$\phi : G \to G'$ - group homomorphism iff

$\forall g_1, g_2 \in G \quad \phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$

Properties

1) Let $\phi : G \to G'$ be surj. group homomorphism
If $G$ is abelian group, so is $G'$

2) Composition of 2 group homomorphisms is a group homomorphism

<u>Proof</u>

Let $\phi_1 : G \to G'$ $\quad \phi_2 : G' \to G''$ be g.h.

Show $\phi_2 \circ \phi_1 : G \to G''$ is a g.h.

for $a, b \in G$

$$
\begin{aligned}
(\phi_2 \circ \phi_1)(a \cdot b) &= \phi_2(\phi_1(a \cdot b)) \\
&= \phi_2(\phi_1(a) \cdot \phi_1(b)) \\
&= \phi_2(\phi_1(a)) \cdot \phi_2(\phi_1(b)) \\
&= (\phi_2 \circ \phi_1)(a) \cdot (\phi_2 \circ \phi_1)(b)
\end{aligned}
$$

3) Let $\phi : G \to G'$ be a g.h.
If $e$ is identity of $G$ then
$\phi(e)$ is identity of $G'$

4) Let $\phi : G \to G'$ be a g.h.
If $a \in G$ then $(\phi(a))^{-1} = \phi(a^{-1})$

<u>Proof</u>

Let $a \in G$, $\exists a^{-1} \in G$ s.t. $aa^{-1} = a^{-1}a = e$

Consider $\phi(e)$, by 3 $\phi(e) = e'$

$$\phi(e) = \phi(aa^{-1}) = \phi(a) \cdot \phi(a^{-1}) = e'$$

so

$$(\phi(a))^{-1} = \phi(a^{-1})$$

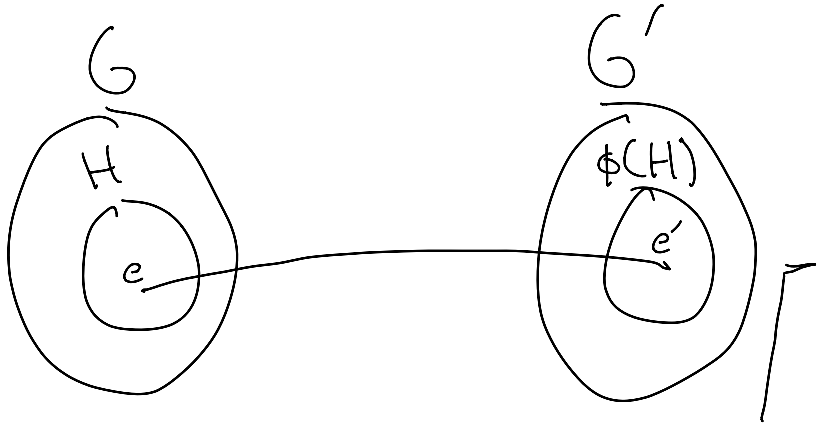
# Definition

Let $f : A \to B$ $\quad C \subseteq A \quad D \subseteq B$

Set $f(C) = \{ f(x) \mid x \in C \}$
is the **image** of $C$ in $B$

The set $f^{-1}(D) = \{x \in A \mid f(x) \in D\}$
is the **pre-image** of $D$ in $A$

5) let $\phi : G \to G'$
If $H \leq G$ then $\phi(H) \leq G'$




Proof

$\phi(H) \subseteq G'$ satisfies conditions:

1. $a', b' \in \phi(H)$ $\exists\, a, b \in H$ $\phi(a) = a'$, $\phi(b) = b'$
2. By prop 3 $\phi(e) = e'$ for $e \in H$ bcs $H \leq G$, thus $e' \in \phi(H)$
3. $a' \in \phi(H)$ $\exists a \in H$ $\phi(a) = a'$ by prop 4, $(\phi(a))^{-1} = \phi(a^{-1})$, where $a^{-1} \in H$ bcs $a \in H$ + $H \leq G$

Thus $(a')^{-1} = (\phi(a))^{-1} = \phi(a^{-1})$

$(a')^{-1} \in \phi(H)$

6) Let $\phi : G \to G'$ be a g.h.

If $H' \leq G'$ then $\phi^{-1}(H') \leq G$

# Definition

Let $\phi : G \to G'$ be a group homomorphism

Then the subgroup

$$\phi^{-1}(\{e'\}) = \{x \in G \mid \phi(x) = e'\}$$
$$= \{x \in G \mid \phi(x) = \phi(e)\}$$
$$= \phi^{-1}(\{\phi(e)\})$$

denoted **ker $\phi$**

## Examples

1) $\phi : S_n \to \mathbb{Z}_2$, $\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ even} \\ 1 & \text{if } \sigma \text{ odd} \end{cases}$

group homomorphism w/

$$\ker\phi = \{\delta \in S_n \mid \phi(\delta) \equiv_2 0\}$$

$$= \{\delta \in S_n \mid \delta \text{ is even}\}$$

$$= A_n \leq S_n$$

alternating group

2) $\phi : \mathbb{Z} \to \mathbb{Z}_n$ $\quad \phi(m) = m \bmod n = r$

where $m = nk + r$

group homomorphism w/

$$\ker\phi = \{m \in \mathbb{Z} \mid \phi(m) \equiv_n 0\}$$

$$= \{m \in \mathbb{Z} \mid m \equiv_n 0\}$$

$$= \{m \in \mathbb{Z} \mid m = kn,\ k \in \mathbb{Z}\}$$

$$= \{kn \mid k \in \mathbb{Z}\}$$

$$= n\mathbb{Z} = \langle n \rangle \leq \mathbb{Z}$$

Why are kernels important? :))