# Chap 9 Isomorphisms

The way to formally express the idea that two different groups have the same 'structure' or 'group properties'

## Eg 9.1

Consider these two groups. $\mathbb{Z}_4$, integers under addition modulo 4

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

complex numbers under mult.

and $\langle i \rangle$, the cyclic subgroup of $\mathbb{C}^*$ generated by $i$.

$$\langle i \rangle = \{1, i, i^2 = -1, i^3 = -i\}$$

Both groups of order four.

Let's look at their Cayley tables.

$\mathbb{Z}_4$

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

$\langle i \rangle$

| $\cdot$ | $1$ | $i$ | $-1$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $i$ | $-1$ | $-i$ |
| $i$ | $i$ | $-1$ | $-i$ | $1$ |
| $-1$ | $-1$ | $-i$ | $1$ | $i$ |
| $-i$ | $-i$ | $1$ | $i$ | $-1$ |

Look at these two tables and ask.

- Are they really that different? No
- Or could they be regarded as similar/equivalent? Yes.

$$\begin{array}{ccc} \mathbb{Z}_4 & & \langle i \rangle \\ 0 & \longleftrightarrow & 1 \\ 1 & \longleftrightarrow & i \\ 2 & \longleftrightarrow & -1 \\ 3 & \longleftrightarrow & -i \end{array} \Bigg\} \text{ mapping}$$

$$\underbrace{2+3=1}_{\text{in } \mathbb{Z}_4} \qquad \underbrace{(-1)\cdot(-i)=i}_{\langle i \rangle}$$

This mapping "preserves"/"fits with" the two group operations.

This is what we call an isomorphism between these two groups.

# Formal def

For two groups $(G,\cdot)$, $(H,\circ)$
we say "G is isomorphic to H"
iff there exists a bijective map

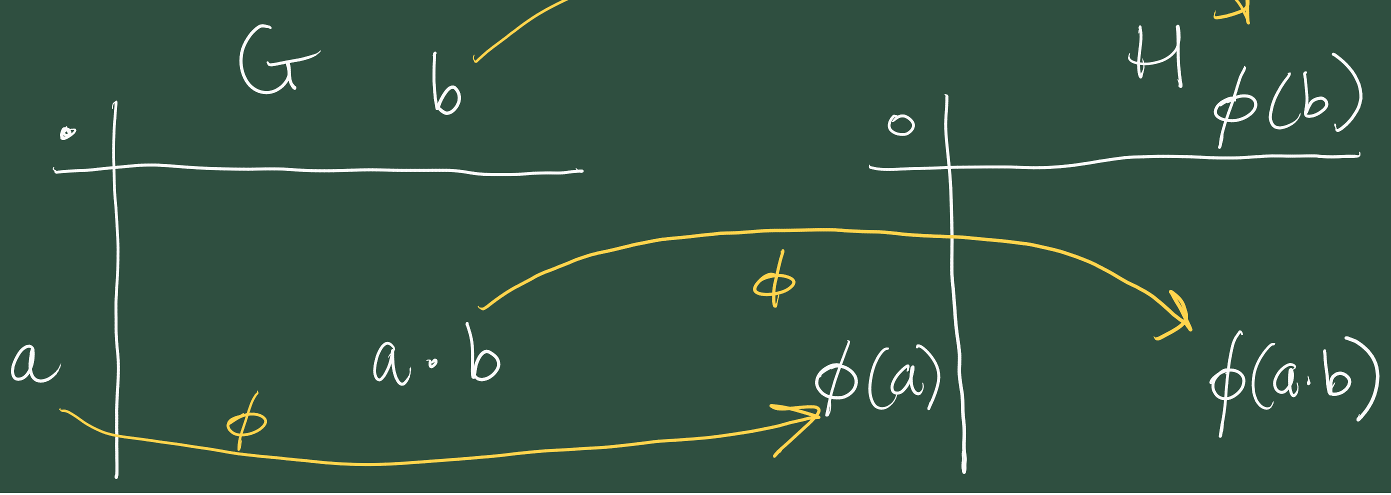
$$\phi : G \longrightarrow H.$$

which satisfies the "homomorphism property"

for all $a, b \in G$.

$$\underbrace{\phi(a\cdot b)}_{\text{prod. in } G} = \underbrace{\phi(a)\circ\phi(b)}_{\text{prod. in } H.}$$

We can write $G \cong H$



So in other words, $\phi$ is not only a mapping of the elements of $G$ to the elements of $H$, it also maps the Cayley table of $G$ exactly to the Cayley table of $H$.

---

Note from your linear algebra study, the def. of linear transformation. vector spaces $U, V$

$$T : U \longrightarrow V$$

$\forall \alpha, \beta \in \mathbb{R}$ $\forall u_1, u_2 \in U$

$$T(\alpha u_1 + \beta u_2) = \alpha T(u_1) + \beta T(u_2)$$

this is an instance of the homomorphism property between the two groups

$$(U, +) \;,\; (V, +).$$

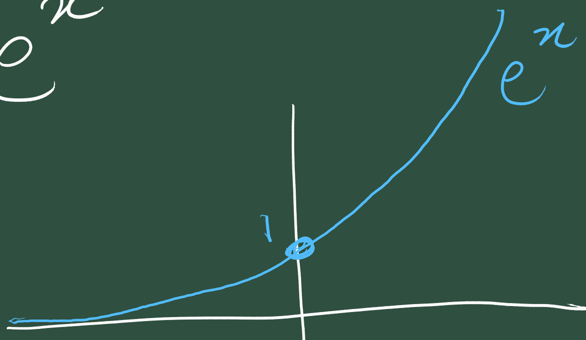
---

Ex 9.2

group under $+$.

group under $\times$

$$\phi : \mathbb{R} \longrightarrow \mathbb{R}^+$$
$$x \longmapsto e^x$$




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

**Ex 9.3**

Consider this map between groups

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Q}^*$$
$$n \longmapsto 2^n$$

$$\phi(m+n) = 2^{m+n} = 2^m \cdot 2^n = \phi(m)\cdot\phi(n)$$

This $\phi$ is injective (1-1) but not onto. But if restrict $\phi$ to.

$$\phi : \mathbb{Z} \longrightarrow H \subset \mathbb{Q}^*$$

$H := \{ 2^n \,;\, n \in \mathbb{Z} \}$

This version of $\phi$ is surjective (onto)

So $\mathbb{Z}$ is Isomorphic to $H$

---

Ex 9.4

$\mathbb{Z}_8, \mathbb{Z}_{12}$ are certainly not Isomorphic. $|\mathbb{Z}_8| = 8$, $|\mathbb{Z}_{12}| = 12$

But if we consider $U(8), U(12)$

$U(8) = \{z \in \mathbb{Z}_8 : \gcd(z, 8) = 1\} = \{1, 3, 5, 7\}$

$U(12) = \{1, 5, 7, 11\}$

Claim: $U(8) \cong U(12)$

Proof Consider the mapping

$$\phi : U(8) \longrightarrow U(12).$$

$$1 \longmapsto 1$$
$$3 \longmapsto 5$$
$$5 \longmapsto 7$$
$$7 \longmapsto 11$$

Can check that the homomorphism property is satisfied eg. $\boxed{\phi(3\cdot 5)}$

$= \phi(7) = 11$

$\stackrel{?}{=} \phi(3)\cdot\phi(5) = 5\cdot 7$

$= 35 \equiv 11$

$\pmod{12}$

---

Example 9.5 $\quad S_3 \stackrel{?}{\cong} \mathbb{Z}_6 \,?$

$S_3$ = group of all permutation of 3 objects.

$= \{(1), (1\,2\,3), (1\,3\,2), (1\,2), (1\,3), (2\,3)\}.$

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}.$

$S_3$ is non-abelian since.

$(1\,2\,3)(1\,2) = (1\,3)$

$(1\,2)(1\,2\,3) = (1)(2\,3) = (2\,3)$

eg. $a = (1\,2\,3)$, $b = (1\,2)$

Can prove by contradiction, that

$$S_3 \not\cong \mathbb{Z}_6.$$

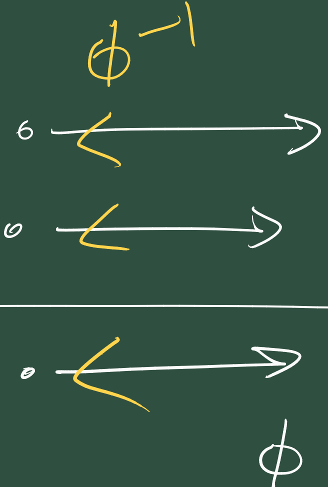
---

$\phi(x) = y.$ $\qquad\qquad \phi(z) = w$

$\phi(x^2) = y^2 \qquad \phi(xz) = yw$

$$\phi(x^2) = \phi(x \cdot x) = \phi(x)\phi(x) = \phi(x)^2 = y^2$$

$$\phi(x^m) = y^m.$$




---

<u>Theorem 9.6</u>

Assume $G \cong H$, i.e. that a mapping $\phi : G \to H$ is an isomorphism. i.e.

- $\phi$ is bijective
- $\forall\, a, b \in G \qquad \phi(ab) = \phi(a)\phi(b)$

1. Firstly $\phi^{-1} : H \to G$ exists since $\phi$ is bijective and $\phi^{-1}$ will be a bijection too.

   Does $\phi^{-1}$ satisfy the homomorphism property?

Let $x, y \in H$. Want to show that

$$\phi^{-1}(xy) = \phi^{-1}(x)\,\phi^{-1}(y).$$

Let $a, b \in G$ satisfying $\phi^{-1}(x) = a$, $\phi^{-1}(y) = b$
or equivalently $\phi(a) = x$, $\phi(b) = y$.

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

$= \phi^{-1}(\phi(ab))$, hom. prop. for $\phi$.

$= ab$, since $\phi^{-1}$ and $\phi$ are inverse maps of each other.

$$= \boxed{\phi^{-1}(x)\,\phi^{-1}(y).}$$

So $H$ is isomorphic $G$.

(2) $|G| = |H|$. Follows immediately from the existence of a bijection between the two sets.

(3). Assume $G$ is abelian.

Let $x, y \in H$, and let $a, b \in G$ satisfying $\phi(a) = x$, $\phi(b) = y$.

$$
\begin{aligned}
xy &= \phi(a)\phi(b) \\
&= \phi(ab), \text{ hom. prop.} \\
&= \phi(ba), \text{ since } G \text{ is Abelian.} \\
&= \phi(b)\phi(a), \text{ hom. prop.} \\
&= yx
\end{aligned}
$$

So $H$ is Abelian.

④. Suppose $G$ is cyclic.
i.e. there exists a generator $g \in G$
with $G = \langle g \rangle$

$$
\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, equal] & H \\
\langle g \rangle & h \\
& \langle \phi(g) \rangle
\end{tikzcd}
$$

Claim: $H = \langle \phi(g) \rangle$

Proof

Let $h \in H$. We have to find an integer $m \in \mathbb{Z}$ such that

$$h = \phi(g)^m$$

Let $a \in G$ be the pre-image of $h$,
i.e. $\phi(a) = h$

Since $G$ is cyclic with generator $g$
$\exists\, m \in \mathbb{Z}$ $a = g^m$.

So $h = \phi(a) = \phi(g^m)$

$$= \phi(g \cdot g \cdot g \cdots g)$$

$$= \phi(g)\phi(g) \cdots\cdots \phi(g)$$

$$= \phi(g)^m$$

This proves $H = \langle \phi(g) \rangle$.

So if $H$ is isomorphic $G$ by $\phi$.

not only is $H$ cyclic iff $G$ is cyclic

but $\phi$ must map generators to generators.

(5). ~~III~~ Claim: If $G$ has a subgroup of order $n$ then so does $H$.

Pf: Let $K \subset G$ be a subgroup of $G$ of order $n$.

Claim: $\phi(K)$. is a subgroup of $H$ of order $n$.

Pf. Consider the subset $\phi(K)$ of $H$.

$$\phi(K) = \{\phi(k) : k \in K\}$$

Note $|\phi(K)| = |K|$ since $\phi$ is a bijection.

1. Claim: identity of $H$ is in $\phi(K)$.

Claim: If $\phi : G \to H$ is an isomorphism and $e$ is the identity of $G$ then $\phi(e)$ is the identity of $H$.

Pf: Let $h \in H$. (and let $a$ be the pre-image of $h$, ie. $\phi(a) = h$).

$$\begin{aligned} h\,\phi(e) &= \phi(a)\phi(e) \\ &= \phi(ae) \quad \text{, hom. prop.} \\ &= \phi(a) \quad \text{, since } e \text{ is the identity of } G \\ &= h \end{aligned}$$

and can also show $\phi(e)h = h$.

So $\phi(e)$ is the identity of $H$.

So $\phi(K)$ does contain the identity of $H$ since $K$ contains the identity of $G$.

2. Let $x, y \in \phi(K)$, with pre-images $a, b$, i.e. $\phi(a) = x$, $\phi(b) = y$ and $a, b \in K$.

$$xy = \phi(a) \cdot \phi(b)$$
$$= \phi(ab), \text{ hom. prop.}$$

and note $\underline{\underline{ab \in K}}$, since $K$ is a subgroup.

$$\Rightarrow \underline{\underline{xy \in \phi(K)}}$$

(3). Claim: If $\phi : G \to H$ is an isomorphism then for every $x \in G$ $\phi(x^{-1}) = \phi(x)^{-1}$

Claim

$$\phi(x^{-1})\phi(x) = \phi(x^{-1} \cdot x), \text{ hom. prop.}$$
$$= \phi(e_G)$$
$$= e_H, \text{ the identity in } H$$

(see above)

Therefore $\phi(x)^{-1} = \phi(x^{-1})$.

So for any $x \in \phi(K)$ with pre-image $a \in K$. $(\phi(a) = x)$.

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

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

and $\underline{\underline{a^{-1} \in K}}$ since $K$ is a subgroup

so $\underline{\underline{x^{-1} \in \phi(K)}}$

So by Prop 3.30 $\phi(K)$ is a subgroup of $H$.

---

$\mathbb{Z}, +$