A&S
HC2

$\mathbb{Z}_3$: $\mathbb{Z}$ met daarop ~
$a \sim b \iff a-b$ deelbaar door 3
verzameling van equivalentieklassen:
$\mathbb{Z}_3 = \{[0],[1],[2]\}$, $k = 3q + r$, $0 \le r < 3$, dan $k \in [r]$

$\mathbb{Z}_n = \{[0],[1],\ldots,[n-1]\}$
optelling en vermenigvuldiging op $\mathbb{Z}_n$:
$[i]+[j]=[i+j]$ en $[i]*[j]=[i*j]$

Eigenschap:

(i) $\exists 0$	neutrale-/eenheidselement
(ii) $\forall a: a+0=0+a=a$	
(iii) $\forall a \exists b$ zdd. $a+b=b+a=0$,	b is inverse/tegengestelde van a
(iv) $\forall a,b,c: (a+b)+c = a+(b+c)$	associatief
(v) $a+b=b+a$, $\forall a,b$	commutatief

→ Definitie van commutatieve groep (Abels)
Als (v) niet geldt dan → groep

Vbd: $\langle \mathbb{Q},+\rangle$ groep ,
$\langle \mathbb{Z},+\rangle$ groep
$\langle \mathbb{Q},*\rangle$ geen groep, [0] heeft geen inverse
$\langle \mathbb{Q}\setminus\{0\},*\rangle$ groep
$\langle \mathbb{R},+\rangle$ groep
$\langle \mathbb{R}\setminus\{0\},*\rangle$ groep
$\langle \mathbb{Z}_n,+\rangle$ groep
$\langle \mathbb{Z}_n\setminus\{0\},*\rangle$: $\mathbb{Z}_6$: [2] heeft geen inverse, [3] en [4] ook niet, deze zijn geen relatief priem met 6

$U(n) = \{[1],[k],\ldots \mid ggd(k,n)=1, \text{mod } n\}$
(unitaire) $= \{k \mid 1 \le k \le n-1,\ ggd(k,n)=1\}$

$U(8) = \{1,3,5,7\}$

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

eenheidselement: 1

stel: $a \in U(n)$ gezocht: $b \in U(n)$ met $a \cdot b = 1 \bmod n$

aangezien $ggd(a,n)=1$, $\exists x,y$: $a \cdot x + ny = 1$

$\Rightarrow ax = 1 \bmod n$

$\Rightarrow a^{-1} = [x]$ $(ggd(x,n)=1)$

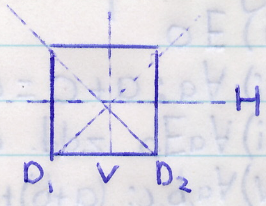
tot slot: $a,b \in U(n) \overset{?}{\Rightarrow} ab \in U(n)$

$ggd(a,n)=1$, $ggd(b,n)=1$

stel p deelt $a \cdot b$ en $p|n$ $ggd(a,n) \neq 1$ of

dan ($p|a$ of $p|b$) en $p|n$ $\Rightarrow$ $ggd(b,n) \neq 1$

D_4 met $\circ$ samenstelling



R_0

R_{90}

R_{270}

R_{180}

bijv: $R_{90} \cdot R_{180} = R_{180} \cdot R_{90} = R_{270}$

$\left.\begin{array}{l} R_{90} \cdot V = D_2 \\ V \cdot R_{90} = D_1 \end{array}\right\}$ niet commutatief

Als G een eindige groep dan heet $|G|$ orde van G,
het aantal elementen.

b.v. $|U(n)| = \varphi(n)$ $|U(8)| = 4$, $|U(10)| = 4$

$g \in G$: dan $|g|$: kleinst $k \geq 1$ z.d.d. $g^k = e$

in $U(8)$: $|3| = |5| = |7| = 2$

in $U(10)$: $|3| = 4$