* → multiplicative group $(R^+, \times)$ Positive Real No. (Not having 0)

$(R - [0], \times)$

:- $a + a^{-1} - aa^{-1} = 0 = a^{-1} + a - a^{-1}a$

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

$a^{-1} = \frac{-a}{1-a} = \frac{a}{a-1}$ (Not imp)

Group theory :-

1. Properties of Abelian group
2. Classic examples of group
3. Properties of groups
4. ~~Proper~~ Powers of element of a group.
5. order of a group
6. Order of an element of a group.
7. Cyclic group.
8. Subgroup.
9. Langrange's theorm

:- Properties of Abelian group :-

* 1. A group $(G, *)$ is Abelian Iff $\forall a, b \in G$ $\boxed{a*b = b*a}$
** 2. " " Iff $\forall a, b \in G$ $\boxed{(a*b)^2 = a^2 * b^2}$
*** 3. If a group $(G, *)$ $\forall a \in G$ $a^{-1} = a \Rightarrow (G, *)$ is Abelian

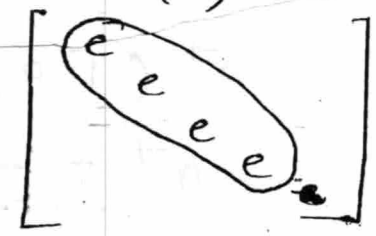
:- If in a group $(G, *)$

$\forall a \in G \quad a^{-1} = a \Rightarrow (G, *)$ is Abelian

(or) (one way, only)

$a^2 = e$

(or)



$\Rightarrow$ all elements of diagonal are entity.

eg:- consider $(G, *)$ a abelian group which is true:

a) $\forall a \in G \quad a^2 = e$ ✗

b) $\forall a \in G \quad a^{-1} = a$ ✗ } can't go reverse

c) $\forall a \in G \quad (a*b)^2 = a^2 * b^2$ ✓

d) G is finite ✗ abelian group may be infinite

:- Classic Examples of group :-

1. $(\{0, 1\}, \oplus)$
2. $(Z_m, +_m)$ $Z_m = \{0, 1, 2, 3 \ldots m-1\}$

   additional modulo m group
3. $(\{1, 2, 3, 4 \ldots p-1\}, \times_p)$

   p has to be Prime Number

   multiplication modulo group.

} all abelian group too

4. Permutation group $(S_n, \cdot)$ (Not abelian group)

$(S_3, \cdot) = \left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \cdots \right\}$

1. $((0,1), \oplus)$

$\oplus$	0	1
0	0	1
1	1	0

2. Abelian group
2. $e = 0$
3. $a^{-1} = a$

$1^{-1} = 1$

$0^{-1} = 0$

4. Automatic error correction.
5. $O(G) = |a| = 2$

2. $(Z_m, +_m)$

Let take $+_4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

1. Abelian group
2. $e = 0$
3. $a +_m a^{-1} = 0$

$a +_m (m-a) = 0$

$a^{-1} = m - a \quad \forall a \neq 0$

$0^{-1} = 0$

or

$a^{-1} = (m-a) \bmod m$

eg: $(Z_{12}, +_{12})$

$2^{-1}, 7^{-1}$

$a +_m a^{-1} = 0$

$a + (m-a) = 0$

$2^{-1} = 12 - 2$

$= 10$

$7^{-1} = 12 - 7$

$= 5$

4. It is used in cryptography. 5. $O(G) = m$
(ceaser's cyptography).

3.) $(\{1, 2, 3, 4 \cdots P-1\}, X_P)$

1. Abelion group
2. $e = 1$
3. ——— ↗
4. used in RSA Algo.
5. $O(G) = P-1$

$\{\{1, 2, 3, 4 — 12\}, X_{13}\}$

$2^{-1}, 3^{-1}$?

$+_{13}$	1	2	3	4	5	6	7	8	9	10	11	12
2											1	
3												1

$2^{-1} = ?$

$2 X_{13} 2^{-1} = 1$

$2 \times 2^{-1} = 13x + 1$

Check integer

$x = 0$ Not $\quad x = 1$

$2 \times 2^{-1} = 13 + 1 = 14$

$2^{-1} = 7$

$2^{-1} = 7, \quad 3^{-1} = 9$

$3 \times 3^{-1} = 13x + 1$

$x = 1 \times$

$x = 2$

$3 \times 3^{-1} = 26 + 1$

$3^{-1} = \frac{27}{3}$

$3^{-1} = 9$

eg: $(\{1, 2, 3, 4, 5\}, X_6)$ ↳ Not a Prime No. (may or may not group)

Not group why ?

Reasons: 1) Not close ✓

2) Not Associative ✗

c) 2^{-1} 3^{-1} not exist ✓

d) identity not exist ✗

Permutation group :- $(S_n, \circ)$

1. Not abelian
2. order(G) = $n!$
3. $e = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ 1 & 2 & 3 & \cdots \end{pmatrix}$
4. Inverse

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 2 & 6 & 7 & 5 \end{pmatrix}$$

$$P^{-1} = \begin{pmatrix} 3 & 4 & 1 & 2 & 6 & 7 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 2 & 7 & 5 & 6 \end{pmatrix}$$

eg: $P = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$$P^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}$$

(Rearrange) $P^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

5. It is used in cryptography.

Que :- How to find even or odd permutation?

:- (1.) Every permutation can be broken down in product of disjunctive cycle.

Cycle permutation :- Permutation with one cycle.

eg. $\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 \end{pmatrix} = (1,3,6)$

$eg_2 \Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 6 & 5 & 4 & 1 & 7 \end{pmatrix} \Rightarrow (1,3,6);(4,5)$

$eg_3 \Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 1 & 2 & 6 & 7 & 5 \end{pmatrix} \Rightarrow (1,3);(2,4);(5,6,7)$

(2.) Every Permutation can be broken down into a product of transposition.

Transposition: cycle of length 2

$(1,3), (2,4)$

Transpositions

(a,b,c,d,e) (in order)

$= (a,e)\cdot(a,d)\cdot(a,c)\cdot(a,b)$

$(5,6,7) = (5,7)\cdot(5,6)$

$\Rightarrow |(1,3),(2,4),(5,7),(5,6)| = 4$

even permutation

$\Rightarrow (1,3,6)\cdot(4,5) = |(1,6)(1,3)\cdot(4,5)| = 3$

odd permutation

→ Identity Permutation is even permutation as product transposition = 0

:- $(S_n, \cdot)$ Group ✓

even Permutation $(E_n, \cdot)$ ~~Group~~ group ✓, subgroup.

odd Permutation $(O_n, \cdot)$ Group ✗

:- odd permutation is not group becoz

a) Not closed ✓

b) Not associative ✗

c) Not ~~Inverse~~ identity ✓

d) Not inverse ✓

Date 01/09/2017

Properties of Group :-

1. Le = Re. $\boxed{e*a = a*e}$
2. identity is unique for the entire group
3. Inverse (a^{-1}) is unique for a given a.
4. $(a^{-1})^{-1} = a$, $a^{-1} = b$ iff $b^{-1} = a$
5. ~~$(ab)^{-1} = b^{-1} \times a^{-1}$~~

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

eg:- let $(G, *)$ be a Abelian group $\forall a, b \in G$

I $(a*b)^{-1} = a^{-1} * b^{-1}$ ✓

II $(a*b)^{-1} = b^{-1} * a^{-1}$ ✓

} Both true (abelian group).

6. In a group both left cancelation & Right cancelation law hold.

$$\boxed{ab = ac \Rightarrow b = c}$$

it is done by inverse property

$$a^{-1}ab = a^{-1}ac \Rightarrow \underline{b=c}$$

$$\boxed{ba = ca \Rightarrow b = c}$$

→ In group & monoid backword is also true. but in monoid, forword is not hold.

$$\boxed{ab = ca \Rightarrow b = c \times}$$

7. $(G, *)$ $a, b, x \in G$

$ax = b$ & $ya = b$

unique solution

$x = a^{-1} * b$ $\quad$ $y = b * a^{-1}$

eg :- $(A_{n\times n}, \times)$ Group ✓

$A_{n\times n}$ → all square matrices

$|A| \neq 0$ (Non Singular matrices) → Inverse exist (as it not have zero)

$|A| = 0$ (singular matrix) → Inverse not exist

8. Binary operation Table of A group = "cayley table"

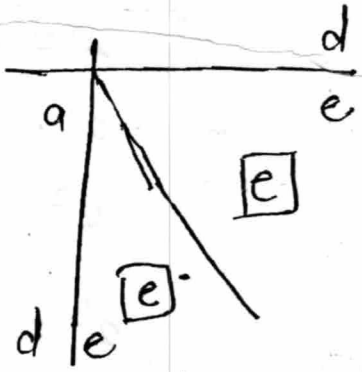
→ No Repeatation in Row or Column

It means a group table (so group)

*	a	b	c	d
a	a	b	c	d
b	b	c	d	d
c	a	c	d	b
d	b	d	c	a

→ repeatition (so not agroup)

9. Cayley table



$a^{-1}a = e = aa^{-1}$

identity will be reflective

eg:-

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

← last row

Its a 'Cayley table' so its a "group"

use, property (i, ii, iv)

:- Powers of an Element of a group :-

$(G, *)$, $\forall a \in G$ $\boxed{a^n} = ?$ $n \in z$

- $a^0 = a$
- $a^1 = a$
- $a^2 = a*a$
- $a^3 = a*a^2 = a^2*a = a*a*a$
- $\boxed{a^m * a^n = a^{m+n} = a^n * a^m}$

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

$a^{-2} = a^{-1} * a^{-2}$

→ $(a^m)^n = a^{mn}$

eg: $(Z, +)$ group

$a^{-1} = -a$

$2^{-2} = 2^{-1} * 2^{-1} = -2 + -2 = -4$

$2^{-1} = -2$

$2^0 = 0(e)$

$2^1 = 2$

$2^2 = 2 * 2 = 2 + 2 = 4$

$2^3 = 2 + 2 + 2 = 6$

$2^n = 2n$

$(R^+, \times)$ group

$a^{-1} = 1/a$

$2^{-2} = 2^{-1} * 2^{-1} = 1/2 \times 1/2 = 1/4$

$2^{-1} = 1/2$

$2^0 = 1$

$2^1 = 2$

$2^2 = 2 * 2 = 2 \times 2 = 4$

$2^3 = 2 * 2^2 = 2 * 2 \times 2 = 8$

$2^n = 2^n$

eg2:- finite group:-

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$a a^{-1} = e$

$e = a$

~~$b^0 = a$~~

$b^1 = b$

$b^2 = c$

$b^3 = d$

$b^4 = a$ identity

$b^{-1} = d$

$b^{-2} = b^{-1} * b^{-1}$

$= d * d$

$= c$

do upto the order

$b^n = b^{n \bmod O(b)}$

order of $b = 4$

$b^0 = a$

$b^{216} = b^0 = b$

:- $((a^7)^{-2}\ a^3 b^{42})^{-1}$

$(a^{-11} \times b^{42})^{-1} = b^{42} \times a^{11}$

$= b^{-42 \bmod 4}$

$\times a \leftarrow$ (identity)

$= b^2 * a = c \times a = c$

:- Order of a Group $(G, *)$:-

$O(G) = |G|$

* order of
^ Permutation group of alternating n letters
or order of Even permutation group

$(En; \cdot) = \frac{n!}{2}$

→ order of group, $(G, *)$ $\forall a \in G$ $\boxed{O(a) = ?}$

$\Rightarrow \boxed{O(a) = \text{smallest positive integer } a^n = e}$

$\boxed{O(a) = 1 \text{ iff } a = e}$ because only order(e) = 1

If $a \neq e$ then its order

$O(a) \geq 2$

:- lets take infinite group $(Z, +)$

→ In finite group, each element have finite order
→ In Infinite group, atleast one element is of finite order i.e. $O(e) = 1$

In group $(Z, +)$

$0(0) = 1$

$0(1) = \infty$

$0(2) = \infty$

$0(3) = \infty$

$0(-1) = \infty$

$1^1 = 1$

$1^2 = 1+1$

$1^3 = 1+1+1$

!

$(-1)^1 = -1$

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

Lets take finite group :-

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

a = identity

$0(a) = 1$

$0(b) = 4$

$0(c) = 2$

$0(d) = 4$

$b^1 = b$

$b^2 = c$

$b^3 = d$

$b^4 = a$

$c^1 = c$

$c^2 = c*c = a$

$d^1 = d$

$d^2 = c$

$d^3 = b$

$d^4 = a$

* :- $\boxed{0(a^{-1}) = 0(a)}$ $\forall a \in (G, *)$

$b^{-1} = d$

$0(b) = 0(d) = 4$

we know, If $0(a) = x$

then $a^x = e$

so $(a^{-1})^x = (a^x)^{-1} = e^{-1} = e$

:- order of a group = no. of elements in the group.

Properties :-

1. $O(a) \leq O(G)$ [Lagrange's theorm] $\Rightarrow$ $O(a) \div O(G)$
2. $O(a^{-1}) = O(a)$
3. $a^n = a^{n \bmod O(a)}$
4. $O(a*b) = O(b*a)$ in a group
   or
   $O(ab) = O(ba)$ True
5. $O(xax^{-1}) = O(a) \quad \forall x \in G$
   (or)
   $O(x^{-1}ax) = O(a)$

:- $O(a) = t$

$O(xax^{-1}) = t$

$O(xax^{-1})^t = e$

$xax^{-1}xax^{-1}xax^{-1}\cdots$

$= xa^t x^{-1}$

$= xex^{-1}$

$= xx^{-1} = e$

eg:- $O(a) = 5$

$bcb^{-1} = a$ then $O(c) = ?$

$c = b^{-1}ab$ (multiply by b^{-1} on left & b on to Right)

So $O(c) = O(a)$

$O(c) = 5$

$O(c) = b^{-1}ab = O(a) = 5$

6. $O(a) = n \Rightarrow a^x = e$.

Iff $x = kn$ $\quad k \in z$

$O(a) = 7$

$a^0 = e$ $\quad a^{-14} = e$

$a^7 = e$

$a^{14} = e$ $\quad a^9 \neq e$

$a^{21} = e$ $\quad$ as 9 not a multiple of 7

:- Cyclic group :-

(G, x) is a cyclic group Iff $\exists g \in G$ → generator element of group)

$\forall a \in G \quad \boxed{a = g^n} \quad \forall n \in z$

$G(g)$ → generator of group

:- Cyclic group is a group which has atleast one generator element

:- Group without generator element is not a cyclic group.

1. $(z, +)$
2. $(z_m, \times_m)$
3. $(n, n^{th}$ roots of unity, $\times)$

$([1], \times)$

$\times$	1	-1
1	1	-1
-1	-1	1

$(\{1, -1\}, \times)$ $\quad (\{1, \omega, \omega^2\}, \times)$

$(\{1, \omega, \omega^2\}, \times)$

$(\{1, -1, i, -i\}, \times)$

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

⇒ e (identity element) can be generator only in trivial group (n, n^m roots of unity, $\times$) groups.

:- g is generator of $(G, \times)$ iff g^{-1} is also generator.

	$g(x)$ (generator)
1. $(Z, +)$, ⟶	$1, -1$
2. $(Z_m, +_m)$ ⟶	$1, m-1$

3. (n, n^m roots of unity, $\times$)

$([1], \times)$ ⟶ 1

$([1, -1], \times)$ ⟶ -1

$(\{1, \omega, \omega^2\}, \times)$ ⟶ ω, ω^2

$(\{1, -1, i, -i\}, \times)$ ⟶ $i, -i$

because $i^0 = 1$
$i^1 = i$
$i^2 = -1$
$i^3 = -i$

Que:-

1)

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

← isomorphic to cyclic group

2)

X_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

identity = 1

2, 3 are generators

so from $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 3$

all elements

cyclic group

$2^7 = 3$ is also generator ← so 2 is a generator

1

★ Properties:-

→ 1) If g is generator, g^{-1} also generator

→ 2) cyclic group always an Abelian group.

:- If a group is not a abelian then it not be cyclic

CG ⇒ AG (one way)

→ 3.) group of prime order ⇒ CG.

→ ~~4)~~ :- ★ group of prime order ⇒ cyclic group with (P-1) generator {except identity element}

↳ Prime No.

4. Finite group $(G, *)$ is a cyclic group

iff $\exists\ a \in G$ $\boxed{O(a) = O(G)}$

$O(a)$: order of element; $O(G)$: order of group

i.e elements which having, order equal to order of group are generators.

eg:- $((a, b, c, d, e, f, g, h), x)$

$O(2, 3, 1, 2, 2, 4, 8, 8) \Rightarrow$ so cyclic group with generators (g, h)

divisor of 8

by Property $O(a) \leq O(G)$

& $O(a) \mid O(G)$

5. $(G, *)$ is a cyclic group with $O(G) = n$ or $|G| = n$

number of generators $= \phi(n)$

$\phi(n)$: Euler quotient function.

eg:- $O(G) = 60$

generator $= \phi(60)$

$\phi(n)$: number of ~~num~~ number $(1$ to $n)$

$-$ GCD $(x, n) = 1$

x is relative prime

$\phi(8) = 4$

1, 2, 3, 4, 5, 6, 7, 8 $\Rightarrow$ $8 - 4 = 4$

$\phi(n) =$ $n = p_1 \cdot p_2 \cdot p_3 \ldots p_r$

2	60
2	30
3	15
	5

$2^2, 3^1, 5^1$ Prime No.

$\phi(n) = \phi(p_1^{n_1} \cdot p_2^{n_2} \ldots p_r^{n_r}) = \phi(p_1^{n_1}) \times \phi(p_2^{n_2})$

$\therefore \phi(60) = \phi(2^2 \cdot 3^1 \cdot 5^1) = \phi(2^2) \times \phi(3^1) \times \phi(5^1)$

$= (2^2 - 2^1) \times (3^1 - 3^0) \times (5^1 - 5^0)$

$= (2) \times 2 \times 4 = 16$ generators

let

$\therefore \phi(8)$

2	8
2	2
2	2
	1

2^3

$\phi(8) = \phi(2^3) = \phi(2^3)$

$= (2^3 - 2^2 - $ ~~2^1~~ $)$

$=$ ~~$8 - 4 - 2 = 2$~~

$= 8 - 4 = (4)$

$$\boxed{\phi(p^n) = p^n - p^{n-1}}$$

Subgroup :-

$(H, *)$ subgroup of $(G, *)$ if

1. $H \subseteq G$
2. $(H, *)$ must itself be a group.

:- Not a subgroup :-

a) $[\{0, 2\}, +_4]$ ✓

$+_4$	0	2
0	0	2
2	2	0

Inverse ✓

Group ✓

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

~~b)~~ $(\{0, 1, 2\}, +_4$

Trivial { c) $(\{0\}, +_4)$ ✓

d) $(\{0, 1, 2, 3\}, +_4)$ ✓

$+_4$	0	1	2
0	0	1	2
1	1	2	3 → Not closed
2	2		

$(\{e\}, *)$ } Trivial subgroup

$(G, *)$ }

:- In a finite group, # of subgroups ? :-

0 → ✗

1 element → $(\{0\}, *)$ → 1

2 element → $(0, 1)$, $(0, 2)$, $(0, 3)$ → 1

✗ ✗

3 element → ✗

4 element → $\{\{0, 1, 2, 3\}, *\}$ → 1

By lagrange's theorm

$$\boxed{O(H) \div O(G)}$$

D_0 # subgroups = 3

⇒ Any group of prime order have only "Trivial Subgroup"

eg:- $(G, *)$ $O(13) \Rightarrow$ subgroup $H(1)$ & $H(13)$

∴ 13 can't be divide by any other no.

⇒ Proper subgroups are subgroups other then trivial subgroups.

↳ $\{\{e\}, *\}$
$\{G, *\}$

⇒ every group have 2 trivial subgroup ✗ (False)

becoz for $\{\{e\}, *\}$ only 1 trivial

Properties:-

★ 1.) $O(H) \div O(G)$

★ 2.) $(H, *)$, $(K, *)$ ⇒ $(H \cap K, *)$ → subgroup.
(H, *) → subgroup, (K, *) → S.G

⇏ $(H \cup K, *)$ → Not subgroup.
↳ closure property violates.

3. $$O(HK) = \frac{O(H) \times O(K)}{O(H \cap K)}$$

where H & K are subgroups.

:- $(H, *), (K, *) \Rightarrow (H \cdot K, *)$ is also subgroup.

↑ Product subgroup.

eg:- $O(H) = 8 \quad O(K) = 7$

$O(H \cap K) = ?$ ⇒ It's a subgroup of H & K which are subgroups of G.

→ By lagrange's theorm

$O(H) \div O(G)$

$\therefore O(H \cap K) \div O(H)$ & $O(K)$

8 and 7

$\therefore O(H \cap K) = 1$

But lagrange's theorm has many results $(H \cap K) = 1, 2, 4$ so for appropriate result use 3rd. Property if all 3 $O(H)$, $O(K)$ & $O(HK)$ are given

→ Every subgroup of cyclic group is a subgroup.