Splitting fields

$F \subset K$ is a splitting extension of $f(x) \in F[x]$ if

1. $f(x) = (x-\alpha_1) \cdots (x-\alpha_n)$ in $K[x]$
2. $K = F[\alpha_1, \ldots, \alpha_n]$.

Theorem: Let $F \subset K$ splitting extension. Take any ~~$\beta \in K[x]$~~ $\beta \in K$ and let $g(x) \in F[x]$ be the min poly of β.
Then $g(x)$ split completely in $K[x]$.
product of linear factors.

Application: $\mathbb{Q} \subset \mathbb{Q}[2^{1/4}]$ is NOT a splitting ext^n of any poly. because $\beta = 2^{1/4}$ violates the thm.

Pf of thm: $\beta \in K = F[\alpha_1, \ldots, \alpha_n]$

$f(x) = (x-\alpha_1)\cdots(x-\alpha_n) \in F[x]$

Know $\beta = p(\alpha_1, \ldots, \alpha_n)$ for some ~~$p \in F[$~~ poly p with coeff in F.

$\beta_1, \beta_2, \ldots, \beta_{n!}$ be the elts of K obtained by permuting $\alpha_1, \ldots, \alpha_n$ & applying p.

Consider $\underbrace{(x-\beta_1)\cdots(x-\beta_{n!})}_{\text{coeff symmetric in } \alpha_1,\ldots,\alpha_n.} = h(x)$.

so lie in F. (using elementary sym poly).

$g(x)$ divides $h(x)$.

$g(x)$: min poly of β

$h(x)$: poly satisfied by β.

Ex. $n=3$

$\beta_1 = \alpha_1^2\alpha_2 + 2\alpha_3 = \beta$

$\beta_2 = \alpha_2^2\alpha_1 + 2\alpha_3$

$\beta_3 = \alpha_3^2\alpha_2 + 2\alpha_1$

$\beta_4 = \cdots$

$\beta_5 = \cdots$

$\beta_6 = \cdots$

Consider $(x-\beta_1)\cdots(x-\beta_6)$ coeff symmetric in $\alpha_1, \ldots, \alpha_n$.

$h(x)$ splits compl. in $K[x]$

$\Rightarrow g(x)$ also does

$\square$

Examples :

$\mathbb{Q} \subset \mathbb{Q}[2^{1/4}]$ Not a splitting extension.

but $\underbrace{\mathbb{Q}[i]}_{F} \subset \underbrace{\mathbb{Q}[i][2^{1/4}]}_{K}$ is a splitting extⁿ. of $X^4 - 2$.

$$K = F[2^{1/4}, 2^{1/4}i, -2^{1/4}, -2^{1/4}i]$$

Find $G = \mathrm{Aut}(K/F)$.

$K \cong F[X]/(X^4-2)$. ← why?

$2^{1/4} \leftarrow\!\!\mapsto X$

$\downarrow$

K

4 possibilities

$X \mapsto 2^{1/4}$
$X \mapsto 2^{1/4}i$
$X \mapsto -2^{1/4}$
$X \mapsto -i2^{1/4}$

Any $\sigma \in G$ must permute the 4 roots.

$G \hookrightarrow S_4 = \{$Permutations of 4 roots$\}$

Key : Only some permutations are valid automorphisms.

$\mathrm{Aut}(K/F)$ has 4 elts.

$2^{1/4} \mapsto 2^{1/4}$, $2^{1/4} \mapsto 2^{1/4}i$, $2^{1/4} \mapsto -2^{1/4}$, $2^{1/4} \mapsto -i2^{1/4}$.

$$K = F[\underset{1}{2^{1/4}}, \underset{2}{i2^{1/4}}, \underset{3}{-2^{1/4}}, \underset{4}{-i2^{1/4}}] \qquad 1, 2, 3, 4$$

$\mathrm{Aut}(K/F)$ consists of $2^{1/4} \mapsto$

$$2^{1/4}, \longrightarrow \text{identity permutation.}$$

$$i2^{1/4}, \longrightarrow (1\ 2\ 3\ 4)$$

$$-2^{1/4} \longrightarrow (1\ 3)(2\ 4)$$

$$-i2^{1/4} \longrightarrow (1\ 4\ 3\ 2)$$

$$\mathrm{Aut}(K/F) \cong C_4$$