PROPOSITION: (16.4.3 (b) + more) Given a field isomorphism $F_1 \xrightarrow{\varphi} F_2$ and two polynomials $f_1(x) \in F_1[x]$ with $\varphi(f_1) = f_2$, $f_2(x) \in F_2[x]$

then one can extend φ to an isomorphism between any splitting fields K_1 for f_1 and K_2 for f_2:

$$\begin{array}{ccc} K_1 & \xrightarrow{\tilde{\varphi}} & K_2 \\ \cup & & \cup \\ F_1 & \xrightarrow{\varphi} & F_2 \end{array}$$

REMARK: our proof will show, in fact, we can make $\tilde{\varphi}$ take any root α_1 of f_1 with $m_{F_1,\alpha_1}(x)$ as min. poly to any root α_2 of $\varphi(m_{F_1,\alpha_1}(x))$

COR: In particular, any two splitting fields K_1, K_2 for $f(x) \in F[x]$ are F-isomorphic:

$$\begin{array}{ccc} K_1 & \xrightarrow{\tilde{\varphi}} & K_2 \\ \cup & & \cup \\ F & \xrightarrow[\mathrm{id}_F = \varphi]{} & F \end{array}$$

(So it is fair to call any of them $\mathrm{split}_F(f(x)) = K$)

4/5/2019>

proof: Induct on $[K_1 : F_1]$. (not the proof in Artin!)

BASE CASE $[K_1 : F_1] = 1$ has $K_1 = F_1$, so $f_1(x)$ splits in F_1 as $c\prod_{i=1}^{n}(x-\alpha_i)$, $\alpha_i \in F_1$,

and then $f_2(x) = \varphi(f_1(x))$ splits in $F_2 = K_2$,

$$= \varphi(c)\prod_{i=1}^{n}(x-\varphi(\alpha_i))$$

so $\tilde{\varphi} = \varphi$ works.

In the INDUCTIVE STEP, pick an irreducible factor $g_1(x)$ of $f_1(x)$ in $F_1[x]$ so that $g_2(x) = \varphi(g_1)$ is an irred factor of $f_2(x)$ in $F_2[x]$.

Letting α_1 be a root of $g_1(x)$ (and $f_1(x)$) in K_1

then let α_2 be any root of $g_2(x)$ (and $f_2(x)$) in K_2; such an α_2 exists since K_2 splits $f_2(x)$.

We can extend φ like this:

$$\begin{array}{ccccc} K_1 & & \cdots \exists \tilde{\varphi} \cdots & & K_2 \\ \cup & & & & \cup \\ F_1(\alpha_1) \cong F_1[x]/g_1(x) & & \xrightarrow{\varphi} & & F_2[x]/g_2(x) \cong F_2(\alpha_2) \\ \cup & & & & \cup \\ F_1 & & \xrightarrow{\qquad\varphi\qquad} & & F_2 \end{array}$$

Now replace F_1, F_2 with $F_1(\alpha_1), F_2(\alpha_2)$, and apply induction. ∎

THEOREM (SPLITTING-THM. 16.3.2): If $\mathbb{K} = \text{split}_{\mathbb{F}}(f(x))$, then any irreducible $g(x) \in \mathbb{F}[x]$ that has one root $\beta \in \mathbb{K}$ will split completely in $\mathbb{K}$.

proof: Let $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$ with $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, so $\mathbb{K} = \mathbb{F}(\alpha_1, \dots, \alpha_n)$

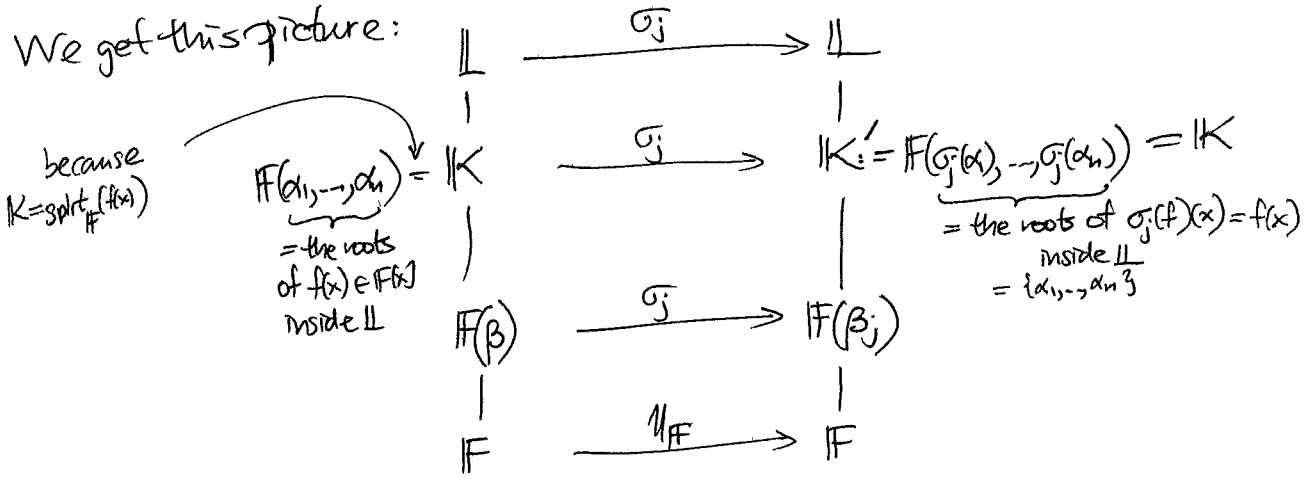
and then let $\mathbb{L} := \text{split}_{\mathbb{K}}(g(x)) = \text{split}_{\mathbb{F}}(f(x)g(x))$

$= \prod_{j=1}^{m}(x-\beta_j)$ (with $\beta = \beta_1$ WLOG)

i.e. $\mathbb{F} \subset \underset{\mathbb{F}(\alpha_1,\dots,\alpha_n)}{\mathbb{K}} \subset \underset{\mathbb{F}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_m)}{\mathbb{L}}$ ($\beta_1 = \beta$)

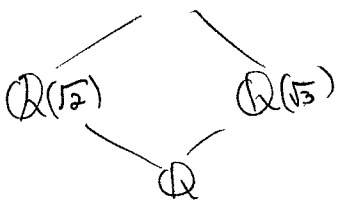
Using our previous PROPOSITION and its proof, for each $j = 2, 3, \dots, m$ extend the identity map $\mathbb{F} \xrightarrow{\mathbb{1}_{\mathbb{F}}} \mathbb{F}$ to an $\mathbb{F}$-automorphism $\mathbb{L} \xrightarrow{\sigma_j} \mathbb{L}$ that takes one root $\beta = \beta_1$ to any of the other roots β_j of $g(x)$, $j = 2, \dots, m$.

We get this picture:



Hence $\beta_j \in \mathbb{K}$ for each $j = 2, 3, \dots, m$, i.e. $g(x)$ splits completely in $\mathbb{K}$ ∎

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



§16.5 Fixed fields

DEFN: Let $\mathrm{Aut}(\mathbb{K}) := \{\text{all field automorphism } \mathbb{K} \xrightarrow{\sigma} \mathbb{K}\}$, as a group:

$\sigma\tau = \sigma \circ \tau : \mathbb{K} \to \mathbb{K}$

$\mathbb{K} \xrightarrow{\tau} \mathbb{K} \xrightarrow{\sigma} \mathbb{K}$

and for an extension $\mathbb{F} \subset \mathbb{K}$

$$\mathrm{Aut}(\mathbb{K}/\mathbb{F}) := \{\text{all } \mathbb{F}\text{-automorphisms } \mathbb{K} \xrightarrow{\sigma} \mathbb{K}\} < \mathrm{Aut}(\mathbb{K}) \quad (\text{subgroup})$$
$$= G(\mathbb{K}/\mathbb{F})$$

$\mathbb{F} = \mathbb{F}$

Given any subgroup $H < \mathrm{Aut}(\mathbb{K})$,

the fixed (sub)field $\mathbb{K}^H := \{\alpha \in \mathbb{K} : h(\alpha) = \alpha \ \forall h \in H\}$

is a subfield of $\mathbb{K}$ (check this!)

and when $H < \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ then $\mathbb{F} \subset \mathbb{K}^H$ by definition

---

Note that if $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_r)$ then any $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$

is completely determined by specifying $\sigma(\alpha_i)$ for $i = 1, 2, \ldots, r$

and if each α_i is algebraic over $\mathbb{F}$ (e.g. if $[\mathbb{K}:\mathbb{F}]$ finite)

then $\sigma(\alpha_i)$ has only finitely many choices, namely

the other roots in $\mathbb{K}$ of $m_{\mathbb{F},\alpha_i}(x)$.

Thus $|G(\mathbb{K}/\mathbb{F})|$ is finite, and we'll later see (THM 16.6.4) it's $\leq [\mathbb{K}:\mathbb{F}]$

(with equality $\underset{\text{DEFN}}{\Leftrightarrow}$ $\mathbb{K}/\mathbb{F}$ Galois

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

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

assuming $\mathrm{char}(\mathbb{F}) = 0$.

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

(85)

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

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

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

(2) (2) (2)

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

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

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

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

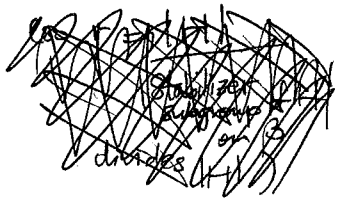
$\langle\sigma_1\rangle \times \langle\sigma_2\rangle$

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

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 $= \{h \in H : h(\beta) = \beta\}$

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

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

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 $\sigma \in S_r$