GALOIS-TEORI

La $F \leq E$ være en endelig kroppsutvidelse. Vi sier utvidelsen er **normal** hvis den er både en rotkropp og separabel.[1]

For en normal utvidelse gjelder

$$[E : F] = \{E : F\} = |G(E/F)|,$$

hvor den første likheten betyr at utvidelsen er separabel, og den andre at utvidelsen er en rotkropp.

Eksempel. For ethvert polynom $f(x) \in \mathbb{Q}[x]$, vil rotkroppen E til $f(x)$ være en normal utvidelse av $\mathbb{Q}$. For eksempel er rotkroppen til $(x^2-2)(x^2-3)$ lik $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \geq \mathbb{Q}$ en normal utvidelse.

Vi lar nå $F \leq E$ være en normal utvidelse, vi ser på gruppa $G(E/F)$. Vi studerer to typer objekter, på den ene siden undergrupper av $G(E/F)$, på den andre siden kroppsutvidelser av F som er inneholdt i E.

$$\{H \mid H \leq G(E/F)\} \quad \text{og} \quad \{K \mid F \leq K \leq E\}$$

Disse to mengdene har naturlige avbildninger mellom seg: Gitt en gruppe $H \leq G(E/F)$, kan vi se på kroppen av elementer fiksert av alle $\tau \in H$

$$E_H = \{\alpha \in E \mid \tau(\alpha) = \alpha \text{ for alle } \tau \in H\},$$

og vi har $F \leq E_H \leq E$. Motsatt, gitt en kropp K med $F \leq K \leq E$, har vi en gruppe

$$G(E/K) = \{\tau \colon E \to E \mid \tau \text{ fikserer } K\} \leq G(E/F).$$

Teorem (Galois-teoriens fundamentalteorem)**.** *La $F \leq E$ være en endelig normal kroppsutvidelse. Vi har inverse bijeksjoner mellom mengden av undergrupper av $G(E/F)$ og mengden av kropper K med $F \leq K \leq E$:*

$$\{H \mid H \leq G(E/F)\} \leftrightarrow \{K \mid F \leq K \leq E\}$$
$$H \mapsto E_H$$
$$G(E/K) \hookleftarrow K$$

Disse tilfredsstiller

(1) *Inklusjoner reverseres:*

$$H_1 \leq H_2 \leq G \Rightarrow E_{H_2} \leq E_{H_1}$$

og

$$F \leq K_1 \leq K_2 \leq E \Rightarrow G(E/K_2) \leq G(E/K_1).$$

(2) *Ordenen til undergruppen H er lik graden til utvidelsen $K \leq E$*

$$|H| = [E : E_H]$$

og

$$[E : K] = |G(E/K)|$$

[1] Vi følger Fraleighs terminologi her, men merk at det ellers er vanligere å kalle en utvidelse som er både rotkropp og separabel for en **Galois**-utvidelse.

(3) *Normale undergrupper av $G(E/F)$ svarer til rotkropper K, det vil si gitt $H \leq G$, har vi*

$$H \leq G \text{ normal} \Leftrightarrow E_H \text{ er en rotkropp over } F,$$

og gitt K med $F \leq K \leq E$, har vi

$$K \text{ er rotkropp over } F \Leftrightarrow G(E/K) \leq G(E/F) \text{ normal.}$$

(4) *Hvis $H \leq G(E/F)$ er normal, så er*

$$G(E/F)/H \simeq G(E_H/F)$$

Skisse av bevis. Vi vil vise at $H \mapsto E_H$ og $K \mapsto G(E/K)$ er inverse bijeksjoner, det vil si at vi har

$$G(E/E_H) = H \text{ og } E_{G(E/K)} = K.$$

Det er lett å se fra definisjonen at

$$H \subseteq G(E/E_H),$$

altså: Hvis $\tau \in H$, og $\alpha \in E_H$, så er $\tau(\alpha) = \alpha$ per definisjon av E_H. Siden dette gjelder for alle $\alpha \in E_H$, så er $\tau \in G(E/E_H)$, og siden dette gjelder for alle $\tau \in H$, er $H \subseteq G(E/E_H)$. Vi kan nå bruke "Artins lemma" (som vi ikke skal vise), som sier at

$$[E : E_H] \leq |H|.$$

Siden $H \subseteq G(E/E_H)$ og $|H| \leq [E : E_H] = |G(E/E_H)|$, må vi da ha $H = G(E/E_H)$.

Vi viser nå

$$K = E_{G(E/K)},$$

Hvis $\alpha \in K$, så har vi for alle $\tau \in G(E/K)$ at $\tau(\alpha) = \alpha$, dermed er $\alpha \in E_{G(E/K)}$.

Det gjenstår å vise at hvis $\alpha \in E$ med $\alpha \notin K$, så er $\alpha \notin E_{G(E/K)}$. Enhver $\alpha \in E \setminus K$ er algebraisk over K av grad ≥ 2. Siden $K \leq E$ er separabel, finnes en konjugert $\beta \neq \alpha$ i E, og det finnes en isomorfi $\psi_{\alpha,\beta} \colon K(\alpha) \to K(\beta)$, som ved isomorfiutvidelsesteoremet kan utvides til en $\tau \in G(E/K)$ med $\tau(\alpha) = \beta$. Siden $\tau(\alpha) \neq \alpha$, er $\alpha \notin E_{G(E/K)}$.

For resten av teoremet:

(1) Følger enkelt fra definisjonene.
(2) Dette er Artins lemma nevnt over.
(3) Man sjekker at for $\tau \in G(E/F)$ har vi

$$\tau G(E/K)\tau^{-1} = G(E/\tau(K)).$$

Videre viser man følgende ekvivalenser

$$\begin{gathered} K \text{ er en rotkropp over } F \\ \Updownarrow \\ \tau(K) = K \text{ for alle } \tau \in G(E/F) \\ \Updownarrow \\ \tau G(E/K)\tau^{-1} = G(E/K) \text{ for alle } \tau \in G(E/F) \\ \Updownarrow \\ G(E/K) \leq G(E/F) \text{ er normal.} \end{gathered}$$

(4) Siden H er normal, er E_H en rotkropp over F ved punkt 3. Dermed vil enhver $\tau \in G(E/F)$ gi en automorfi $\tau|_{E_H} \in G(E_H/F)$. Avbildningen $G(E/F) \to G(E_H/F)$ definert av $\tau \mapsto \tau|_{E_H}$ er en gruppehomomorfi, surjektiv ved isomorfiutvidelsesteoremet, og med kjerne
$$G(E/E_H) = H.$$
Dermed får vi $G(E/F)/H \simeq G(E_H/F)$.

□

Eksempel. For enhver endelig normal utvidelse $F \leq E$ har vi undergruppene $\{e\} \leq G(E/F)$ og $G(E/F) \leq G(E/F)$, og vi har
$$E_{\{e\}} = E, \qquad E_{G(E/F)} = F.$$

Eksempel. Utvidelsen $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ har Galoisgruppe $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}, \psi_{\sqrt{2},-\sqrt{2}}\} \simeq \mathbb{Z}_2$. Denne har to undergrupper som svarer til kroppene $\mathbb{Q}$ og $\mathbb{Q}(\sqrt{2})$.

Eksempel. For utvidelsen $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, har vi beregnet at
$$G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\psi_{00}, \psi_{01}, \psi_{10}, \psi_{11}\},$$
hvor, for $a, b, c, d \in \mathbb{Q}$,
$$\psi_{ij}(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + (-1)^i b\sqrt{2} + (-1)^j\sqrt{3} + (-1)^{i+j}\sqrt{6}$$
Denne Galois-gruppa er isomorf med $\mathbb{Z}_2 \times \mathbb{Z}_2$. Den har fem undergrupper:
$$\{\psi_{00}\}, \quad \langle\psi_{10}\rangle, \quad \langle\psi_{01}\rangle, \quad \langle\psi_{11}\rangle, \quad G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}).$$
De tilhørende mellomkroppene er
$$\begin{aligned} E_{\{\psi_{00}\}} &= \mathbb{Q}(\sqrt{2}, \sqrt{3}), \\ E_{\langle\psi_{10}\rangle} &= \mathbb{Q}(\sqrt{3}), \\ E_{\langle\psi_{01}\rangle} &= \mathbb{Q}(\sqrt{2}), \\ E_{\langle\psi_{11}\rangle} &= \mathbb{Q}(\sqrt{6}), \\ E_{G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})} &= \mathbb{Q}. \end{aligned}$$
For eksempel fikserer ψ_{10} elementene i $\mathbb{Q}(\sqrt{3})$, mens den sender $\sqrt{2}$ til $-\sqrt{2}$. Tilsvarende fikserer ψ_{01} kroppen $\mathbb{Q}(\sqrt{2})$, og ψ_{11} fikserer kroppen $\mathbb{Q}(\sqrt{6})$. Siden $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ er abelsk, er alle undergruppene normale, og derfor er alle mellomkroppene rotkropper over $\mathbb{Q}$.