M.Nt CH [2] 1=77 ① [2·1-1]

GROUPS

B.Sc - Method - Chapter 2

Binary Operation :- (B.O)

B.O is a rule from $S \times S \to S$ i.e. which assigns to each element of $S \times S$ a unique element of S. where S is a non-empty set.

So a B.O on a nonempty set S can be defined as a fn which associates, with each $(a,b) \in S \times S$ a unique element of S. If this B.O, as a fn from $S \times S \to S$ is denoted by $*$ then the image of $(a,b) \in S \times S$ under $*$ is denoted by $a * b$. $\{a * b \in S\}$

If $*$ is a B.O in S then we say that S is closed under the B.O $*$.

i.e For $a, b \in S$, $a *$

$*$ may be '+', '·', '−' '÷'

Examples In the set Z of integers, ordinary addition denoted by '+', is a B.O in Z. ∵ the ordinary addition '+' associates with each ordered pair (a,b) of integers a unique integer which we denote by $a+b$

$2, 3 \in Z$. $2+3 = 5 \in Z$. Hence Z is closed under '+'

Similarly ordinary multiplication '·' is a B.O in Z.

$2, 3 \in Z$ $2 \cdot 3 = 6 \in Z$. Hence Z is closed under '·'

Similarly ordinary subtraction '−' is a B.O in Z

$2, 3 \in Z$ $2 - 3 = -1 \in Z$ Hence Z is closed under '−'

∴ ordinary division '÷' is not defined in Z

∵ as $2, 3 \in \mathbb{Z}$ but $2 \div 3 = \frac{2}{3} \notin \mathbb{Z}$

Note

1) A B.O $*$ may and may not be commutative.
If $a * b = b * a$ for all $a, b \in S$ then $*$ is said to be a commutative binary operation.

2) A B.O $*$ may and may not be Associative.
If $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$ then $*$ is said to be an Associative B.O.

3) Existence of an Identity element.
An element 'e' of S is said to be an identity element in S w.r.t $*$.
if $a * e = e * a = a$ for all $a \in S$.

$\begin{cases} a \cdot 1 = 1 \cdot a = a \ \forall a \in R \\ a + 0 = 0 + a = a \ \forall a \in R \end{cases}$

4) Inverse of an Element.
Let $a \in S$. An element $a' \in S$ is said to be inverse element of a w.r.t $*$ if
$a * a' = a' * a = e$

$\begin{cases} a \cdot \frac{1}{a} = 1 \\ a + (-a) = 0 \end{cases}$

Group:

A non-empty set G is said to be a group if
(i) there is a B.O $*$ defined in G i.e for any two elements a, b of G, $a * b \in G$.
(ii) the B.O in G is associative i.e
for $a, b, c \in G$ $(a * b) * c = a * (b * c)$

(iii) w.r.t the B.O $\star$ there exists an identity element 'e' in G. i,e

$$a \star e = e \star a = a. \qquad \forall\, a \in G$$

(iv) For each $a \in G$, there exists an inverse element $a' \in G$ such that

$$a \star a' = a' \star a = e$$ i,e each element of G has inverse element.

This Group is specified by the pair $(G, \star)$

Another Def. A pair $(G, \star)$ where G is non-empty set and $\star$ is a B.O in G is called a Group if the following conditions are satisfied in G.

(i) The B.O $\star$ is associative in G

(ii) Identity element exists in G w.r.t $\star$ $e \star a = a \star e = a$

(iii) Inverse element 'b' exist in G for every element 'a' of G

$$a \star b = b \star a = e$$

Abelian Group :-

A Group $(G, \star)$ is said to be abelian if $a \star b = b \star a$ for all $a, b \in G$.

Note (1) A Groupoid $(S, \star)$ is an ordered pair consisting of a non-empty set S and a B.O $\star$ defined in S. (Closure property)

(2) A Groupoid $(S, \star)$ is called a Semigroup if B.O $\star$ is Associative if Identity element exists in a Semigroup then it is called Monoid and for every element of Monoid, if there exists inverse element then Monoid is called a Group

Example 1 $G = [1, -1]$

B.O defined on G be the ordinary multiplication.

·	1	-1
1	1	-1
-1	-1	1

Group table

(i) Associative $(1\cdot1)\cdot1 = 1\cdot(1\cdot1)$ ✓

$(1\cdot-1)\cdot1 = 1\cdot(-1\cdot1)$ ✓

(ii) Identity $e*a = a*e = a$ (def)

$e = 1$ $\because 1\cdot(-1) = (-1)\cdot1 = -1$

(iii) Inverse $ab = ba = e$ (def)

$(1)(1)^{-1} = 1\left(\frac{1}{1}\right) = 1 = e$

$(1)^{-1}(1) = \left(\frac{1}{1}\right)1 = 1 = e$

$(-1)(-1)^{-1} = (-1)\left(\frac{1}{-1}\right) = 1 = e$

$(-1)^{-1}(-1) = \left(\frac{1}{-1}\right)(-1) = 1 = e$

All the three conditions are satisfied hence G is group

Example 2 $(Z, +)$ is a group. '+' is ordinary addition

Z is set of integers. 1, e

$Z = \{0, \pm1, \pm2, \pm3, \ldots\}$

Let $4, 5, 6 \in Z$.

$(4+5)+6 = 4+(5+6)$

$15 = 15$ Hence Associative

(ii) Identity $e*a = a*e = a$ $e, a \in Z$.

$0+4 = 4+0 = 4$ Hence $e = 0 \in Z$.

(iii) Inverse $a*b = b*a = e$ $a, b \in Z$

$4+(-4) = (-4)+4 = 0$ $4, -4 \in Z$

Inverse of each element of z exists

Hence $(Z, +)$ is a group

Similarly $(Q, +), (R, +), (C, +)$ are groups.

In $(C, +)$ $0 + i0 = e$ $A = (a_1 + ib_1)$ $C = (a_3 + ib_3)$

$A, B, C \in C$. where $B = (a_2 + ib_2)$ $-A = -a_1 - ib$

2·1-5

$(Q,+)$ is a group with '0' as identity element and '$-\frac{a}{b} \in Q$' as additive inverse for each '$\frac{a}{b} \in Q$'. Associativity can be proved easily by taking any three elements, $\frac{a}{b}, \frac{c}{d}, \frac{p}{q}$

$(Q,\cdot)$ is not a group because '0' has no multiplicative inverse in Q. The identity of $(Q,\cdot)$ is '1'.

$(Q-\{0\},\cdot)$ is a group with '1' as identity element and $\frac{a}{b}$ as Multiplicative inverse for each $\frac{b}{a} \in Q$

$(R,+)$ is a group with 0 as identity element and '$-a' \in R$' as additive inverse for each '$a' \in R$. Associativity can be proved easily.

$(R,\cdot)$ is not a group because '0' has no multiplicative inverse in R. The identity of $(R,\cdot)$ is '1'.

$(R-\{0\},\cdot)$ is a group with 1 as identity element and '$\frac{1}{a} \in R-\{0\}$' as multiplicative inverse for each $a \in R-\{0\}$

Neither $(N,+)$ nor $(N,\cdot)$ is a group $\because$ N has no identity element w.r.t '+' and has no inverse element w.r.t '$\cdot$'.

Neither $(W,+)$ nor $(W,\cdot)$ is a group $\because$ For $a \in W$ there does not exist '$-a' \in W$' w.r.t '+' and For $a \in W$, there does not exist $\frac{1}{a} \in W$. (i.e Inverse does not exist)

2.1-6

$(C,+)$ and $(C-\{0\},\cdot)$ are groups $\quad a+ib \in C$.

For $(C,+)$ identity $= 0+i0$ Inverse $= -a-ib$ for $a+ib$

'+' is associative in C.

For $(C-\{0\},\cdot)$ Identity $= 1+0i$, For every $A = a+ib$ there exist $A^{-1} = \frac{1}{a+ib} = \frac{a-ib}{a^2+b^2}$

'$\cdot$' is associative in $C-\{0\}$

$$AA^{-1} = (a+ib)\frac{(a-ib)}{a^2+b^2} = 1 = 1+0i$$

Let M_2 be the set of all 2×2 matrices,

$A = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}$ a_1, b_1, a_2, b_2 are real numbers such that A is non singular i.e $|A| = a_1b_2 - b_1a_2 \neq 0$

$B = \begin{bmatrix} a_1' & b_1' \\ a_2' & b_2' \end{bmatrix}$

$$AB = \begin{bmatrix} a_1a_1' + b_1a_2' & a_1b_1' + b_1b_2' \\ a_2a_1' + b_2a_2' & a_2b_1' + b_2b_2' \end{bmatrix}$$

$\in |AB| \neq 0$ Hence $AB \in M_2$. So M_2 is closed under Matrix Multiplication

Also $(AB)C = A(BC)$ for all $A, B, C \in M_2$ can be verified easily

Identity Matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ w.r.t '$\cdot$' $\quad A \cdot I = I \cdot A = A$

Moreover for each $A = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}$ in M_2 there exist A^{-1} s.t

$$A^{-1} = \begin{bmatrix} \frac{b_2}{a_1b_2 - b_1a_2} & \frac{-b_1}{a_1b_2 - b_1a_2} \\ \frac{-a_2}{a_1b_2 - b_1a_2} & \frac{a_1}{a_1b_2 - b_1a_2} \end{bmatrix}$$

Now $AA^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

So $(M_2, \cdot)$ is a group.

2·1-7

$G = \{1, \omega, \omega^2\}$ and '·' is defined by the table

·	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(i) Associative B.O

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

$\omega\cdot\omega^2 = 1\cdot 1$

$1 = 1$

(ii) Identity $1 = e$ $\quad e\cdot a = a\cdot e = a$

(iii) Inverse

Inverse of ω is ω^2

Inverse of ω^2 is ω

Inverse of 1 is 1

$ab = ba = e \;\Big|\; \because \omega^3 = 1,\ \omega\omega^2 = 1$

$\omega\omega^2 = \omega^2\omega = 1$

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

Hence $(G, \cdot)$ is a group.

The set $\{1, -1, i, -i\}$ and '·' is defined by table.

·	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	$+i$
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

Associative B.O

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

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

$-i = -i$

Identity '1' is identity $\quad a\cdot e = e\cdot a = a$

Inverse Inverse of 1 is 1

= = (−1) is (−1)

= = i is $-i$

= = $-i$ is i

Hence group

$(i)^{-1} = \frac{1}{i} = \frac{i}{i^2} = -i$

Order of a Group The number of elements in a group G is called order of that group. & denoted by |G|

Finite Group If number of elements in a group are finite then it is finite group.

Infinite Group If number of elements in a group are infinite then it is infinite.

$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Q}-\{0\},\cdot)$, $(\mathbb{R}-\{0\},\cdot)$ are all infinite groups.

The group of $\{1, \omega, \omega^2\} = \{1, -1, i, -i\}$ are finite groups

Cancellation Law

If $a,b,c \in G$ then (i) $a\cdot b = a\cdot c \Rightarrow b=c$ left Cancell

(ii) $b\cdot a = c\cdot a \Rightarrow b=c$ Right Cancell

Proof Let $a\cdot b = a\cdot c$ given

$\bar{a}^1\cdot(a\cdot b) = \bar{a}^1\cdot(a\cdot c)$ pre multiplying by $\bar{a}^1$

$(\bar{a}^1 a)\cdot b = (\bar{a}^1 a)\cdot c$ ∵ Associative Law.

$e\cdot b = e\cdot c$ ∵ $\bar{a}^1 a = e$

$b = c$ ∵ e is identity.

Hence $a\cdot b = a\cdot c \Rightarrow b=c$.

Similarly we can prove Right Cancellation Law.

Example: $S = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ be the set of residue classes modulo 5

To show $(S, +)$ is a group

We construct the group table

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

For $\bar{a}, \bar{b} \in S$

$\bar{a} + \bar{b} = \bar{r}$

where r is the remainder after division of $a+b$ by 5

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

$(\bar{2}+\bar{3})+\bar{4} = \bar{2}+(\bar{3}+\bar{4})$

$\bar{0} + \bar{4} = \bar{2} + \bar{2}$

$\bar{4} = \bar{4}$

ii) Identity $a * e = e * a = a$

Here $\bar{0}$ is identity

$\bar{0}+\bar{0} = \bar{0}$ $\quad \bar{0}+\bar{1} = \bar{1}$ $\quad \bar{0}+\bar{2} = \bar{2}$ $\quad \bar{0}+\bar{3} = \bar{3}$ $\quad \bar{0}+\bar{4} = 4$.

iii) Inverse. $a * b = b * a = e$.

$\bar{1}+\bar{4} = \bar{0}$ $\quad \bar{2}+\bar{3} = \bar{0}$ $\quad \bar{0}+\bar{0} = 0$.

Hence Inverse element exists for each element of set S under addition modulo 5.

All conditions satisfied So $(S, +)$ is a group.

2.1 – 10

Example 9 Let $\bar{Z}'_5 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ be the set of non-zero residue classes modulo 5 and multiplication defined is multiplication modulo 5. To Prove $(\bar{Z}'_5, \cdot)$ is a group

We construct group table

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

For $\bar{a}, \bar{b} \in \bar{Z}'$

$\bar{a} \cdot \bar{b} = r$

where r is the remainder obtained after dividing the usual product ab of $a \times b$ by 5

i) Associative $(\bar{2} \cdot \bar{3}) \cdot \bar{4} = \bar{2} \cdot (\bar{3} \cdot \bar{4})$

$\bar{1} \cdot \bar{4} = \bar{2} \cdot \bar{2}$

$\bar{4} = \bar{4}$

ii) Identity $a \cdot e = e \cdot a = a$

Here identity w.r.t multiplication modulo 5 is $\bar{1}$

$\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{1} \cdot \bar{2} = \bar{2}$, $\bar{1} \cdot \bar{3} = \bar{3}$ $\bar{1} \cdot \bar{4} = \bar{4}$

iii) Inverse $a \cdot b = b \cdot a = e$

$\bar{1} \cdot \bar{1} = \bar{1}$ $\bar{2} \cdot \bar{3} = \bar{1}$ $\bar{4} \cdot \bar{4} = \bar{1}$

Hence inverse for each element of set $\bar{Z}'_5$ exists

All conditions are satisfied

$\therefore (\bar{Z}'_5, \cdot)$ is a group.

Theorem (Solution of Linear Eq)

For any two elements a, b in a group G, the eqs $ax = b$ & $ya = b$ have unique sol

Proof $\because (G, \cdot)$ is a group & $a, b \in G$, so inverse of each element of G exists in G. Let $\bar{a}^1$ be inverse of a in G then

$ax = b$	$ya = b$
premultiply by $\bar{a}^1$ $\quad \bar{a}^1 a x = \bar{a}^1 b$	$ya\bar{a}^1 = b\bar{a}^1$ Post-multiply by a^{-1}
$\bar{x}^1 = e \quad (e)x = \bar{a}^1 b$	$y(e) = b\bar{a}^1$
$x = \bar{a}^1 b$	$y = b\bar{a}^1$

So $x = \bar{a}^1 b$ is a sol of $ax = b$ — So $y = b\bar{a}^1$ is a sol of $ya = b$

Now we prove the uniqueness of the solution of $ax = b$

Let x', x'' be two solutions of $ax = b$.

Then $ax' = b$ & $ax'' = b$

$ax' = ax''$ ∴ left cancellation law

$x' = x''$

Similarly let y', y'' be the sol' of $ya = b$

$\therefore \quad y'a = b \quad \& \quad y''a = b$

$y'a = y''a$ Right Cancellation Law

$y' = y''$

which proves the uniqueness of the theorem.

2·1-12

Theorem For a, b in a group G, $(ab)^{-1} = b^{-1}a^{-1}$

Proof $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$ — Associative Law

$= aea^{-1}$ — $bb^{-1} = e$

$= aa^{-1}$ — e = Identity

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

Pre-multiply by $(ab)^{-1}$: $(ab)^{-1}(ab)(b^{-1}a^{-1}) = (ab)^{-1}.e$

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

$b^{-1}a^{-1} = (ab)^{-1}$ Proved.

This result can be generalised for a product of finite no of elements of G.

i.e for $a_1, a_2, a_3, \ldots\ldots a_n \in G$.

$(a_1 a_2 a_3 \ldots\ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots\ldots a_3^{-1} a_2^{-1} a_1^{-1}$

Th For an element a of a group G, the following exponentiation rules hold.

(i) $a^m = a.a.a \ldots\ldots a$ m factors

Put $m = 1$ $a^1 = a$ 1 factor — c-1 is satisfied

Put $m = K$ $a^K = a.a.a \ldots$ K factors — Supposed true

$a^K(a) = (a.a \ldots a$ K factors$).a$

$a^{K+1} = a.a \ldots\ldots$ K+1 factors

K is replaced by K+1 Hence it is true

2·1-13

(iii) $(a^{-1})^m = a^{-m}$ To Prove $m \in Z$

For $m=1$ $(a^{-1})^1 = a^{-1}$ C-1 is satisfied

For $m=K$ $(a^{-1})^K = a^{-K}$ supposed true

Now consider $(a^{-1})^{K+1} = (a^{-1})^K (a^{-1})^1 = (a^{-K})(a^{-1})$ using supposition

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

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

$(a^{-1})^{K+1} = a^{-(K+1)}$ True for $m=K+1$

(iii) $a^m \cdot a^n = a^{m+n}$ $m, n \in Z^+$. i.e $m>0$ $n>0$

Case 1. $m>0$ & $n>0$

Put $n=1$

$a^m \cdot a^1 = a^{m+1}$ C-1 is satisfied

Put $n=K$ $a^m \cdot a^K = a^{m+K}$ Suppose true

Now Consider $a^m \cdot a^{K+1} = a^m \cdot (a^K a) = (a^m a^K) \cdot a$ Associative

$= (a^{m+K}) \cdot a$ using supposition

$a^m \cdot a^{K+1} = a^{m+K+1}$ C-2 is satisfied

Hence $\boxed{a^m \cdot a^n = a^{m+n}}$

Case 2 when $m<0$ & $n<0$

Let $m=-p$ $n=-q$. $p, q \in Z^+$

$\therefore a^{m+n} = a^{-p-q} = a^{-(p+q)} = (a^{-1})^{p+q}$

$= (a^{-1})^p \cdot (a^{-1})^q = a^{-p} \cdot a^{-q}$

from (i) $\because (a^{-1})^m = a^{-m}$

$\boxed{a^{m+n} = a^m \cdot a^n}$ Proved

Case 3 Suppose $m = 0$ & $n \neq 0$ To Prove $a^{m+n} = a^m a^n$

using $m=0$ $\quad a^{m+n} = a^{0+n} = a^n = ea^n = a^0 a^n$

$\therefore a^{0+n} = a^0 a^n$

Similarly when $m \neq 0$ & $n = 0$

then $a^{m+0} = a^m = a^m e = a^m a^0$

$a^{m+0} = a^m a^0$

Case 4 Suppose $m > 0$ & $n < 0$ s.t $m+n \geq 0$

$a^{m+n} = a^{m+n} \cdot e$ $\quad \because e$ is identity

$= a^{m+n}(a^{-n} a^n)$

$= (a^{m+n-n}) a^n$

$= (a^{m+n-n}) a^n \quad (\because n<0 \Rightarrow -n>0)$

$a^{-n} a^n = e.$

Note $a^{-n} a^{+n} = a \cdot a \cdot a \cdots a \overbrace{a^{-1}a^{-1}a^{-1}\cdots}^{n \text{ times}}$ (n this)

$= a \cdot a \cdot a \cdots (aa^{-1})a^{-1} \cdots$

$= a \cdot a \cdots a(e)a^{-1}a^{-1} \cdots$

$= a \cdot a \cdots (aa^{-1})a^{-1} \cdots$

$= a \cdot a \cdots a(e)a^{-1}$

$a^{m+n} = a^m a^n$

Similarly $a^{m+n} = a^m \cdot a^n$ for $m<0$ & $n>0$ s.t $m+n \geq 0$

Case 5 Let $m > 0$ $n < 0$ s.t $m+n < 0 \Rightarrow -(m+n) > 0$

Now $a^{m+n} = a^{m+n} \cdot e$

$= (a^{m+n})(a^{-n} a^n)$

$= a^{m+n} \cdot (a^{-m-n} a^m) \cdot a^n$

$= (a^{m+n-m-n}) a^m a^n$

$a^{m+n} = e(a^m a^n) = a^m a^n$

Note $a^{-(m+n)} \cdot a^m = a^{-m-n} a^m$

$= a^{-m-n+m}$

$= a^{-n}$ $\quad (\because -m-n) > 0$ & $m > 0$ So by (1)

Hence we have $a^{m+n} = a^m \cdot a^n \quad \forall m, n \in \mathbb{Z}$

2-1-15

(iv) To Prove $(a^m)^n = a^{mn}$ $\forall m, n \in \bar{Z}$

Case 1 when $n > 0$

Put $n = 1$ $\quad (a^m)^1 = a^{m \cdot 1}$

$a^m = a^m$ C-1 is satisfied

Put $n = K$ $\quad (a^m)^K = a^{mK}$ Supposed true

Now $(a^m)^{K+1} = (a^m)^K (a^m)^1$

$= a^{mK} \; a^m$ $\longrightarrow$ using supposition

$= a^{mK+m}$ $\longrightarrow$ using $a^{m+n} = a^m \cdot a^n$

$(a^m)^{K+1} = a^{m(K+1)}$ C-2 is satisfied

Hence $(a^m)^n = a^{mn}$ $\forall m \in Z$ & $n \in Z^+$

Case 2 When $n < 0$

Let $n = -r$ where $r \in Z^+$

$(a^m)^n = (a^m)^{-r}$

$= \left((a^m)^{-1}\right)^r$, Th. (ii) $(a^{-1})^m = a^{-m}$

$= (a^{-m})^r$

$= a^{-mr}$

$= a^{m(-r)}$

$(a^m)^n = a^{mn}$

Case 3 Let $n = 0$

$\Rightarrow (a^m)^n = (a^m)^0 = e = a^0 = a^{m0}$

Hence $(a^m)^n = a^{mn}$ $\forall m, n \in Z$,

2-1-16

Order of an element

Let 'a' be an element of a group G

A +ive integer 'n' is said to be the order of 'a' if $a^n = e$

(Example $G = \{1, \omega, \omega^2\}$ $O(\omega) = 3$ $\because \omega^3 = 1 = e$
$G = \{1, -1, i, -i\}$ $O(-1) = 2$ $\because (-1)^2 = 1 = e$)

where n is least +ive integer.

It is denoted by $O(a) = n$ or $|a| = n$

If there does not exist 'n' s.t $a^n = e$ then a is said to be of Infinite Order.

i.e If $n = 0$ is the only integer for which $a^n = e$ then a is said to be of infinite order

Example: $S = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ To Prove group under '×' modulo 8

×	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

(i) Associative $(\bar{3} \times \bar{5}) \times \bar{7} = \bar{3} \times (\bar{5} \times \bar{7})$

$\bar{7} \times \bar{7} = \bar{3} \times \bar{3}$

$\bar{1} = \bar{1}$

(ii) Identity $e = 1$

$\bar{1} \times \bar{1} = \bar{1}$
$1 \times \bar{3} = \bar{3}$
$1 \times \bar{5} = \bar{5}$
$1 \times \bar{7} = \bar{7}$

(iii) Inverse. For each element of S there exist inverse element.

as $\bar{1} \times \bar{1} = \bar{1}$
$\bar{3} \times \bar{3} = \bar{1}$
$\bar{5} \times \bar{5} = \bar{1}$
$\bar{7} \times \bar{7} = \bar{1}$

each element of S is inverse of itself

To Find Order $a^n = e$

$a^n = e$ n is order of 'a'

Order of $\bar{1}$ is 2 $\because (\bar{1})^2 = \bar{1}$

order of $\bar{3}$ is 2 $\because (\bar{3})^2 = \bar{3} \times \bar{3} = \bar{1}$

order of $\bar{5}$ is 2 $\because (\bar{5})^2 = \bar{5} \times \bar{5} = \bar{1}$

order of $\bar{7}$ is 2 $\because (\bar{7})^2 = \bar{7} \times \bar{7} = \bar{1}$

Example 11 — 2-1-17

Show that $O(a) = O(a^{-1})$

Let G be a group & $a \in G$.

Suppose $O(a) = m \Rightarrow a^m = e$ where m is least +ive integer

& $O(a^{-1}) = n \Rightarrow (a^{-1})^n = e$ ∴ n is least +ive integer

Now $a^m = e$ (We have to prove that $m = n$)

$a^m a^{-m} = e a^{-m}$

$a^{m-m} = a^{-m}$

$e = (a^{-1})^m$ but $(a^{-1})^n = e$

$\Rightarrow m > n$ ——— (1) (∵ n is least +ive integer)

Similarly let $(a^{-1})^n = e$

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

$a^n a^{-n} = a^n$

$a^{n-n} = a^n$

$e = a^n$ but $a^m = e$

$\Rightarrow n > m$ ——— (2) (∵ m is least +ive integer)

So from (1) & (2)

$n = m$ Hence $O(a) = O(a^{-1})$

(ii) The orders of ab and ba are equal

$O(ab) = O(ba)$ To Prove.

Let G be a group & $a, b \in G$

Suppose $O(ab) = n \iff (ab)^n = e$

Thus $(ab)^n = e \iff ab \cdot ab \cdot ab \cdots$ n times $= e$

pre multiply by b^{-1}

$\Leftrightarrow a^{-1}.ab.ab.ab.\ldots\ldots ab = a^{-1}e$

$\Leftrightarrow (a^{-1}a)b.ab.ab\ldots\ldots ab = a^{-1}$

$\Leftrightarrow e(ba).ba.\ldots\ldots ab = a^{-1}$

Post multiply by a

$\Leftrightarrow (ba)(ba).\ldots(ba).b = a^{-1}$

$\Leftrightarrow (ba).(ba)\ldots\ldots(ba).ba = a^{-1}a$

$\Leftrightarrow (ba)^m = e$

Hence the orders of ab & ba are equal.

Q)

7h The orders of a & bab^{-1} are equal.

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

Let $a, b \in G$. Then the order of a is m i.e $a^m = e$

$\therefore a^m = e$

$\Leftrightarrow a\,a\,a\ldots\ldots m\text{ times} = e$

$\Leftrightarrow aeaeae\ldots\ldots m\text{ times} = eeee\ldots m\text{ times}$

$\Leftrightarrow a(b^{-1}b)a(b^{-1}b)a\ldots a(bb^{-1}) = e$

$\Leftrightarrow ab^{-1}(bab^{-1})(bab^{-1})\ldots(bab^{-1})b = e$

pre x by b

$\Leftrightarrow (bab^{-1})(bab^{-1})(bab^{-1})\ldots(bab^{-1})b = be$

$\Leftrightarrow (bab^{-1})(bab^{-1})(bab^{-1})\ldots(bab^{-1})b = b$

Post x by b^{-1}

$\Leftrightarrow (bab^{-1})(bab^{-1})(bab^{-1})\ldots\ldots(bab^{-1})bb^{-1} = bb^{-1}$

$\Leftrightarrow (bab^{-1})(bab^{-1})(bab^{-1})\ldots\ldots(bab^{-1})e = e$

$\Leftrightarrow (bab^{-1})^m = e$ $\quad \therefore m$ times (bab^{-1})

Hence order of bab^{-1} is m i.e $O(bab^{-1}) = m$.

So $O(a) = O(bab^{-1})$

Exercise # 2.1

Q#16 Let G be a group such that $(ab)^n = a^n b^n$ ——— ①

For three consecutive nos $m-2, m-1, m$. ① holds i.e

$\because (ab)^m = a^m b^m$

$\Rightarrow (ab)^{m-1}(ab) = a^m b^m$

$\Rightarrow (a^{m-1} b^{m-1})(ab) = a^m b^m$

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

Pre Multiply by a^{-m+1}

$\Rightarrow a^{-m+1} a^{m-1}(b^{m-1}a)b = a^{-m+1} a^m (ab)$

$\Rightarrow e(b^{m-1}a)b = a^{-m+1} a^m b$

$(b^{m-1}a)b = ab^m$

Post Multiply by b^{-1}

$\Rightarrow (b^{m-1}a)bb^{-1} = (ab^m)b^{-1}$

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

$b^{m-1}a = ab^{m-1}$

Thus $(ab)^m = a^m b^m \Rightarrow b^{m-1}a = ab^{m-1}$ ——— ②

Put $m = m-1$ in ②

$\Rightarrow (ab)^{m-1} = a^{m-1} b^{m-1} \Rightarrow b^{m-1-1}a = ab^{m-1-1}$

$\Rightarrow b^{m-2}a = ab^{m-2}$ ——— ③

$(ab)^{m-2} = a^{m-2} b^{m-2}$

$(ab)^{m-1} = a^{m-1} b^{m-1}$

$(ab)^m = a^m b^m$

{We have to prove G abelian i.e $ab = ba$

(Asso Law.)

2nd Method Easy

Let m, m+1, m+2, be three consecutive numbers

$(ab)^m = a^m b^m$ —— ①

$(ab)^{m+1} = a^{m+1} b^{m+1}$ —— ⑪

$(ab)^{m+2} = a^{m+2} b^{m+2}$ —— ⑪⑪

$\Rightarrow (ab)^{m+1}(ab) = (a^{m+1} a b^{m+1} b)$

using ⑪ $\Rightarrow a^{m+1} b^{m+1}(ab) = (a^{m+1} a b^{m+1})b$

by Asso Law $\Rightarrow a^{m+1}(b^{m+1}a)b = a^{m+1}(ab^{m+1})b$

by Right Cancellation Law $\Rightarrow a^m a(b^{m+1}a) = a^m(ab^{m+1})$

by Left Cancellation Law $\Rightarrow a^m b^m(ba) = a^{m+1} b^{m+1}$

using ① $\Rightarrow (ab)^m(ba) = (ab)^{m+1}$ using ⑪

$\Rightarrow (ab)^m(ba) = (ab)^m(ab)$

Left Cancellation Law $\Rightarrow ba = ab$

Hence G is abelian

$\therefore b^{m-1}a = (bb^{m-2})a$

$= b(b^{m-2}a)$ Asso Law.

$= b(ab^{m-2})$ using ③

$b^{m-1}a = (ba)b^{m-2}$ ——— (A)

Similarly $ab^{m-1} = (ab)b^{m-2}$ ——— (B)

From ② $b^{m-1}a = ab^{m-1}$

use (A) & (B) in ② $(ba)b^{m-2} = (ab)b^{m-2}$

By Right Cancellation Law. $ab = cb \Rightarrow a = c$ commutative law provid.

$ba = ab$

Hence G is abelian

×———×

(18) Q4 $S = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ To Prove S is group under multiplication modulo 9.

•	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{5}$	$\bar{7}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{7}$	$\bar{2}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\bar{2}$	$\bar{7}$	$\bar{8}$	$\bar{4}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{1}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{8}$	$\bar{7}$	$\bar{5}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

Associative

$\bar{4}\cdot(\bar{5}\cdot\bar{7}) = (\bar{4}\cdot\bar{5})\cdot\bar{7}$

$\bar{4}\cdot\bar{8} = \bar{2}\cdot\bar{7}$

$\bar{5} = \bar{5}$

Identity $e * a = a * e = a$

$e = 1$ First row shows that identity is $\bar{1}$

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

For each element of S there exists inverse element.

$\bar{1}\cdot\bar{1} = \bar{1}$ $\bar{2}\cdot\bar{5} = \bar{1}$ $\bar{4}\cdot\bar{7} = \bar{1}$ $\bar{8}\cdot\bar{8} = \bar{1}$

2-1-21

Q+⑤ Is (Z, o) a group where o is defined by

$a \circ b = 0$ for all $a, b \in Z$.

Associative: $2, 3, 4 \in Z$ — for any $a, b, c \in Z$, $(a \circ b) \circ c = a \circ (b \circ c)$

$(2 \circ 3) \circ 4 = 2 \circ (3 \circ 4)$

$0 \circ 4 = 2 \circ 0$

$0 = 0$

Identity: $a * e = e * a = a$

Let $e = 0$: $2 \circ 0 = 0$, $3 \circ 0 = 0$

Let $e = 1$: $2 \circ 1 = 0$, $4 \circ 1 = 0$

Neither 0 is identity Nor 1 is identity

Here no element of Z can be taken as the identity element

So (Z, o) is not a group.

---

⑥ Q9 Group G is such that $x \cdot x = e$ for all $x \in G$ where e is the identity element of G, then to Prove G is abelian

Let $a, b \in G$ then by def $a \cdot a = e$ & $b \cdot b = e$

Now $a, b \in G \Rightarrow ab \in G$ (∵ G is group so G is closed)

So $(ab).(ab) = e$

Now $a \cdot a = e \Rightarrow a = a^{-1}$ — ① (∵ By def of inverse if $ab = e$ then a is inverse of b)

$b \cdot b = e \Rightarrow b = b^{-1}$ — ②

$(ab) \cdot (ab) = e \Rightarrow ab = (ab)^{-1}$

$= b^{-1}a^{-1}$ ∵ $(ab)^{-1} = b^{-1}a^{-1}$

$ab = ba$ (commutative) using ① & ②

Hence G is an Abelian Group.

Q10 If a group G has three elements then show that it is abelian

Sol Since the group G has three elements & by def of group one of those elements must be identity element.

Let $G=\{e,a,b\}$ e is identity

As $a\in G$ so $a\cdot a=a^2\in G$ ∵ G is a group (closure property)

then we have the following cases.

$a^2=e$
or $a^2=a$
or $a^2=b$

Case 1 Let $a^2=e \Rightarrow a\cdot a=e \Rightarrow a=\bar{a}^1$ ——— (1)

Also $a,b\in G \Rightarrow ab\in G$ ∵ G is a group.

∴ $ab=e$
or $ab=a$
or $ab=b$

If $ab=e \Rightarrow b=\bar{a}^1 \Rightarrow b=a$ using (1) which is a contradiction.

If $ab=a \Rightarrow ab=ae \Rightarrow b=e$ left Cancellation law which is a contradiction.

If $ab=b \Rightarrow ab=eb \Rightarrow a=e$ again a contradiction ∵ a & e are distinct.

Hence we conclude that $a^2\neq e$

Case 2

If $a^2=a \Rightarrow a\cdot a=ae \Rightarrow a=e$ Contradiction ∵ a & e distinct ∴ $a^2\neq a$

∵ we have proved in Case 1 & Case 2 that $a^2\neq e$ & $a^2\neq a$

So we are left with only one possibility that $a^2=b$

So G becomes $\{e,a,a^2\}$. Since G becomes cyclic group generated by a & we know that every cyclic group is abelian, so G is abelian.

Q#2 Prove that if every non-identity element of a group G is of order 2 then G is abelian.

Sol For all non-identity elements $x \in G \Rightarrow x^2 = e$ (Given)

$\therefore$ For all $a, b \in G \Rightarrow ab \in G$ Closure property

So $a^2 = e$, $b^2 = e$, $(ab)^2 = e$ etc

Now $(ab)^2 = e$

$(ab)(ab) = e$

$a(ba)b = e$

$aa(ba)b = ae$ $\quad \because a^2 = e$

$e(ba)b = a$

$(ba)bb = ab$ $\quad \because b^2 = e$

$(ba)e = ab$

$(ba) = ab$

2nd Method

For all non-identity elements $x \in G \Rightarrow x^2 = e$

$\because$ For all $a, b \in G \Rightarrow a^2 = e \Rightarrow a^{-1}a^2 = a^{-1}e \Rightarrow a = a^{-1}$

For all $b \in G \Rightarrow b^2 = e \Rightarrow b^{-1}b^2 = b^{-1}e \Rightarrow b = b^{-1}$

$\because G$ is a group So for all $a, b \in G \Rightarrow ab \in G$ Closure Property

So $(ab)^2 = e$

$(ab)^{-1}(ab)^2 = (ab)^{-1}$

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

$ab = ba$ $\quad \because b^{-1} = b \text{ & } a^{-1} = a$

2·1-21

(17) If every element of a group G, is its own inverse show that G is abelian.

Let $a, b \in G \Rightarrow a = a^{-1}$ & $b = b^{-1}$

$\because a, b \in G$ so $ab \in G$ $\because$ G is a group (closure P)

So $ab = (ab)^{-1}$

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

$ab = ba$ $\because a = a^{-1}$ & $b = b^{-1}$

Hence G is abelian

Q11 Which of the following statements are correct.

(i) A group can have more than one identity.

Incorrect.

$\because$ Identity element in a group G is unique.

(ii) The null set can be considered to be a group

Incorrect.

$\because$ A group is always a non-empty set.
secondly the null set can not contain identity element.

(iii) There may be groups where cancellation law holds

Incorrect

$\because$ cancellation law holds for all groups.

(iv) Every set of numbers which is a group under addition is also a group under multiplication & vice versa

Incorrect

$\because (R, +)$ is group but $(R, \cdot)$ is not a group.

2·1-25

(v) The set R of all real numbers is a group with respect to subtraction

Incorrect.

∵ subtraction is not associative in the set of all real nos

Let 2, 3, 4 ∈ R

$$2-(3-4) = (2-3)-4$$
$$2-(-1) = (-1)-4$$
$$3 \neq -5$$

(vii) To each element of a group there corresponds no inverse element.

Incorrect.

∵ Each element in a group G has its unique inverse.

vi) The set of all non-zero integers is a group w.r.t division

Incorrect

∵ Associative Law does not hold.

$2, 3, 4 \in Z'$

$$(2 \div 3) \div 4 = 2 \div (3 \div 4)$$
$$\frac{2}{3} \div 4 = 2 \div \frac{3}{4}$$
$$\frac{2}{3} \times \frac{1}{4} = 2 \times \frac{4}{3}$$
$$\frac{2}{12} \neq \frac{8}{3}$$

viii) To each element of a group, there corresponds only one inverse element.

Correct

Each element in a group G has its unique inverse.

ix) For each element of a group, there correspond more than one inverse element.

Incorrect.

∵ Each element in a group G has its unique inverse.

:5

6 ⓐ $G = \{I, A, B, C\}$

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \quad C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

To Prove: These matrices form a Group under matrix multiplication.

We construct Group table

·	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

We observe that the matrix multiplication is closed in this set $G = \{I, A, B, C\}$ i.e. the product of any two members of G belongs to G.

e.g.
$$A \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = C \in G$$

Hence closed.

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

$$I \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = A$$

$$I \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} - & 0 \\ 0 & 1 \end{bmatrix} = B$$

$$I \cdot C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = C$$

Hence $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is Identity element of Set G.

Inverse element of each element of G exists

$ab = I$ (Def of inverse)

From table $I \cdot I = I$; $A \cdot A = I$, $B \cdot B = I$, $C \cdot C = I$

Associative Law holds for all members of Set G.

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

$C \cdot C = A \cdot A$

$I = I$

All axioms of group are satisfied hence G is a Group

2·1-27

Table required for assignment

(18) Let $G = \{I, f, g, h\}$ where

$I(z) = z \quad f(z) = -z \quad g(z) = \frac{1}{z} \quad h(z) = -\frac{1}{z}$ where $z \in \mathbb{C}'$

To Prove G is a group under composition of functions defined by $(g \circ f)(z) = g(f(z))$

Associative

$$((g \circ f) \circ h)(z) = (g \circ (f \circ h))(z) \quad f, g, h \in G$$

$(g \circ f)(h(z)) = g((f \circ h)(z))$

$g(f(h(z))) = g(f(h(z)))$

$g\left(f\left(-\frac{1}{z}\right)\right) = g\left(f\left(-\frac{1}{z}\right)\right)$

$g\left(\frac{1}{z}\right) = g\left(\frac{1}{z}\right)$

$z = z$

$(g \circ h)(z) = g(h(z)) \quad g, h \in G$

$= g(h(z))$

$= g\left(-\frac{1}{z}\right)$

$= -z$

$= f(z) \in G$ Hence G is closed under '$\circ$'

Hence Associative

Identity $e \cdot a = a \cdot e = a$ Def of Identity

$(I \circ f)(z) = I(f(z)) = I(-z) = -z = f(z)$

$(I \circ g)(z) = I(g(z)) = I\left(\frac{1}{z}\right) = \frac{1}{z} = g(z)$

$(I \circ h)(z) = I(h(z)) = I\left(-\frac{1}{z}\right) = -\frac{1}{z} = h(z)$

$(I \circ I)(z) = I(I(z)) = I(z) = z = I(z)$

Hence $I(z)$ is Identity element of G.

Inverse $a\,b = b\,a = e$

$(g \circ g)(z) = g(g(z)) = g\left(\frac{1}{z}\right) = z = I(z)$ Identity

$(h \circ h)(z) = h(h(z)) = h\left(-\frac{1}{z}\right) = z = I(z)$ Identity

$(f \circ f)(z) = f(f(z)) = f(-z) = z = I(z) =$

$(I \circ I)(z) = I(z)$

Hence f, g, h are inverses of themselves

All axioms satisfied hence G is a group.

12-1-28

(ii) Q8 $C = 2^K$; $K = 0, \pm 1, \pm 2 \ldots\ldots$

To Prove C is a group under multiplication '.'

Let $2^K, 2^l, 2^m \in C$ $\quad K, l, m = 0, \pm 1, \pm 2 \ldots\ldots$

$$(2^K \cdot 2^l) \cdot 2^m = 2^K \cdot (2^l \cdot 2^m)$$

$$2^{K+l} \cdot 2^m = 2^K \cdot 2^{l+m}$$

$$2^{K+l+m} = 2^{K+l+m}$$

Hence Associative law holds

$2^K \cdot 2^l = 2^{K+l} \in C$

Hence multiplication is closed in C

Identity $a \cdot e = e \cdot a = a$.

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

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

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

Hence $2^0 \in C$ is Identity element of C.

Inverse $a \cdot b = b \cdot a = e$

For each $2^K \in C$ there exist $2^{-K} \in C$

$$2^K \cdot 2^{-K} = 2^{K-K} = 2^0$$ Identity

Hence C is a group under multiplication

× ——————— ×

(ii) Q13 Let $a, b \in ab$ all have order 2 in the group G.

$\therefore O(a) = 2 \Rightarrow a^2 = e \Rightarrow a^{-1}a^2 = a^{-1}e \Rightarrow a = a^{-1}$

$O(b) = 2 \Rightarrow b^2 = e \Rightarrow b^{-1}b^2 = b^{-1}e \Rightarrow b = b^{-1}$

$O(ab) = 2 \Rightarrow (ab)^2 = e \Rightarrow (ab)^{-1}(ab)^2 = (ab)^{-1}e \Rightarrow ab = (ab)^{-1}$

$\because (ab) = (ab)^{-1} \Rightarrow ab = b^{-1}a^{-1} = ba$ Proved $\quad \because a = a^{-1}, \; b = b^{-1}$

(13) (i) The identity element is unique. (TO Prove)

Let e & $\acute{e}$ be the identity elements in a group G w.r.t $0.0 \star$.

Then $e \star \acute{e} = e$ —(I) $\because \acute{e}$ is identity element

$e \star \acute{e} = \acute{e}$ —(II) $\because e$ is identity element

$\therefore e = \acute{e}$

Hence Identity element is unique

($\because$ LHS of (I) & (II) are same
SO RHS are same.)

(ii) The inverse of each element in a group G is unique

Let $a \in G$ and $\acute{a}$ & $\acute{a}' \in G$ be the two inverses of a.

$\because G$ is a group so Associative Law holds in G

$\therefore (\acute{a} \star a) \star \acute{a}' = \acute{a} \star (a \star \acute{a}')$ —(I)

LHS $(\acute{a} \star a) \star \acute{a}'$

$= e \star \acute{a}'$ $\because \acute{a}$ is inverse of a

$(\acute{a} \star a) \star \acute{a}' = \acute{a}'$ —(II) e is the identity

RHS $\acute{a} \star (a \star \acute{a}')$

$= \acute{a} \star e$ $\because \acute{a}'$ is inverse of a

$\acute{a} \star (a \star \acute{a}') = \acute{a}$ —(III) e is the identity

$\therefore \acute{a}' = \acute{a}$ using (II) & (III) in (I)

×——————×

Q 14
$(ab)^2 = a^2b^2$ for all a, b in group G.

To Prove G is abelian.

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

$(ab)(ab) = (aa)(bb)$

$a(ba)b = a(ab)b$ (Associative Law.

$\bar{a}^1 a(ba)b = \bar{a}^1 a(ab)b$ $\quad a^{-1} \in G$ ∵ G is group.

$e(ba)b = e(ab)b$ $\quad e$ is identity. $a \cdot e = a$

$(ba)bb^{-1} = (ab)bb^{-1}$ $\quad b^{-1} \in G$.

$(ba)e = (ab)e$

$ba = ab$ Hence G is abelian

Now: To Prove $(ab)^2 = a^2b^2$

$ab = ba$ (given.)

$(ab)^2 = (ab)(ab) = a(ba)b$ Associative Law

$= a(ab)b$ ∵ $ab = ba$.

$= (aa)(bb)$

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

Proved.

Q15 Let G be a group which has only one element of order 2. $\therefore a^2 = e$

Let x be any element of G. Now consider the element xax^{-1}.

$a^2 = e \Rightarrow (xax^{-1})^2 = (xax^{-1})(xax^{-1})$

$= xa(x^{-1}x)ax^{-1}$

$= xaeax^{-1}$

$= xa^2x^{-1}$

$\because a^2 = e$

$= xex^{-1}$

$= xx^{-1}$

$(xax^{-1})^2 = e$

$\therefore xax^{-1}$ is of order 2.

but according to Question there is only one element of order 2

$\therefore xax^{-1} = a$

$(xax^{-1})x = ax$

$xa(x^{-1}x) = ax$

$xa(e) = ax$

$xa = ax$ for all $a \in G$.

proved

IInd Method

we know from Example II that orders of a & $bab^{-1}a$ are equal

$\therefore$ order of a & xax^{-1} are 2, but there is only one element of order 2 in G

$\therefore xax^{-1} = a$

$xa(x^{-1}x) = ax$

$xa = ax$

proved.

(iii) Q17 To Prove $(ab)^n = a^n b^n$ G is abelian (given)

We prove it by principal of Mathematical Induction

Put $n=1$ $(ab)^1 = a^1 b^1$ C-I is satisfied

Put $n=k$ $(ab)^k = a^k b^k$ supposed to be true

Multiply by ab

$$(ab)^k (ab) = a^k b^k (ab)$$

$$(ab)^{k+1} = a^k (b^k a) b \qquad \text{Associative Law}$$

$$= a^k (a b^k) b \qquad \because G \text{ is abelian}$$

$$= a^{k+1} b^{k+1}$$

C-II is satisfied

Now when $n=0$ in $(ab)^n$

$$(ab)^0 = e = e \cdot e = a^0 \cdot b^0$$

$$(ab)^0 = a^0 b^0$$

When $n = -p$ $\quad p \in z^+$

$$(ab)^n = (ab)^{-p} = \left[(ab)^{-1}\right]^p$$

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

$$= b^n a^n$$

$$(ab)^n = a^n b^n \qquad \because G \text{ is abelian}$$

×