4/12/2019
(90)

Let's finally work in splitting fields with the other definitions of Galois:

THEOREM (Characterizing Galois extensions)
(16.6.4) Let $\mathbb{K} \supset \mathbb{F}$ have $[\mathbb{K}:\mathbb{F}]$ finite, and $\mathrm{char}(\mathbb{F}) = 0$ $(= \mathrm{char}(\mathbb{K}))$

Then T.F.A.E.:

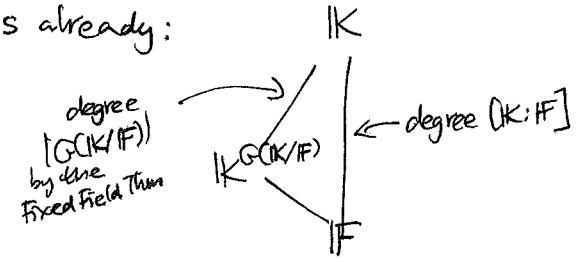
(a) $\mathbb{K}/\mathbb{F}$ is Galois, i.e. the inequality $|G(\mathbb{K}/\mathbb{F})| \le [\mathbb{K}:\mathbb{F}]$ is actually equality: $|G(\mathbb{K}/\mathbb{F})| = [\mathbb{K}:\mathbb{F}]$.

(b) The inclusion $\mathbb{F} \subset \mathbb{K}^{G(\mathbb{K}/\mathbb{F})}$ is an equality: $\mathbb{F} = \mathbb{K}^{G(\mathbb{K}/\mathbb{F})}$

(b′) $\mathbb{F} = \mathbb{K}^H$ for ~~some~~ $H \le \mathrm{Aut}(\mathbb{K})$ (and in this case, $H = G(\mathbb{K}/\mathbb{F})$)

(c) $\mathbb{K} = \mathrm{split}_{\mathbb{F}}(f(x))$ for some $f(x) \in \mathbb{F}[x]$.

Proof: (a) $\Leftrightarrow$ (b): We've seen this already:



Hence $|G(\mathbb{K}/\mathbb{F})| = [\mathbb{K}:\mathbb{F}] \Leftrightarrow \mathbb{K}^{G(\mathbb{K}/\mathbb{F})} = \mathbb{F}$
(a) (b)

(b) $\Rightarrow$ (b′) trivially: Let $H = G(\mathbb{K}/\mathbb{F})$

(b′) $\Rightarrow$ (b) since if $\mathbb{F} = \mathbb{K}^H$ for some $H \le \mathrm{Aut}(\mathbb{K})$
then $H \le \mathrm{Aut}(\mathbb{K}/\mathbb{F}) = G(\mathbb{K}/\mathbb{F})$

and Fixed Field Thm says $|H| = [\mathbb{K}:\overset{\mathbb{K}^H}{\mathbb{F}}] \ge |G(\mathbb{K}/\mathbb{F})|$

so $H = G(\mathbb{K}/\mathbb{F})$.

(91) (a)$\Leftrightarrow$(c): Since $[\mathbb{K}:\mathbb{F}]$ is finite and $\mathrm{char}(\mathbb{F})=0$,

pick $\gamma\in\mathbb{K}$ with $\mathbb{K}=\mathbb{F}(\gamma)$. Let $f(x):=\min_{\mathbb{F},\gamma}(x)$,

and let $\{\gamma_1,\gamma_2,\dots,\gamma_r\}$ ($=\{\gamma\}$) be the roots of $f(x)$ lying in $\mathbb{K}$.

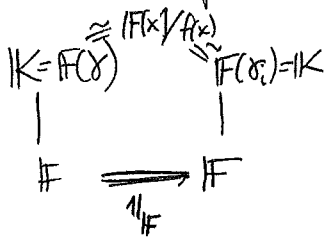
Note that every $\sigma\in G(\mathbb{K}/\mathbb{F})$ must send $\gamma\xrightarrow{\sigma}\gamma_i$ for some $i=1,2,\dots,r$

and this determines σ completely, so $|G(\mathbb{K}/\mathbb{F})|\le r$.

But since every γ_i has $[\mathbb{F}(\gamma_i):\mathbb{F}]=\deg f(x)=[\mathbb{K}:\mathbb{F}]$,

they all have $\mathbb{K}=\mathbb{F}(\gamma_i)$, and hence our isomorphism

extension theorem lets us produce such a $\sigma_i\in G(\mathbb{K}/\mathbb{F})$ sending $\gamma\mapsto\gamma_i$:



Hence $|G(\mathbb{K}/\mathbb{F})|=r$.

On the other hand, $\mathbb{K}=\mathrm{split}_{\mathbb{F}}(f(x))\iff r=\deg(f)=[\mathbb{K}:\mathbb{F}]$

since $\mathbb{K}$ has at least one root of $f(x)$ $\iff$ $\mathbb{K}=\mathrm{split}_{\mathbb{F}}(g(x))$ for any $g(x)\in\mathbb{F}[x]$

$|G(\mathbb{K}/\mathbb{F})|$ $[\mathbb{K}:\mathbb{F}]$ ∎

COROLLARY (16.6.5): If $\mathbb{K}\supset\mathbb{F}$ has $\mathrm{char}(\mathbb{F})=0$ and $[\mathbb{K}:\mathbb{F}]$ finite,

then we can embed it in a Galois extension $\mathbb{K}'\supset\mathbb{F}$. ($\mathbb{K}\hookrightarrow\mathbb{K}'$)

proof: By Prim. Element Thm, $\mathbb{K}=\mathbb{F}(\gamma)$ for some $\gamma\in\mathbb{K}$

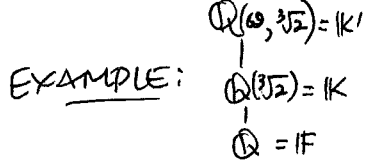
so let $\mathbb{K}'=\mathrm{split}_{\mathbb{K}}(m_{\mathbb{F},\gamma}(x))=\mathrm{split}_{\mathbb{F}}(m_{\mathbb{F},\gamma}(x))$.

$\mathbb{K}'=\mathrm{split}_{\mathbb{F}}(f(x))=\mathrm{split}_{\mathbb{K}}(f(x))$ where $f(x)=m_{\mathbb{F},\gamma}(x)\in\mathbb{F}[x]\subset\mathbb{K}[x]$

i.e. (Galois) $\mathbb{K}=\mathbb{F}(\gamma)$

$\mathbb{F}$ ∎

EXAMPLE:



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

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

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 $|H|$

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

degree $|G|$

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

$\mathbb{F}$

(93)

EXAMPLES:

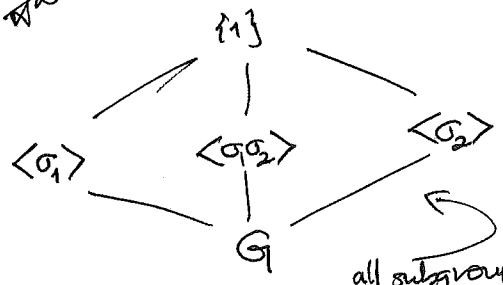
(1) $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{K} = \mathbb{K}^{\{1\}}$

$\mathbb{K}^{\langle\sigma_1\rangle} = \mathbb{Q}(\sqrt{2})$, $\mathbb{K}^{\langle\sigma_1\sigma_2\rangle} = \mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{3}) = \mathbb{K}^{\langle\sigma_2\rangle}$

$\mathbb{Q} = \mathbb{F} = \mathbb{K}^G$

(all extensions ~~Galois~~ Galois here)

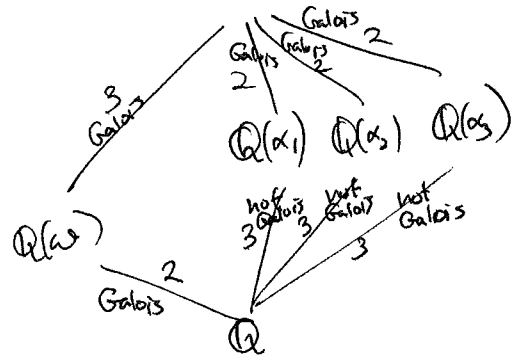
$G = G(\mathbb{K}/\mathbb{F}) = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\} \cong V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

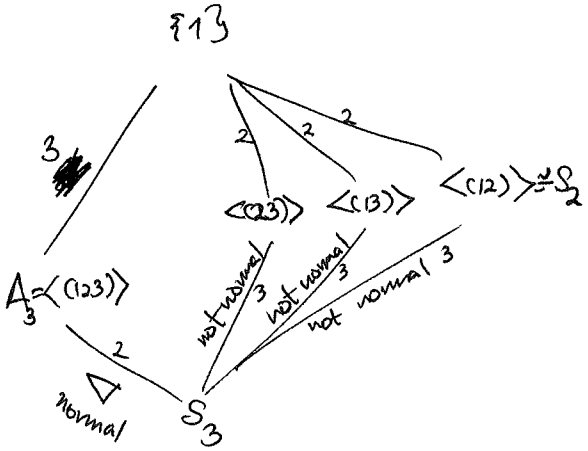


all subgroups normal, since G abelian.

---

(2) $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) = \mathbb{K} = \mathbb{Q}(\omega, \sqrt[3]{2}^{\alpha_1})$





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 $H \xmapsto{g} \mathbb{K}^H \xmapsto{f} G(\mathbb{K}/\mathbb{K}^H) = H$ (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 ~~$\mathbb{K}/\mathbb{F}$ 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 $\mathbb{L} \xmapsto{f} G(\mathbb{K}/\mathbb{L}) \xmapsto{g} \mathbb{K}^{G(\mathbb{K}/\mathbb{L})} = \mathbb{L}$ $(\text{i.e. } g\circ f = 1\!\!1)$

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

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