Definition of Group

G be a set of elements with operation $\cdot$

and satisfy:

closure : $a \cdot b \in G \quad \forall a, b \in G$

identity : $e \in G$ such that $e \cdot a = a \cdot e = a$, $\forall a \in G$

inverse : b is inverse of a if $a \cdot b = b \cdot a = e$, $\forall a \in G$
$b \in G$

associative : $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$,

$(G, \cdot)$ is a group.

Outline

1) Definition of group
   - closure
   - identity
   - inverse
   - associative

2) Finite vs infinite, order of a group

3) Abelian vs non-abelian

4) Operation table

5) Direct product

6) Isomorphism

Examples

① $(\mathbb{Z}_{26}, +)$ is a group of size 26

② $(\mathbb{Z}_n, +)$ is a group of size n.

$\mathbb{Z}_n$ = set of remainders modulo n $= \{0, 1, 2, \dots, n-1\}$

③ $(\mathbb{Z}, +)$ is a group of infinite size:

closure : $\forall a, b \in \mathbb{Z}$, $a+b \in \mathbb{Z}$
identity : $0 \in \mathbb{Z}$ and $0+a = a+0 = a \quad \forall a \in \mathbb{Z}$
inverse : $\forall a \in \mathbb{Z}$, $-a \in \mathbb{Z}$ and $a+(-a) = 0$
associative : $\forall a, b, c \in \mathbb{Z}$: $(a+b)+c$ is equal to $a+(b+c)$

④ $(\mathbb{Z}, *)$ is not a group.
↖ integer multiplication
identity $= 1$, $1 * a = a * 1 = a \quad \forall a \in \mathbb{Z}$
$2 \in \mathbb{Z}$ $\quad 2 * b = 1$ if $b = \frac{1}{2} \notin \mathbb{Z}$

There is no inverse for 2.

Finite group vs Infinite group

Definition: If $(G, \cdot)$ is a group of size n, then the order of G is n.

Abelian vs non-abelian

In $(\mathbb{Z}_{26}, +)$: $a+b = b+a \quad \forall a, b \in \mathbb{Z}_{26}$ commutative

A group that satisfy commutativity is a abelian group.

Homework

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$$

With operation $*$ = matrix multiplication

is a non-abelian group.

(matrix multiplication is not commutative: $A * B \neq B * A$ for some matrices A, B)

Operation table

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

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

0 is identity

each row has identity 0

Observation :

① unique identity

② unique inverse

Lemma

Given a group $(G, \cdot)$, show that

(a) the identity of $(G, \cdot)$ is unique

If there are two identities e, f

$$e \cdot a = a \cdot e = a$$
$$f \cdot a = a f = a$$

Show that e is equal to f

(b) $\forall a \in G$, the inverse of a is unique.

Direct product

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +) = \{ (a, b) \mid a \in \mathbb{Z}_2, b \in \mathbb{Z}_3 \}$

$= \{ (0,0), (0,1), (0,2), (1,0), (1,1), (1,2) \}$ of order 6

$(a,b), (c,d) \in (\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$

$(a,b) \times (c,d) = (a+c, b+d)$

Two groups $(G, \cdot)$, $(H, *)$, we can create a group $(G, \cdot) \times (H, *)$

$= \{ (g,h) \mid g \in G, h \in H \}$

with ~~operation~~ $\times$ such that

$(g,h) \times (g', h') = (g \cdot g', h * h')$

---

order of $(G, \cdot) \times (H, *)$ = order of $(G, \cdot)$ $\times$ order of $(H, *)$

Proof that $(G, .) \times (H, *)$ is a group

closure : $(g, h), (g', h') \in (G, .) \times (H, *)$

$$(g, h) \times (g', h') = (g . g', h * h') \in G \times H$$

$g . g' \in G$

$h * h' \in H$

identity: $(e_G, e_H) \times (g, h) = (e_G . g, e_H * h) \quad \forall g \in G, h \in H$

$= (g, h)$

$(g, h) \times (e_G, e_H) = (g . e_G, h * e_H)$

$= (g, h)$

inverse : $\forall g \in G, h \in H,$

$\exists$ inverse for g denoted as g^{-1}

inverse for h denoted as h^{-1}

$$(g, h) \times (g^{-1}, h^{-1}) = (g . g^{-1}, h * h^{-1})$$

$$= (e_G, e_H)$$

$$(g^{-1}, h^{-1}) \times (g, h) = (e_G, e_H)$$

associative : operation is element-wise

Isomorphism

Two groups G, H are isomorphic if

there exists a bijective map from elements in G to

elements in H that preserve the operations of

the group elements.

$$f : (G, \cdot) \longrightarrow (H, *)$$

$$\forall\, g, g' \in G$$

$$f(g \cdot g') = f(g) * f(g')$$

$$\boxed{\begin{array}{l} \text{If } g \cdot g' = \bar{g} \\ \text{then} \\ \quad f(g) * f(g') = f(\bar{g}) \end{array}}$$

Examples

1) $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$ is isomorphic to $(\mathbb{Z}_3, +) \times (\mathbb{Z}_2, +)$

2) $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$ is isomorphic to $(\mathbb{Z}_6, +)$

3) $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ is not isomorphic to $(\mathbb{Z}_4, +)$

① $(\mathbb{Z}_2,+)\times(\mathbb{Z}_3,+)$ is isomorphic with $(\mathbb{Z}_3,+)\times(\mathbb{Z}_2,+)$

$(0,0) \xrightarrow{f} (0,0)$

$(0,1) \longrightarrow (1,0)$

$(0,2) \longrightarrow (2,0)$

$(1,0) \longrightarrow (0,1)$

$(1,1) \longrightarrow (1,1)$

$(1,2) \longrightarrow (2,1)$

Let $f((a,b)) = (b,a)$

show that f preserves the operations.

w.t.s $f((a,b))\times f((c,d))$
$= f((a,b)\times(c,d))$

$$f((a,b))\times f((c,d)) = (b,a)\times(d,c)$$
$$= (b+d,\ a+c)$$
$$= f((a+c,\ b+d))$$
$$= f((a,b)\times(c,d)) \quad \square$$

Suppose $G \simeq H$ (G is isomorphic to H).
and f is an isomorphism of G and H.

Show that

① $f(e_G) = e_H$

② Let g' be the inverse of $g \in G$.

$f(g')$ is the inverse of $f(g) \in H$

---

① W.t.S: $f(e_G) \cdot h = h \cdot f(e_G) = h, \forall h \in H$

$f(e_G) \cdot h = f(e_G) \cdot f(g)$ where $f(g) = h$

$= f(e_G \cdot g)$

$= f(g)$

$= h$

$h \cdot f(e_G) = f(g) \cdot f(e_G)$

$= f(g \cdot e_G)$

$= f(g) = h$

② $g' \cdot g = g \cdot g' = e$ by definition

w.t.s $f(g') \cdot f(g) = f(g) \cdot f(g') = e$

$f(g') \cdot f(g) = f(g' \cdot g) = f(e) = e_H$

$f(g) \cdot f(g') = f(e) = e_H$

(2) Show that $(\mathbb{Z}_6, +) \cong (\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$

$(\mathbb{Z}_6, +)$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$

×	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)

$f : (a,b) \longrightarrow 3a + 2b$

1. bijective
2. $f((a,b) \times (c,d)) = f((a,b)) \times f((c,d))$

$$0 \to 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5$$

f

$$(0,0) \to (1,1) \longrightarrow (0,2) \longrightarrow (1,0) \longrightarrow (0,1) \longrightarrow (1,2)$$

$$0 \to 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5$$

$$(0,0) \to (0,2) \longrightarrow (0,1) \longrightarrow (0,0) \to (0,2) \longrightarrow (0,1)$$

is not a right map

There could be more than one map!

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, leftrightarrow, "f"'] & 1 \arrow[r] \arrow[d, leftrightarrow] & 2 \arrow[r] \arrow[d, leftrightarrow] & 3 \arrow[r] \arrow[d, leftrightarrow] & 4 \arrow[r] \arrow[d, leftrightarrow] & 5 \arrow[d, leftrightarrow] \\
(0,0) \arrow[r] & (1,1) \arrow[r] & (0,2) \arrow[r] & (1,0) \arrow[r] & (0,1) \arrow[r] & (1,2)
\end{tikzcd}$$

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$

×	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)

$\xrightarrow{f}$

	0	4	2	3	1	5
0	0	4	2	3	1	5
4	4	2	0	1	5	3
2	2	0	4	5	3	1
3	3	1	5	0	4	2
1	1	5	3	4	2	0
5	5	3	1	2	0	4

This operation table represents $(\mathbb{Z}_6, +)$!

③ Show that $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_4$

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

$\mathbb{Z}_2 \times \mathbb{Z}_2$

In $\mathbb{Z}_2 \times \mathbb{Z}_2$: $(a,b) + (a,b) = (0,0) \quad \forall (a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$

In $\mathbb{Z}_4$: $a + a \neq 0$ except when $a = 0$

An isomorphism f should map the inverse of an element $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ to the inverse of $f((a,b)) \in \mathbb{Z}_4$.

For all $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, (a,b) is its own inverse.

So, $f((a,b)) \in \mathbb{Z}_4$ should also be its own inverse. But in $\mathbb{Z}_4$, all non-zero element is not its own inverse.