Ch. 6 Isomorphism

Some groups look quite "similar"

e.g. consider

$\mathbb{Z}_6$ and $\langle a \rangle$, where $\mathrm{ord}(a) = 6$

These two groups have many things in common:

- both have 6 elements
- both are cyclic
- both have 2 generators

  $\mathbb{Z}_6$: $\{1, 5\}$ $\langle a \rangle$: $\{a, a^5\}$

- group operation similar

  $i+j \bmod 6$ $\sim$ $a^i a^j = a^{i+j \bmod 6}$

want to make precise when two groups are "essentially the same"

Def. Let G and $\overline{G}$ be groups

A map $\phi: G \to \overline{G}$ is called an isomorphism if it satisfies

(a) ϕ is one-to-one (injective)

(b) ϕ is onto (surjective)

→ (c) ϕ is compatible with group operations, i.e.

$$\phi(ab) = \phi(a)\,\phi(b) \quad \text{for all } a, b \text{ in } G$$

Remark If $|G| = n < \infty \underset{(a)\&(b)}{\Longrightarrow} |\overline{G}| = n$

$$\Big(\quad \#\{g,\ g \in G\} \underset{\text{prop. (a)}}{=} \#\{\phi(g),\ g \in G\} \subset \overline{G}$$

$$\left.\begin{array}{l} \Rightarrow |G| \le |\overline{G}| \\ \phi \text{ onto} \Rightarrow |\overline{G}| = \#\{\phi(g).\ g \in G\} \le |G| \end{array}\right\} |G| = |\overline{G}|$$

Question If $|G| = |\overline{G}|$, can we always find an isom. ?

Answer No (more later)

Examples: ① $G = (\mathbb{R}, +) = \mathbb{R}$ with oper. $+$

$\overline{G} = (\mathbb{R}_+, \cdot) =$ pos. real. numbers with op. $\cdot$

Is there an isom. between G and $\overline{G}$?

need to find $\phi : \mathbb{R} \to \mathbb{R}_+$

$$\phi(x+y) = \phi(x)\phi(y)$$

recall: $e^x e^y = e^{x+y}$ (c) ✓

Try: $\boxed{\phi(x) = e^x}$ exponential function.

only need to check 1-1 and onto

known from calculus:

$x \to e^x$ strictly increasing

- if $x \neq y$, say $x < y \Rightarrow e^x < e^y \Rightarrow e^x \neq e^y$

  $\Rightarrow$ 1-1

- onto: given $y \in \mathbb{R}_+$

  $\Rightarrow e^{\ln y} = y$

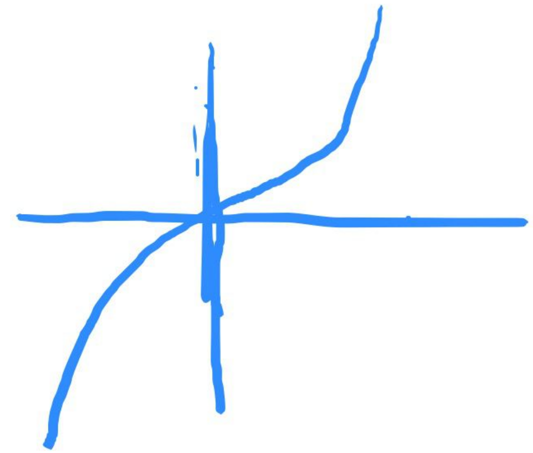
  $\Rightarrow e^x = y$ for $x = \ln y$ ✓

Add to definition above:

Two groups G and $\overline{G}$ are called isomorphic if there exists an isom. $\phi: G \to \overline{G}$

$\Rightarrow$ $(\mathbb{R}, +)$ and $(\mathbb{R}_+, \cdot)$ are isomorphic groups

② $\varphi: \; x \to x^3$
$\mathbb{R} \to \mathbb{R}$



φ: 1-1 and onto

Is φ isom. $(\mathbb{R},+) \to (\mathbb{R},+)$?

need to check: $\varphi(x+y) \overset{!}{=} \varphi(x) + \varphi(y)$

$$(x+y)^3 \overset{!}{=} x^3 + y^3$$

$\Rightarrow$ not an isom.

3. Consider $\langle a \rangle$, $a \in G$

a. $ord(a) = \infty$ i.e. $a^i \neq e$ for $i \neq 0$

claim: $\langle a \rangle$ is isomorphic to $\mathbb{Z}$

proof. need to find isom. $\phi: \mathbb{Z} \to \langle a \rangle$

$$\boxed{i \in \mathbb{Z} \mapsto a^i}$$

check: 1-1 and onto ✓

$$\phi(i+j) = a^{i+j} = a^i a^j = \phi(i)\phi(j)$$

✓

b. $ord(a) = n$

claim: $\langle a \rangle$ is isomorphic to $\mathbb{Z}_n$

proof. let $\phi: i \mapsto a^i$ $\Rightarrow \phi(\mathbb{Z}_n) = \langle a \rangle$ onto!

$\mathbb{Z}_n = \{0, 1, 2, .., n-1\}$ and 1-1: assume $\underset{\phi(i)}{a^i} = \underset{\phi(j)}{a^j}$ $\Rightarrow a^{i-j} = e$

$\Rightarrow n \mid (i-j)$

but as $i,j \in \{0,1,\ldots,n-1\}$

$\Rightarrow |i-j| < n$

$\Rightarrow n \mid (i-j)$ only if $i=j$.

$\Rightarrow$ map is 1-1.

<u>Result</u> The cyclic group $\langle a \rangle$ is isomorphic to $\mathbb{Z}_n$ if $ord(a)=n$

and it is isom. to $\mathbb{Z}$ if $ord(a)=\infty$

$\Rightarrow$ For each n there is only one cyclic group G with $|G|=n$ up to isom.

This means: every cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

More properties of isomorphisms.

(See Theorem 6.2 in book).

Let $\phi: G \to \overline{G}$ be an isom.

$\Rightarrow$ ① $\phi(e) = \overline{e}$ where $e, \overline{e}$ are the identities of G and $\overline{G}$

② $\phi(a^n) = \phi(a)^n$

③ $ab = ba \iff \phi(a)\phi(b) = \phi(b)\phi(a)$

proof ① by prop. of identity

$$\underbrace{\overline{e}\,\phi(e)}_{\in \overline{G}} = \phi(e) = \phi(ee) \overset{!}{=} \phi(e)\phi(e)$$

use isom. prop

$\Rightarrow \overline{e}\,\phi(e) = \phi(e)\phi(e)$ | multiply by $\phi(e)^{-1}$ from right.

$\overline{e} = \phi(e)$ ✓

proof of (3) assume $ab = ba$

$$\Rightarrow \phi(a)\phi(b) \underset{\text{isom.}}{=} \phi(ab) \underset{\text{assumption}}{=} \phi(ba) \underset{\text{isom}}{=} \phi(b)\phi(a)$$

<u>Application</u> The groups S_3 and $\mathbb{Z}_6$ are NOT isom.

proof. by contradiction: assume we have an isom.

$$\phi : \mathbb{Z}_6 \to S_3$$

ϕ is surj. $\Rightarrow$ $\exists\, i$ s.t. $\phi(i) = (12)$

j s.t. $\phi(j) = (23)$

$$\Rightarrow \underset{\substack{\| \\ (123)}}{(12)(23)} = \phi(i)\phi(j) = \phi(i+j) = \phi(j+i) = \phi(j)\phi(i)$$

$$= \underset{\substack{\| \\ (132)}}{(23)(12)}$$

$$\neq$$

Reason in plain English:

If $\phi: G \to \overline{G}$ is an isom.

and G is abelian

$\Rightarrow$ $\phi(G) = \overline{G}$ is abelian

$-$