# Isomorphisms

**Def.** A homomorphism from a group $(G, \circ_G)$ to a group $(H, \circ_H)$ is a map $\phi : G \to H$ which preserves the group operation, in that

$$\phi(g_1 \circ_G g_2) = \phi(g_1) \circ_H \phi(g_2), \qquad (\star)$$

for any $g_1, g_2 \in G$. We call $\phi$ an isomorphism if it is additionally a bijection of sets. In that case, we say that $G$ is isomorphic to $H$, and write $G \cong H$.

A fancier way to express $(\star)$ is as a commutative diagram:

$$\begin{tikzcd} G \times G \arrow[r, "\circ_G"] \arrow[d, "\phi \times \phi"'] & G \arrow[d, "\phi"] \\ H \times H \arrow[r, "\circ_H"] & H \end{tikzcd}$$

$\phi$ is a homomorphism iff this diagram commutes.

**Thm.** Isomorphism is an equivalence relation on the class of all groups.

## Examples

① The group

$$R(n) = \{ e^{2\pi i k/n} \mid 0 \le k \le n-1 \} \subset \mathbb{C}^*$$

is isomorphic to $\mathbb{Z}_n$.

Let $\xi_n \in R(n)$ be a primitive $n^{th}$ root of unity (e.g., $\xi_n = e^{2\pi i/n}$) and define

$$\begin{aligned} \phi : \mathbb{Z}_n &\longrightarrow R(n) \\ k &\longmapsto \xi_n^k . \end{aligned}$$

- Surjective, since each elt of $R(n)$ has the form $\xi_n^k$.
- injective b/c a surjection between sets of the same finite size must be so.
- homomorphism:

$$\begin{aligned} \phi(k+m) &= \xi_n^{k+m} \\ &= \xi_n^k \xi_n^m \\ &= \phi(k)\,\phi(m). \end{aligned}$$

$\boxtimes$

② Check: $\begin{aligned} \phi : \mathbb{Z} &\longrightarrow n\mathbb{Z} \\ k &\longmapsto nk \end{aligned}$ is an isomorphism.

③ $\mathbb{Z}_n \not\cong \mathbb{Z}_m$ if $n \neq m$, since an isomorphism is required to be a bijection.

④ $\mathbb{Z}_6 \not\cong D_3$, even though there are bijections btwn them.

Suppose there were an isom. $\phi : \mathbb{Z}_6 \to D_3$.
Choose $m, n \in \mathbb{Z}_6$ s.t. $\phi(m) = r$, $\phi(n) = s$.

$$\begin{aligned} \Rightarrow \quad rs = \phi(m)\phi(n) &= \phi(m+n) = \phi(n+m) \\ &= \phi(n)\phi(m) = sr. \quad \times \end{aligned}$$

⑤ Find all six isomorphisms btwn $U(8)$ & $U(12)$.

## Important properties

**Thm.** Let $\phi: G \to H$ be an isomorphism of groups. Then:

① $\phi^{-1}: H \to G$ is an isomorphism;

② $|G| = |H|$;

③ if $G$ is abelian, then $H$ is abelian;

④ if $G$ is cyclic, then $H$ is cyclic;

⑤ if $G$ has a subgroup of order $n$, then $H$ has a subgroup of order $n$.

This allows us to prove a classification result.

**Thm.** A cyclic group $G$ is isomorphic to $\mathbb{Z}_n$, if $|G| = n$, and is isomorphic to $\mathbb{Z}$, if $|G|$ is infinite.

(Proof.) Let $a \in G$ be a generator of $G$, so that

$$G = \{a^k \mid k \in \mathbb{Z}\}$$

We define a map $\phi: \mathbb{Z}_{|G|} \to G$ (where $\mathbb{Z}_{|G|} = \mathbb{Z}$
$k \mapsto a^k$ if $|G| = \infty$).

- homomorphism:
$$\phi(k+m) = a^{k+m} = a^k a^m = \phi(k)\,\phi(m)$$
- Surjection b/c every elt of $G$ has the form $a^k$

- injection: if $|G|$ is finite, automatic.

  Suppose $|G|$ is infinite and $\phi(k) = \phi(m)$, for some $k \leq m \in \mathbb{Z}$.

  $$\phi(k) = \phi(m) \Rightarrow a^k = a^m$$
  $$\Rightarrow e = a^{m-k}$$

  Since $a$ has infinite order, $m-k$ must be $0$.

  i.e., $m = k$. $\blacksquare$

**Cor** Up to isomorphism, $\mathbb{Z}_p$ is the unique group of order $p$.

(Proof.) Suppose $|G| = p$ is prime.

$$\forall g \in G, \ |g| \mid |G| \Rightarrow |g| = 1 \text{ or } |g| = p.$$

If $g \neq e$, then $|g| = p$.

So $\langle g \rangle = G$.

So $G$ is cyclic, and the theorem gives us $G \cong \mathbb{Z}_{|G|} = \mathbb{Z}_p$. $\blacksquare$

Tomorrow: Cayley's theorem

Every group is isomorphic to a group of permutations.