Isomorphisms

Two Groups $(G, \cdot)$, and $(H, \circ)$ are isomorphic if $\exists$ a 1-1 and onto map $\phi : G \to H$ such that the group operation is persvered

$$\phi(a \cdot b) = \phi(a) \circ \phi(b) \qquad \forall a, b \in G.$$

ϕ is a called an isomorphism

write

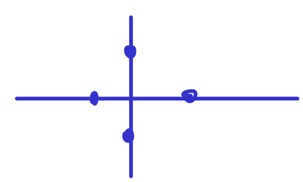
$$G \cong H \quad \text{or} \quad G \simeq H$$

Ex) Show $\mathbb{Z}_4 \cong \langle i \rangle$ = the 4th roots of unity, complex solutions of $z^4 = 1$

$$= \{1, -1, i, -i\}$$

Define a map $\phi : \mathbb{Z}_4 \to \langle i \rangle$

$$: n \mapsto i^n$$



$\phi(0) = 1$

$\phi(1) = i$

$\phi(2) = -1$

$\phi(3) = -i$ $\quad \therefore \quad \phi$ is 1-1 and onto

$$\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n)$$

$\therefore \phi$ is an isomorphism.

Ex) $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ is an isomorphism

$x \longmapsto e^x$ is 1-1 and onto by calculus

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y).$$

Ex] $|\mathbb{Z}_8| \neq |\mathbb{Z}_{12}|$

$U(8) \simeq U(12)$

$\{1,3,5,7\}$ $\{1,5,7,11\}$

$$\phi : \begin{array}{l} 1 \mapsto 1 \\ 3 \mapsto 5 \\ 5 \mapsto 7 \\ 7 \mapsto 11 \end{array}$$

$$\begin{aligned} \phi(3\cdot 5 \bmod 8) &= \phi(7 \bmod 8) \\ &= 11 \bmod 12 \\ &= 35 \bmod 12 \\ &= 5\cdot 7 \bmod 12 \\ &= \phi(3 \bmod 8)\,\phi(5 \bmod 8) \end{aligned}$$

Ex] $|S_3| = |\mathbb{Z}_6|$ but $\mathbb{Z}_6 \not\simeq S_3$.

Proof

Suppose $\exists$ an isomorphism $\phi : \mathbb{Z}_6 \to S_3$.

Let $a, b \in S_3$ s.t. $ab \neq ba$

Since ϕ is an isomorphism there must exist

$$\phi(m) = a, \quad \phi(n) = b$$

$$ab = \phi(m)\phi(n) = \phi(m+n) = \phi(n+m) = \phi(n)\phi(m)$$
$$= ba$$

but $ab \neq ba$ so this a contradiction ∎.

Theorem Let $\phi : G \to H$ be an isomorphism of Groups; we have

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

2) $|G| = |H|$

3) G abelian iff H is abelian

4) G cyclic iff H is cyclic

5) G has a subgroup of order n iff H has a subgroup of order n.

Proof:

1,2 are true since ϕ is a bijection

3) $g_1 g_2 = g_2 g_1 \quad \forall g_1 g_2 \in G$ all $h_1, h_2 \in H$ have the form

$$\phi(g_1) = h_1 \quad , \quad \phi(g_2) = h_2$$

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1)$$
$$= h_2 h_1 .$$

■.

Theorem 9.7 All cyclic groups of infinite order are isomorphic to $\mathbb{Z}$.

Proof:

Let $G = \langle a \rangle$ be a cyclic group $|G| = |a| = \infty$.

Define a map

$$\phi: \mathbb{Z} \to G$$
$$n \mapsto a^n$$

Then

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$$ $\therefore$ operation is perserved.

Let $m, n \in \mathbb{Z}$ $m \neq n$, $m > n$

Suppose $a^m = a^n \Rightarrow a^{m-n} = e$ and $m-n > 0$

This is a contradiction since $|a| = \infty$. $\therefore$ ϕ is 1-1.

Since G is cyclic for all $g \in G$ $g = a^n = \phi(n)$ $\therefore$ onto

$G \cong \mathbb{Z}$.

■

Theorem | If G is a cyclic group of order n, then

$$G \cong \mathbb{Z}_n .$$

Proof:

Let $G = \langle a \rangle$, $a \in G$, $|a| = n$

$$\phi : \mathbb{Z}_n \to G$$

$$k \mapsto a^k \qquad 0 \le k < n$$

$\Leftarrow k_1 + k_2 \bmod n$

$$\phi(k_1 + k_2 + cn) = a^{k_1 + k_2 + cn} = a^{k_1} a^{k_2} \underbrace{a^{cn}}_{e} = a^{k_1} a^{k_2}$$

$$= \phi(k_1)\,\phi(k_2) .$$

$\blacksquare$