Eksempler:

$f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$

irreduksibel !

$F = \mathbb{Z}_2[x]/(f(x)) \simeq GF(8)$

Elementer: $\{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_2\}$

$\alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 1$ $(\text{char } \mathbb{Z}_2 = 2)$

$(\alpha = x + (f(x)))$

$g(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$ irreduksibel !

$GF(27) = \mathbb{Z}_3[x]/(g(x))$ Elementer $\{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_3\}$

$\alpha^3 + 2\alpha + 1 = 0$

$\alpha^3 = -2\alpha - 1 = \alpha + 2$

Teorem 4.4.

p primtall $n \geq 1$.

La $h(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$, og la E være rotkroppen til $h(x)$

(altså $\mathbb{Z}_p \subseteq E$ og E minste kroppsutvidelse som inneholder alle røttene til h).

Da er alle røttene til $h(x)$ i E forskjellige, og $E = \{\text{røttene til } h(x)\}$, altså $|E| = p^n$.

Eks:

La $h(x) = x^4 - x = x^4 + x \quad \in \mathbb{Z}_2[x]$

$GF(2^2)$ er rotkroppen til h

$h(x) = \underbrace{x(x+1)}_{\text{har rotter i } \mathbb{Z}_2}(x^2+x+1) \Rightarrow$ La $\alpha = x + (x^2+x+1)$ i $\mathbb{Z}_2[x]/(x^2+x+1) = E$

$\alpha^2 = \alpha + 1$

$(\alpha+1)^2 + \alpha + 1 + 1 = \alpha^2 + 1 + \alpha + 1 + 1$

$= \alpha + 1 + 1 + \alpha + 1 + 1 = 0.$

Elementene i E er $\{0, 1, \alpha, \alpha+1\}$ ($\alpha+1 = \alpha^2$)

så E er rotkroppen til $h(x)$ = rotkroppen til x^2+x+1

NB! La E være rotkroppen til $h(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$

La $p(x) \in \mathbb{Z}_p[x]$ være irredusibel av grad n.

Da er $\mathbb{Z}_p[x]/(p(x))$ en kropp med p^n elementer så

$\alpha^{p^n} - \alpha = 0$ for alle $\alpha \in \mathbb{Z}_p[x]/(p(x))$ $\Rightarrow$ Alle α rot i $x^{p^n} - x = 0$

Dermed $p(x) \mid h(x)$.

Oppgave: (øving 4) $p(x) \in \mathbb{Z}_p[x]$ irredusibel med $d = \deg p(x)$

Da er $p(x) \mid h(x) = x^{p^n} - x$

$\Leftrightarrow d \mid n$

Eks: Over $\mathbb{Z}_2$ har vi $x^{16} - x$

$= x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

Bevis: $h'(x) = p^n x^{p^n-1} - 1 = -1$ (siden char $E = p$)

$\Rightarrow$ ingen multiple røtter!

La $\alpha, \beta \in E$ være røtter

Char $E = p \Rightarrow (\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \alpha^{p^n} = \alpha \pm \beta$ $\Rightarrow \alpha \pm \beta$ rot

$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$

$(\alpha\beta^{-1})^{p^n} = \alpha\beta^{-1}$ $\Rightarrow \alpha\beta^{-1}$ rot

Mengden av røtter er en underkropp av E,
men må da være lik E, siden E er pr. def. den minste
kroppen som omholder alle røttene, siden røttene er
forskjellige: $|E| = p^n$.

Korollar: Det finnes en kropp med p^n elementer
for alle primtall p og alle $n \geq 1$, altså
en kroppsutvidelse $\mathbb{Z}_p \subseteq E$ med $[E : \mathbb{Z}_p] = n$.

Teorem 4.5. F kropp med p^n elementer og $m \geq 1$.
Da finnes en kroppsutvidelse $F \subseteq E$ med
$[E : F] = m$.

Bevis: (se bok)

Litt gruppeteori.

(1) G endelig gruppe, $g \in G$. Ordenen til g er minste n slik at $g^n = 1$, og vi må ha $n \mid |G|$. (Lagrange)

(2) Eksponenten til G, $e(G)$ er minste n s.a. $g^n = 1$ for alle $g \in G$
$= m.f.m$ (ordenen til alle elementer)
(Eks: $e(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$ $e(\mathbb{Z}_4) = 4$)
Merk: $e(G) \mid |G|$

(3) Hvis G er en endelig abelsk gr $(\Rightarrow G \simeq \mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_t^{r_t}})$
finnes et element $g \in G$ s.a. ordenen til G er $e(G)$ ($g = (1, \dots, 1)$ har orden $\operatorname{lcm}\{p_i^{r_i}\} = e(G)$.

(Eks. $\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_8 = G$ $e(G) = 9 \cdot 8 = 72$.)
$\mathbb{Z}_9 \times \mathbb{Z}_8 = G$ $e(G) = 72 \Rightarrow G$ syklisk)
$\simeq \mathbb{Z}_{72}$

(4) G er syklisk $\Leftrightarrow e(G) = |G|$

Teorem 4.6.

F endelig kropp. Da er $F^* = F \setminus \{0\}$ en syklisk gruppe (under mult. i F)

Bevis: La $e = e(F^*)$. Da er $\alpha^e = 1$ $\forall \alpha \in F^*$, så alle elementer i F er rot av $t(x) = x^e - 1$, som har $\le e$ røtter. Altså $|F^*| \le e$.
Men $e \mid |F^*| \Rightarrow e = |F^*| \Rightarrow F^*$ er syklisk.

Eksempel: $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ irreducibel.
$\Rightarrow F[x] = \mathbb{Z}_3[x]/(x^2+1)$ kropp med $3^2 = 9$ elementer.
$\alpha = x + I$ alg. over $\mathbb{Z}_3$ med minimal polynom $f(x)$ ($\alpha^2 + 1 = 0$, $\alpha^2 = -1$, $\alpha^4 = 1$, α ikke generator)
$F = \mathbb{Z}_3(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_3\}$
$F^* = \{1, -1, \alpha, -\alpha, 1+\alpha, 1-\alpha, -1+\alpha, -1-\alpha\}$
$(1+\alpha)^2 = -\alpha$ $(1+\alpha)^4 = -1$
$(1+\alpha)^3 = 1-\alpha$ $\Rightarrow 1+\alpha$ generator for F^*.

Kor. 4.7

F end. kropp og $F \subseteq E$ endelig kroppsutvidelse.

Da finnes $\alpha \in E$ slik at $E = F(\alpha)$

Bevis: $[E] < \infty \Rightarrow E^*$ syklisk, dvs $E^* = \langle \alpha \rangle$

$\Rightarrow E = F(\alpha)$ (den minste under kroppen som inneholder α, inneholder α^i for alle i, altså hele E.

Teorem 4.8.

La F være endelig kropp, og la $n \in \mathbb{N}$. Da finnes et irred. polynom av grad n.

Bevis: Teo 4.5 $\Rightarrow \exists\, E \supseteq F$ med $[E:F] = n$

4.7 $\Rightarrow E = F(\alpha)$ for en $\alpha \in E$

La $p(x)$ være min. polynomet til α over F

$\Rightarrow [F(\alpha):F] = n = \deg p(x)$.

$(F(\alpha) = E)$.

Separable utvidelser

Definisjoner. (F kropp)

(1) Et irredusibelt polynom i $F[x]$ kalles separabelt, dersom alle røttene i rotkroppen er enkle, dvs $p(x)$ har ingen multiple røtter.

(2) Et generelt polynom $f(x) \in F[x]$ er separabelt dersom alle irreduserbe faktorer i $f(x)$ er separable.

(3) $F \subseteq E$ kroppsutvidelse, $\alpha \in E$ alg. over F. Da kalles α separabel, hvis min.-polynomet er separabelt

(4) $F \subseteq E$ separabel kroppsutvidelse, hvis hver $\alpha \in E$ er separabel (NB! $\Rightarrow E$ algebraisk)

(5) F perfekt kropp, dersom alle algebraiske kroppsutvidelser $F \subseteq E$ er separable.

Husk: Teorem 3.5 $\Rightarrow$

Hvis $\text{char } F = 0$ er alle irred. polynomer over F separable $\Rightarrow$ F er en perfekt kropp.

Skal se: endelige kropper er også perfekte

Anta $F = GF(p^n)$

La $p(x) \in F[x]$ være et irred. polynom.

Anta at $p(x)$ har en multippel rot.

Cor 3.5. $\Rightarrow$ det finnes et polynom $g(x) \in F[x]$

s.a. $p(x) = g(x^p)$

Skriv $g(x) = a_t x^t + \dots + a_1 x + a_0 \quad (a_i \in F)$

Husk: $a^{p^n} = a$ for alle $a \in F$

Teor. 4.3. $p(x) = g(x^p) =$

$$= a_t x^{pt} + \dots + a_1 x^p + a_0$$

$$= a_t^{p^n} x^{pt} + \dots + a_1^{p^n} x^p + a_0^{p^n}$$

$$= \left(a_t^{p^{n-1}} x^t\right)^p + \dots + \left(a_1^{p^{n-1}} x\right)^p + \left(a_0^{p^{n-1}}\right)^p$$

$$= \left(a_t^{p^{n-1}} x^t + \dots + a_1^{p^{n-1}} x + a_0^{p^{n-1}}\right)^p$$

$\uparrow$

$\text{char } F = p$

Motsier at $p(x)$ er irreduserbel.

$\Rightarrow$ $p(x)$ er separabel

$\Rightarrow$ Hver alg. utvidelse av F er separabel

$\Rightarrow$ F er perfekt.

Altså: Endelige kropper og kropper F med $\text{char } F = 0$ er perfekte

Teorem 5.2.

F kropp og $F \subseteq E$ endelig separabel utvidelse.

Da er E en simpel utvidelse, altså $E = F(\alpha)$ for $\alpha \in E$.

Bevis: Hvis $|F| < \infty$, dette er kor. 4.7.

Dette anta $|F| = \infty$.

Siden E er en endelig ekstensjon, så er E end.gen over F

(La $\{\alpha_i\}$ være basis til $E \setminus F$, da er $E = F(\alpha_i, \gamma)$

La $E = F(\alpha_1, \dots, \alpha_n)$.

Per induksjon: kun anta $n = 2$. $E = F(\alpha, \beta)$

La $p_\alpha(x), p_\beta(x) \in F[X]$ være min. polynomene til α, β.

La $\alpha_1, \dots, \alpha_s$ være røttene til $p_\alpha(x)$ og

$\beta_1, \dots, \beta_t$ —"— til $p_\beta(x)$. (i E) (og $\alpha_1 = \alpha$, $\beta_1 = \beta$ i E)

Siden E separabel er $\alpha_i \neq \alpha_j$ og $\beta_i \neq \beta_j$ når $i \neq j$.

Påstand: det finnes en $\gamma \in F$ s.a. $\gamma \neq \frac{\alpha_i - \alpha_1}{(\beta_1 - \beta_j)}$ for alle i, j

Følger av at $|F| = \infty$.

La $w = \gamma\beta + \alpha$ $(= \gamma\beta_1 + \alpha_1)$

$\neq \gamma\beta_j + \alpha_i$ $\forall i, j$.

Har da $F \subseteq F(w) \subseteq E$. Påstår $F(w) = E$.

La $q(x) = p_\alpha(w - \gamma x) \in F(w)[x]$ (Husk $\gamma \in F$)

Har da $q(\beta) = p_\alpha(w - \gamma\beta) = p_\alpha(\alpha) = 0$

For $j \neq 1$, har vi $q(\beta_j) = p_\alpha(w - \gamma\beta_j) \neq 0$ siden

$w - \gamma\beta_j = \gamma\beta + \alpha - \gamma\beta_j \neq \alpha_i$ $\left(\gamma \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}\right)$

Betrakt $p_\beta(x)$ som polynom i $F(w)[x]$.

La $f(x) \in F(w)[x]$ være min. pol. til β over $F(w)$.

Da har vi $f(x) \mid q(x)$ (siden $q(\beta)=0$).

og $f(x) \mid p_\beta(x)$ (husk $p_\beta(x)$ min. pol. til β over F).

Dermed: enhver rot i $f(x)$ er rot i både $q(x)$ og $p_\beta(x)$.

Vi har vist: $q(\beta_j) \neq 0$ for $j \neq 1$, der $\{\beta_j\}$ er røttene til $p_\beta(x)$.

Altså har $f(x)$ bare én rot, og dermed $f(x) = x - \beta$

(separabel $\Rightarrow$ simple røtter, monisk siden minimalpolynom).

$\Rightarrow \beta \in F(w)$

$\Rightarrow \alpha - \gamma\beta \in F(w)$ $\quad (\gamma \in F,\ \beta, w \in F(w))$

$\Rightarrow F(\alpha,\beta) \subseteq F(w)$

$F(w) \subseteq F(\alpha,\beta)$ siden $w \in F(\alpha,\beta)$

Altså $F(\alpha,\beta) = F(w)$.

Oppgave:

a) Det finnes to grupper av orden 6.
Hva er de? Finn elementene og undergruppene. Hvilke undergrupper er normale?

b) La $f(x) = x^3 - 2 \in \mathbb{Q}[x]$
Vis at røttene er $E = \mathbb{Q}(2^{1/3}, \omega)$, der $\omega^3 = 1$.
Forklar hvorfor $[E:\mathbb{Q}] = 6$ og finn basis for E over $\mathbb{Q}$.

c) La $G = G(E/\mathbb{Q}) = \{\sigma \in Aut_{\mathbb{Q}}(E)\}$ - alle $\mathbb{Q}$-automorfier $\sigma: E \to E$
$\sigma|_{\mathbb{Q}} = id_{\mathbb{Q}}$

Husk røttlemma: [$g(x) \in \mathbb{Q}(x)$ $\alpha \in E$ rot i $g(x) \Rightarrow \sigma(\alpha)$ rot i $g(x)$, når σ er $\mathbb{Q}$-automorfi].

- Beskriv de seks elementene $\{\sigma_i\}$ i G (skal se $|G(E/\mathbb{Q})| = [E:\mathbb{Q}]$.
- Beskriv $\langle\sigma_i\rangle$-undergruppa generert av hver σ_i

d) Hvilken av gruppene i a) er G isomorf med?

e) For hver undergruppe $H \leq G$, finn $E_H = \{x \in E \mid \sigma(x) = x \ \forall \sigma \in H\}$
For hvilke H er E_H en normal utvidelse av $\mathbb{Q}$?
(og hvorfor $E_H \subseteq E$ - undergrupp)

b) Rotkroppen til $f(x) = x^3 - 2$

$f(x)$ har røttene $\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}$ der $w = e^{\frac{2\pi i}{3}}$

$$\mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}) = \mathbb{Q}(w, \sqrt[3]{2})$$

$\subseteq$ ok

$\supseteq$ ok, siden $w = \frac{w\sqrt[3]{2}}{\sqrt[3]{2}}$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ med minimalpolynom $f(x)$

$[\mathbb{Q}(w, \sqrt[3]{2}) : \mathbb{Q}] = 2$ med min.pol. $g(x) = x^2 + x + 1$

Siden $x^3 - 1 = (x-1)(x^2+x+1)$

så w, w^2 er rot i $g(x)$ og

$g(x)$ er irred. siden i $\mathbb{Q}(\sqrt[3]{2})$

(siden ingen reelle røtter)

Basis for $\mathbb{Q}E$ blir da

$$\{1, 2^{1/3}, 2^{2/3}, w, w2^{1/3}, w2^{2/3}\}$$

$\sigma \in Aut_{\mathbb{Q}}(E)$ bestemt av $\sigma(2^{1/3}) \in \{2^{1/3}, w2^{1/3}, w^2 2^{1/3}\}$

og $\sigma(w) \in \{w, w^2\}$.

Dette gir seks mulige valg av σ

Siden $|G(E/\mathbb{Q})| = 6$ må hver av de seks mulighetene

være ok (dvs. automorfier)

	$2^{1/3}$ ↓	w ↓	orden
$\sigma_1 = id$	$2^{1/3}$	w	1
σ_2	$w2^{1/3}$	w	3
σ_3	$w^2 2^{1/3}$	w	3
σ_4	$2^{1/3}$	w^2	2
σ_5	$w2^{1/3}$	w^2	2
σ_6	$w^2 2^{1/3}$	w^2	2

$2^{1/3} \xrightarrow{\sigma_5} w2^{1/3} \xrightarrow{\sigma_5} (w^2)(w2^{1/3}) = 2^{1/3}$

$w \xrightarrow{\sigma_5} w^2 \xrightarrow{\sigma_5} w^4 = w$

(Tilsvarende for σ_6)

Altså har $H_{\sigma_2} = \langle \sigma_2 \rangle$

og H_{σ_3} har orden 3

og $H_{\sigma_4}, H_{\sigma_5}, H_{\sigma_6}$ har orden 2

a) d) Sammenlign med S_3.

$(1,2), (2,3), (3,1)$ har orden 2.

$(1,2,3), (1,3,2)$ — " — 3

$\langle (1,2) \rangle = \{id, (1,2)\}$ ikke normal undergruppe

mens

$\langle (1,2,3) \rangle = \langle (1,3,2) \rangle$ har orden 3, og er dermed normal

Hva med $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

$|\langle 1 \rangle| = 6 = |\langle 5 \rangle|$ alle undergrupper normale, siden

$|\langle 2 \rangle| = |\langle 4 \rangle| = 3$ $\mathbb{Z}_6$ er abelsk

$|\langle 3 \rangle| = 2$

d) Altså er $G(E/\mathbb{Q}) \cong S_3$.

e) $E_{\langle \sigma_2 \rangle} = E_{\langle \sigma_3 \rangle} = Sp\{1, w^2\}$

$= \mathbb{Q}(w)$ – normal utvidelse siden røtter i x^2+x+1

$E_{\langle \sigma_1 \rangle} = \mathbb{Q}(2^{1/3})$

$E_{\langle \sigma_5 \rangle} = \mathbb{Q}(w2^{1/3})$

$E_{\langle \sigma_6 \rangle} = \mathbb{Q}(w^2 2^{1/3})$

} ikke-normale utvidelser

Merk:

$G(E/E_{\langle \sigma_2 \rangle}) \leq G(E/\mathbb{Q})$ $\quad \mathbb{Q} \subseteq E$

$\langle \sigma_2 \rangle = \{\sigma_1, \sigma_2, \sigma_3\}$ undergruppe.

Normal (siden index 2)

$G(E/E_{\langle \sigma_4 \rangle}) \subseteq G(E/\mathbb{Q})$

$\{\sigma_1, \sigma_4\} = \langle \sigma_4 \rangle$

ikke-normal undergruppe