48 1-19
49 1-12

Forelesning, 8. april 2024

Dagens tema: Isomorfier / automorfier av kroppsutvidelser.

Def. 48.1

$F \leq E \Rightarrow \alpha, \beta$ alg. utv. $\quad \operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F) \iff \alpha, \beta$ KONJUGERTE over F.

Ex.

1) $\sqrt{2}$ og $-\sqrt{2}$ er konjugerte over $\mathbb{Q}$

2) $f(x) = x^2 + x + 1 \Rightarrow x = \frac{-1 \pm \sqrt{1-4}}{2} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$

$\alpha = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \qquad \beta = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$

konjugerte

Thm 48.3

F kropp, α, β algebraiske elementer / F, $\deg(\alpha, F) = n$

$$\psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta), \quad \alpha \longmapsto \beta, \quad \psi_{\alpha,\beta}\big|_F = \mathrm{id}_F$$

$\psi_{\alpha,\beta}$ isomorfi $\iff \alpha, \beta$ konjugerte / F

Bevis.

La $\operatorname{irr}(\alpha, F) = f(x)$ og anta $\psi_{\alpha,\beta}$ er iso. Da har vi

$$0 = \psi_{\alpha,\beta}(f(\alpha)) = f(\beta)$$

som betyr $\operatorname{irr}(\alpha, F) \mid \operatorname{irr}(\beta, F)$. Siden $(\psi_{\alpha\beta})^{-1} = \psi_{\beta\alpha}$ har vi $\operatorname{irr}(\beta, F) \mid \operatorname{irr}(\alpha, F) \Rightarrow \operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$ og α, β er konjugerte.

Anta α, β konjugerte, dvs $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F) = f(x)$. Det betyr

$$(f(x)) = \ker \varphi_\alpha \subset F[x] \xrightarrow{\varphi_\alpha} F(\alpha)$$
$$\text{(=)} \quad \text{(=)}$$
$$(f(x)) = \ker \varphi_\beta \subset F[x] \xrightarrow{\varphi_\beta} F(\beta)$$

Vi har $F[x]/_{\ker \varphi_\alpha} \overset{\varphi_\alpha}{\cong} F(\alpha)$ og $F[x]/_{\ker \varphi_\beta} \overset{\varphi_\beta}{\cong} F(\beta)$ som gir isomorfi $\psi_{\alpha\beta} = \varphi_\beta \varphi_\alpha^{-1}$ og $\psi_{\alpha\beta}(\alpha) = \varphi_\beta(\varphi_\alpha^{-1}(\alpha)) = \varphi_\beta(x) = \beta$.

Vi skal bruke dette teoremet på følgende situasjon:

1) α algebraisk$/F$

$$\begin{array}{ccc} F & & F \\ \text{VI} & & \text{VI} \\ F(\alpha) & \xrightarrow[\cong]{\psi} & E \\ \text{VI} & & \text{VI} \\ F & \xrightarrow{=} & F \end{array} \quad \Rightarrow \quad \operatorname{irr}(\psi(\alpha), F) = \operatorname{irr}(\alpha, F)$$

2) $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F) \Rightarrow$

$$\begin{array}{ccc} F & & F \\ \text{VI} & & \text{VI} \\ F(\alpha) & \xrightarrow[\cong]{\exists!\, \psi_{\alpha\beta}} & E \\ \text{VI} & & \text{VI} \\ F & = & F \end{array}$$

$\psi_{\alpha,\beta}(\alpha) = \beta$

Mht. for 1) hvis: $\operatorname{irr}(\alpha, F) = f(x)$ så har vi $f(\alpha) = 0$. Det betyr at $f(\psi(\alpha)) = \psi(f(\alpha)) = 0 \Rightarrow \operatorname{irr}(\psi(\alpha), F) = \operatorname{irr}(\alpha, F)$.

For 2) $\begin{array}{ccc} F(\alpha) & \xrightarrow{\text{iso}} & E \\ \text{VI} & & \text{VI} \\ F & = & F \end{array}$ er bestemt av verdien på α.

Konsekvens.

$f(x) \in \mathbb{R}[x]$

$f(a+ib) = 0 \Rightarrow f(a-ib) = 0$

Bevis $\operatorname{irr}(i, \mathbb{R}) = x^2+1$
$= \operatorname{irr}(-i, \mathbb{R})$

$\Rightarrow i, -i$ er konjugerte

$\Rightarrow \mathbb{R}(i) \xrightarrow[\psi_{i,-i}]{\cong} \mathbb{R}(-i)$ (iso)

$\Rightarrow \psi_{i,-i} f(a+ib) = f(a-ib)$

$\quad\quad\quad \overset{\shortparallel}{0} \Rightarrow \overset{\shortparallel}{0}$

AUTOMORFI $\begin{array}{ccc} \psi: E & \to & E \\ \text{VI} & & \text{VI} \\ F & = & F \end{array}$

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \xrightarrow{\psi_{\sqrt{2},-\sqrt{2}}} & \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}) \\ \text{VI} & & \text{VI} \\ \mathbb{Q} & & \mathbb{Q} \end{array}$$

$\Rightarrow \psi_{\sqrt{2},-\sqrt{2}}(a+\sqrt{2}\,b) = a-\sqrt{2}\,b$ isomorfi

$$\begin{array}{ccc} \psi: E & \longrightarrow & E \\ \text{VI} & & \text{VI} \\ F & = & F \end{array}$$ Automorfi av E som fikserer F.

Thm 48.11 $\psi : E \longrightarrow E$ Automorfi.

$\Rightarrow E_{\{\psi\}} = \{ a \in E \mid \psi(a) = a \} \leq E$

underkropp

Bevis: $a, b \in E_{\{\psi\}} \Rightarrow \psi(a \pm b) = \psi(a) \pm \psi(b) = a \pm b$

$\psi(ab) = \psi(a)\psi(b) = ab$

$\psi\left(\frac{a}{b}\right) = \frac{\psi(a)}{\psi(b)} = \frac{a}{b} \quad b \neq 0$

$\psi(0) = 0, \psi(1) = 1.$

$\Rightarrow E_{\{\psi\}} \leq E$

kropp. □

Kalles fix-kroppen til ψ.

Ex $\mathbb{C}_{\psi i, -i} = \mathbb{R}$, $\mathbb{Q}(\sqrt{2})_{\psi_{\sqrt{2}, -\sqrt{2}}} = \mathbb{Q}$.

Thm 48.14.

Mengden av automorfier av E danner en gruppe under komposisjon

Thm 48.15

$F \leq E$

1) $G(E/F) = \{ \psi : E \xrightarrow{\sim} E \mid \psi|_F = id \} \leq Aut(E)$

2) $F \leq E_{G(E/F)}$

Bevis 1) $\sigma, \tau \in G(E/F) \Rightarrow \sigma \circ \tau(a) = \sigma(\tau(a)) = \sigma(a) = a \quad \forall a \in F.$

$id \in G(E/F)$, $\sigma \in G(E/F) \Rightarrow \sigma^{-1} \in G(E/F)$.

2) opplagt.

Defn 48.16.

$G(E/F)$: Automorfismen av E som fikser F

eller

Automorfismegruppa til E over F

Ex. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ / $\mathbb{Q}(\sqrt{3})$ / $\mathbb{Q}$

$\psi_{\sqrt{2},-\sqrt{2}}(a+\sqrt{2}b) = a-\sqrt{2}b \quad , a,b \in \mathbb{Q}(\sqrt{3})$

$\Rightarrow \quad G\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{3})\right) \simeq \mathbb{Z}_2$

$G\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right) = \{id, \psi_{\sqrt{2},-\sqrt{2}}, \psi_{\sqrt{3},-\sqrt{3}}, \psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}}\} \simeq \mathbb{Z}_2\times\mathbb{Z}_2$

$\Rightarrow \quad \left| G\left(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}\right)\right| = \left[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}\right]$

ordn til gruppa = dimensjon av vektorrom

—o—o—o—

F / E / $F(\alpha)$ / F — $E \xrightarrow{\simeq} E'$, $F(\alpha) \xrightarrow{\psi_{\alpha,\beta}} F(\beta)$, $F \xrightarrow{=} F$

algebraisk utv

Ved Zorns Lemma

Allerede vist

Thm 49.7

F / E / F — $E \xrightarrow{\psi} E'$, $F \xrightarrow{=} F$

Antall isomorfier $E \xrightarrow{\psi} E'$ slik at $\psi|_F = id$ er bestemt av E og F.

$= \{E : F\}$

Kalles INDEKSEN AV E OVER F.

$\Rightarrow$ K / E / F gir $\{K:F\} = \{K:E\}\{E:F\}$

Ex.

$\{\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}\} = \{\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})\} \cdot \{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\}$

$id, \psi_{\sqrt{3},-\sqrt{3}}$ $\qquad$ $id, \psi_{\sqrt{2},-\sqrt{2}}$

Sammenheng mellom $[E:F]$ og $\{E:F\}$

La $E = F(\alpha)$, $\deg(\text{irr}(\alpha, F)) = n$

$$[E:F] = \dim_F(E) = n \quad \text{Basis } \{1, \alpha, \alpha^2, \dots \alpha^{n-1}\}$$

$$\{E:F\} = \#\left(\begin{array}{ccc} F(\alpha) & \overset{\Psi}{\underset{\simeq}{\rightarrow}} & E \\ \text{VI} & & \text{VI} \\ F & = & F \end{array} \right) \Rightarrow E = F(\beta) \text{ hvor } \text{irr}(\alpha, F) = \text{irr}(\beta, F)$$

$\Rightarrow \alpha \longmapsto$ en annen rot i det irreduksible polynomet av grad n.

$$= n$$

$$\Rightarrow [F(\alpha):F] = \{F(\alpha):F\}$$

Ex $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $\alpha^3 = 2 \Rightarrow \alpha = \sqrt[3]{2}$, andre rotter $\omega\alpha, \omega^2\alpha$ $(\omega^3 = 1)$

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

$$\{\mathbb{Q}(\alpha):\mathbb{Q}\} = 3 \; ; \; \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha), \; \mathbb{Q}(\alpha) \to \mathbb{Q}(\omega\alpha) \; \mathbb{Q}(\alpha) \to \mathbb{Q}(\omega^2\alpha)$$

$$G(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{id\} \quad |G(\mathbb{Q}(\alpha)/\mathbb{Q})| = 1$$

$$E = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \simeq \mathbb{Q}(\alpha, \omega)$$

$$[E:\mathbb{Q}] = [E:\mathbb{Q}(\omega)]\,[\mathbb{Q}(\omega):\mathbb{Q}] = 6$$

Basis: $\{1, \alpha, \alpha^2\}$ Basis $\{1, \omega\}$ $\omega^2 = -1 - \omega$

$\omega^2\alpha = \frac{(\omega\alpha)^2}{\alpha}$

$$\{E:\mathbb{Q}\} = 6$$

α	α	α	$\omega\alpha$	$\omega\alpha$	$\omega^2\alpha$	$\omega^2\alpha$
$\omega\alpha$	$\omega\alpha$	$\omega^2\alpha$	α	$\omega^2\alpha$	α	$\omega\alpha$

$$|G(E/\mathbb{Q})| = 6 = \{E:\mathbb{Q}\}$$