Klassifikasjon av sykliske grupper

Obs: G gruppe, $a \in G$. Anta at $a^i = a^j$ for $i < j$.

$a^0 = a^j \mid \cdot a^{-i} \Rightarrow e = a^i a^{-i} = a^j \cdot a^{-i} = a^{j-i}$.

$\Rightarrow a^{j-i} = e$.

Lemma 13 $G = \langle a \rangle$ syklisk gruppe med generator $a \neq e$. Anta at $a^m = e$ med $m > 0$ og minst mulig. Da er

$$G = \{e, a, a^2, \dots, a^{m-1}\} \text{ og } |G| = m.$$

Bevis: 1) Alle elem. i G er på formen a^i med $0 \leq i < m$.
La $b \in G$. Da er $b = a^n$ for en $n \in \mathbb{Z}$. Har $n = qm + r$ for $q, r \in \mathbb{Z}$ med $0 \leq r < m$.
$\Rightarrow a^n = a^{qm+r} = a^{qm} \cdot a^r = \underbrace{(a^m)^q}_{e} a^r = e^q a^r = a^r$.
Dvs. 1) holder.

2) Alle $\{a^i\}_{i=0}^{m-1}$ forskjellige: Anta at

$$a^i = a^j \quad \text{for} \quad 0 \leq i < j < m$$

Har sett $a^{j-i} = e$, der $0 < j - i \leq j < m$
Dette er en selvmotsigelse, slik at 2) holder. □

Setning 14
La $G = \langle a \rangle$ være en syklisk gruppe med generator $a \neq e$.
(a) Hvis ordenen til G er ∞, da er $G \simeq (\mathbb{Z}, +)$.

7F

(b) Hvis ordenen til G er endelig, da er $G \cong (\mathbb{Z}_n, +)$, der $n = |G|$.

Bevis: (a) Definer $\varphi : \mathbb{Z} \longrightarrow G$ ved at $\varphi(i) = a^i$.
Har

$$\varphi(i+j) = a^{(i+j)} = a^i \cdot a^j = \varphi(i)\varphi(j)$$

dvs. φ er en hom. av grupper.

φ er 1-1: $\varphi(i) = \varphi(j) \Rightarrow a^i = a^j \Rightarrow a^{j-i} = e$.

Hvis $i \neq j$, så $\exists m \in \mathbb{Z}^+$ slik at $a^m = e$ og G blir G endelig, ⚡. $\Rightarrow i = j$ og φ er 1-1.

φ er på: Gitt $a^i \in G$, da er $\varphi(i) = a^i$, og φ er på.

$\Rightarrow \varphi$ er en isomorfi og $G \cong \mathbb{Z}$.

(b) G endelig, betrakt $\{e, a, a^2, \ldots, a^i, \ldots, a^j, \ldots\}$. Må ha $a^i = a^j$ for $i < j$, så $\exists m \in \mathbb{Z}^+$ slik at $a^m = e$.
Velg $m > 0$ minst mulig. Har satt:

$$G = \{e, a, a^2, \ldots, a^{m-1}\}.$$

Definer

$$\varphi : \mathbb{Z}_m \longrightarrow G$$

ved at $\varphi(\bar{i}) = a^i$
$\varphi(\bar{i} + \bar{j}) = \varphi(\bar{i})\varphi(\bar{j})$?

Husk: $\bar{i} + \bar{j} = \bar{r}$ når $i + j = qm + r$ for $0 \leq r < m$.

$\varphi(\bar{i}+\bar{j}) = \varphi(\bar{r}) = a^r$

$\varphi(\bar{i})\varphi(\bar{j}) = a^i a^j = a^{i+j} = a^{qm+r} = \underbrace{a^{qm}}_{e} a^r = a^r$

$\Rightarrow \varphi$ er en gruppehomomorfi.

Klart at φ er på. Like mange elementer i $\mathbb{Z}_m$ og G.
$\Rightarrow \varphi$ er 1-1 $\Rightarrow \varphi$ er en isomorfi.
$\Rightarrow G \simeq \mathbb{Z}_m$. □

Eksempel $G = \mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\}$.

- $\langle\bar{0}\rangle = \{\bar{0}\}$
- $\langle\bar{1}\rangle = \mathbb{Z}_{12}$
- $\langle\bar{2}\rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$
- $\langle\bar{3}\rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$
- $\langle\bar{4}\rangle = \{\bar{0}, \bar{4}, \bar{8}\}$
- $\langle\bar{5}\rangle = \{\bar{0}, \bar{5}, \bar{10}, \bar{3}, \bar{8}, \bar{1}, \ldots\} = \mathbb{Z}_{12}$
- $\langle\bar{6}\rangle = \{\bar{0}, \bar{6}\}$
- $\langle\bar{7}\rangle = \{\bar{0}, \bar{7}, \bar{2}, \bar{9}, \bar{4}, \bar{11}, \bar{6}, \bar{1}, \ldots\} = \mathbb{Z}_{12}$
- $\langle\bar{8}\rangle = \{\bar{0}, \bar{8}, \bar{4}\}$
- $\langle\bar{9}\rangle = \{\bar{0}, \bar{9}, \bar{6}, \bar{3}\}$
- $\langle\bar{10}\rangle = \{\bar{0}, \bar{10}, \bar{8}, \bar{6}, \bar{4}, \bar{2}\}$
- $\langle\bar{11}\rangle = \{\bar{0}, \bar{11}, \ldots\} = \mathbb{Z}_{12}$.

"$-\bar{1} \Rightarrow \bar{1} \in \langle\bar{11}\rangle$"