Setning 82 (23.6)
La F være en endelig kropp. Da er $(F\setminus\{0\}, \cdot)$ en syklisk gruppe.

Bevis: Vet: $(F\setminus\{0\}, \cdot)$ er en endelig gruppe
Siden F er en komm. ring, så er $(F\setminus\{0\}, \cdot)$ en endelig abelsk gruppe.
Teorem 33 $\Longrightarrow$

$$\underbrace{F\setminus\{0\}}_{\text{multiplikativ}} \xrightarrow{\varphi} \underbrace{\mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_t^{r_t}}}_{\text{additiv}} = G$$

der p_i primtall, $r_i \geq 1$.

La $m = \operatorname{lcm}(p_1^{r_1}, p_2^{r_2}, \ldots, p_t^{r_t}) \leq p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t} = |G|$

Påstår: G er syklisk av orden m.

La $g = (\bar{z}_1, \bar{z}_2, \ldots, \bar{z}_t)$ i G. Siden $p_i^{r_i} \cdot \bar{z}_i = \bar{0}$ for alle i, vil ordenen til $\bar{z}_i$ dele $p_i^{r_i}$.
Tilsvarende som i Setn 31 følger det at $m \cdot g = \bar{0}$, dvs. $m \cdot y = 0$ for alle elementer $y \in G$ som løsninger, $|G| = p_1^{r_1} \cdots p_t^{r_t}$ løsninger.
Ved avbildningen φ svarer likningen

$$m \cdot y = 0 \quad \text{til}$$

$$\varphi(m y) = \varphi(\underbrace{y + y + \cdots + y}_{m \text{ ganger}}) = \underbrace{\varphi(y)\varphi(y)\cdots\varphi(y)}_{m \text{ ganger}} = \varphi(y)^m$$

$$\varphi(0) = 1_F$$

$\Longrightarrow x^m - 1_F = 0$ har $|G|$ løsninger i $F\setminus\{0\}$.
Korollar 77 $\Rightarrow x^m - 1 = 0$ har høyst m røtter i F
$\Rightarrow$ Løsninger

$\Rightarrow m \geq p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ $\qquad m$

$\Rightarrow m = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t} = \operatorname{lcm}(p_1^{r_1}, \ldots, p_t^{r_t}) \gcd(p_1^{r_1} \cdots p_t^{r_t})$ $\qquad$ m

$\Rightarrow \gcd(p_1^{r_1}, p_2^{r_2}, \ldots, p_t^{r_t}) = 1$

$\Rightarrow p_i \neq p_j$ for $i \neq j$.

Setn 32 $\Rightarrow$ G er en syklisk gruppe.
$\Rightarrow (F^\times, \{0\}, \cdot)$ er en syklisk gruppe. $\square$

Idealer

Motivasjon: $(x^2+1)\mathbb{R}[x] \hookrightarrow \mathbb{R}[x] \xrightarrow{\varphi_i} \mathbb{C}$, $\ker \varphi_i$

Som grupper: $\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$

Fra nå av: Alle ringer er kommutative med 1.

DEF: En ikke-tom delmengde $I \subseteq R$ er et ideal hvis
(i) $(I, +) \leq (R, +)$ er en undergruppe.
(ii) $\forall r \in R, \forall a \in I \Rightarrow ra\ (=ar) \in I$

Eksempel

$R = \mathbb{Z}$, $I = n\mathbb{Z}$ ideal:

Vet: (i) $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$ undergruppe.
(ii) $r \in \mathbb{Z}$, $a = nq \in I \Rightarrow ra = r(nq) = n(rq) \in n\mathbb{Z} = I$
$\Rightarrow I = n\mathbb{Z}$ er et ideal.

Har sett: Alle undergrupper av $\mathbb{Z}$ er av formen $n\mathbb{Z}$, for en $n \in \mathbb{Z}$.

$\Rightarrow$ Alle idealene i $\mathbb{Z}$ er av formen $n\mathbb{Z}$, for en $n \in \mathbb{Z}$.