Isomorfisætning, orden af et element, cykliske grupper.

Lad G og K være grupper og lad $\phi : G \to K$ være en homomorfi.
Lad $N = \ker \phi$.
Så er $\tilde{\phi} : G/N \to \phi(G)$ givet ved $\tilde{\phi}(gN) = \phi(g)$ veldefineret og $\tilde{\phi}$ er en isomorfi.

G/N og $\phi(G)$ er altså isomorfe grupper.
Uformelt: G/N og $\phi(G)$ er "den samme" gruppe.
Og tilsvarende ϕ "den samme" homomorfi som den kanoniske homomorfi $G \mapsto G/N$.

Definition. Hvis g er element i en gruppe G og $n \in \mathbb{Z}$ så defineres g^n (eller ng hvis kompositionen er $+$) rekursivt for $n \geq 0$ ved

Basis: $g^0 = e$ (det neutrale element).

Rekursion: hvis $n \geq 1$ er $g^n = g^{n-1}g$.

For $n < 0$ defineres: $g^n = (g^{-1})^{-n}$.

Proposition. For alle $n, m \in \mathbb{Z}$ er $g^{n+m} = g^n g^m$.
Dermed er $f_g : \mathbb{Z} \to G$ givet ved $f_g(n) = g^n$ en homomorfi.

Definition. Ifølge 2.4.9 er $f_g(\mathbb{Z})$ en undergruppe af G. Den betegnes $\langle g\rangle$ og kaldes **undergruppen frembragt** af g.

Ordenen af $\langle g\rangle$ kaldes **orden**en af g, skrives ord(g).

Proposition.
Hvis g har uendelig orden så er $g^i \neq g^j$ når $i \neq j$ og $\langle g\rangle \cong \mathbb{Z}$.

Hvis ord(g) er endelig $g^n = e \Leftrightarrow \mathrm{ord}(g) \mid n$ og

$$\mathrm{ord}(g) = \min\{n > 0 \mid g^n = e\}.$$

$g^i = g^j$ hvis og kun hvis ord$(g) \mid i - j$.
Desuden er $\langle g\rangle \cong \mathbb{Z}/m\mathbb{Z}$, hvor $m = \mathrm{ord}(g)$.

Proposition. Hvis G er en endelig gruppe og $g \in G$ så er

- ord(g) en divisor i $|G|$ og
- $g^{|G|} = e$.

Eksempel. Eulers Sætning.
Gruppen $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ er en gruppe af orden $\varphi(n)$.
For $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ har vi derfor

$$[a]^{\varphi(n)} = [1],$$

i $(\mathbb{Z}/n\mathbb{Z})^*$.
For $a \in \mathbb{Z}$ betyder det at hvis gcd$(a,n) = 1$ så er $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$ og dermed

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Definition. En gruppe G siges at være **cyklisk** hvis der findes $g \in G$ så $G = \langle g \rangle$.

Proposition. Hvis G er en cyklisk gruppe så er

- enten $G \cong \mathbb{Z}$
- eller $G \cong \mathbb{Z}/n\mathbb{Z}$, for et $n \geq 1$.