A&S
HC4

$\varphi : (G_1, *_1) \to (G_2, *_2)$ heet isomorfisme
indien: • φ bijectief is
• $\varphi(g_1 *_1 g_1') = \varphi(g_1) *_2 \varphi(g_1')$, $g_1, g_1' \in G_1$

Beschouw groep G, een permutatie op G is een bijectie $\varphi : G \to G$

Vb.d: $\{1,2,3\}$ $\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix}$

	1 2 3
σ_1	1 3 2
	2 1 3
	3 1 2
σ_2	2 3 1
	3 2 1
$\sigma_2 \sigma_1$:	2 1 3

groep onder samenstelling: S_3, niet commutatief
stel $|G| = n$, groep, dan bestaat er ondergroep
H van S_n zdd: $G \sim H$
Bewijs: $\varphi \; G \to S_n$ • injectief
• $\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2)$
dan $H = \varphi(G)$

$G = \{g_1, g_2 \to g_n\}$, $\varphi(g_1) = (g_1 g_1, g_1 g_2, \dots, g_1 g_n)$
Vb.d: $= (g_3, g_7, \dots g_{n-1})$

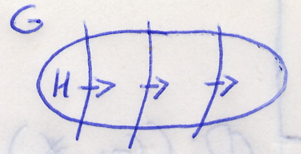
$\begin{matrix} 1 & 2 & \cdots & n \\ \downarrow & \downarrow & & \downarrow \\ 3 & 7 & & n-1 \end{matrix}$

Dus: $\varphi(g_k) = (g_k g_1, g_k g_2, g_k g_3, \dots, g_k g_n) \Rightarrow$ injectief

$\varphi(g_1 \cdot g_2) : G \to G$, $g \in G$
$\varphi(g_1 \cdot g_2)(g) = (g_1 \cdot g_2 \cdot g) = g_1 \cdot (g_2 \cdot g) = g_1 (\varphi(g_2)(g)) = \varphi(g_1)(\varphi(g_2)(g))$
$= (\varphi(g_1) \circ \varphi(g_2))(g)$

Als $\varphi : G_1 \to G_2$ voldoet aan:
• $\varphi(g_1 *_1 g_2) = \varphi(g_1) *_2 \varphi(g_2)$
• injectief
dan is $\varphi(G_1)$ ondergroep van G_2

H ondergroep van G, $|G| < \infty$
dan $|H|$ deelt $|G|$. Gevolg: stel $|G| = P$, priem
G heeft alleen $\{e\}$ en zichzelf als ondergroepen.
Stel $g \in G$, $g \neq e$, $\langle g \rangle = \{g^0, g, g^2, \dots g^k, \dots\}$ is ondergroep van G
$|\langle g \rangle| > 1$ en dus $G = \langle g \rangle$
$\varphi : G \to \mathbb{Z}_p$ door $\varphi(g^k) = k$



$H \subset G$ ondergroep:

Def: (nevenklasse/coset) $a \in G$: $aH = \{ah \mid h \in H\}$

Vbd: $G = \mathbb{Z}$, $H = \{3\text{-vouden}\}$

$0.H = \{3k \mid k \in \mathbb{Z}\}$ $\quad 3.H = \{3+3k \mid k \in \mathbb{Z}\} = 0.H$

$1 \cdot H = \{1+3k \mid k \in \mathbb{Z}\}$

$2 \cdot H = \{2+3k \mid k \in \mathbb{Z}\}$

Eigenschap: $a, b \in G$, dan: $aH \cap bH = \emptyset$ òf $aH = bH$

Bewijs: stel $aH \cap bH \neq \emptyset$, dan bestaat er $x \in (aH \cap bH)$

$x \in aH \Rightarrow x = ah_1$, $\quad x \in bH \Rightarrow x = b h_2$

$\Rightarrow \boxed{a.h_1 = b.h_2} \Rightarrow a = b h_2 h_1^{-1}$

kies $y \in aH \Rightarrow y = a h_3 = b \underbrace{h_2 h_1^{-1} h_3}_{\in H} \Rightarrow y \in bH$

Zo ook $z \in bH \Rightarrow \dots \Rightarrow z \in aH$

G kies in elke nevenklasse a_i, $i = 1..k$, $\bigcup_{i=1}^{k} a_i H = G$

$|G| = \sum_{i=1}^{k} |a_i H| = \sum_{i=1}^{k} |H| = k \cdot |H|$, dus $|H|$ deelt $|G|$

$\psi: aH \to bH$, $\quad \psi(ah) = bh$, bijectief

Gevolg: $|g|$ is deler van $|G|$

want $H = \{g^0, g, g^2, \dots, g^{|g|-1}\}$, $\quad |H| = |g|$

Gevolg: $|g|$ deelt $|G|$, $|G| = k \cdot |g|$

$g^{|G|} = g^{|g| k} = (g^{|g|})^k = e^k = e$