12/08/2021

Unit - 3: Group Theory

Natural NO $\{1,2,3,---\}$

N.NO $\{0,1,2,3,---\}$

Intergs $z = \{---,-2,-1,0,1,2,---\}$

$= \{0, \pm 1, \pm 2 ---\}$

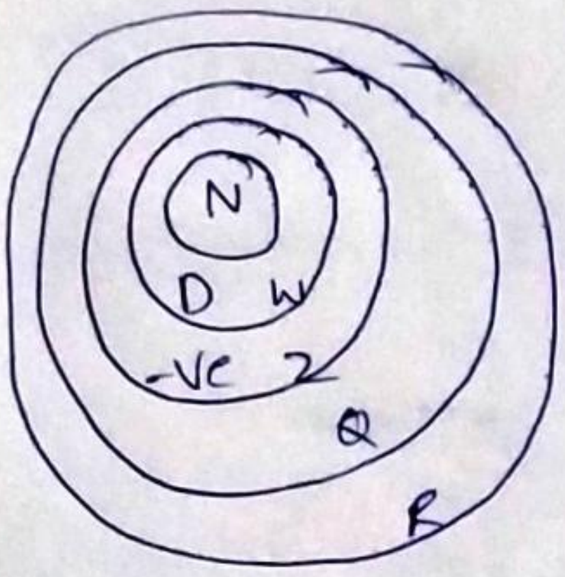
$x + 0$

$x = -1$

$ax = 1$

$x = \frac{1}{a}$

Rotational $Q = \{a/b, a,b \in z, b \neq 0\}$



$\frac{1}{3} = 0.333---$

$1.2.3.4 = \frac{1234}{1000}$

$\frac{1}{2}, \frac{1}{3}$

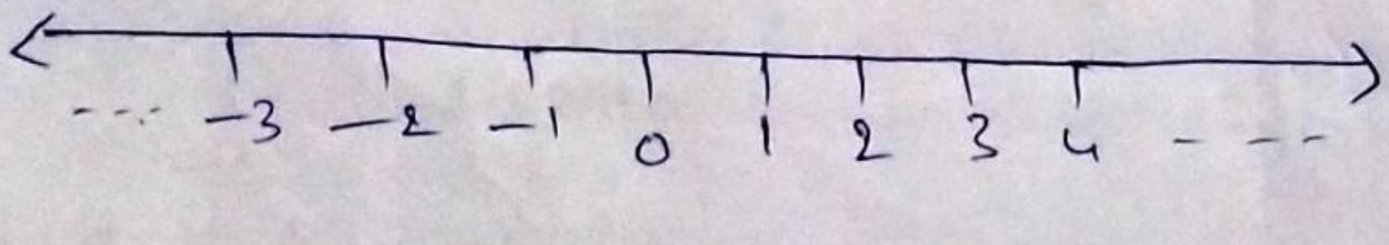
$1.2223---$

$1.434648---$

$1.123123122---$

$\frac{22}{7} \simeq \pi$

Realno:



Finite - $\{---\}$

Infinite <

Cartesian product

A - Set, B - set

$A \times B = \{(a,b) / a \in A, b \in B\}$

$A \times A = \{(a,b)/a,b \in A\}$ $A = \{1,2\}$

$A \times A = \{(1,1)(1,2)(2,1)(2,2)\}$

$+, -, \times$ $A, A^c \rightarrow$ unar

$+(2,10) = 2+10 = 12 \in N$

$* : N \times N \rightarrow N,$

$*$ is closed

$(N, *)$ is closed

$2 - 8 = -6 \notin N$

$(N, -)$ not closed

$(N, \cdot)$ — closed

$(N, \%)$ — Not closed

$(Z, +)$ - closed

$(Z, -)$ - closed

Associative :

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

$a - (b - c) = (a - b) - c$

$2 - (7 - 3) = 2 - 4$

$= -2$

$(2 - 7) - 3 = -5 - 3$

$= -8$

Identity :

$a * e = e * a = a$

$a+e = 0+a = a$

$a \times 1 = 1 \times a = 1$

Inverse:

$a+a = 0 \Rightarrow a+(-a) = 0$

$a^{-1} = -a$

$(x, *)$ is said to semi group

① closure ② ASSO

Ex:) $(N,+)$ semigroup, $(Z,+)$, $(Z,-) \rightarrow$ not

$(A,+)$ is monoid

closure ASSO & identity

$(N,+)$ not monoid

$(Z,+)$ monoid $(N,\cdot)$ monoid

$(N,\cdot)$ not a group $\pm x_{\Sigma}^{1} = 1$

$\frac{1}{2} \notin N$

$(N,+)$ group $Z = \{0, \pm 1, \pm 2 \ldots\}$ (0 = iden)

$a+(-a) = 0$

$(Z,+)$ group

$m - 2 \times 2$ (matrice)

$(M,+)$ group $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} - I$ $\quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 2 & +1 \\ 4 & 6 \end{pmatrix} + \begin{pmatrix} -2 & -1 \\ -4 & -6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

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

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

$(\mathbb{Z}, \cdot)$ not group

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$

$= 2, 1/2$

18/08/2021

Def!

$* : (A \times A) \longrightarrow A \quad a \times b \in A$

closure property!

$\forall a, b \in A, \; a * b \in A$

Assosiative:

$\forall a, b, c \in A$

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

Identity!

$\exists$ an element $e \in A$ such that

$e * a = a * e = a \quad \forall a \in A$

Inverse!

For any $a \in A$, $\exists \; a^{-1} \in A$ such that

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

commutative!

$\forall a, b \in A \;,\; a * b = b * a$

$(\mathbb{Z}, \%)$ – Group semi group monoid None

semi – closure + Asso

monoid – clo + Asso + Iden

Grop – 4

abelian – group + comm

$\frac{1}{2} = \underline{0.5} \notin \mathbb{Z}$.

$N = \{1, 2, 3 - - - \}$

$\mathbb{Z} = \{0, \pm 1, \pm 2, - - - \}$

$\mathbb{Q} = \{ a/b \mid a, b \in \mathbb{Z}, b \neq 0 \}$

$\mathbb{R}$ = $\mathbb{Q}$ Union

$(\mathbb{Z}, \cdot)$ – closure ✓

– Assosiative ✓

– Identity (1 is iden element)

– Inverse ×

H.W:

$(\mathbb{Z}, \cdot)$ monoid

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

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

$(\mathbb{R}, \cdot)$ $(\mathbb{Z}, -)$

problems!

eg:

Finite group

1. check whether the set $\{1, -1, i, -i\}$ is a group (or) not

sol

0	1	-1	+i	-i
1	1	-1	+i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

closure ✓

Asso ✓

Identity -1

Inverse

Invers of 1 : 1

-1 : -1

i : -i

-i : i

$-1 \times -1 = 1$

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

2. $\{1, w, w^2\}$ - cube roots of unity

Sol $x^3 = 1$

$x^3 - 1 = 0$

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

$x = 1, w, w^2$

	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

$w^4 = w^3 \cdot w$

$= 1 \cdot w$

1- identity

inverse

1 - 1

$w - w^2$

$w^2 - w$

Z_n,

$Z = \{0, \pm 1, \pm 2, ----\}$

$[0] - \{0, \pm 5, \pm 10, ---\}$

$[1] - \{6, 1, 11, 16, ---\}$

$[2], [3], [4]$

$Z_5 = \{[0], [1], [2], [3], [4]\}$

3. check $(Z_5, +)$, $(Z_5, *)$ - group (or) not

Sol

	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$4 +_5 4 = \frac{8}{5}$

Identity - 0

$0 \to 0$

[1] - 4

[2] - 3

[3] - 2

[4] - 1

properties:

Identity elem in a group is unique

proof: suppose e_1, e_2 are 2 identity element.

(∵ $a * e = e * a = a$)

Given e_1 is identity element

$$e_1 * e_2 = e_2 * e_1 = e_2 \quad \text{—①}$$

e_2 identity

$$e_1 * e_2 = e_2 * e_1 = e_1 \quad \text{—②}$$

comparing ① & ②

$$e_1 * e_2 = e_2 = e_1$$

$$\Rightarrow \boxed{e_1 = e_2}$$

Inverse of each elem is unique.

proof: let $a \in G$

b, c are inverses of a.

since a, b are inverses of each other

$$a * b = b * a = e$$

(a,c) $a*c = c*a = e$

$a*b = e = a*c$

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

$\boxed{b = c}$

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

inverse of

1 - 1

4 - 4

2 - 3

19/08/2021

$(Z_n, +_n)$ group any n

$(Z_4, +_4)$

0 - 0

3 - 4, 2 - 2

$(Z_4 - \{0\}, X_6)$

Z_n, X_n

Z_n groups - n prime

$Z_4 - \{0\} = \{1, 2, 3\}$

$(Z_5 - \{0\}, X_5)$ - forms group

X_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

X_4	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

If $(G,*)$ is an abelian group then for all $a,b \in G$. s.T

$(a*b)^2 = a^2 * b^2$ in general $(a*b)^n = a^n * b^n$

proof: Given group with comm is abelian group

i.e $\forall a,b \in G \Rightarrow a*b = b*a$

L.H.S $(a*b)^2 = (a*b) * (a*b)$

$= a*(b*a) * b$ (asso)

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

$= (a*a) * (b*b) = (a^2 * b^2)$

subgroups:

0 set along binary op

closure, Asso, Iden, Inverse.

A subset of a group satisfies group properities is called subgroup.

$(z, +)$ - group $z = \{0, \pm 1, \pm 2, \pm 3, \pm 4 \cdots\}$

$(2z, +)$ - group $2z = \{0, \pm 2, \pm 4, \pm 6, \cdots\}$

$(2z, +)$ is sub gp of $(z, +)$

(odd integers, +) - ! $1+3 = 4 \notin$ odd no

closure $\not\in$ $(n z, +)$ is a subgp of $(z,+)$

theorem: The necc and suff. condn for a subsets to be a subgroup is $\forall a,b \in S \Rightarrow a * b^{-1} \in S$

In other words

let $(G,*)$ be a group let $S \subseteq G$. $(S,*)$ is a subgroup of $(G,*)$ iff $\forall a,b \in S \Rightarrow a * b^{-1} \in S$.

proof: let $(G,*)$ be a group

Let $S \subseteq G$

G = clos
= ass
= ide
= inv

Assume: $(S,*)$ is a subgroup (S itself is group)

S = clos
= Ass
= Ide
= Inv

let $a,b \in S$

To prove: $a * b^{-1} \in S$

$a,b \in S \Rightarrow a^{-1}, b^{-1} \in S$ (Inverse prop)

Consider $a, b^{-1} \in S \Rightarrow a * b^{-1} \in S$ ($\because$ S is closed $a,b \in G \Rightarrow a * b \in G$)

Assume that

For all $a,b \in S$, $a * b^{-1} \in S$, then $(S,*)$ is subgroup

Identity:

let $a \in S$,

$a, a \in S$

By assumption $a * a^{-1} \in S$

$e \in S$

Identity of S is an element of S

Inverse:

let $a \in S$ already proved $e \in S$

$a, e \in S$

by assumption $e, a \in S$

$\Rightarrow e * a^{-1} \in S$

$a^{-1} \in S$

For any

$a \in S \Rightarrow a^{-1} \in S$

Inverse exists

for all elements in S.

closure:

let $a, b \in S$

since for any $a \in S$, $a^{-1} \in S$

$\therefore b \in S \Rightarrow b^{-1} \in S$

By assumption $(a, b \in S \Rightarrow a * b^{-1} \in S)$

$a, b^{-1} \in S \Rightarrow a * (b^{-1})^{-1} \in S$

$\Rightarrow a * b \in S$

$\therefore$ S is closed

closure

$a, b \in S \Rightarrow a * b \in S$

Always ass group is inherited form.

$\therefore$ S is a group

Hence the proof.

23/08/2021

1. show that $(R-\{-1\}, *)$ is an abelian group where $a*b = a+b+ab$ for all a,b in $R-\{-1\}$

Sol

1) closure:

$a, b \in R - \{-1\}$

To prove $a*b \in R - \{-1\}$

abelian { closure, Asso, Iden, Inve, comm } group

$a * b = a+b+ab$

$a*b+1 = a+b+ab+1$

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

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

TO prove

$a * b \neq -1$

if $a*b = -1$ $\quad a*b+1 = 0$

i.e $(a+1)(b+1) = 0$

$a+1 = 0$ (or) $b+1 = 0$

$a = -1, b = -1$

2) Associative:

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

$a*b = a+b+ab$

L.H.S $= a*(b*c)$

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

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

$+a(b+c+bc)$

$= a+b+c+bc+ab+ac+abc$ — (1)

R.H.S $= (a*b)*c$

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

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

$(a+b+ab)c$

$= a+b+ab+c+ac+bc+abc$ — (2)

L.H.S = R.H.S

3) Identity:

$a * e = e * a = a$

$a * e = a$

$a + e + ae = a$

$e + ae = 0$

$e(1+a) = 0$

$e = 0$ (or) $1 + a = 0$

$a = -1$

$a \in R - \{-1\}$

$a \neq -1$

$\therefore e = 0$

4) Inverse:

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

$a * a^{-1} = 0$

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

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

$a^{-1} = \frac{-a}{1+a} \in R - \{-1\}$

$\therefore$ Inverse exists for any $a \in R - \{-1\}$

($R - \{-1\}$ group w.r.t $*$) $R^* = R - \{-1\}$

5) commutative:

$a * b = b * a$

$a * b = a + b + ab$ ($\because +, \times$ in R is comm)

$= b + a + ba$

$= b * a$

then $(R-\{-1\}, *)$ is an abelian group.

H.W

2. show that $(R-\{+1\}, *)$ is an abelian group where $a*b = a+b$

$+ab$ for all a, b in $R-\{1\}$ Fourth root of unity.

Under

(4) Fourth root of unity $\{1, w, w^2, w^3\}$

$1 + w + w^2 + w^3 = 0$ & $w^4 = 1$

	1	w	w^2	w^3
1				
w				
w^2				
w^3				

$x^4 = 1 \quad x = 1$

$x = 1^{1/4}$

$x^4 - 1 = 0$

$(x-1)(x^3 + \text{--} \;)$

$x = 1, w, w^2, w^3$

$(w^4 = 1)$

problems:

1. show that the set of all non zero real numbers is an abelian group under the operation $*$ defined by $a*b = ab/2$

Sol closure & Asso prove

identity:

$a*e = e*a = a$

$a*e = a$

$\frac{ae}{2} = a$ $\quad (a * 1 = \frac{a * 2}{2} = a)$ verified

$\boxed{e = 2}$

Inverse: $\quad a \in R^*$

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

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

$\frac{aa^{-1}}{2} = 2$

$aa^{-1} = 4$

$a^{-1} = \frac{4}{a} \in R$

$\frac{(a * \frac{4}{a})}{2} = 2$

2. Show that $(Z_m, +_m)$ is an abelian group

$(Z_6, +6)$, $(Z_5, +5)$

3. Show that $(Z_5^*, 5)$ is an abelian group

property - ①: If every element in a group its own inverse, then the group must be abelian (or) if $a^2 = e$ with $a \neq e$, then G is abelian.

4. Show that if every element in a group G has its own inverse, then the group G must be abelian and discuss about its converse.

Sol

For any $a \in G$,

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

TO prove: commutative

① $a * b = b * a$

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

$a*b = b*a$

Note:

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

By defn $a, b \in g$

$\Rightarrow a*b \in G$

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

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

&

$\{1, -1\}$

	1	-1
1	1	-1
-1	-1	1

IL G is abelian, it is not nec

Ex: $(Z, +)$ - abelian

inverse $a \rightarrow (-a)$

$2 \rightarrow (-2)$

$(-5) \rightarrow (5)$

$2, 3 \in R$

$2 * 3$

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

Sol) $(a*b)^{-1} * (a^{-1} * b^{-1})$ $\quad a^{-1}=b \quad a*b = b*a = e$

$b^{-1}=a$

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

In an abelian ~~group~~ given

In any group

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

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

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

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

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

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

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

In abelian

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

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

property ②: If G is a group of even order, then it has an element $a \neq e$ such that $a^2 = e$.

order of a gp - |G|

O(a) - not eq to a

$\{1, -1, i, -i\}$

$3(-i) = -i^2$

$= -(-1)$

$= 1$

$i \neq -i$

property ③ :

In a group G, the left and right cancellation laws hold.

left cancellation law:

For any $a, b, c \in G$, $a * b = a * c \Rightarrow b = c$

Rt.

Given

$a * b = a * c$

left a^{-1} on both

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

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

$e * b = e * c \Rightarrow b = c$

rt

$b * a = c * a$

$b = c$

25/08/2021

property - ② ! If G is a group of even order then it has an element $a \neq e$ such that $a^2 = e$

let $o(G) = 2n$

wkT inverse of identity element $e = e$

$2n - 1$,

we need invers remaining $\boxed{2n-1}$ elements

when we pair element & inverse

So, except identity element, there will be one more elem -nt for which inverse is itself

(i.e) $a^{-1} = a$

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

$\boxed{e = a^2}$ $\boxed{e * e = e}$

$\{1, -1\}$	$\{1, -1, i, -i\}$
$1 - 1$	$1 - 1$ ✓
$-1 - -1$	$-1 - -1$ ✓
	$\boxed{i - i}$

property - ④ The identity element of a group is unique.

(or)

If $(G, *)$ is a group and 'e' is an identity element of G then no other element of G is an identity element of G.

property-(5):

The inverse of any element in a group G is unique.

property-(6):

A group cannot have any element which is idempotent other than the identity element.

Idempotent : $\rightarrow a*a = a$

$\boxed{e*e=e}$ in group

let $a \in G$ be idempotent element $a \neq e$

$a*a = a$ & $a*e = e*a = a$

$a = a*a = a*e$

$\boxed{a=e}$ (left cancellation $a*b = a*c \Rightarrow b=c$)

property-(7):

If a is an element of a group G, then $(a^{-1})^{-1} = a$

i.e If inverse of a is a^{-1} then the inverse of a^{-1} is a.

let inverse of a is a^{-1}

i.e $a*a^{-1} = a^{-1}*a = e$

a inverse of (a^{-1}) is $(a^{-1})^{-1}$

let inverse of a^{-1} is a

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

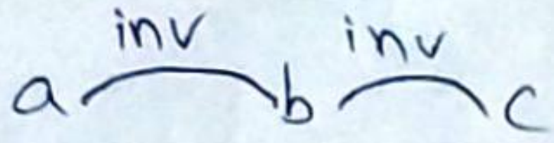
$a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * a^{-1} = e$

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

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

property-⑧ :

If a has inverse b and b has inverse c, then $a = c$



$a = c$

Given inverse of a is b | inverse of b is c

$a * b = b * a = e$ | $b * c = c * b = e$

$e = a * b$

$e = b * a = b * c$

$\boxed{a = c}$

problem-⑨ :

G is abelian iff $(a*b)^2 = a^2 * b^2$

problem-⑩ :

If $(G, *)$ is an abelian group, then for all $a, b \in G$

$(a*b)^n = a^n * b^n$

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

In abelian group

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

$$\boxed{(AB)^{-1} = B^{-1}A^{-1}}$$

proof:

G is abelian

$a*b = b*a$ — (1)

L.H.S $= (a*b)^2$

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

$= a*(b*a)*b$ (Assoc)

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

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

$= a^2 * b^2$

Assume $(a*b)^2 = a^2*b^2$

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

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

(right & left cancellation)

$\boxed{b*a = a*b}$

∴ commutative property holds good

G is abelian

Subgroups:

G – group

G = {e, a, b, c}

$2^4 - 16$

2^n – subsets

{1, -1, i, -i} – group

{1, -i} – group {i}

∴ {1, -i} is a subgroup of {1, -1, i, -i}

{1, i} – subgroup ?

	1	i
1	1	i
i	i	-1

{1, +i} not a subgroup

closure ×

	i	-i
i	-1	1
-i	1	-1

{i, -i} – ?

{1} – sub group

{i} – subgroup

closure ×

$Z = \{0, \pm 1, \pm 2, \cdots\}$

$(Z, +)$ is group

Sub group of $(Z, +)$, — ?

$2Z \subset Z$

$2Z = \{\vec{0}, \pm 2, \pm 4, \cdots\}$

add even not even closure even

$(2n, +)$ is group

$2Z = \{0, \pm 2, \pm 4, \pm 6, \cdots\}$

$(2Z, +)$ - group odd - group

① Take 2 elem in $2Z$,

$2n, 2m$ $2n + 2m = 2(m+n)$

$=$ even $\in 2Z$

$(2Z, +)$ is group

26/08/2021

subgroup:

Let $(G, *)$ be a group

A subset $H \subseteq G$ is said to be a subgroup of G

if $(H, *)$ is a group

Then

let G be a group $H \subseteq G$ be a subset

⓪

$2n + 2m$

$= 2(n+m)$

$\in Z$

H is a subgroup iff $a,b \in H \Rightarrow a * b^{-1} \in H$

$(Z, +)$ group

H - set of odd no in Z Here $H \subseteq Z$

$H = \{\pm 1, \pm 3, \pm 5, ---\}$

$1 + 3 = 4 \notin H$ ×

$0 \notin H$

$(3Z, +)$ is group?

$3Z = \{0, \pm 3, \pm 6, \pm 9, \pm 12, ---\}$

$(nZ, +)$ is group

subgroup of $(Z, +)$ are $(nZ, +)$

$n \in Z$.

$a * b^{-1} \in H$, whenever $a, b \in H$

H_1 — subgroup G

H_2 — " G

$H_1 \cap H_2$ — ?

$a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1 \Rightarrow a * b^{-1} \in H_1$

$\Rightarrow a, b \in H_2 \Rightarrow a * b^{-1} \in H_2$

$\therefore a * b^{-1} \in H_1 \cap H_2$

$\therefore H_1 \cap H_2$ is a subgroup

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$6Z = \{0, \pm 6, \pm 12, \cdots\}$

$Z_n = \{0, 1, 2, 3, \cdots, n-1\}$

$(Z_6, +_6)$ is subgroup

subgroup — ?

$(Z_6, +_6)$ group trivial $Z_6 \subset Z_6$ $\emptyset \subset Z_6$

$+_6$	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

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

$H_1 = \{0, 3\}$ - sub

$H_2 = \{0, 2, 4\}$ $\{0, 1, 5\}$

cyclic group:

$\{1, -1, i, -i\}$ — $\langle i \rangle$

$i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, $i^5 = i^1 = i$

cyclic group

$H = \{1, -1, i, -i\}$ $H = \langle i \rangle$

$\{1, -1\}$ — cyclic ?

$(-1)^1 = -1$

$(-1)^2 = 1$

Cyclic groups are abelian

proof:

let G be a cyclic group

let

$\langle a \rangle = G$

$x, y \in G$ then $x = a^n$, $y = a^m$ $m, n \in Z$

$x * y = a^n * a^m$

$= a^{n+m}$

$= a^{m+n} = a^m * a^n = y * x$

$\therefore$ G is abelian

coset: $(5Z, +)$ — group

$0 + 5Z = \{-10, -5, -1, 0, 5, 10, \cdots\}$

$1 + 5Z = \{-9, -4, 1, 6, 11, 16 \cdots\}$

$2+5_2 = \{-8, -3, 2, 7, 12, 17, \ldots\}$

$3+5_2 = \{-7, -2, 3, 8, 13, 18, \ldots\}$

$4+5_2 = \{-6, -1, 4, 9, 14, 19, \ldots\}$

$5+5_2 = \{-10, -5, 0, 5, 10, 15, \ldots\} = 5_2$

$(\mathbb{Z}, +)$ is a group

$(5_2, +)$ is a subgroup of $(\mathbb{Z}, +)$

G - group, H - subgroup of G

left coset $= \{a * H / a \in G\} = aH$

$\boxed{aH}$ - left coset

rt coset $= \{H * a / a \in G\} = Ha$

Union of all coset $= G$

$(0+5_2) \cup (1+5_2) \cup (2+5_2) \cup (3+5_2) \cup (4+5_2) = \mathbb{Z}$

All left coset are distinct

What is a coset?

In group theory, if G is a finite group, and H is a subgroup of G, and if g is an element of G, then;

gH = {gh: h an element of H} is the left coset of H in G with respect to the element of G and

Hg = {hg: h an element of H} is the right coset of H in G with respect to the element of G.

Now, let us have a discussion about the lemmas that helps to prove the lagrange theorem.

Lemma-1: If G is a group with subgroup H, then there is a one to one correspondence b/w H and any coset of H.

Lemma-2: If G is a group with subgroup H, then the left coset relation, $g_1 \sim g_2$ if and only if $g_1 * H = g_2 * H$ is an equivalence relation.

Lemma-3: Let S be a set and $\sim$ be an equivalence relation on S. If A and B are 2 equivalence classes with $A \cap B = \emptyset$, then $A = B$.

28/08/2021

Theorem: the no. of elements in H & its left cosets are same

there is a 1-1 correspondance between 2 left cosets.

Proof: Define $f: H \to aH$

by $f(h) = a * h$

H it self a coset

$e \in H$,

$e * H = H$

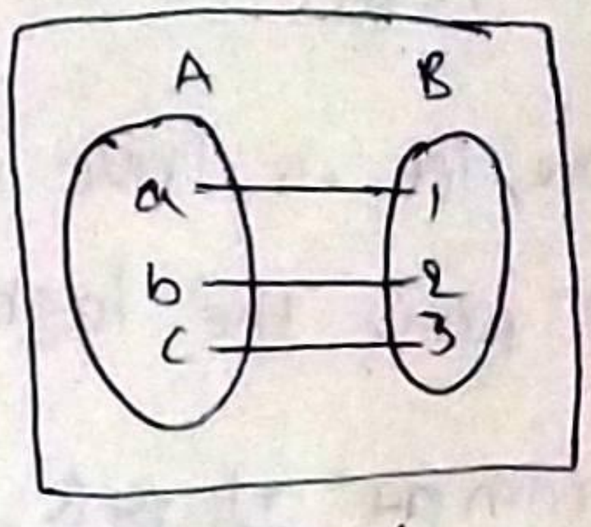
To prove: f is 1-1 & onto

$f(h_1) = f(h_2)$

$a * h_1 = a * h_2$ (left cancellation law)

$h_1 = h_2$

$\therefore$ f is 1-1



one-one:

$f(a) = f(b)$

$\Rightarrow a = b$

For any $a * h \in aH$, $\exists a$

For any $x \in aH$

then $x = a * h$ for some $h \in H$

$\therefore$ For any $x \in aH$ $\exists$ $h \in H$ such that

$f(h) = a * h$

$\therefore$ f is 1-1 & onto

∴ No. of element in H & its left cosets are same

Any 2 left cosets have the same no. of elements.

theorem: Any 2 left cosets are either identical (or) disjoint

proof:

Let aH & bH be 2 left cosets then either

$aH \cap bH = \emptyset$ (or) $aH = bH$

Let $c \in aH \cap bH$

$c \in aH \rightarrow c = a * h_1$,

$c \in bH \rightarrow c = b * h_2$

$a * h_1 = b * h_2$

(b's multiply h_1^{-1})

$a = (b * h_2) * h_1^{-1}$

$= b * (h_2 * h_1^{-1})$ (Asso property)

$a = b * h_3$

[∵ H - group
$h_2 * h_1^{-1} \in H$]

$h_3 \in H$

$a \in bH$

∴ $aH = bH$

(1+5 2) = (6+5 2)

6 ∈ 5

1+5 2 = 6+5 2

∴ 2 left cosets are either disjoint (or) identical.

All element of aH are of the form $a * (\text{ele of } H)$

$a * h$

All elements of bH are of the form $b * h$

All left cosets forms a partion of G_1

(ie) $G_1 = \bigcup aH$

$a \in G_1$

H is a subgroup, aH - coset

$\bigcup aH \subseteq G_1$

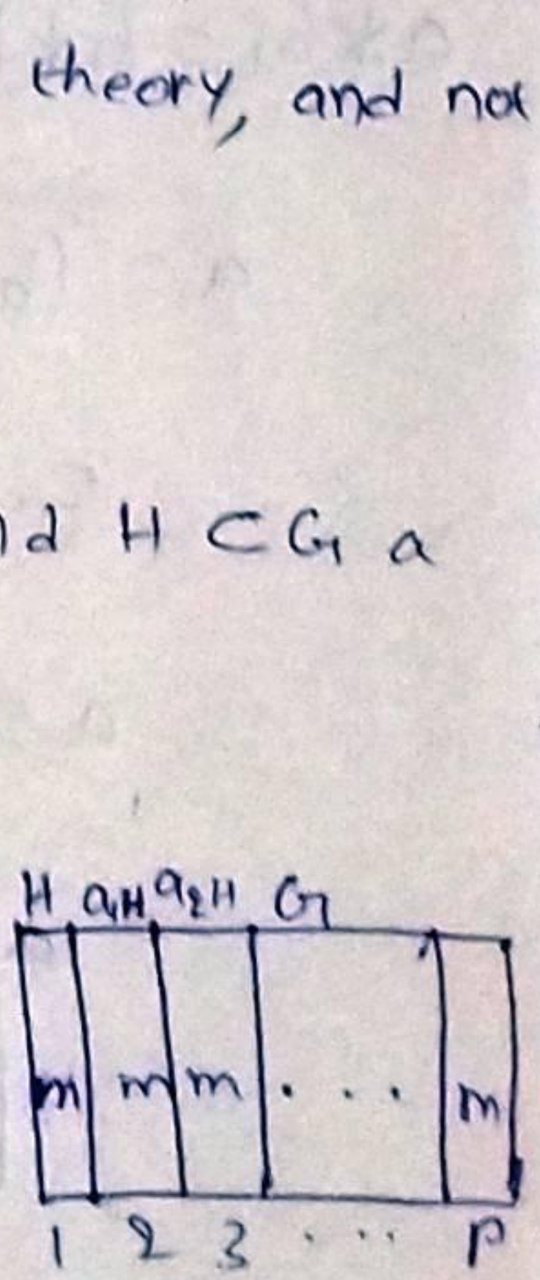
$x \in G_1$

$x * e \in x \in H$

$\therefore \bigcup aH = G_1$

Lagrange's theorem: theorem is about finite groups and their subgroups. It is very important in grap theory, and not just because it has a name

theorem - 1: let G_1 be a finite group and $H \subset G_1$ a subgroup of G_1. then $|H|$ divides $|G_1|$



proof: let G_1 be a group

$O(G_1) = n$

H be a subgroup of G_1

Let $O(H) = m$

There are p no'of distince left cosets

Also $\bigcup_{a \in G} aH = G$

$$O\left(\bigcup_{a \in G} aH\right) = O(G)$$

$$O(a_1H \cup a_2H \cup \cdots \cup a_pH) = O(G)$$

$$O(a_1H) + O(a_2H) + \cdots O(a_pH) = O(G)$$

$$m + m + \cdots + m(p \text{ times}) = n$$

$$pm = n \Rightarrow \frac{n}{m} = p$$

m divides n

$\therefore O(G) = n$

O(H) divides O(G)

eg:

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

$O(G) = 4$ $O(H) = 2$

converse of lagrangels theorem true (or) not?

$G = \{1, -1, i, -i\}$ - $O(G) = 4$

2^4 - subsets ϕ

$\{1\}, \{-1\}$ - single element set

$\{\}$ - 2 element set

- 3 " " ×

$\{1, -1, i, -i\}$ - 4 " "

3/4-3 doesn't divides 4

so cannot forms subgroup whose order is 3

{1, i} - not a subgroup