Hence $g(x)$ has coefficients lying in $\mathbb{K}^H$, so $g(x) \in \mathbb{K}^H[x]$.

On the other hand, we claim any $f(x) \in \mathbb{K}^H[x]$ with $f(\beta)=0$ must be divisible by $g(x)$, since

$$\begin{array}{ccccc} x-\beta & \text{divides } f(x) & \Rightarrow & h(x-\beta) \text{ divides } h(f(x)) & \forall h \in H \\ \| & & & \| & \| \leftarrow \text{since } f(x) \in \mathbb{K}^H[x] \\ x-\beta_1 & & & x-h(\beta) & f(x) \\ & & & \| & \\ & & & x-\beta_i & \\ & & & \text{for some } i=1,2,\dots,r & \end{array}$$

and since $\{\beta_1,\dots,\beta_r\}$ is the H-orbit of β,

this shows each $(x-\beta_i)$ divides $f(x)$

so $\underbrace{(x-\beta_1)\cdots(x-\beta_r)}_{= g(x)}$ divides $f(x)$ by unique factorization.

Thus $g(x) = m_{\mathbb{K}^H,\beta}(x)$. The rest follows ∎

DEF'N: An extension $\mathbb{K} \supset \mathbb{F}$ with $[\mathbb{K}:\mathbb{F}]$ finite is called Galois if $[\mathbb{K}:\mathbb{F}] = |G(\mathbb{K}/\mathbb{F})|$.

The next result will show why $[\mathbb{K}:\mathbb{F}] \geq |G(\mathbb{K}/\mathbb{F})|$ always... When $\mathrm{char}(\mathbb{K})=0$,

THEOREM (16.5.4) (The fixed field thm) If $H < \mathrm{Aut}(\mathbb{K})$ is a finite subgroup, then $\mathbb{K} \supset \mathbb{K}^H$ has $[\mathbb{K}:\mathbb{K}^H] = |H|$

proof: By the previous theorem, every $\beta \in \mathbb{K}$ is algebraic over $\mathbb{K}^H$, with $[\mathbb{K}^H(\beta):\mathbb{K}^H]$ dividing $|H|$, so at most $|H|$.

We'd like to conclude $[\mathbb{K}:\mathbb{K}^H]$ is finite from this, by applying this LEMMA (16.5.3): If $\mathbb{F}$ has characteristic 0, and every $\beta \in \mathbb{K} \supset \mathbb{F}$ has $[\mathbb{F}(\beta):\mathbb{F}] \leq N$ for some N, then $[\mathbb{K}:\mathbb{F}]$ is finite.

FALSE if $\mathrm{char}(\mathbb{F})\neq 0$, e.g. with $N=2$:
$\mathbb{F}_2(\sqrt{x_1},\sqrt{x_2},\dots) = \mathbb{K}$
|
$\mathbb{F}_2(x_1,x_2,\dots) = \mathbb{F}$

proof of LEMMA: Assume $[\mathbb{F}(\beta):\mathbb{F}] \leq N \ \forall \beta \in \mathbb{K}$ but $[\mathbb{K}:\mathbb{F}]=\infty$; we'll get a contradiction. Pick $\alpha_1 \in \mathbb{K} \sim \mathbb{F}$, so $[\mathbb{F}(\alpha_1):\mathbb{F}] < \infty \Rightarrow \mathbb{F}(\alpha_1) \subsetneq \mathbb{K}$.
Then pick $\alpha_2 \in \mathbb{K} \sim \mathbb{F}(\alpha_1)$, so $[\mathbb{F}(\alpha_1,\alpha_2):\mathbb{F}] < \infty \Rightarrow \mathbb{F}(\alpha_1,\alpha_2) \subsetneq \mathbb{K}$. (Prim. Element Thm)
Repeat to get $\mathbb{F} \subsetneq \mathbb{F}(\alpha_1) \subsetneq \mathbb{F}(\alpha_1,\alpha_2) \subsetneq \cdots$, and let γ_i have $\mathbb{F}(\gamma_i) = \mathbb{F}(\alpha_1,\alpha_2,\dots,\alpha_i)$.
Then $[\mathbb{F}(\gamma_i):\mathbb{F}]$ are unbounded ∎

(87) Now that we know $[\mathbb{K}:\mathbb{K}^H]$ is finite, pick $\gamma \in \mathbb{K}$ with $\mathbb{K} = \mathbb{K}^H(\gamma)$. ← Prim. Element Thm

If γ has H-orbit $\{\gamma_1, \gamma_2, \dots, \gamma_r\}$ of size r, then the previous theorem tells us $r = [\mathbb{K}^H(\gamma):\mathbb{K}^H] = [\mathbb{K}:\mathbb{K}^H]$.

On the other hand, since every automorphism $\mathbb{K} \xrightarrow{\sigma} \mathbb{K}$ in H
($\mathbb{K}^H(\gamma)$ → $\mathbb{K}^H(\gamma)$)
is determined once we choose the image $\gamma_i = \sigma(\gamma)$ with $i = 1, 2, \dots, r$
(and one can pick any γ_i to be this image since $\gamma_1, \dots, \gamma_r$ are the roots of $m_{\mathbb{K}^H, \gamma}(x)$), it must be that $|H| = r = [\mathbb{K}:\mathbb{K}^H]$ ∎

COROLLARY (LEMMA 16.6.2)

(a) In a finite extension $[\mathbb{K}:\mathbb{F}] < \infty$, one always has $|G(\mathbb{K}:\mathbb{F})|$ finite.

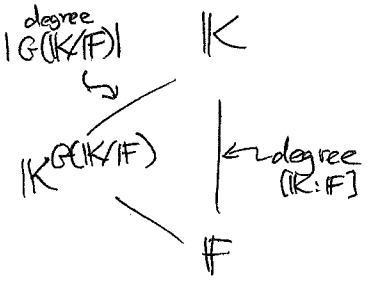
This was what Artin refers to as LEMMA 16.4.2(d) in the latest edition, but it is missing there!

(b) When $\mathrm{char}(\mathbb{K}) = 0$, furthermore
$|G(\mathbb{K}/\mathbb{F})|$ divides $[\mathbb{K}:\mathbb{F}]$,
with equality $|G(\mathbb{K}/\mathbb{F})| = [\mathbb{K}:\mathbb{F}]$ (so $\mathbb{K}/\mathbb{F}$ Galois)
$\iff$ the inclusion $\mathbb{F} \subset \mathbb{K}^{G(\mathbb{K}/\mathbb{F})}$
is an equality: $\mathbb{F} = \mathbb{K}^{G(\mathbb{K}/\mathbb{F})}$.

(c) Conversely, when $\mathrm{char}(\mathbb{K}) = 0$, for every finite subgroup $H < \mathrm{Aut}(\mathbb{K})$,
$\mathbb{K}/\mathbb{K}^H$ is a Galois extension
with $G(\mathbb{K}/\mathbb{K}^H) = H$.

proof: (a) $[\mathbb{K}:\mathbb{F}]$ finite $\iff$ $\mathbb{K} = \mathbb{F}(\alpha_1, \dots, \alpha_n)$ α_i algebraic over $\mathbb{F}$
$\Rightarrow$ every $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ is determined by
the choice of $\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)$,
with only finitely many choices for each $\sigma(\alpha_i)$,
namely the other roots in $\mathbb{K}$ of $m_{\mathbb{F},\alpha_i}(x)$.

(b) Once we know $G(\mathbb{K}/\mathbb{F})$ is finite, the previous theorem applies here:



$\Rightarrow |G(\mathbb{K}/\mathbb{F})|$ divides $[\mathbb{K}:\mathbb{F}]$, with equality exactly when $\mathbb{F} = \mathbb{K}^{G(\mathbb{K}/\mathbb{F})}$

(c) The previous theorem says that for $H < \mathrm{Aut}(\mathbb{K})$, we have $|H| = [\mathbb{K}:\mathbb{K}^H]$.

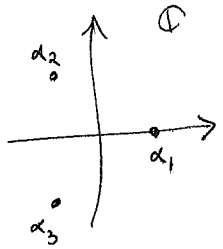
Now certainly $H \leq G(\mathbb{K}/\mathbb{K}^H)$

so $|H| \leq |G(\mathbb{K}/\mathbb{K}^H)| \leq [\mathbb{K}:\mathbb{K}^H]$ (part (b))

and since the two ends are equal, all are equal, with $H = G(\mathbb{K}/\mathbb{K}^H)$ and $\mathbb{K}/\mathbb{K}^H$ Galois ∎

4/10/2019 >

(BIG) EXAMPLE: Let's analyze in $\mathbb{F}=\mathbb{Q} \subset \mathbb{K}_1 = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{K}_2 = \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$, where $\alpha_1 = \sqrt[3]{2}$, $\mathbb{K}_1 = \mathbb{Q}(\sqrt[3]{2})$, $\mathbb{K}_2 = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$



the groups $G(\mathbb{K}_1/\mathbb{F})$, $G(\mathbb{K}_2/\mathbb{F})$ ← 2 as in EXER. 17.4.1 on HW4

Since $m_{\mathbb{Q},\sqrt[3]{2}}(x) = x^3 - 2$ has only $\alpha_1,\alpha_2,\alpha_3$ as roots, with $\mathbb{K}_1 = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ and $\alpha_2, \alpha_3 \notin \mathbb{R}$

any $\sigma \in G(\mathbb{K}_1/\mathbb{F}) = G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ must have $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, and hence $\sigma = 1_{\mathbb{K}_1}$

So $G(\mathbb{K}_1/\mathbb{F}) = \{1\}$, and $\mathbb{F} = \mathbb{Q} \subsetneq \mathbb{K}_1^{G(\mathbb{K}_1/\mathbb{F})} = \mathbb{K}_1^{\{1\}} = \mathbb{Q}(\sqrt[3]{2})$. Thus $\mathbb{K}_1/\mathbb{F}$ is not Galois (not splitting either)

(89) Any $\sigma \in G(\mathbb{K}_2/\mathbb{F}) = G(\mathbb{K}_2/\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3))$ must permute $\{\alpha_1,\alpha_2,\alpha_3\}$

and will be completely determined once we specify this permutation

$\sigma(\alpha_i) = \alpha_{\sigma(i)}$, so we get an injective group homomorphism

$$G(\mathbb{K}_2/\mathbb{F}) \xrightarrow{\varphi} S_3$$

We claim every $\sigma \in S_3$ can be achieved (i.e. $|\operatorname{im}\varphi| = 6 = |S_3|$)

because after lifting
$$\begin{array}{ccc} \mathbb{Q}(\omega) & \overset{\sigma}{\dashrightarrow} & \mathbb{Q}(\omega) \\ 2\,| & & |2 \\ \mathbb{Q} & = & \mathbb{Q} \end{array}$$
in two ways: $\omega \mapsto \omega$ OR $\omega \mapsto \omega^2$ (since $m_{\mathbb{Q},\omega}(x) = x^2+x+1 = (x-\omega)(x-\omega^2)$)

then we can still further lift
$$\begin{array}{ccc} \mathbb{Q}(\omega,\sqrt[3]{2}) & \overset{\sigma}{\dashrightarrow} & \mathbb{Q}(\omega,\sqrt[3]{2}^?) \\ 3\,| & & |3 \\ \mathbb{Q}(\omega) & \xrightarrow{\sigma} & \mathbb{Q}(\omega) \\ | & & | \\ \mathbb{Q} & = & \mathbb{Q} \end{array}$$
in three ways:

$\sqrt[3]{2} \mapsto \sqrt[3]{2} = \alpha_1$

OR

$\sqrt[3]{2} \mapsto \omega\sqrt[3]{2} = \alpha_2$

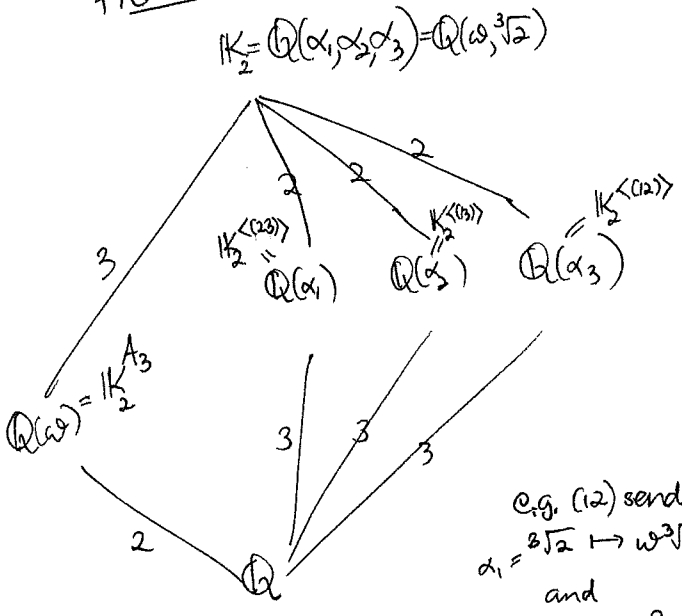
OR

$\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} = \alpha_3$

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

So $\mathbb{K}_2/\mathbb{F}$ is Galois (and a splitting field)

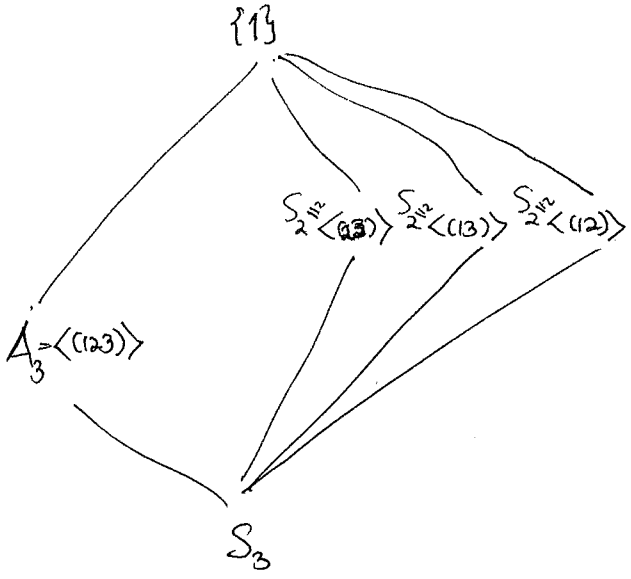
Picture:



e.g. (12) sends $\alpha_1 = \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} = \alpha_2$ and $\omega \mapsto \omega^2$, fixing $\omega^2\sqrt[3]{2} = \alpha_3$

intermediate subfields $\mathbb{F}'$ between $\mathbb{Q} \subset \mathbb{F}' \subset \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$

$\mathbb{F}$ $\quad$ $\mathbb{K}_2$



subgroups H of S_3

(drawn upside down!)