Grupper

En **komposition** $\circ$ på en mængde S: for hver $a, b \in S$ er $a \circ b$ et element i S.

En komposition er altså en funktion $\circ : S \times S \mapsto S$.

Det er vigtigt at S er lukket under kompositionen, altså at produktet af to elementer i S også ligger i S.

En **gruppe** er en mængde G med en komposition $\circ$, der opfylder

0. $\circ$ er en komposition på G. (Veldefineret og G lukket under $\circ$.)

1. $\circ$ er **associativ**: $a \circ (b \circ c) = (a \circ b) \circ c$ for alle $a, b, c \in G$,

2. der er et **neutralt element** $e \in G$, dvs.: $a \circ e = e \circ a = a$ for alle $a \in G$, og

3. ethvert element $a \in G$ har et **invers** element a^{-1}, dvs. $a \circ a^{-1} = a^{-1} \circ a = e$.

Hvis $\circ$ er kommutativ: $a \circ b = b \circ a$, for alle $a, b \in G$, så siger vi at G er abelsk.

Eksempel. Kvaternionsgruppen.
$G = \{1, -1, i, -i, j, -j, k, -k\}$ med komposition angivet ved følgende **kompositionstavle**.

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

I en kompositionstavle står hvert element i G præcis én gang i hver række og én gang i hver søjle.

Restklasser modulo n

Lad n være et positivt helt tal.
På mængden $\mathbb{Z}$ af hele tal har vi defineret relationen kongruens modulo n:

$$a \equiv b \pmod{n} \Leftrightarrow n|a-b.$$

Denne relation giver anledning en klassedeling/partition (se Proposition 2.1.2) af $\mathbb{Z}$ i klasser på formen

$$[a] = a + n\mathbb{Z} = \{a + nx \mid x \in \mathbb{Z}\}.$$

Disse mængder kaldes også restklasser, da de består af alle tal, der har samme rest ved division med n.

Mængden af de n forskellige restklasser modulo n betegnes $\mathbb{Z}/n\mathbb{Z}$.

Eksempel. Restklasser modulo 5.

$\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$, hvor

$[0] = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}$
$[1] = \{\ldots, -9, -4, 0, 6, 11, 16, \ldots\}$
$[2] = \{\ldots, -8, -3, 0, 7, 12, 17, \ldots\}$
$[3] = \{\ldots, -7, -2, 0, 8, 13, 18, \ldots\}$
$[4] = \{\ldots, -6, -1, 0, 9, 14, 19, \ldots\}$

Desuden er f.eks. $[5] = [0]$ og $[-7] = [3] = [18]$.

Addition er en *veldefineret* komposition på $\mathbb{Z}/n\mathbb{Z}$ givet ved

$$[a] + [b] = [a + b].$$

$(\mathbb{Z}/n\mathbb{Z}, +)$ er en abelsk gruppe af orden n.

(Dette er det vigtigste og mest simple eksempel på endelige grupper.)