Undergrupper og sideklasser

Lad $(G, \circ)$ være en gruppe med neutralt element e og lad $H \subseteq G$ være en ikke-tom delmængde.

Definition Hvis ($\circ$ er en komposition på H og) $(H, \circ)$ er en gruppe så siger vi at H er en **undergruppe** af G.
Skrives $H \leq G$.

Sætning $(H, \circ)$ er en undergruppe af G hvis og kun hvis

1. $e \in H$,
2. $x^{-1} \in H$ for ethvert $x \in H$,
3. $x \circ y \in H$ for alle $x, y \in H$

3. betyder at $\circ$ er en komposition på H. Kompositionen er associativ i hele G og dermed i H. 1. og 2. svarer til de to andre krav i definitionen af en gruppe.

Beviset for "kun hvis" delen af sætningen skal gøre rede for at hvis $(H, \circ)$ er en gruppe med neutralt element e' så er $e' = e$. Og at hvis $x \in H$ har invers y i $(G, \circ)$ og invers z i $(H, \circ)$ så er $y = z$.

Proposition Lad H være en undergruppe af $(\mathbb{Z}, +)$.
Så findes der et entydigt tal $d \in \mathbb{Z}$, $d \geq 0$, som opfylder at

$$H = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\}.$$

Omvendt er $d\mathbb{Z}$ en undergruppe af $\mathbb{Z}$ for ethvert $d \in \mathbb{Z}$.

F.eks.:
$0\mathbb{Z} = \{0\}$
$1\mathbb{Z} = \mathbb{Z}$
$2\mathbb{Z} = \{\dots, -2, 0, 2, 4, 6, \dots\}$
$3\mathbb{Z} = \{\dots, -3, 0, 3, 6, 9, \dots\}$
$\vdots$

Definition.
Lad H være en undergruppe af G.
Mængden $gH = \{gh \mid h \in H\}$ kaldes en (venstre-)**sideklasse** af H.
Mængden $Hg = \{hg \mid h \in H\}$ kaldes en højre-**sideklasse** af H.

Eksempel: Undergruppen $d\mathbb{Z}$ af $(\mathbb{Z}, +)$ har sideklasser:

$$a + d\mathbb{Z} = d\mathbb{Z} + a,$$

altså restklasserne som vi tidligere har set på.

Lad H være en undergruppe af G.

De forskellige venstre-sideklasser af H udgør en klassedeling (partition) af G, altså: hvert element er i præcis én af disse mængder.
$xH = yH$ hvis og kun hvis $x^{-1}y \in H$.

De forskellige højre-sideklasser af H udgør en klassedeling af G.
$Hx = Hy$ hvis og kun hvis $xy^{-1} \in H$.

Enhver sideklasse af H har samme kardinalitet som H.

Lagrange: Hvis H er en endelig undergruppe af G så er

$$|G| = [G : H]|H|,$$

hvor $[G : H]$ betegner antallet af forskellige venstre-sideklasser af H i G, som også kaldes H's **index** i G.
Ordenen af H går altså op i ordenen af G.