} := \mathbb{K}^H \longleftarrow\!\shortmid H$

In particular, there are only finitely many such $\mathbb{L}$ with $\mathbb{F} \subset \mathbb{L} \subset \mathbb{K}$.

(b) the bijections reverse inclusions:

$$\begin{array}{ccc} \mathbb{K} = \mathbb{K}^{\{1\}} & & \{1\} \\ \cup & & \wedge \\ \mathbb{L}' = \mathbb{K}^{H'} & & H' = G(\mathbb{K}/\mathbb{L}') \\ \cup & \longleftrightarrow & \wedge \\ \mathbb{L} = \mathbb{K}^{H} & & H = G(\mathbb{K}/\mathbb{L}) \\ \cup & & \wedge \\ \mathbb{F} = \mathbb{K}^{G} & & G \end{array}$$

(c) if $\mathbb{L} \leftrightarrow H$ then $[\mathbb{K}:\mathbb{L}] = |H|$ with $\mathbb{K}/\mathbb{L}$ always Galois and $H = G(\mathbb{K}/\mathbb{L})$

while $[\mathbb{L}:\mathbb{F}] = [G:H]$, but $\mathbb{L}/\mathbb{F}$ is Galois $\iff H \trianglelefteq G$ (normal), in which case $G/H \cong G(\mathbb{L}/\mathbb{F})$

Picture:

$\mathbb{K}$

| ← always Galois, $G(\mathbb{K}/\mathbb{L}) = H$, degree $|H|$

$\mathbb{L} = \mathbb{K}^H$

| ← always degree $[G:H]$, but Galois $\Leftrightarrow H \trianglelefteq G$ and then $G(\mathbb{L}/\mathbb{F}) \cong G/H$

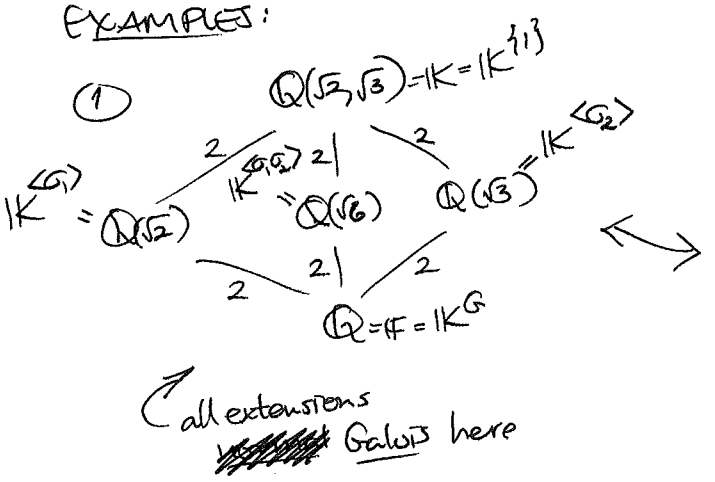
$\mathbb{F}$

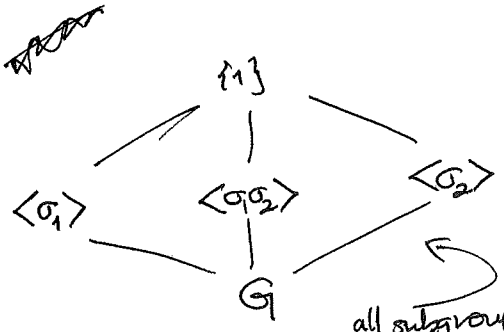
degree $|G|$

(93)

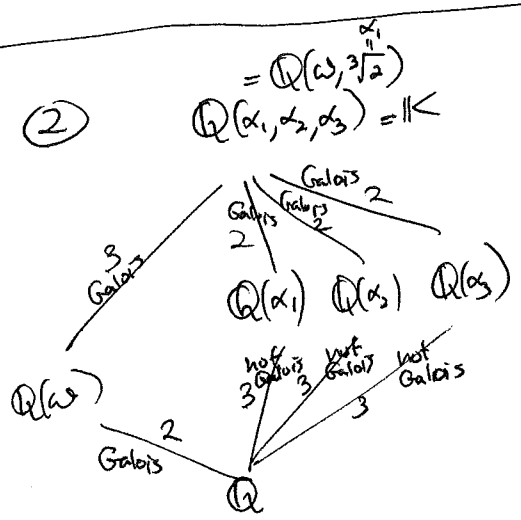
EXAMPLES:

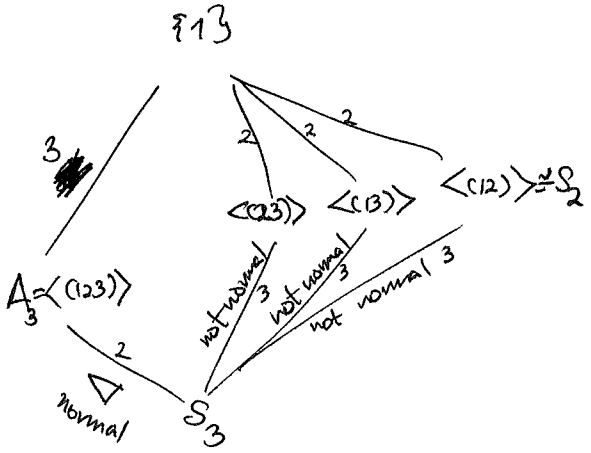
(1)





(2)





4/15/2019>

proof of MAIN THEOREM:

(a): We've seen that starting with $H \leq \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ $(\leq \mathrm{Aut}(\mathbb{K}))$, ($H$ finite)

one has $H \xrightarrow{g} \mathbb{K}^H \xrightarrow{f} G(\mathbb{K}/\mathbb{K}^H) = H$ (the fixed field theorem) $(\text{i.e. } f \circ g = 1\!\!1)$

On the other hand, starting with any $\mathbb{L}$ having $\mathbb{F} \subset \mathbb{L} \subset \mathbb{K}$,

since ~~$\mathbb{K}$~~ $\mathbb{K}/\mathbb{F}$ Galois $\Rightarrow \mathbb{K} = \mathrm{split}_{\mathbb{F}}(f(x))$ for some $f(x) \in \mathbb{F}[x]$

$\Rightarrow \mathbb{K} = \mathrm{split}_{\mathbb{L}}(f(x))$

$\Rightarrow \mathbb{K}/\mathbb{L}$ is Galois,

one also has $\mathbb{L} \xrightarrow{f} G(\mathbb{K}/\mathbb{L}) \xrightarrow{g} \mathbb{K}^{G(\mathbb{K}/\mathbb{L})} = \mathbb{L}$ $(\text{i.e. } g \circ f = 1\!\!1)$

(since $\mathbb{K}/\mathbb{L}$ Galois)

(b): The fact that f, g reverse inclusions is from their definitions!

(c): We just showed in the proof of (a) that if $\mathbb{L} = \mathbb{K}^H$ then $\mathbb{K}/\mathbb{L}$ is always Galois, and $\mathbb{L} = \mathbb{K}^{G(\mathbb{K}/\mathbb{L})}$ with $H = G(\mathbb{K}/\mathbb{L})$.
($\mathbb{K}/\mathbb{L} = \mathbb{K}/\mathbb{K}^H$, $\mathbb{L} = \mathbb{K}^H$)

This also shows $[\mathbb{K}:\mathbb{L}] = |H|$, and hence $[\mathbb{L}:\mathbb{F}] = \frac{[\mathbb{K}:\mathbb{F}]}{[\mathbb{K}:\mathbb{L}]} = \frac{|G|}{|H|} = [G:H]$.

To show $\mathbb{L}/\mathbb{F}$ Galois $\iff H \trianglelefteq G$,
start by picking $\beta \in \mathbb{L}$ with $\mathbb{L} = \mathbb{F}(\beta)$ by the Prim. Element Thm.

Then we know $m_{\mathbb{F},\beta}(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_r)$ where $\{\beta_1,\dots,\beta_r\} \in \mathbb{K}$ are the G-orbit of β, i.e. $\{g(\beta)\}_{g\in G}$ ($\beta = \beta_1$)
(since $\mathbb{F} = \mathbb{K}^G$)

Also, note that $\sigma \in G$ has $g(\beta) = \beta \iff \sigma$ acts as $1_{\mathbb{L}}$ on $\mathbb{L}(=\mathbb{F}(\beta))$
$\iff \sigma \in G(\mathbb{K}/\mathbb{L}) = H$ where $\mathbb{L} = \mathbb{K}^H$

Now $\mathbb{L}/\mathbb{F}$ is Galois $\iff \mathbb{L} = \text{split}_{\mathbb{F}}(m_{\mathbb{F},\beta}(x))$
(since $\beta \in \mathbb{L} = \mathbb{F}(\beta)$, $\{\sigma(\beta)\}_{g\in G} = \{\beta_1,\dots,\beta_r\} \subset \mathbb{L}$)
$\iff g(\beta) \in \mathbb{L}\ (\in \mathbb{K}^H)\ \forall g \in G$
$\iff hg(\beta) = g(\beta)\ \forall g \in G, h \in H$
i.e. $ghg^{-1}(\beta) = \beta$
i.e. $ghg^{-1} \in H$
$\iff H \trianglelefteq G$

Furthermore, when this holds (i.e. $\mathbb{L}/\mathbb{F}$ Galois, so $H \trianglelefteq G$)

since $g(\beta) \in \{g_1,\dots,g_r\} \subset \mathbb{L}\ \forall g \in G$,
$g(\mathbb{L}) \subset \mathbb{L}\ \forall g \in G$, i.e. <u>$G$ acts on $\mathbb{L}$ via restriction</u>.

So we get a homomorphism $G \xrightarrow{\varphi} G(\mathbb{L}/\mathbb{F})$, $g \longmapsto g|_{\mathbb{L}}$

which <u>surjects</u> since we can find g sending $\beta \mapsto \beta_i$ for each $i = 1, 2, \dots, r$
and has $\ker\varphi = \{g \in G : g|_{\mathbb{L}} = 1_{\mathbb{L}}\} = G(\mathbb{K}/\mathbb{L}) = H$. Thus $G/H \cong G(\mathbb{L}/\mathbb{F})$ by Noether's 1st iso thm. ∎

§16.2, 16.8, 16.9 Galois groups and the discriminant

How to describe the Galois group $G(\mathbb{K}/\mathbb{F})$ for $\mathbb{K}/\mathbb{F}$ Galois??
It's a bit tricky in general, but there are some things we can say easily.

THEOREM (16.6.6): If $\mathrm{char}(\mathbb{F})=0$ and $\mathbb{K}/\mathbb{F}$ is Galois with $\mathbb{K}=\mathrm{split}_{\mathbb{F}}(f(x))$ having roots $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, $\alpha_i\in\mathbb{K}$
then $G=G(\mathbb{K}/\mathbb{F})$ permutes $\{\alpha_1,\dots,\alpha_n\}$
giving an injective homomorphism $G\longrightarrow S_n$, i.e. $G\subset S_n$
Furthermore, if $f(x)$ is irreducible, then G is a transitive subgroup of S_n, i.e. G has only one orbit on $\{\alpha_1,\dots,\alpha_n\}$.

proof: We know G must permute $\{\alpha_1,\dots,\alpha_n\}$ since $f(x)\in\mathbb{F}[x]$ so $\sigma(f)=f$ $\forall\sigma\in G=G(\mathbb{K}/\mathbb{F})$.
We also know $\mathbb{K}=\mathbb{F}(\alpha_1,\dots,\alpha_n)$ so every $\sigma\in G$ is determined by how it permutes the $\{\alpha_1,\dots,\alpha_n\}$, giving injectivity. We also know when $f(x)$ is irreducible, so $f(x)=m_{\mathbb{F},\alpha_i}(x)$ for $i=1,\dots,n$, we can find $\sigma_i\in G$ sending $\alpha_1\xmapsto{\sigma_i}\alpha_i$ $\forall i=1,\dots,n$, so there is only one G-orbit. ∎

4/17/2019>

EXAMPLES:

① If $[\mathbb{K}:\mathbb{F}]=2$ then $\mathbb{K}=\mathbb{F}[\sqrt{a}]$ for some $a\in\mathbb{F}$ that is not a square
(since any $\beta\in\mathbb{K}-\mathbb{F}$ has $m_{\mathbb{F},\beta}(x)=x^2+bx+c$, so $\beta=\frac{-b\pm\sqrt{b^2-4c}}{2}$ and $a=b^2-4c$ works)

Here $G=S_2$ where $\sigma:\sqrt{a}\mapsto-\sqrt{a}$
$\|$
$\langle\sigma\rangle$

② If $\mathbb{K}=\mathrm{split}_{\mathbb{F}}(f(x))$ for some irreducible cubic $f(x)=x^3+bx^2+cx+d\in\mathbb{F}[x]$
$=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\in\mathbb{K}[x]$

then $G=G(\mathbb{K}/\mathbb{F})$ is a transitive subgroup of S_3, so either $A_3=\langle(123)\rangle$ and $[\mathbb{K}:\mathbb{F}]=3$
or S_3 itself and $[\mathbb{K}:\mathbb{F}]=6$