$= \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$

(85)

EXAMPLE: $\mathbb{K} = \mathbb{Q}(\sqrt{2},\sqrt{3})$ has $\mathrm{Aut}(\mathbb{K}) = \{\begin{matrix}\sqrt{2}\mapsto\pm\sqrt{2}\\ \sqrt{3}\mapsto\pm\sqrt{3}\end{matrix}\}$

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

$\mathbb{K}^{\langle\sigma_1\rangle} = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6}) = \mathbb{K}^{\langle\sigma_3\rangle}$, $\mathbb{Q}(\sqrt{3}) = \mathbb{K}^{\langle\sigma_2\rangle}$, $\mathbb{Q} = \mathbb{K}^{\langle\sigma_1,\sigma_2,\sigma_3\rangle} = \mathbb{K}^{G(\mathbb{K}/\mathbb{F})}$

(each $\mathbb{Q}(\sqrt{2}) \subset \mathbb{K}$ has degree 2; $\mathbb{Q} \subset \mathbb{Q}(\sqrt{6})$ has degree 2; $\mathbb{Q}(\sqrt{6}) \subset \mathbb{K}$ has degree 2; $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3})$ has degree 2; $\mathbb{Q} \subset \mathbb{K}$ has degree 2)

$= \{1_{\mathbb{K}}, \sigma_1: \sqrt{2}\mapsto+\sqrt{2}, \sqrt{3}\mapsto-\sqrt{3}, \sigma_2: \sqrt{2}\mapsto-\sqrt{2}, \sqrt{3}\mapsto+\sqrt{3}, \sigma_3: \sqrt{2}\mapsto-\sqrt{2}, \sqrt{3}\mapsto-\sqrt{3}\}$

Note $\sigma_3 = \sigma_1\sigma_2$ (and $\sigma_1 = \sigma_2\sigma_3$ and $\sigma_2 = \sigma_1\sigma_3$; σ_i, σ_j all commute)

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

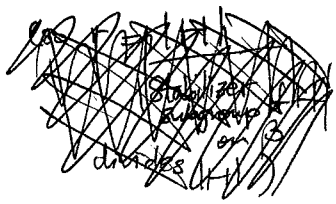
$\langle\sigma_1\rangle \times \langle\sigma_2\rangle$

$= \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$

4/8/2019 >

Let's work toward those equivalences...

THEOREM (16.5.2): When $H < \mathrm{Aut}(\mathbb{K})$ and $\beta \in \mathbb{K}$ has H-orbit $\{\beta_1, \dots, \beta_r\}$ ($\beta = \beta_1$)



then $m_{\mathbb{K}^H,\beta}(x) = (x-\beta_1)\cdots(x-\beta_r)$

and hence $[\mathbb{K}^H(\beta) : \mathbb{K}^H] = r = \dfrac{|H|}{|H_\beta|}$ divides $|H|$

(Orbit-Stabilizer Lemma)

$H_\beta :=$ Stabilizer of β in H $= \{h \in H : h(\beta) = \beta\}$

EXAMPLE: $x^4 - 10x^2 + 1 = m_{\mathbb{Q},\sqrt{2}+\sqrt{3}}(x) = \prod_{+/-\text{ signs}} (x - (\pm\sqrt{2} \pm \sqrt{3}))$

proof: First note that $g(x) := (x-\beta_1)\cdots(x-\beta_r)$

$= x^r - \underbrace{(\beta_1+\dots+\beta_r)}_{s_1(\beta_1,\dots,\beta_r)}x^{r-1} + \underbrace{(\beta_1\beta_2+\beta_1\beta_3+\dots+\beta_{r-1}\beta_r)}_{s_2(\beta_1,\dots,\beta_r)}x^{r-2} - \dots + (-1)^r\underbrace{\beta_1\beta_2\cdots\beta_r}_{s_r(\beta_1,\dots,\beta_r)}$

where $s_k(\beta_1,\dots,\beta_r) \overset{\text{DEFN}}{:=}$ the k^{th} elementary symmetric polynomial in $\beta_1,\dots,\beta_r$

$:= \sum_{1\le i_1<\dots<i_k\le r} \beta_{i_1}\beta_{i_2}\cdots\beta_{i_k}$

(We skipped this from §16.1)

and each $s_k(\beta_1,\dots,\beta_r) \in \mathbb{K}^H$ since $h(s_k(\beta_1,\dots,\beta_r)) = s_k(h(\beta_1),\dots,h(\beta_r))$

$= s_k(\beta_{\sigma(1)},\dots,\beta_{\sigma(r)})$ for some $\sigma \in S_r$

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

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

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: 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. (16.5.3)

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 $\alpha_1 \in \mathbb{K}-\mathbb{F}$, so $[\mathbb{F}(\alpha_1):\mathbb{F}]<\infty \Rightarrow \mathbb{F}(\alpha_1) \subsetneq \mathbb{K}$. Then pick $\alpha_2 \in \mathbb{K}-\mathbb{F}(\alpha_1)$, 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 ∎

FALSE if $\mathrm{char}(\mathbb{F})\neq 0$, e.g. with $N=2$:

$$\begin{array}{c} \mathbb{F}_2(\sqrt{x_1},\sqrt{x_2},\dots) = \mathbb{K} \\ | \\ \mathbb{F}_2(x_1,x_2,\dots) = \mathbb{F} \end{array}$$

(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 $\{\gamma_1, \gamma_2, \ldots, \gamma_r\}$ 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 (with $\mathbb{K}^H(\gamma)$ and $\mathbb{K}^H(\gamma)$ underneath)

is determined once we choose the image $\gamma_i = \sigma(\gamma)$ with $i = 1, 2, \ldots, r$ (and one can pick any γ_i to be this image since $\gamma_1, \ldots, \gamma_r$ 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 $H < \mathrm{Aut}(\mathbb{K})$,

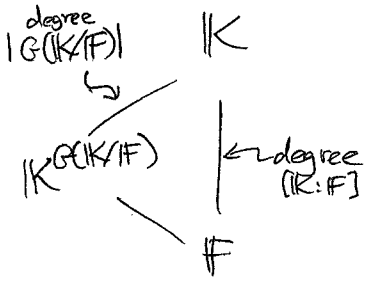
$\mathbb{K}/\mathbb{K}^H$ is a Galois extension

with $G(\mathbb{K}/\mathbb{K}^H) = H$.

Proof: (a) $[\mathbb{K}:\mathbb{F}]$ finite $\iff$ $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ α_i algebraic over $\mathbb{F}$

$\Rightarrow$ every $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ is determined by the choice of $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$, 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 $|H| = [\mathbb{K}:\mathbb{K}^H]$.

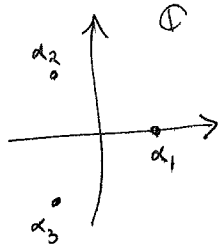
Now certainly $H \leq G(\mathbb{K}/\mathbb{K}^H)$

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 $\alpha_1=\sqrt[3]{2}$, $\alpha_2=\omega\sqrt[3]{2}$, $\alpha_3=\omega^2\sqrt[3]{2}$



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