Thm 53.6, pkt 3

$H \leq G(K/F)$ $\quad K_H = \{\alpha \in K \mid \psi(\alpha) = \alpha \ \forall \psi \in H\}$

$\Rightarrow \lambda(K_H) = G(K/K_H) = H$

Bevis

1) $H \leq G(K/K_H)$

La $\psi \in H$ og $\alpha \in K_H$. $\Rightarrow \psi(\alpha) = \alpha$ siden $\psi \in H$.

$\Rightarrow \psi \in G(K/K_H)$

2) Anta $H \lneq G(K/K_H)$

i) Vi har $K = K_H(\alpha)$, $\alpha \in K$

K, rotkropp gir $[K : K_H] = \{K : K_H\} = |G(K/K_H)| = n$

ii) Siden $H \neq G(K/K_H) \Rightarrow |H| < n$ og $|H| < [K : K_H]$

iii) $H = \{\sigma_1, \ldots, \sigma_{|H|}\}$; $f(x) = \prod_{i=1}^{|H|} (x - \sigma_i(\alpha))$; $\deg(f) < n$

iv) Koeff. til f er symmetriske i røttene

$\Rightarrow$ invariant under $\sigma \in H$

$\Rightarrow f(x) \in K_H[x]$ og $f(\alpha) = 0$ siden $\sigma_i = id$ for en i

v) $\deg(\alpha, K_H) \leq |H| < n = [K : K_H] = [K_H(\alpha) : K_H]$

Motsigelse

Thm 53.6 - pkt 5

$$\begin{array}{l} K \\ | \\ E \\ | \\ F \end{array}$$ normal $\iff$ $\lambda(E) = G(K/E) \leq G(K/F)$ (normal undergr.)

og $G(E/F) \simeq G(K/F)/G(K/E)$

Bevis:

$$\begin{array}{l} K \\ | \\ E \\ | \\ F \end{array}$$ normal $\iff \forall \sigma \in G(K/F),\ \alpha \in E;\ \sigma(\alpha) \in E$

i)

$$\begin{array}{ccc} K & \xrightarrow{\simeq} & K \\ | & & | \\ E & \longrightarrow & E' = E \\ | & & | \\ F & = & F \end{array}$$ (E rotthespp/F)

ii) $E = E_{G(K/E)} \iff \sigma(\alpha) \in E$ hviss $\forall \tau \in G(K/E)$

$\tau\sigma(\alpha) = \sigma(\alpha)$

$\Updownarrow$

$\sigma^{-1}\tau\sigma(\alpha) = \alpha$

dvs $G(K/E) \leq_{\text{normal}} G(K/F)$

iii) For $\sigma \in G(K/F)$; $\sigma_E = \sigma|_E \in G(E/F)$ Automorfi siden E normal/F

$$\begin{array}{ccc} G(K/F) & \longrightarrow & G(E/F) \\ \sigma & \longmapsto & \sigma_E \end{array}$$

- surjektivt siden $\tau \in G(E/F)$ kan utvides til hele K; $\sigma \in G(K/F)$ slik at $\sigma_E = \tau$.
- Kjernen er alle σ slik at $\sigma_E = id$, dvs $\sigma|_E = id$, eller $\sigma \in G(K/E)$

$\Rightarrow$ $G(E/F) \simeq G(K/F)/G(K/E)$

Ex $f(x) = x^4+1 \in \mathbb{Q}[x]$ irreducibelt / $\mathbb{Z}$

Rødder $\frac{\pm 1 \pm i}{\sqrt{2}}$



sett $\alpha = \frac{1}{\sqrt{2}}(1+i) \Rightarrow$ Rødder er $\alpha, \alpha^3, \alpha^5, \alpha^7$ $\alpha^4 = -1$

$\Rightarrow \mathbb{Q}(f(\alpha)) = \mathbb{Q}(\alpha)$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ Basis $\{1, \alpha, \alpha^2, \alpha^3\}$

$|G(\mathbb{Q}(\alpha)/\mathbb{Q})| = 4$ $\sigma \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$

gitt ved $\sigma(\alpha) = \alpha^3$

$G(K/\mathbb{Q})$

$\langle\tau\rangle$ $\langle\sigma\rangle$ $\langle\sigma\tau\rangle$

$\{e\}$

$\Rightarrow \sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\alpha^3) = (\sigma(\alpha))^3 = \alpha^9 = \alpha$

τ gitt ved $\tau(\alpha) = \alpha^5$

$\Rightarrow \tau^2(\alpha) = \tau(\tau(\alpha)) = \tau(\alpha^5) = \tau(\alpha)^5 = \alpha^{25} = \alpha$

$\Rightarrow G(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

$K = \mathbb{Q}(\alpha)$

$K_{(\sigma)} = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 = b \mid \sigma(b) = b\}$

$\downarrow \sigma$

$a_0 + a_1\alpha^3 + a_2\alpha^2 + a_3\alpha$ dvs. $a_1 = a_3$ $a_2 = 0$

$K_{(\tau)}$: $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 = a_0 + a_1\alpha + a_2\alpha^2 - a_3\alpha^3$

dvs. $a_1 = a_3 = 0$

$\sigma\tau(\alpha) = \sigma(\alpha^5) = (\alpha^3)^5 = \alpha^{15} = -\alpha^3$

$K_{(\sigma\tau)}$: $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 = a_0 + a_1\alpha^3 + a_2\alpha^2 - a_3\alpha$

dvs. $a_1 = -a_3$ $a_2 = 0$

$\mathbb{Q}$

$\mathbb{Q}(i)$ $\mathbb{Q}(\sqrt{2}i)$ $\mathbb{Q}(\sqrt{2})$

K

$\Rightarrow K_{(\sigma)}$: $a_0 + a_1\left(\frac{1+i}{\sqrt{2}} + \frac{-1+i}{\sqrt{2}}\right) = a_0 + a_1\sqrt{2}i$

$K_{(\tau)}$: $a_0 + a_2 i$

$K_{(\sigma\tau)}$: $a_0 + a_1\left(\frac{1+i}{\sqrt{2}} - \frac{-1+i}{\sqrt{2}}\right) = a_0 + a_1\sqrt{2}$

Ex $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ (irreducible)

Røtter $\alpha = \sqrt[4]{2}, -\alpha, i\alpha, -i\alpha$ $\quad i^2 = -1$

$\Rightarrow K = \mathbb{Q}(f(x)) = \mathbb{Q}(\alpha, i)$ siden $i = \frac{i\alpha}{\alpha}$

$\mathbb{Q}(\alpha)$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, basis $\{1, \alpha, \alpha^2, \alpha^3\}$

$[K : \mathbb{Q}(\alpha)] = 2$, basis $\{1, i\}$

$\Rightarrow [K : \mathbb{Q}] = 8$ basis $\{1, \alpha, \alpha^2, \alpha^3, i, \alpha i, \alpha^2 i, \alpha^3 i\}$

$\psi \in G(K/\mathbb{Q})$ bestemt av verdien på røttene,
derfor bestemt av $\psi(\alpha)$ og $\psi(i)$

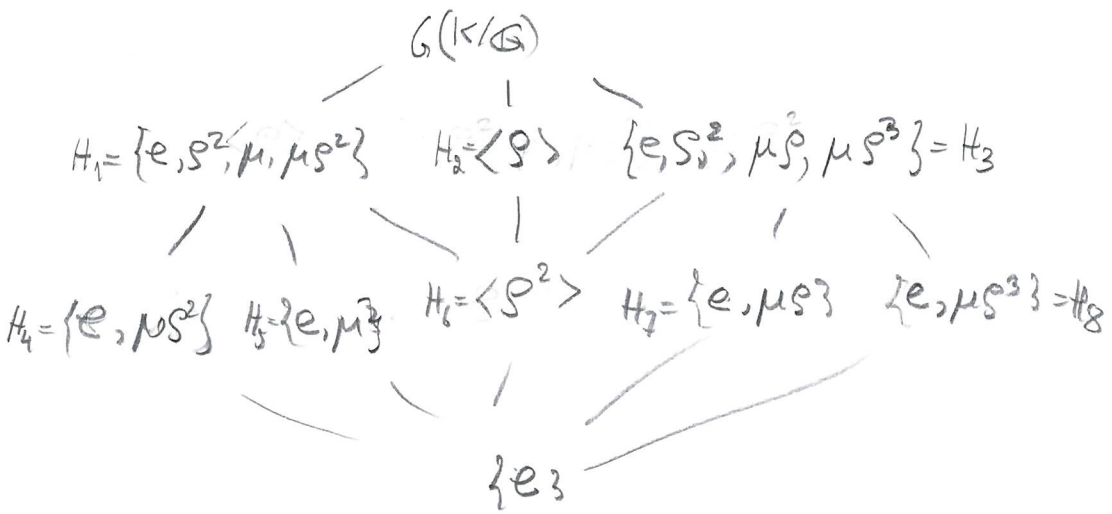
$\operatorname{irr}(\psi(\alpha), \mathbb{Q}) = \operatorname{irr}(\alpha, \mathbb{Q})$
$\operatorname{irr}(\psi(i), \mathbb{Q}) = \operatorname{irr}(i, \mathbb{Q})$

$\rho(\alpha) = i\alpha$, $\rho^4 = id$ $\quad \mu(i) = -i$ $\quad \mu^2 = id$
$\rho(i) = i$ $\quad \mu(\alpha) = \alpha$

$\mu\rho \begin{cases} \alpha \mapsto -i\alpha \\ i \mapsto -i \end{cases}$

$\rho^3\mu \begin{cases} \alpha \mapsto -i\alpha \\ i \mapsto -i \end{cases}$ $\Big\}$ $\mu\rho = \rho^3\mu$

$\Rightarrow G(K/\mathbb{Q}) \simeq \langle \mu, \rho \mid \mu^2 = \rho^4 = (\rho\mu)^2 = e \rangle = D_4$



	1	α	α^2	α^3	i	αi	$\alpha^2 i$	$\alpha^3 i$
e	1	α	α^2	α^3	i	αi	$\alpha^2 i$	$\alpha^3 i$
ρ	1	$i\alpha$	$-\alpha^2$	$-i\alpha^3$	i	$-\alpha$	$-\alpha^2 i$	α^3
ρ^2	1	$-\alpha$	α^2	$-\alpha^3$	i	$-i\alpha$	$\alpha^2 i$	$-\alpha^3 i$
ρ^3	1	$-i\alpha$	$-\alpha^2$	$i\alpha^3$	i	α	$-\alpha^2 i$	$-\alpha^3$
μ	1	α	α^2	α^3	$-i$	$-i\alpha$	$-\alpha^2 i$	$-\alpha^3 i$
$\mu\rho$	1	$-i\alpha$	$-\alpha^2$	$i\alpha^3$	$-i$	$-\alpha$	$\alpha^2 i$	α^3
$\mu\rho^2$	1	$-\alpha$	α^2	$-\alpha^3$	$-i$	αi	$-\alpha^2 i$	$\alpha^3 i$
$\mu\rho^3$	1	$i\alpha$	$-\alpha^2$	$-i\alpha^3$	$-i$	α	$\alpha^2 i$	$-\alpha^3 i$

Invariant for ρ: i

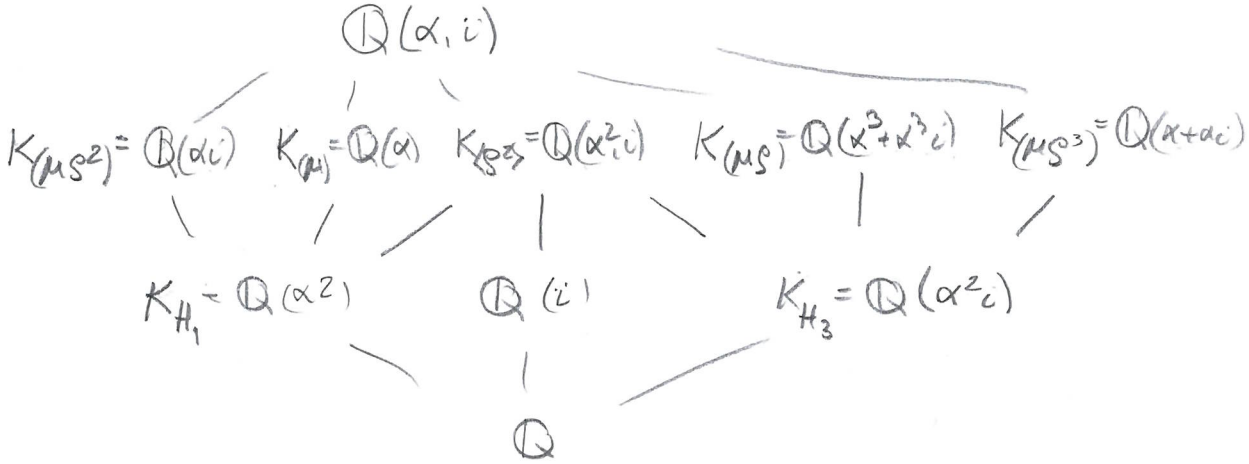
for ρ^2: α^2, i

for μ: α

for $\mu\rho$: $\alpha^3+\alpha^3 i$

for $\mu\rho^2$: $\alpha^2, \alpha i$

for $\mu\rho^3$: $\alpha+\alpha i$



$$(\alpha^3+\alpha^3 i)^2 = \alpha^6 + 2\alpha^6 i - \alpha^6$$
$$= 4\alpha^2 i$$
$$(\alpha+\alpha i)^2 = \alpha^2 + 2\alpha^2 i - \alpha^2$$
$$= 4\alpha^2 i$$