x^3+x^2+x+1
$-1 \quad 1 \quad -1$

Eksempel.

p primtall. $\Phi_p(x) = x^{p-1} + \dots + x + 1 \in \mathbb{Q}[x]$

Påstand I. $\Phi_p(x)$ er irreduksibel

Triks I $\quad \Phi_p(x) = (x^p - 1)/(x-1)$

Triks II $\quad g(x) = \Phi_p(x+1) = \frac{1}{x}\left(x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x\right)$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}$$

Eisensteins kriterium (med p): $\left(p^2 \nmid \binom{p}{p-1} = \frac{p!}{(p-1)!} = p\right)$

$\Rightarrow$ $g(x)$ irreduksibel $\Rightarrow$ $\Phi_p(x)$ irreduksibel.

Siden $x^p - 1 = (x-1)\Phi_p(x)$ er røttene til $\Phi_p(x)$ $\{\alpha^i \mid 1 \le i \le p-1\}$

der $\alpha = e^{2\pi i/p}$

Dermed $\mathbb{Q}(\alpha)$ inneholder alle røttene til $\Phi_p(x)$ og er altså rotfeltet til $\Phi_p(x)$, og dermed en normal ekstensjon. Den er også endelig og separabel, så en Galois ekstensjon.

GT $\Rightarrow$ $|G(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha):\mathbb{Q}] = p-1$ $(= \deg \Phi_p(x))$

og $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \dots + a_{p-2}\alpha^{p-2} \mid a_i \in \mathbb{Q}\}$.

Hvis $\sigma \in G = G(\mathbb{Q}(\alpha)/\mathbb{Q})$ $\Rightarrow$ σ bestemt av $\sigma(\alpha)$

($\sigma(a) = a$ $a \in \mathbb{Q}$, $\sigma(\alpha^i) = \sigma(\alpha)^i$).

Påstand II La $\sigma_i(\alpha) = \alpha^i$

Da er $\sigma_i : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ en automorfi

for $i = 1, \dots, p-1$.

(sjekk).

Dermed blir $G(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{\sigma_i\}_{i=1}^{p-1}$, siden $|G(\mathbb{Q}(\alpha)/\mathbb{Q})| = p-1$.

Påstand III $G(\mathbb{Q}(\alpha)/\mathbb{Q})$ er syklisk!

Husk (fra tallteori): Ethvert primtall p har en primitiv rot t $(1 < t < p)$ dvs.

$\{t, t^2, \dots, t^{p-1}\} = \{1, 2, \dots, p-1\}$ mod p.

($\mathbb{Z}_p^*$ syklisk gruppe).

$\langle t \rangle$

Vi har $\sigma_t^j(\alpha) = (\alpha^t)^j = \sigma_{t^j}(\alpha)$

Dermed $\{\sigma_t^1, \dots, \sigma_t^{p-1}\} = \{\sigma_1, \dots, \sigma_{p-1}\}$ (husk $\alpha^p = 1$)

Altså er $G(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma_t \rangle$ der t er gen. for $\mathbb{Z}_p^*$

NB! ~~$\mathbb{Q}(x) : x^3$~~

$f(x) = x^3 + x^2 + x + 1$ er ikke irreducibel!

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

18.1. Enhetsrøtter og syklotomiske polynomer.

Def: Et element w i en kropp F kalles en n'te enhetsrot, dersom $w^n = 1$, og en primitiv n'te enhetsrot, dersom i tillegg $w^m \neq 1$ for $1 \leq m < n$

NB! Det vil alltid finnes enhetsrøtter til 1 (for enhver n), i en kropp eller alg. tilluknung av F (rot i $f(x) = x^n - 1$),
men (skal se): det finnes ikke nødvendigvis primitive enhetsrøtter.

Teorem 1.1 F kropn

a) U en endelig undergr. av $F^* = F \setminus \{0\} \Rightarrow U$ er syklisk.

b) Røttene til $f(x) = x^n - 1 \in F[x]$ danner en syklisk gruppe

NB! (Spesielt F endelig kropp $\Rightarrow F^*$ syklisk (vet tidligere i kap 16.4)

Bevis: U er en abelsk endelig gruppe, så

$U \cong U_1 \times U_2 \times \dots \times U_K$ der U_i er gruppe av orden $p_i^{r_i}$
for $i = 1, \dots, K$ og $p_i \neq p_j$ (når $i \neq j$)
primtall

Påstår at hver U_i er syklisk

La $a \in U_i$ være elm med maksimal orden i U_i. Da må

$O(a) = p_i^{s_i}$ for $s_i \leq r_i$ (Lagrange).

Vi har at $O(x) = p_i^{t_i}$ for $t_i \leq s_i$ for hvert elm $x \in U_i$

Altså $x^{p_i^{t_i}} = e = \left(x^{p_i^{t_i}}\right)^{p_i^{(s_i - t_i)}} = e = x^{p_i^{s_i}}$.

Altså: $x^{p_i^{s_i}} = e \quad \forall x \in U_i$. Men $x^{p_i^{s_i}} = 1$ har høyst $p_i^{s_i}$ røtter,
og U_i har $p_i^{r_i}$ elementer så $r_i \leq s_i$

Altså $r_i = s_i$, og U_i er syklisk.

Dermed er også U syklisk (oppgave: U_1, U_2 syklisk av orden $p_i^{r_i} \Rightarrow U_1 \times U_2$ syklisk av orden $p_1^{r_1} p_2^{r_2}$.)

b) Røttene danner også en gruppe $\alpha^n = 1 = \beta^n \Rightarrow (\alpha\beta)^n = 1$

$(\alpha\alpha^{-1} = 1, \alpha^n = 1 \Rightarrow (\alpha^{-1})^n = 1 \ldots)$

og har $\leq n$ elementer (NB! her ikke sagt at vi faktisk har enkle røtter)

Teorem 1.2.

F kropp $n \in \mathbb{Z}_+$ Da er $\operatorname{Char} F = 0$ eller $\operatorname{Char} F \nmid n$ $\Leftrightarrow$ det finnes en primitiv n'te enhetsrot i en kroppsutvidelse E av F

Bevis: La $f(x) = x^n - 1 \in F[x]$

$\Rightarrow f'(x) = n x^{n-1}$

Kap 16.4

$\Rightarrow$) $\operatorname{Char} F = 0$ v $\operatorname{Char} F \nmid n \Rightarrow f'(x) \neq 0 \Rightarrow n$ forskjellige røtter

Teo 1.1

$\Rightarrow$ gruppa H av røtter er syklisk gr. med n elementer

$\Rightarrow \exists$ generator w for H, dvs $w^n = 1$ og $w^m \neq 1$ for $|m| < n$

$\Rightarrow w$ er primitiv rot.

$\Leftarrow$) Motsatt. Anta w primitiv n-te rot $\Rightarrow 1, w, w^2, \ldots w^{n-1}$ for n forskjellige røtter $\Rightarrow f(x)$ har ikke multiple røtter $\Rightarrow$ (Kap 16.4) $f'(x) \neq 0$

$\Rightarrow n x^{n-1} \neq 0$

$\Rightarrow \operatorname{Char} F \nmid n$ eller $\operatorname{Char} F = 0$.

Def: $n \in \mathbb{Z}_+$ F kropp med $\operatorname{char} F = 0$ eller $\operatorname{char} F \nmid n$

$$\Phi_n(x) = \prod_{w} (x - w)$$

Kalles det n'te cyklotomiska polynomet.

w prim. n'te enhetsrot

$\mathbb{Q} = F$

Ex: $\Phi_1(x) = x - 1$ $\quad \Phi_2(x) = x + 1$

$\Phi_4(x) = x^2 + 1 = (x - i)(x + i)$

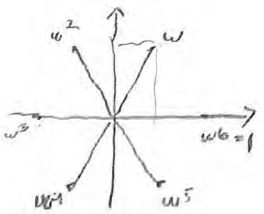
$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ när p primtal

eftersom p'te rötterna av gruppen av ordning p,

$\Rightarrow$ Lagrange alla element (utom identiteten) har ordning p

och vi vet $x^p - 1 = \prod_{\text{enhetsrot}} (x - u) = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$.

Ex: $\Phi_6(x) = ?$



w, w^5 är primitiva.

$(x - w)(x - w^5) = x^2 - (w + w^5)x + 1 =$

$x^2 - x + 1$

$w = \frac{1}{2} + \frac{\sqrt{3}}{2} i$ $\Rightarrow$ $w + w^5 = 1$

$w^5 = \frac{1}{2} - \frac{\sqrt{3}}{2} i$

Husk (talteori): Eulers totient / Φ-funktion.

n heltal > 0

$\phi(n)$ = antal pos. heltal $< n$ som är rel. prima till n

$\phi(p) = p - 1$ p primtal

$\phi(p^k) = p^k - p^{k-1}$

$\phi(p_1^{r_1} \cdots p_t^{r_t}) = \prod \phi(p_i^{r_i})$

Thm: $\mathbb{Z}_n$ har $\phi(n)$ generatorer.

Teorem 1.3.

$\Phi_n(x) = \prod_{\omega} (x-\omega) \in \mathbb{C}[x]$ er

ω primitiv n'te enhetsrot

et irreduserbelt polynom av grad $\varphi(n)$ i $\mathbb{Z}[x]$

Bevis:

I. $\Phi_n(x) \in \mathbb{Q}[x]$

La E være rotkroppen til $x^n - 1 \in \mathbb{Q}[x]$

E er da en Galois utvidelse (endelig, rotkropp ($\Rightarrow$ normal), separabel (siden $\operatorname{char} \mathbb{Q} = 0$))

$\Rightarrow$ Fikspunktkroppen til $G(E/\mathbb{Q})$ er $\mathbb{Q}$

FTGT

La $\sigma \in G(E/\mathbb{Q})$ ω primitiv n'te rot

$\Rightarrow$ $\sigma(\omega)$ primitiv n'te rot [forts: $\sigma(\omega^m) = (\sigma(\omega))^m$]

La $\sigma^* : E[x] \to E[x]$

være gitt ved $\sum a_i x^i \mapsto \sum \sigma(a_i) x^i$

σ^* anvendt på $\Phi_n(x)$ vil da bare permutere faktorene $(x-\omega)$

dermed $\sigma(a_i) = a_i$ for koeffisientene til $\Phi_n(x)$

$\Rightarrow a_i \in \mathbb{Q}$. $\Rightarrow \Phi_n(x) \in \mathbb{Q}[x]$

II. $\Phi_n(x) \in \mathbb{Z}[x]$.

Vi har $x^n - 1 = h(x) \cdot \underbrace{\Phi_n(x)}_{\text{monisk}}$ $\Rightarrow$ $h(x)$ monisk.

m $h(x) = \bar{h}(x)$ $\bar{h}(x) \in \mathbb{Z}[x]$ m = mfm av koeff. i h

n $\Phi_n(x) = \bar{\Phi}_n(x)$ $\bar{\Phi}_n(x) \in \mathbb{Z}[x]$

$\bar{h}(x) = r\bar{\bar{h}}(x)$ $\bar{\bar{h}}(x) \in \mathbb{Z}[x]$ primitiv r = gcd av koeff. i $\bar{h}$

$\bar{\Phi}_n(x) = s\bar{\bar{\Phi}}_n(x)$ $\bar{\bar{\Phi}}(x) \in \mathbb{Z}[x]$ —"—

$$x^n - 1 = h(x)\,\Phi_n(x) = \frac{rs}{mn}\,\bar{h}(x)\,\bar{\Phi}_n(x) \xrightarrow{\text{Gauss-Lemma}} |rs| = |mn|$$

$h(x) = \frac{r}{m}\,\bar{h}(x) \Rightarrow \left|\frac{r}{m}\right| \le 1$ siden $h(x)$ monisk og $\bar{h}(x) \in \mathbb{Z}[x]$.

$\Phi_n(x) = \frac{s}{n}\,\bar{\Phi}_n(x) \Rightarrow \left|\frac{s}{n}\right| \le 1$

$\Rightarrow |r| = |n|$ og $|s| = |n| \Rightarrow \Phi_n(x) = \pm\bar{\Phi}_n(x) \in \mathbb{Z}[x]$

$|rs| = |mn|$

III. $\Phi_n(x)$ irredusibel.

Se boka....

IV. $\Phi_n(x)$ har orden $\phi(n)$. tallteori....

$\#$ primitive n'te røtter $(\cdot$

Teorem 1.4.

w primitiv n'te enhetsrot i $\mathbb{C} \Rightarrow \mathbb{Q}(w)$ = rotkroppen til $\Phi_n(x)$ og rotkroppen til $x^n - 1 \in \mathbb{Q}[x]$

Dessuten: $[\mathbb{Q}(w) : \mathbb{Q}] = \phi(n) = |G(\mathbb{Q}(w)/\mathbb{Q})|$

og $G(\mathbb{Q}(w)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$

(multiplikative gr. av enhetene i $\mathbb{Z}_n$.)

Bevis:

Teorem 1.3 $\Rightarrow$ $\Phi_n(x)$ er min. polynomet til w.

w primitive n'te enhetsrot $\Rightarrow$ alle n'te enhetsrøtter er i $\mathbb{Q}(w)$.

Altså: $\mathbb{Q}(w)$ er rotkroppen til $\Phi_n(x)$ og $x^n - 1$.

Vi har $[\mathbb{Q}(w) : \mathbb{Q}] = \deg \Phi_n(x) = \phi(n)$

FAKT $\|$

$|G(\mathbb{Q}(w)/\mathbb{Q})|$