

# Binary Operation

~~5~~ ~~2~~  $\rightarrow$   $(2) \times (2) \rightarrow (4)$

$S \rightarrow$  Set  
 $(*)$  mapping

$S \times S \rightarrow S$  is defined as  $*$   $(a, b)$   
 $a * b$

$(+)$

$2 + 2 = 4$   
 $\sqrt{2} + \sqrt{3} \neq \sqrt{5}$   
 $a = 2 + \sqrt{3}$   
 $b = -\sqrt{3}$   
 $a, b \in \mathbb{R}$

$a + b = 2$   $\notin \mathbb{R}/\mathbb{Q}$

## Groupoid

$(G)$

$(G, *)$   
 $(G, +)$

## Semigroup

$(G, *)$

$a * (b * c) = (a * b) * c$

## Monoid

$\rightarrow (G, *)$

$a * (b * c) = (a * b) * c$

$\exists e \in G$  such that  $a * e = e * a = a$   
 $\forall a \in G$

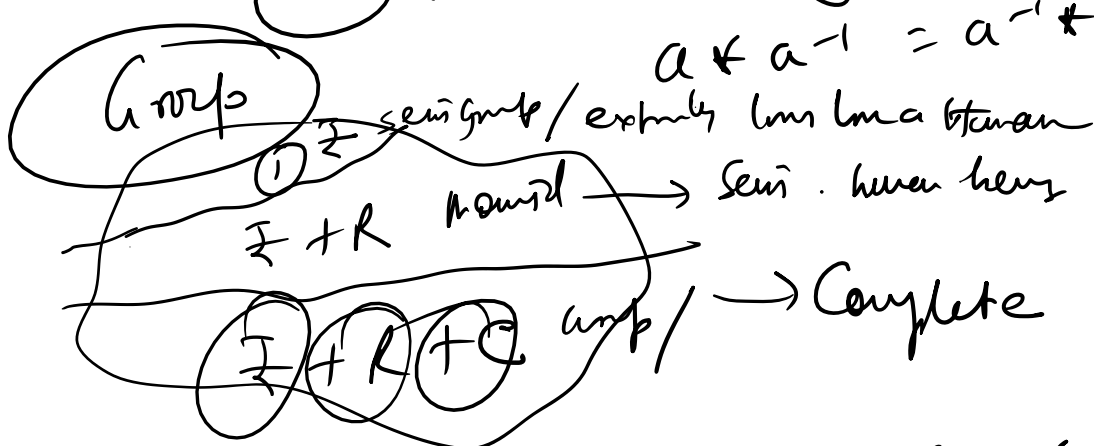
Group

$(G, *)$

- (i) ✓
- (ii) ✓
- (iii)  $\forall a \in G$

$\exists a^{-1} \in G$

$\forall a \in G \quad \exists a^{-1} \in G$   
 $a * a^{-1} = a^{-1} * a = e$



Mahatma  
 Gandhi

$\mathbb{C} + \mathbb{R}$   
 $\{0\}$   
 $n=1$   
 $\{ \}$   
 $2+3=6$   
 $5 \times 0 = 0$   
 $n=0$

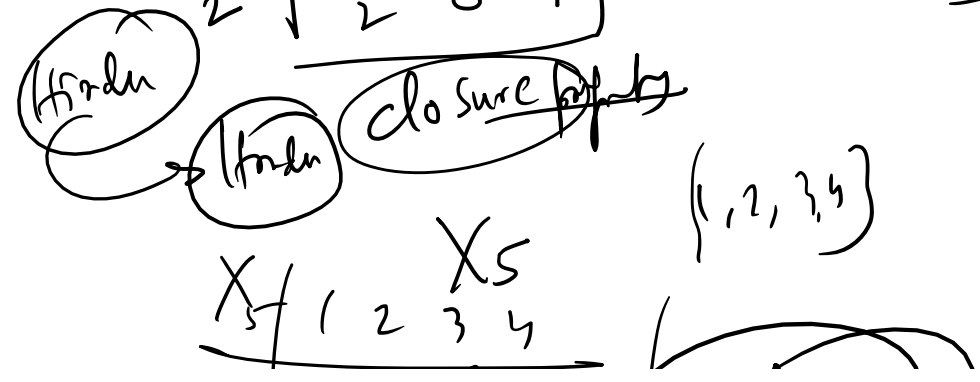
Example

Matrices  
 addition  
 $m \times n$   
 addition

$\mathbb{Z}_3 = \{0, 1, 2\}$

$+_3$		0	1	2
0		0	1	2
1		1	2	0
2		2	0	1

modulo...  
 $\frac{7}{5} \quad R=2$   
 $\frac{a}{b} \quad R=a < b$   
 $\frac{5}{7} \quad R=5$



$\lambda$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Close

Ring

$$(a^{-1})^{-1} = a$$

$$a + b = b + a$$

Empty set  $\begin{cases} + \\ \times \end{cases}$

$$a + b = b + a$$

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

~~$$a + 0 = a$$~~

$$(a) + (b + c)$$

$$a + 0 = a$$

Associative ??

Commutative Ring:  $ab = ba$

9062395723

Field

A Commutative Ring

with unity  $\rightarrow$   
 $\forall$  element non 0 element  $\neq$  0

$$G = \{5, 15, 25, 35\}$$

$\times$  modulo of 40

Modular

$$a \equiv b \pmod{n}$$

# Modular

$$a \equiv b \pmod{n}$$

Longhand

$$\begin{array}{r} \text{Reminders} \rightarrow (-2) \quad 1 - (-2) \\ 16 \equiv 1 \pmod{3} \rightarrow (-1) \quad \Rightarrow 3 \\ 14 \equiv 2 \pmod{3} \quad 2 - (-1) \\ \hline 30 \equiv 3 \pmod{3} \\ 30 \equiv 0 \pmod{3} \end{array}$$

$$a_1 \equiv b_1 \pmod{c}$$

$$a_2 \equiv b_2 \pmod{c}$$

$$\hline a_1 a_2 \equiv b_1 b_2 \pmod{c}$$

$$2^{55} + 1 \quad \text{is it divisible by } \underline{11}$$

$$\begin{array}{l} 2^{55} \\ (2^5)^{11} \end{array} \quad \begin{array}{l} 2^5 = 32 \equiv 10 \pmod{11} \\ 32 \equiv -1 \pmod{11} \\ (32)^{11} \equiv (-1)^{11} \pmod{11} \\ 2^{55} = 32^{11} \equiv -1 \pmod{11} \end{array}$$

$$2^{55} + 1 \equiv -1 + 1 \pmod{11}$$

$$2^{55} + 1 \equiv 0 \pmod{11}$$

$$2^{55} + 1$$

$\rightarrow 11$  Annulle  $\rightarrow \dots$

$\hookrightarrow$  11 Annulle

$G = \{5, 15, 25, 35\}$  mod 40

$$\begin{array}{r} 35 \times 20 \\ = 700 \\ \underline{175} \\ 825 / 21 \\ \underline{840} \\ 35 \end{array}$$

$X_{i0}$	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

$$\begin{array}{r} 40 \mid 5 \ 25 / 13 \\ \underline{520} \\ 5 \end{array}$$

$$2 \mid \begin{array}{r} 35 \\ 25 \end{array}$$

$$\underline{875}$$

Idemto  $\rightarrow$  25 Bm  $\textcircled{9}$

$G$  from a group  
 order  $\textcircled{4}$  finite  $a \in G \quad a = a^{-1}$   
 $a^2 = e$

$O(25) = 1$   $\textcircled{1 \text{ or } 2}$   
 exponent =  $\textcircled{2}$

Lagrange's Thm. order of Subgroup

of a finite group

divides the order of the group.





Indicates the order of the group.

$$O(H \times K) = \frac{O(H) \cdot O(K)}{O(H \cap K)}$$

Abelian group

Commutative  $ab = ba \quad \forall a, b \in G$

$(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$

$(\mathbb{Q}, \cdot)$ ,  $(\mathbb{R}, \cdot)$ ,  $(\mathbb{C}, \cdot)$

Normal Subgroup: A subgroup  $H$  of a group  $G$   
 if  $Ha = aH \quad \forall a \in G$

2011  $G$  denotes a group  $2 \times 2$  invertible matrix ( $0 \neq 0$ )

$$H_1 = \{ A \in G, \det(A) = 1 \}$$

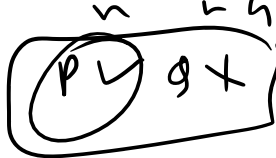
$$H_2 = \{ A \in G, A \text{ is upper triangular} \}$$

$P: H_1$  is a normal subgroup of  $G$  ✓

$Q: H_2$  is " " X

a)  $P, Q$  are

b)



c)  $P \times Q \cup$

d)  $P \times Q \times$

i)  $A, B \in H_1 \Rightarrow A, B \in G \quad |A| = 1 \quad |B| = 1$

$$\dots |AB| = |A||B|^{-1} = |A||B|^{-1} \quad \square$$

$$i) \quad A, B \in H_1 \Rightarrow A, B \in U \quad |A| = 1 \quad |B| = 1$$

$$|AB^{-1}| = |A||B^{-1}| = |A||B|^{-1} = 1 \cdot 1 = 1$$

$$\Rightarrow |A| \cdot \frac{1}{|B|} = 1 \cdot 1 = 1 \quad \left[ |B|^{-1} = |B|^{-1} \right]$$

$H_1$  is a subgroup of  $G$

Let,  $A \in H_1$ ,  $P \in G$

$|A| = 1$ ,  $P$  is an invertible mapping,  $P^{-1}$  exists

$$|P^{-1}AP| = |P^{-1}||A||P| = |P^{-1}||P| = 1 \quad \left[ |A| = 1 \right]$$

$$P^{-1}AP \in H_1, \forall A \in H_1$$

$P \in G \Rightarrow H_1$  is a normal subgroup of  $G$ .

(ii)  $A, B \in H_2$

$A, B \in G$  such that  $A, B$  are U/T/M

$B^{-1}$  is also an invertible U/T/M.

$AB^{-1} \rightarrow$  is U/T/M.

$AB^{-1} \in H_2 \forall A, B \in H_2$  is a subgroup

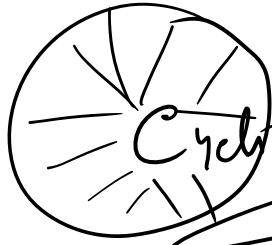
$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

$$B^{-1}AB = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 4 \\ -1 & 1 \end{bmatrix} \notin H_2$$

$$v = \begin{bmatrix} 3 & 4 \\ -1 & 1 \end{bmatrix} \notin H_2$$

$H_2$  is not a normal subgroup of  $G$ .



Cyclic Group

$$b \in G$$

any element of  $G$

is a power of  $\langle b \rangle$

$b \rightarrow$  Generator of  $G$   $\langle b \rangle$

$G = \langle b \rangle$  then  $o(a) = o(b)$

ex

$\circledast \{1, \omega, \omega^2\} \rightarrow$  Generated by  $\omega$   
 $\circledast \{1, -1, i, -i\}$  finite root of unity  
 $i = \sqrt{-1}$   
 $\circledast \{(-1)^k\}$   
 $\Rightarrow \circledast (-1)$