# Homomorphisms

**Def:** Suppose $(G, \circ)$ and $(H, *)$ are groups. A map $\phi: G \to H$ which satisfies $\phi(x \circ y) = \phi(x) * \phi(y)$, $\forall x, y \in G$, is called a <u>homomorphism</u> from $G$ to $H$.

A homomorphism $\phi: G \to H$ is called:

- a <u>monomorphism</u> if it is injective
- an <u>epimorphism</u> if it is surjective
- an <u>isomorphism</u> if it is bijective

Notation: $G \cong H$.

An isomorphism $\phi: G \to G$ is called an <u>automorphism</u> of $G$.

Exs:

0) For any groups $G$ and $H$, the map $\phi: G \to H$ defined by $\phi(g) = e_H$, $\forall g \in G$, is a homomorphism. (<u>trivial homomorphism</u>)

$\forall x, y \in G$, $\phi(xy) = e_H = e_H \cdot e_H = \phi(x) \cdot \phi(y)$.

1) $G = (\mathbb{R}, +)$, $H = (\mathbb{R}_{>0}, \cdot)$ (positive reals)

Def. $\phi: G \to H$ by $\phi(x) = e^x$.

Then, $\forall x, y \in \mathbb{R}$, $\phi(x+y) = e^{x+y} \overset{\text{(props. of exp.)}}{=} e^x e^y = \phi(x) \cdot \phi(y)$.

(bin. op. in G) (bin. op. in H)

Also, $\phi$ is a bijection, so it is an isomorphism.

2) $G = (GL_2(\mathbb{R}), \cdot)$, $H = (\mathbb{R} \setminus \{0\}, \cdot)$

Def. $\phi : G \to H$ by $\phi(A) = \det(A)$.

(props. of det)

Then $\forall A, B \in G$, $\phi(AB) = \det(AB) = \det(A) \cdot \det(B) = \phi(A)\,\phi(B)$.

(mult. of 2x2 matrices) (mult. of real numbers)

Here, $\phi$ is an epimorphism, but it is not injective.

3) $G = H = (\mathbb{Z}, +)$, $n \in \mathbb{Z}$

Def. $\phi : G \to H$, $\phi(k) = nk$.

Then, $\forall k, \ell \in \mathbb{Z}$, $\phi(k+\ell) = n(k+\ell) = nk + n\ell = \phi(k) + \phi(\ell)$.

So $\phi$ is a homomorphism:

- If $n = 0$ it is neither injective nor surjective.
- If $n = \pm 1$ it is an automorphism.
- If $|n| \geq 2$ it is a monomorphism, but not surjective.

4) $G = \mathbb{Z}$, $H = \mathbb{Z}/n\mathbb{Z}$, def. $\phi : G \to H$ by $\phi(k) = \bar{k}$. $(\bar{k} = k + n\mathbb{Z})$

Then $\forall k, \ell \in \mathbb{Z}$, $\phi(k+\ell) = \overline{k+\ell} = \bar{k} + \bar{\ell} = \phi(k) + \phi(\ell)$.

(def. of + in H)

Here, $\phi$ is an epimorphism, but it is not injective.

5) $G = C_n = \langle x \mid x^n = e \rangle$, $H = \mathbb{Z}/n\mathbb{Z}$

Recall (Subgroups video):

- $G = \{e, x, x^2, \dots, x^{n-1}\}$, and
- $x^i = x^j$ for $i, j \in \mathbb{Z}$ iff $i \equiv j \mod n$

Def. $\phi : G \to H$ by $\phi(x^k) = \bar{k}$.

(well defined) $\Leftarrow$

Then $\phi(x^k x^\ell) = \phi(x^{k+\ell}) = \overline{k+\ell} = \bar{k} + \bar{\ell} = \phi(x^k) + \phi(x^\ell)$.

Also, $\phi$ is a bijection, so $C_n \cong \mathbb{Z}/n\mathbb{Z}$.

(This shows that any two finite cyclic groups of the same order are isomorphic)

6) $G = H = \mathbb{Z}/n\mathbb{Z}$, $a \in \mathbb{Z}$, $\phi : G \to H$, $\phi(k) = ak \mod n$.

Then $\phi(k+\ell) = a(k+\ell) = ak + a\ell = \phi(k) + \phi(\ell)$.

Note that $\phi$ is:

- injective $\Leftrightarrow (a,n) = 1$ :

If $k, \ell \in G$ then $\phi(k) = \phi(\ell) \Leftrightarrow ak = a\ell \mod n$

$\Leftrightarrow a(k-\ell) = 0 \mod n$

(write $d = (a,n)$, $b = a/d$) $\Leftrightarrow b(k-\ell) = 0 \mod \left(\frac{n}{d}\right)$

$\Leftrightarrow k = \ell \mod \left(\frac{n}{d}\right)$

- surjective $\Leftrightarrow (a,n) = 1$

If $(a,n) = 1$ then $\forall \ell \in H$, $\exists k \in G$ s.t. $ak = \ell \mod n$.

If $(a,n) > 1$ then the equation $ak = 1 \mod n$ has no solution.

Therefore:
- If $(a,n) = 1$ then $\phi$ is an automorphism.
- If $(a,n) > 1$ then $\phi$ is neither injective nor surjective.

7) Let $G$ be a group and $\forall g \in G$ define $\tau_g : G \to G$

by $\tau_g(h) = ghg^{-1}$. Then, $\forall g \in G$, $\tau_g$ is:

(conjugation by $g$)

- a homomorphism ✓

$\forall h_1, h_2 \in G$,

$$\tau_g(h_1 h_2) = g(h_1 h_2)g^{-1} = gh_1(g^{-1}g)h_2 g^{-1}$$

$$= (gh_1 g^{-1})(gh_2 g^{-1}) = \tau_g(h_1)\tau_g(h_2).$$

- injective ✓

If $h_1, h_2 \in G$ and $\tau_g(h_1) = \tau_g(h_2)$ then $gh_1 g^{-1} = gh_2 g^{-1} \Rightarrow h_1 = h_2$.

- surjective ✓

Suppose $k \in G$, let $h = g^{-1}kg$.

Then $\tau_g(h) = ghg^{-1} = g(g^{-1}kg)g^{-1} = (gg^{-1})k(gg^{-1}) = k$.

Therefore, $\forall g \in G$, $\tau_g$ is an automorphism of $G$.