7/8/23

Binary operation

A mapping $*$ is called binary operation on a non-empty set G if,

$*(a,b)$ is $a*b$ (we get Element of same set after operation)

$*: G \times G \to G$.

s.t, $*: (a,b) \to a*b$.

Algebraic structure

If $*$ is a binary operation over G, then the ordered pair $(G,*)$ is called Algebraic structure.

Group :

In an algebraic structure $(G,*)$ is called a group, if it satisfies the following properties:

(i) Closure law.

If $a, b \in G$, then $a*b \in G$.

(ii) Associative Law

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

(iii) Existence of Identity

$\forall a \in G$, $\exists e \in G$ s.t, $a*e = a = e*a$.

(iv) Existence of Inverse

$\forall a \in G$, $\exists b \in G$

s.t, $a*b = e = b*a$.

Group :

$(G, *)$

(a) Closure law

$a, b \in G \Rightarrow a * b \in G.$

(b) Associative law $\quad a, b, c \in G$

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

(c) Existence of Identity. $\forall a \in G, \exists e \in G$

$a * e = a = e * a.$

(d) Existence of Inverse.

$\forall a \in G, \exists b \in G$

such that $ab = e = ba$.

---

	group	
$(N, +)$	✗	(additive identity do not exist) nor inverse
$(N, *)$	✗	(Multiplicative Inverse do not exist)
$(W, +)$	✗	(No additive inverse)
$(W, *)$	✗	(No multiplicative inverse)
$(I, *)$	✗	(No multiplicative inverse)
$(I, +)$	✓	
$(Q, +)$	✓	
$(Q, *)$	✓	

$N \subset W \subset I \subset Q \subset R \subset C$

✗ ✗ + + → (group)

* →

Once started, It will follow on for other groups also.

like $(I, +)$, $(Q, +)$ $(R, +)$ $(C, +)$ are all groups.

Reason as, $I \subset Q \subset R \subset C$

$*$ → binary operation

Abelian group

(already 4 definitions are true)

* group $(G,*)$ is called abelian group, if commutative law holds,

ie, $\forall a,b \in G$, $a*b = b*a$.

Eg: $(I,+)$ $(Q,*)$.

Groupoid $(G,*)$ (one law holds)

An algebraic structure is called groupoid if closure law holds.

Eg: $(I,-)$ ✓

$(N,-)$ ✗

semi group $(G,*)$ (2 laws hold)

↳ closure and associative law holds, then algebraic structure is called semi group.

Eg – $(N,+)$

Monoid (3 laws hold)

↳ Algebraic structure, if closure, associative & identity law holds, then called Monoid.

Eg – $(I,*)$

order of group:

→ No. of elements in a group

→ denoted by $O(G)$.

Q show that set $M=\{ a+b\sqrt{2} ; a,b \in I\}$ is an abelian group.

$(M,+)$ → ab group.

(1) Closure Law

let, $a+b\sqrt{2}, c+d\sqrt{2} \in M$, $a,b,c,d \in I$, then,

$(a+b\sqrt{2}) + (c+d\sqrt{2})$

$(a+c) + \sqrt{2}(b+d)$. ($\because (I,+)$ is ab group)

I is closed with '+'

(2) Associative law

$a+b\sqrt{2}$, $c+d\sqrt{3}$ $e+f\sqrt{2}$.

LHS: $(a+b\sqrt{2})+((c+d\sqrt{2})+(e+f\sqrt{2})$.

$= \left((a+c)+\sqrt{2}(b+d)\right)+(e+f\sqrt{2})$

$= \left((a+c)+e\right)+\sqrt{2}\left((b+d)+f\right)$

$= \left(a+(c+e)\right)+\sqrt{2}\left(b+(d+f)\right)$

$(\because (I,+)$ ab group)

or

$(I,+)$ is associative.

$\Rightarrow (a+b\sqrt{2})+\left((c+e)+\sqrt{2}(d+f)\right)$

$(a+b\sqrt{2})+(c+d\sqrt{2})+(e+f\sqrt{2})$.

LHS = RHS

(3)

→ Element of Id.

$\forall\ a+b\sqrt{2} \in G \quad \exists \quad 0+0\sqrt{2} \in G$ (e)

st, $(a+b\sqrt{2})+(0+0\sqrt{2})$

$= (a+0)+(b+0)\sqrt{2}$

$= a+b\sqrt{2}$ $\because (I,+)$ is ab grp

(4) Element of Inverse.

$\forall\ a+b\sqrt{2} \quad \exists\ -a-b\sqrt{2} \in G$

st, $(a+b\sqrt{2})+(-a-b\sqrt{2})$

$(a-a)+(b-b)\sqrt{2}$

$= 0+0\sqrt{2}$ $\because (I,+)$ is ab grp.

$= 0$

⑤ Commutative law

$\forall\ a+b\sqrt{2} \in G$ and $c+d\sqrt{2} \in G$

$$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d\sqrt{2}) = (c+d\sqrt{2})+(a+b\sqrt{2})$$

$\because$ (Integer Addition is commutative)

Q Show that the set of all +ve Rational Numbers forms an abelion group under the composition defined as

$\mathbb{Q}^+$ $\quad a*b = \frac{ab}{2}$.

Sol^n $\quad$ TST: $(\mathbb{Q}^+, *)$ ab group.

① Closure law

$\forall a, b \in \mathbb{Q}^+$

$$a*b = \frac{ab}{2} \in \mathbb{Q}^+$$

($\because (\mathbb{Q}^+, \cdot)$ is ab group)

② Associative law

$$(a*b)*c$$

$$\left(\frac{ab}{2}\right)*c = \frac{\left(\frac{ab}{2}\right)c}{2}$$

$= a\left(\frac{bc}{2}\right)$ $\left(\because (\mathbb{Q}^+, \cdot) \text{ ab group}\right)$

$a * \left(\frac{bc}{2}\right)$

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

(3) E. of Id.

$\forall\, a \in \mathbb{Q}^+, \exists\, e \in \mathbb{Q}^+$ st,

$a * e = a$

$\frac{ae}{2} = a$

$a(e-2) = 0$

$e = 2$, as $a \neq 0$. (Reason $a \in \mathbb{Q}^+$)

(4) E. of Inverse

$\forall\, a \in \mathbb{Q}^+, \exists\, b \in \mathbb{Q}^+$ st

$a * b = e$

$\frac{ab}{2} = 2$

$ab = 4$

$b = \frac{4}{a}$. exists.

(5) Commutative Law

$a, b \in \mathbb{Q}^+$

LHS: $a * b = \frac{ab}{2}$

$= \frac{ba}{2}$ $\left(\because (\mathbb{Q}^+, \cdot) \text{ ab group.}\right)$

$= b * a.$

Q Show that set of all integers (I) forms a group wrt binary operation * defined as

$$a*b = a+b+1 \quad \forall\ a,b \in I.$$

Soln TST: $(I,*)$ group.

① Closure law

$\forall\ a,b \in I$,

$$a*b = a+b+1 \in I \quad (\because (I,+) \text{ group})$$

② Associative law

LHS = $(a*b)*c = (a+b+1)*c$

$= (a+b+1)+c+1$

$= a+b+c+2$ (For Addition use this approach)

RHS: $a*(b*c)$

$= a*(b+c+1)$

$a+(b+c+1)+1$

$= a+b+c+2.$

$= \text{LHS}.$

③ E of Id.

$\forall\ a \in I, \exists\ e \in I$ st,

$a*e = a$

$a+e+1 = a$

$e = -1 \in I.$

④ Existence of Inverse

$\forall a \in I, \exists\ b \in I$ st,

$a*b = e$

$a+b+1 = -1$

$a+b = -2$

$b = -2-a.$

Q Show that the set of all $m \times n$ matrices having their elements as integers forms an ∞ abelian group. wrt the composition Matrix addition.

$$M = \{[a_{ij}]_{m \times n} : a_{ij} \in I\}$$

$O \rightarrow$ null matrix

TST: $(M, +)$ ab grp.

Soln

① Closure law

$\forall A, B \in M$, $a_{ij}, b_{ij} \in I$

$$A+B = [a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}] \in M$$

$(\because (I, +)$ ab grp$)$

or $\therefore$ M is closed wrt '+'.

② Associative law

$(A+B)+C$

$$([a_{ij}] + [b_{ij}]) + [c_{ij}]$$

$$[a_{ij} + b_{ij}] + [c_{ij}]$$

$$= [(a_{ij} + b_{ij}) + c_{ij}]$$

$$= [a_{ij} + (b_{ij} + c_{ij})]$$

$$= [a_{ij}] + [b_{ij} + c_{ij}]$$

$$= A + (B+C)$$

③ E of Id.

$\forall A \in M$, $\exists O \in M$ st,

$$A + O = [a_{ij}]_{m \times n} + [0]_{m \times n}$$

$$= [a_{ij} + 0]_{m \times n}$$

$$= [a_{ij}]$$

$$= A$$

④ Existence of Inv.

$\forall A \in M$, $\exists B \in M$ where $B = -A$. st,

$$A + (-A) = [a_{ij}] + [-a_{ij}]$$

$$= [0]_{m \times n}$$

$$= O$$

⑤ Commutative law

$$A+B = [a_{ij}] + [b_{ij}]$$

$$= [a_{ij} + b_{ij}]$$

$$= [b_{ij} + a_{ij}]$$

$$= [b_{ij}] + [a_{ij}] = B+A. = \text{RHS}$$

Thus, it forms an abelian group.

$(M, +)$ ab grp.

Eg: For $(M, \cdot)$

↳ Pay heed to commutative law as Matrix multiplication is not commutative.

Q Show that $G = \{ \ldots 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3 \ldots \}$ forms an abelion group wrt multiplication.

Soln TST: $(G, \cdot)$ ab grp.

(a) Closure law

$\forall a, b \in I$ $\quad 2^a, 2^b \in G$

$2^a \cdot 2^b = 2^{a+b} \in G$ $(\because (I,+)$ abgrp.

(b) Associative law.

$2^a, 2^b, 2^c \in G \qquad \forall a, b, c \in I.$

$(2^a \cdot 2^b) \cdot 2^c = (2^{a+b}) \cdot 2^c$

$= 2^{(a+b)+c}$

$= 2^{a+(b+c)}$ $\because (I,+)$ ab grp

$= 2^a \cdot 2^{b+c}$

$= 2^a \cdot (2^b \cdot 2^c)$

$=$ RHS.

(c) E of Identity.

$\forall 2^a \in G, \exists\ 2^0 \in G$ st,

$2^a \cdot 2^0 = 2^{a+0}$

$= 2^a$ $(\because (I,+)$ abgrp)

(d) E of Inverse

$\forall 2^a \in G, \exists\ 2^{-a} \in G$ st

$2^a \cdot 2^{-a} = 2^{a-a} = 2^0$ (e)

(e) Commutative law

$\forall 2^a, 2^b \in G$

$2^a \cdot 2^b = 2^{a+b} = 2^{b+a}$

$= 2^b \cdot 2^a$ $(\because (I,+)$ abgrp)

$=$ RHS.

Thus, $(G, \cdot)$ is an abelion group.

• Finite Sets

Q Show that the set of cube roots of unity forms an abelion group wrt multiplication.

soln TST $(G, \cdot)$ abgroup.

let $G = \{1, \omega, \omega^2\}$

(e) →	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

→ Composition Table.

① Closure law.

It is clear from the Table that $\forall\ a, b \in G,\ a.b \in G$

② Associative law

LHS: $(1.(w).w = w^2.w = 1$

RHS: $1.(w^2.w) = 1.w^3 = 1.$

LHS = RHS

③ E. of Id. → (where row Repeats)

$e = 1$

④ E of Inv.

$1 - 1$

$w - w^2.$

$w^2 - w$

⑤ Commutative law

$\forall\ a, b \in G.$

$a.b = b.a$

$\therefore (G, \cdot)$ abelian group.

Trick:

For Matrix

$A = A^T$

Symmetric

→ commutative law holds true.

Q Show that the set of all 4 4^{th} roots of unity forms an abelian group wrt Multiplication.

Soln

$x = (1)^{\frac{1}{4}}$

$x^4 = 1$

$x^4 - 1 = 0$

$(x^2-1)(x^2+1) = 0$

$(x-1)(x+1)(x^2+1) = 0$

$x = 1, -1, +i, -i.$

$G = \{1, -1, +i, -i\}$

TS $T(G, \cdot)$ abgrp

Soln Composition Table

$\cdot$	1 (e)	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	$+1$
$-i$	$-i$	$+i$	1	-1

① Closure law

↳ From the composition table

$\forall a, b \in G$

$a * b \in G$

ie $a.b \in G$

② Associative law

$LHS = 1 \cdot (i \cdot -i) = 1 \cdot (-1) = +1$

$RHS = (1 \cdot i) \cdot -i = i \cdot -i = +1$

$RHS = LHS$

③ E of Identity.

$e = 1$

④ E of Inverse

$1 - 1$

$i - -i$

$-i - +i$

$-1 - -1$

⑤ Commutative law

$i \cdot -i = -i^2 = 1$

$-i \cdot i = -i^2 = 1$

$RHS = LHS.$

Or $\forall a, b \in G$

$a.b = b.a$

→ holds true.

10/8/23

Q Show that the set of 4 matrices, forms a multiplicative group which is abelion.

$$\underset{A}{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}, \quad \underset{B}{\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}}, \quad \underset{C}{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}, \quad \underset{D}{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}}$$

Soln — First labelling (A, B, C, D)

$G = \{A, B, C, D\}$

TST: $(G, \cdot)$ grp.

·	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

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

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

$CB = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = D$

① Closure law

From the table, (composition table)

$\forall A, B \in G_1$

$A \cdot B \in G_1$.

② Associative law. (Eg - Only for finite grp)

LHS $= (D \cdot B) \cdot C = C \cdot C = A$

RHS $D \cdot (B \cdot C) = D \cdot D = A$.

LHS = RHS.

③ E of Id.

$e = A$.

④ E of Inverse.

A – A

B – B

C – C

D – D.

$\therefore (G_1, \circ)$ grp.

⑤ Commutative law

$\forall A, B \in G_1$.

$A \cdot B = B \cdot A$

$\therefore (G, \cdot)$ ab group.

Q If G_1 is the set of 4 special functions f_1, f_2, f_3, f_4, defined on the set of complex numbers as,

$G_1 = \{f_1, f_2, f_3, f_4\}$

where $f : \mathbb{C} \to \mathbb{C}$

$f_1(z) = z$, $f_2(z) = -z$, $f_3(z) = \frac{1}{z}$, $f_4(z) = -\frac{1}{z}$.

TST: $(G_1, \cdot)$ ab grp

(ab grp as composite of 2 Mappings).

↳

$\cdot$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

(e)

① Closure law

From the table

$\forall f, g \in G$

$f \cdot g \in G$

② Associative law.

$LHS = (f_4 \cdot f_2) \cdot f_3 = f_3 \cdot f_3 = f_1$

$RHS = f_4 \cdot (f_2 \cdot f_3) = f_4 \cdot f_4 = f_1$

$LHS = RHS$

③ $e = f_1$

④ $f_i - f_i \quad i = 1, 2, 3, 4$

⑤ $\forall f, g \in G.$

$fog = gof.$

$f_1 \cdot f_1(z) = f_1(f_1(z))$

$= f_1(z)$

$f_1 \cdot f_2(z) = f_1(f_2(z))$

$= f_1(-z)$

$= -z$

$= f_2(z)$

$f_1 \cdot f_3(z) = f_1\left(\frac{1}{z}\right) = \frac{1}{z} = f_3(z)$

$f_2 \cdot f_2(z) = f_2(f_2(z)) = f_2(-z)$

$= +z = f_1(z)$

$f_2 \cdot f_3(z) = f_2\left(\frac{1}{z}\right) = \frac{-1}{z} = f_4$

$f_2 \cdot f_4(z) = f_2(f_4(z)) = f_2\left(\frac{-1}{z}\right)$

$+\frac{1}{z} = f_3$

$f_3 \cdot f_3(z) = f_3\left(\frac{1}{z}\right) = z = f_1$

$f_4 \cdot f_4(z) \Rightarrow f_4(f_4(z)) = f_4\left(\frac{-1}{z}\right)$

$\Rightarrow +z = f_1$

(Bincary Operations)

- **Addition Modulo m:**

$$a +_m b = r$$

If a, b be any two integers, then the operation of Addition Modulo m is defined as the least non-negative remainder 'r' when the ordinary sum of a & b is divided by m where $m \in I^+$

$3 +_5 6 \Rightarrow \quad \frac{3+6}{5} = \frac{9}{5} \rightarrow r = 4.$

For -ve.

$-21 +_4 7 = \quad \frac{-21+7}{4} \Rightarrow \frac{-14}{4} \Rightarrow (-2+m)$

$\Rightarrow -2+4 = 2.$

$4\overline{)-14}\ (-3$
$+12$
$\overline{-2}$

- **Multiplication Modulo m:**

$\cdot_m$ or $*_m$

$a, b \in I$

$a \cdot_m b = r$

$\frac{a.b}{m}$

→ (Multiplication Modulo m is) defined as the least non negative 'r' when ordinary product of a & b is divided by m.

Q PT, $G = \{0, 1, 2, 3, 4, 5\}$ is a finite ab group w.r.t. (addition Modulo 6) $(+_6)$.

Sol^n TST: $(G, +_6)$ ab group

$+_6$	0 (e)	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

From the composition Table.

① Closure law → $\forall a, b \in G$
$a +_6 b \in G$.

② Associative law.

LHS = $(3 +_6 5) +_6 4 = 2 +_6 4 = 0$

RHS = $3 +_6 (5 +_6 4) = 3 +_6 3 = 0$.

LHS = RHS.

③ $e = 0$

④
0 − 0
1 − 5
2 − 4
3 − 3
4 − 2
5 − 1

* (For Inverse, always list the Elements).

⑤ Commutative law
$\forall a, b \in G$
$a +_6 b = b +_6 a$.

$\therefore (G, +_6)$ is an abelion group

Q Is $G = \{1, 2, 3, 4, 5\}$ a group under Addition & multiplication modulo 6. or not.

$(G, +_6)$

Sol^n

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

① Closure Law.

$\because$ As $1 +_6 5 = 0 \notin G$

Therefore G is not closed wrt $+_6$

$\therefore (G, +_6)$ not a group.

$\circ_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1.

① closure law

$\because 2 \circ_6 3 = 0 \notin G.$

$\therefore$ G is not closed wrt '$\circ_6$'

$(G, \circ_6)$ → not an abelion group.
nor a group.

Q Check whether the following are groups or not?

(a) $G = \{0, 1, 2, 3\}$

$(G, +_4)$ gp ?

(b) $G = \{1, 2, 3, 4, 5, 6\}$

$(G, \cdot_7)$ gp ?

Soln (a) ✓ group..

(b) ✓ group.

Theory.

THEORMS

For Addition – 0 to m-1 Elements in set

$(G, +_m) \rightarrow$ group forms.

For Multiplication – 1 to m-1 elements in the set

$(G, \cdot_m) \rightarrow$ grp forms if ($m \rightarrow$ prime no.)

14/8/2023.

Q Check whether set $G = \{1, 5, 7, 11\}$ forms a group wrt $\cdot_{12}$.

TST: $(G, \cdot_{12})$?

Soln Forming composition Table:

$\cdot_{12}$	1 (e)	5	7	11
1	1	7	5	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

① Closure law ✓

② Associative law.

LHS $= (5 \cdot_{12} 7) \cdot_{12} 11 = 11 \cdot_{12} 11 = 1$.

RHS $= 5 \cdot_{12} (7 \cdot_{12} 11) = 5 \cdot_{12} 5 = 1$.

③ $e = 1$

④ 1^{-1}

5^{-5}

7^{-7}

11^{-11}

Thus, forms a group.

Order of an Element of group

→ let G be a group wrt multiplication $(G, \cdot)$ and $a \in G$, then the order of 'a' is the least positive integer 'n', such that

$\boxed{a^n = e}$ denoted as $o(a) = n$.

Eg $G = \{1, \omega, \omega^2\}$

$(G, \cdot)$ grp.

$(1)^1 = 1 \Rightarrow o(1) = 1$.

$(\omega)^3 = 1 \Rightarrow o(\omega) = 3$.

$(\omega^2)^3 = 1 \Rightarrow o(\omega^2) = 3$.

(*) For addition group → $\boxed{na = e}$.

Q $G = \{0, 1, 2, 3, 4, 5\}$

$(G, +_6)$

find order.

Sol^n $0 \Rightarrow o(0) = 1$

$1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0$

$o(1) = 6$.

$\{0, 1, 2, 3, 4, 5\}$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$1 \quad 6 \quad 3 \quad 2 \quad 3 \quad 6$.

Subgroup

A non Empty subset $(H \subseteq G)$ is called subgroup of G, if H itself is a group wrt same Binary operations.

$(I, +) \longrightarrow (E, +)$

$H_1 = \{-2, -1, 0, 1, 2\}$ ⟶ proper/non-trivial subgroups

$E = \{-4, -2, 0, 2, 4\}$

$O = \{-3, -1, 1, 3\}$

$H_3 = \{0\}$ ⟶ trivial.

(0 can be repeated)

$(G, *)$ grp

G $\quad$ $\{e\}$ ⟶ Trivial/Improper

but not $\{1\}$

Cyclic group:

Eg: $G_1 = \{1, \omega, \omega^2\}$

$(G_1, \cdot)$ grp.

ω, ω^2 are generators

grp is cyclic.

$1^1 = 1$	$(\omega)^3 = 1$	$(\omega^2)^3 = 1$
$1^2 = \omega$	$(\omega)^1 = \omega$	$(\omega^2)^2 = \omega$
$1^3 = \omega^2$	$(\omega)^2 = \omega^2$	$(\omega^2)^1 = \omega^2$

⊙ * group $(G_1, \cdot)$ is called cyclic if $\exists a \in G_1$, such that every element $x \in G_1$

if $x = a^n$

then G_1 is called cyclic group and 'a' is called it's generator.

Q $G_1 = \{0, 1, 2, 3, 4, 5\}$

$(G_1, +_6)$

Sol^n generators are 1, 5

① → $1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 \Rightarrow 0$

1

(#) Ring $(R, +, \cdot)$

An algebraic structure $(R, +, \cdot)$ is called a ring if

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ is semi group.
3. Left & Right distribution law holds.

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \left.\right] \rightarrow \text{any one.}$$
$$(b+c) \cdot a = b \cdot a + c \cdot a$$

Eg $(I, +, \cdot) \rightarrow$ Smallest ring structure.

$(\mathbb{Q}, +, \cdot)$

$(R, +, \cdot)$

$(C, +, \cdot)$

$(G, +_6, \cdot_6) \rightarrow$ Ring.

- **Types of Rings**

① **Ring with unity.**

$(R, +, \cdot, 1)$

if $\exists\ 1 \in R$ st,

$$a \cdot 1 = a = 1 \cdot a$$

Eg $(I, +, \cdot)$. $\exists\ 1 \in I$ st

Ring (Jisme 1, multiplicative identity bhi ho.)

② **Commutative Ring**

$(R, +, \cdot)$ ring.

$\forall a, b \in R$, st

$$a \cdot b = b \cdot a$$

$(I, +, \cdot)$ ring.

Ring (Jisme commutative law bhi follow ho multiplication mein).

16/8/2023.

Zero Divisors.

R- Ring

$a, b \in R$.

if $a \cdot b = 0 \Rightarrow a \neq 0$ nor $b \neq 0$

then a, b are called zero divisors. and R is said to be ring with zero divisors.

Without zero divisors. $a, b \in R$

if $ab = 0 \Rightarrow a = 0$ or $b = 0$

→ a, b are called Non zero divisors. or without zero divisors

Eg - $(I, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$ $(C, +, \cdot)$

Eg $(G, +_6, \cdot_6)$

$G = \{0, 1, 2, 3, 4, 5\}$

↳ ring with zero divisors.

$2 \cdot_6 3 = 0$

$3 \cdot_6 4 = 0$.

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Eg $(M_{(n \times n)}, +, \cdot)$ ⟶

$(M, +)$ → ab group.

$(M, \cdot)$ → Semi grup $A.(B.C) = (A.B).C$

Integers follow associative law

$A \cdot (B+C) = A.B + A.C$.

$(A+B) \cdot C = A.C + B.C$.

and now,

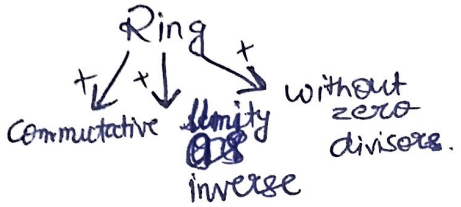
Eg

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

↳ Ring with zero divisors.

Integral Domain

→ Ring which is a commutative ring with unity and without zero divisors



① $(I,+)$ ab grp
② $(I,\cdot)$ semigrp
③ LD/RD.
④ Commutative
⑤ unity
⑥ Without zero divisors.

Eg: $(I,+,\cdot)$

Field.

An Algebraic structure $(F,+,\cdot)$ is called a field, if
① $(F,+)$ ab grp
② $(F,\cdot)$ ab grp
③ LD/RD.

Eg $\quad I \subset Q \subset R \subset C$
(Q → field)

Q Let $S = \{0,2,4,6,8\}$

① Is $(S, +_{10}, \cdot_{10})$ → Integral domain
② Is $(S, +_{10}, \cdot_{10})$ → field ?

Sol^r

$+_{10}$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

(e) = 0

$\cdot_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

(e) = 6

→ yaha 6 nahi hai

① Part

↳ ① $(S, +_{10})$ → abgroup.

→ Closure law – Clear from table that all elements $\in S$.

→ Associative law. $(2 +_{10} 4) +_{10} 8 = 2 +_{10} (4 +_{10} 8)$

$= 6 +_{10} 8 = 2 +_{10} 2$

$4 = 4$

→ $e = 0$

→ Inverse $0 - 0$
$2 - 8$
$4 - 6$
$6 - 4$
$8 - 2.$

→ Commutative $a +_{10} b = b +_{10} a.$

(semigroup)

② $(S, \cdot_{10})$ → closure law holds

→ Associative law

$(6 \cdot_{10} 4) \cdot_{10} 2 = 6 \cdot_{10} (4 \cdot_{10} 2)$

$4 \cdot_{10} 2 = 6 \cdot_{10} (8)$

$8 = 8.$

③ LD / RD.

$LHS = 4 \cdot_{10} (6 +_{10} 8) = 4 \cdot_{10} 4 = 6$

$RHS = 4 \cdot_{10} 6 +_{10} 4 \cdot_{10} 8 = 4 +_{10} 2 = 6$

$LHS = RHS$

④ Unity.

$\forall a \in S. \ \exists \ 6 \in S.$

st, $a \cdot_{10} 6 = a.$

⑤ Commutative.

$a \cdot_{10} b = b \cdot_{10} a.$

⑥ If $a \cdot_{10} b = 0$

⇒ Either $a = 0$ or $b = 0.$

So, $(S, +_{10}, \cdot_{10})$ is an ID.

② Part → as $0 \cdot_{10} b \neq 6$ (Inverse for 0 do not exist)

→ not $(S, \cdot_{10})$ ← an abelion group

So, $(S, +_{10}, \cdot_{10})$ → not a field.

Q Let $I = \{0, 1\}$,

Is $(I, +_2, \cdot_2)$ → an Integral domain.? or field?

Ans -

$+_2$	0	1 ← e
0	0	1
1	1	0

$\cdot_2$	0	1 ← e
0	0	0
1	0	1

→ Missing 1.

→ we can repeat any one Element for associative.

① $(I, +_2)$ → ab grup

② $(I, \cdot_2)$ → Semi grup

③ distributive

$RHS = 0 \cdot_2 (0 +_2 1) = 0 \cdot_2 (1) = 0$ LHS = RHS.

$RHS = 0 \cdot_2 0 +_2 0 \cdot_2 1 = 0 +_2 0 = 0$

④ Commutative ring → As $a \cdot_2 b = b \cdot_2 a$. (as Transpose is same).

⑤ Unity

$e = 1$

⑥ Without zero divisors

$1 \cdot_2 1 = 1$

from Table.

→ So $(I, +_2, \cdot_2)$ is an integral domain.

17/08/2023.

field ?

↳ (7) Inverse

$a \circ_2 b = 1$

as $0 \circ_2 b \neq 1$ (no Inverse of zero)

∴ Inverse of zero does not exist..

∴ $(I, +_2, \cdot_2)$ not a field.

Q Check whether the set $I\sqrt{2} = \{a+b\sqrt{2} : a, b \in I\}$ field or not

Soln (1) $(I\sqrt{2}, +)$ ab grp ?

↳ Yes (done previously)

(2) $(I\sqrt{2}, \cdot)$ ab grp?

↳ closure law

(a) $(a+b\sqrt{2}).(c+d\sqrt{2})$

$= (ac+2bd) + \sqrt{2}(ad+bc) \in I\sqrt{2}$

∵ $(I, +)$ is an ab grp

or (I is closed wrt '+', '·').

(b) Associative law.

LHS $= \left((a+b\sqrt{2})(c+d\sqrt{2})\right)(e+f\sqrt{2})$.

$= (ac+2bd)+\sqrt{2}(ad+bc).(e+f\sqrt{2})$

$= ace + 2bde + \sqrt{2}\,ade + \sqrt{2}\,bce + acf\sqrt{2} + 2\sqrt{2}\,bdf + 2\,adf + 2bcf.$

$RHS = (a+b\sqrt{2}).((c+d\sqrt{2})(e+f\sqrt{2}))$

$= (a+b\sqrt{2})((ce+2df)+\sqrt{2}(cf+de))$

$(a+b\sqrt{2})((ce+2df)+\sqrt{2}cf+\sqrt{2}de)$

$= ace+2adf+\sqrt{2}cfa+\sqrt{2}ade+\sqrt{2}bce+2\sqrt{2}bdf+2bcf+2bde.$

$LHS = RHS.$

(c) E of Id

$\forall\ a+b\sqrt{2} \in I\sqrt{2}$

$\exists\ 1+0\sqrt{2}.$

such that $(a+b\sqrt{2}).(1+0\sqrt{2})$

$= a+b\sqrt{2}.$

Thus $\boxed{e = 1+0\sqrt{2}}$

(d) E of Inverse.

$\forall\ a+b\sqrt{2} \in I\sqrt{2}$

$\exists\ x+y\sqrt{2}.$

Such that

$(a+b\sqrt{2}).(x+y\sqrt{2}) = 1+0\sqrt{2}$

$x+y\sqrt{2} = \frac{1+0\sqrt{2}}{(a+b\sqrt{2})}\frac{(a-b\sqrt{2})}{(a-b\sqrt{2})}$

$x+y\sqrt{2} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{\sqrt{2}(-b)}{a^2-2b^2}$

$\notin I$

- So Inverse does not exists.
  → Thus, It is not a field.

(Inverse for Dhyan Rakhna aise mein)

18/8/23

Unit - 03
Graph Theory

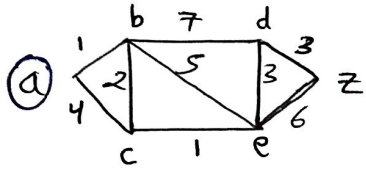
Refer
Koneth Rosen
from NOW

Shortest path

Dijkstra's Algorithm:

1. Find a shortest path from A to z in the following weighted graph.
(weighted – Edges are associated with some Number)

↳



$V = \{a, b, c, d, e, z\}$

(I) $S = \{a\}$ $R = \{b, c, d, e, z\}$

$l(b) = (1)$ → minimum.
$l(c) = 4$
$l(d) = \infty$
$l(e) = \infty$
$l(z) = \infty$

∴ b is selected (a–b)

Algorithm constantly compares old & New paths.

(II) $S = \{a, b\}$, $R = \{c, d, e, z\}$

$l(c) = \min(\overset{old}{4}, \overset{new}{1+2}) = (3)$ → minimum. (Now at b)
$l(d) = \min(\infty, 1+7) = 8$
$l(e) = \min(\infty, 1+5) = 6$
$l(z) = \min(\infty, 1+\infty) = \infty$

∴ C is selected (a–b–c)

(III) $S = \{a, b, c\}$ $R = \{d, e, z\}$

→ $l(d) = \min(8, 3+\infty) = 8$
$l(e) = \min(6, 3+1) = 4$ → minimum.
$l(z) = \min(\infty, 3+\infty) = \infty$.

∴ e is selected (a-b-c-e)

(IV) $S = \{a, b, c, e\}$ $R = \{d, z\}$

$l(d) = \min(8, 4+3) = 7$
$l(z) = \min(\infty, 4+6) = 10$ → minimum

∴ d is selected. (a-b-c-e-d)

(V) $S = \{a, b, c, e, d\}$ $R = \{z\}$

$l(z) = \min(10, 7+3) = 10$

∴ z is selected. (a-b-c-e-d-z)
Soln ①.

(a-b-c-e-z). Soln ②.

Shortest path length → always same / only one.