



Group Homomorphism
 $(G, \cdot, e, x, y \in G, (xy) \cdot z)$
 $\varphi: G \rightarrow H$

~~$\Rightarrow \varphi(x) = \varphi(y)$~~
 $\forall x, y \in G$
 $\varphi(xy) = \varphi(x) * \varphi(y)$
 $= \varphi(x) * \varphi(y)$

2. in
 $\forall a, b \in \mathbb{Z}, x =$

$f(a+b) = f(a) + f(b)$
 $\forall a, b \in \mathbb{Z}$
 by definition $f(a+b) = \overline{a+b}$
 $= \overline{a} + \overline{b}$
 $= f(a) + f(b)$

$g: \mathbb{Z}/6\mathbb{Z} \rightarrow S_3$

- $\bar{0} \mapsto 1$
- $\bar{1} \mapsto (1\ 2)$
- $\bar{2} \mapsto (1\ 3)$
- \vdots
- $\bar{3} \mapsto (2\ 3)$
- $\bar{4} \mapsto (1\ 2\ 3)$
- $\bar{5} \mapsto (1\ 3\ 2)$

Proof by counter example

$g(\bar{1} + \bar{1}) \neq g(\bar{1}) \circ g(\bar{1})$
 $g(\bar{2}) \quad (1\ 2) \circ (1\ 2)$

$(1\ 3) \neq 1$

last time we showed that
 mapping everything to the
 identity works

- $\bar{0} \mapsto 1$
- $\bar{1} \mapsto (1\ 2)$
- $\bar{2} \mapsto 1$
- $\bar{3} \mapsto (1\ 2)$
- $\bar{4} \mapsto 1$
- $\bar{5} \mapsto (1\ 2)$

$h(\bar{3}) = h(\bar{2} + \bar{1})$
 $= h(\bar{2}) \circ h(\bar{1})$

New Concept

Isomorphism

Defn A map from

$\phi: G \rightarrow H$ is called an isomorphism if it is a homomorphism and it is bijective

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

We say G is isomorphic to H if there exists an isomorphism from the group G to the group H

denoted as $G \cong H$

We can also say that G and H are isomorphic

iff that G and H are of the same isomorphic type

* Consider the inverse map.

Suppose $\phi: G \rightarrow H$ is an isomorphism then

$\phi^{-1}: H \rightarrow G$ is an isomorphism
injective

$$\forall x \in G \quad \phi(x) = H(x)$$

$$\exists y \in H \quad \text{s.t. } G(x) = H(y) \\ \Rightarrow H^{-1}(H(y)) = G(x)$$

Proof Since ϕ is an isomorphism it is in particular bijective
 $\therefore \phi^{-1}: H \rightarrow G$ exists and is an isomorphism.

is also bijective

It remains to show

$$e^{-1}(h_1 h_2) = e^{-1}(h_1) e^{-1}(h_2) \text{ for any } h_1, h_2 \in H$$

$\forall h_1, h_2 \in H$

Note that

$$e(e^{-1}(h_1 h_2)) = h_1 h_2 \text{ and } e(e^{-1}(h_1) e^{-1}(h_2)) = h_1 h_2 \checkmark$$

$$e^{-1}(e^{-1}(h_1 h_2)) = e^{-1}(h_1) e^{-1}(h_2)$$

Identity group: $G \rightarrow G$
 $g \mapsto g$
 is an isomorphic group
 in $(\mathbb{R}, +)$ and (\mathbb{R}^+, \cdot) isomorphic

$$\left. \begin{aligned} e(e^{-1}(g)) &= g + g \\ e^{-1}(e(g)) &= g \cdot g \end{aligned} \right\} = e$$

exp: $\mathbb{R} \rightarrow \mathbb{R}^+$
 $x \mapsto e^x$
 inv: $\mathbb{R}^+ \rightarrow \mathbb{R}$
 $\ln(x) \mapsto x$

$$\left. \begin{aligned} \exp(x+y) &= e^{x+y} \\ &= e^x e^y \\ &= \exp(x) \exp(y) \end{aligned} \right\}$$

Proposition

if $e: G \rightarrow H$ is an isomorphism

then:

- (1) the cardinalities of the sets G and H are the same
 $|G| = |H|$

(2) Group G is an abelian group iff H is an abelian group

(3) for any $x \in G$ $|x| = |e(x)|$
 order of the element x in G is equal to order of $e(x)$ in H

Suppose that

$$\mathbb{Z}/6\mathbb{Z} \cong S_3$$

then

both

$\mathbb{Z}/6\mathbb{Z}$ & S_3 is abelian

but S_3 is not abelian

thus

$\mathbb{Z}/6\mathbb{Z}$ is not isomorphic
to S_3

$$\mathbb{R} \rightarrow (\mathbb{R} - \{0\})$$

\downarrow

no such
order

of 2

for any
element

\downarrow

order of $(-1) = 2$

Suppose $f: A \rightarrow B$

is bijective do we

have $S_A \cong S_B$

~~Yes~~

HW 3

§ 1.7

Defn: A group action of a

group G on set A is a

map from $G \times A$ to A , sending

$g \in G$ and $a \in A$ to $g \cdot a \in A$

st. action on a group operation

$$(1) g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$$

for any $g_1, g_2 \in G$
 $a \in A$

(2) $1 \cdot a = a$ for any
identity
in G

Check that the group S_n on
the set $A = \{1, 2, \dots, n\}$

by $\sigma \cdot a := \sigma(a)$ for any
 $\sigma \in S_n$
and $a \in A$

$$\sigma(a) \cdot a = \sigma \cdot a \cdot a$$

Let $\sigma_1, \sigma_2 \in S_n$ and $a \in A$

$$\text{Then } \sigma_1(\sigma_2 \cdot a) = \sigma_1(\sigma_2(a)) \\ = \sigma_1(\sigma_2(a))$$

recall

S is the composition

so test the RHS

$$(\sigma_1 \circ \sigma_2) \cdot a = (\sigma_1 \circ \sigma_2)(a)$$

$$1 \cdot a = 1(a) = a \text{ for any } a \in A$$

identity
in S *identity*
in A

Given any group G
and any nonempty set A

we can define the trivial
action of G on A by

$$g \cdot a = a \text{ for any } a \in A, g \in G$$

Given a group G we
can define an action of
 G on G by just interpreting
the underlying set

$$g \cdot a = ga$$

the operation in G

Given a field F

then (F^k, \circ) is a group
 F^k acting on the vector
space F^3 is $\begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix} \in F$

we can act on the
group by scalar multiplication

Given an action of a group
 G on a set A
then for each $g \in G$
we can define

$$\sigma_g : A \rightarrow A \\ a \mapsto ga$$

$$\ell : G \rightarrow SA$$

gives rise to a map
 $g \mapsto \sigma_g$