

Chapter 2: Groups.

Def: A binary operation on a set G is a function that assigns to each ordered pair of elements in G an element in G . (closed binary operation)

exp: on \mathbb{Z} . $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$

$$(m, n) \rightarrow m + n$$

$$m, n \in \mathbb{Z}$$

$$m + n, m, n \in \mathbb{Z}$$

$$g: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

$$(m, n) \rightarrow m \cdot n$$

} are binary operations

$$h: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$

$$(m, n) \rightarrow \frac{m}{n}$$

$$m, n \in \mathbb{Z} \text{ but } \frac{m}{n} \notin \mathbb{Z}$$

} is not a binary operations

Def: Let G be a nonempty set, let $*$ be binary operation on G . Then $(G, *)$ is called a group iff: ① closure.

1. **Associative:** $\forall a, b, c \in G \rightarrow (a * b) * c = a * (b * c)$

2. **Identity:** $\exists e \in G, e * a = a \quad \forall a \in G$. (e called an Identity).

3. **Inverse:** $\forall a \in G, \exists b \in G, a * b = b * a = e$. (b called an Inverse for a).

$$* : +, \cdot, -, \wedge$$

exp:

1. $(\mathbb{Z}, +)$ is a group.
- a. Associative : yes, $(a+b)+c = a+(b+c)$
 - b. Identity : 0 is the identity, $0+a = a$
 - c. Inverse : $-a$ is the inverse of a , $-a+a = 0$

2. (\mathbb{R}^*, \cdot) is a group.
- a. Associative : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
 - b. Identity : 1 is the identity.
 - c. Inverse : $a^{-1} = \frac{1}{a}$ is the inverse.

3. (\mathbb{Q}^*, \cdot) is a group.

4. $(M_{2 \times 2}, +)$ is a group.

5. $(GL(2, \mathbb{R}) = \{A \in M_{2 \times 2}(\mathbb{R}) \mid \det A \neq 0\}, \cdot)$ is a group.

a. Associative ✓

b. Identity : $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

c. Inverse : $A^{-1} = \frac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

6. $(\{1, -1, i, -i\}, \cdot)$ is a group.

$i = \sqrt{-1}$ $i^2 = -1$

\odot	1	-1	i	-i	Identity is 1
1	1	-1	i	-i	Identity = 1
-1	-1	1	-i	i	Inverse : 1 is 1
i	i	-i	-1	1	-1 is -1
-i	-i	i	1	-1	i is -i -i is i

exp: $(\mathbb{Z}_4, \oplus_4) = \{ [0], [1], [2], [3] \}$

\oplus_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

Associative.

Identity = 0

Inverse \Rightarrow 0 is 0

1 is 3

2 is 2

3 is 1

Identity is 0 and 0 is identity

Inverse

its a group.

Note: $\mathbb{Z}, \mathbb{R} = \text{relation}$

$a \equiv b \text{ iff } 4 | a - b$

ref.

sym.

tran.

$[0] = \{ \dots -8, -4, 0, 4, 8, 12, \dots \}$

$[1] = \{ \dots -1, -3, 1, 5, 9, 13, \dots \}$

$[2] = \{ \dots -6, -2, 2, 6, 10, 14, \dots \}$

$[3] = \{ \dots -5, -1, 3, 7, 11, 15, \dots \}$

exp: (\mathbb{Z}_4, \otimes) . its not a group.

exp: $(\mathbb{Z}_5^*, \otimes_5)$: $\{[1], [2], [3], [4]\}$

\otimes	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

its a group.

Def: A group G is commutative (abelian) iff $a * b = b * a \quad \forall a, b, c \in G$.

$GL(2, \mathbb{R})$ is a nonabelian group.

Def: A group G is finite iff G has finite number of elements.
otherwise G is infinite.

Thm: let $(G, *)$ be a group then e is unique.

pf: spse that e, \bar{e} are two identities, Then

$$e = e * \bar{e} = \bar{e}$$

since \bar{e} is the identity \leftarrow \rightarrow since e is the identity.

$$\Rightarrow e = \bar{e}$$

So its one identity.

Thm: If G is a group and $b \in G$ then b^{-1} is unique.

pf: suppose $\bar{b}, \bar{\bar{b}}$ are two inverses for b , then

$$(\bar{b} * b) * \bar{\bar{b}} = \bar{b} * (b * \bar{\bar{b}})$$

$$e * \bar{\bar{b}} = \bar{b} * e$$

$$\bar{\bar{b}} = \bar{b} \quad \#$$

Thm: cancellation: let G be a group, let $a, b, c \in G$ Then

if $a * b = a * c$ then $b = c$.

if $b * a = c * a$ then $b = c$.

pf: suppose, $a * b = a * c$

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

$$(a^{-1} * a) * b = (a^{-1} * a) * c$$

$$e * b = e * c$$

$$b = c \quad \#$$

exp. to groups:

1. $(\mathbb{Z}, +)$

2. $(\mathbb{Q}, +)$

3. $(\{ \neq 1 \}, \cdot)$

4. (\mathbb{Q}^*, \cdot)

5. $(GL(n, \mathbb{R}), \cdot)$, $GL(n, \mathbb{R}) = \{ A \in M_{n \times n}, |A| \neq 0 \}$

* $\mathbb{Z}_n :=$ the set of all equivalence classes mod n .
 $= \{ [0], [1], [2], \dots, [n-1] \}$.

Fact: $(\mathbb{Z}_n, +)$ forms a Group.

→ Question: Could we define $[x][y] = [xy]$ and make a group??

exp: $n=6$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	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

examples :

① show that $GL(2, \mathbb{R}), \cdot$ is not commutative :

$$A = \begin{bmatrix} 3 & 2 \\ 4 & 2 \end{bmatrix} \quad B = \begin{bmatrix} 5 & 3 \\ 6 & 2 \end{bmatrix}$$

Notice that $AB \neq BA$.

② Find $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}^{-1}$ in $GL(2, \mathbb{R})$.

$$A^{-1} = \frac{1}{(2)(5) - (6)(3)} \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix}$$

exp. which of the following is a group, justify :

① (\mathbb{Q}^+, \cdot) : Associative ✓

identity = 1

inverse of $\frac{m}{n}$ is $\frac{n}{m}$ so its a group.

② $(\mathbb{Q}^{\sqrt{2}}, \cdot)$: Not Associative, $\sqrt{2} \times \sqrt{2} = 2 \notin \mathbb{Q}^{\sqrt{2}}$

No Identity

so not group.

③ $(M_{2 \times 2}(\mathbb{R}), \cdot)$: No inverse For $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

so not group.

④ $(\mathbb{Z}_4, \otimes_4)$: 0, 2 not inverse

so not group

Just Jz
→

$$⑤ \mathbb{R}^2 = \left(\{ (a,b) \mid a,b \in \mathbb{R} \}, + \right)$$

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

Associative ✓

identity = (0,0).

$$\text{inverse for } (a,b) = (-a, -b) \rightarrow (a,b) + (-a, -b) = (0,0) = e$$

So its a group.

$$⑥ \text{SL}(2, \mathbb{R}) = \{ A \in M_{2 \times 2} \mid |A| = 1 \}, \cdot \text{ its a group}$$

$$⑦ \text{GL}(2, \mathbb{Z}_7) = \{ A \mid \det A \neq 0 \} \text{ group}$$

$$\text{exp } \begin{bmatrix} 3 & 1 \\ 4 & 1 \end{bmatrix} \Rightarrow 3 - 8 = -5 \xrightarrow{\text{mod } 7} = 2$$

$$\text{inverse: } \frac{1}{2} \begin{bmatrix} 1 & -2 \\ -4 & 3 \end{bmatrix} \xrightarrow{\text{mod } 7} = 4 \begin{bmatrix} 1 & 5 \\ 3 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 20 \\ 12 & 12 \end{bmatrix}$$

$$\text{mod } 7 \text{ مود } = \begin{bmatrix} 4 & 6 \\ 5 & 5 \end{bmatrix}$$