Chapter No. 2 (Mathematical Methods)

GROUPS

Shahzad Ahmad Khan
Lecturer (Mathematics)
Govt.College Kot Sultan
District Layyah.

Binary ~~Relation~~ operation

A binary ~~relation~~ operation on a non-empty set A is a function $*: A\times A\to A$. So, for each (a,b) in $A\times A$, we associate an element $*(a,b)$ of A. We shall denote $*(a,b)$ by $a*b$. If A is a non-empty set with a binary operation " $*$ " then A is said to be closed under " $*$ ".

Group

A pair $(G,*)$, where G is a non-empty set and " $*$ " is a binary operation on G is called a *group* if the following conditions, called axioms of a group are satisfied in G.

(I) The binary operation " $*$ " is associative. That is

$$(a*b)*c = a*(b*c);\ \forall\, a,b,c \in G.$$

(II) There is an element e in G such that

$$a*e = e*a = a\ ;\ \forall\, a \in G.$$

(III) For each $a\in G$, there is an $a'\in G$ such that

$$a*a' = a'*a = e\ ;\ a' \text{ is called the inverse of } a.$$

Examples

The pairs $(Z,+)$, $(Q,+)$, $(R,+)$, $(C,+)$ and $(Q-\{0\},\bullet)$, $(R-\{0\},\bullet)$, $(C-\{0\},\bullet)$ are groups.

Abelian Group

A group $(G,*)$ is called an abelian group if

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

If there is a pair of elements $a,b\in G$ such that $a*b \neq b*a$, then G is called non-abelian group.

Note: (i) If $(G,+)$ is a group then $a^{-1} = -a$

(ii) If $(G,\bullet)$ is a group then $a^{-1} = \frac{1}{a}$

(iii) In practice, the product $a.b$ of two elements in a group G under multiplication is written simply as ab. Also, we shall denote a group $(G,\bullet)$ by G only.

Idempotent Element

An element x of a group G is said to be idempotent if $x^2 = x$

Theorem

The only idempotent element in a group is the identity element.

Proof:

Let $x\in G$ be an idempotent element.

Then $x^2 = x$

$\Rightarrow\ x^{-1}.x^2 = x^{-1}.x$

$\Rightarrow\ x^{-1}.x.x = e$

$\Rightarrow\ e.x = e$

$\Rightarrow\ x = e$ Hence the proof.

Cayley's Table

To verify that a finite set is a group we list the products in the form of a table called *Cayley's Multiplication Table.* This is illustrated by the following examples.

Example

Let $G = \{1, \omega, \omega^2\}$, where ω is the complex cube root of unity. Show that $(G, \bullet)$ is a group.

Solution

$\bullet$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(I) " $\bullet$ " is closed over G.
$\because\ a \bullet b \in G, \forall\, a, b \in G.$
(It is clear from the table.)

(II) " $\bullet$ " is associative over G.
i.e.. $(a \bullet b) \bullet c = a \bullet (b \bullet c); \forall\, a, b, c \in G.$
($\because$ Associative law w.r.t. " $\bullet$ " holds in the set of complex numbers.)

(III) "1" is the identity element in G w.r.t. " $\bullet$ ".
(It is clear from the table.)

(IV) $(1)^{-1} = 1$; $(\omega)^{-1} = \omega^2$; $(\omega^2)^{-1} = \omega$
(It is clear from the table.)

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

Example

Let $G = \{1, -1, i, -i\}$ of all the fourth roots of unity. Show that $(G, \bullet)$ is a group.

Solution

$\bullet$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(I) " $\bullet$ " is closed over G.
$\because\ a \bullet b \in G, \forall\, a, b \in G.$
(It is clear from the table.)

(II) " $\bullet$ " is associative over G.
i.e.. $(a \bullet b) \bullet c = a \bullet (b \bullet c); \forall\, a, b, c \in G.$
($\because$ Associative law w.r.t. " $\bullet$ " holds in the set of complex numbers.)

(III) "1" is the identity element in G w.r.t. " $\bullet$ ".
(It is clear from the table.)

(IV) $(1)^{-1} = 1$, $(-1)^{-1} = -1$, $(i)^{-1} = -i$, $(-i)^{-1} = i$
(It is clear from the table.)

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

Example

Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Show that G is a group under the multiplication of symbols defined by

$$ij = k \qquad ji = -k \qquad i^2 = -1$$
$$jk = i \qquad kj = -i \qquad j^2 = -1$$
$$ki = j \qquad ik = -j \qquad k^2 = -1$$

Solution

(I) "Multiplication" is closed over G. $\because ab \in G, \forall\, a, b \in G$

(It is clear from the table.)

$\bullet$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

(II) "Multiplication" is associative over G.

$\because\ (ab)c = a(bc);\ \forall\, a, b, c \in G$.

Take $i, j, k \in G$

$(ij)k = (k)k = k^2 = -1$ $\qquad$ $i(jk) = i(i) = i^2 = -1$

Thus $\quad (ij)k = i(jk)$

Similarly by taking any three elements of G we can prove the associative property.

(III) "1" is the identity element in G w.r.t. "Multiplication"

(It is clear from the table.)

(IV) $(1)^{-1} = 1,\quad (-1)^{-1} = -1,\quad (i)^{-1} = -i,\quad (-i)^{-1} = i$

$(j)^{-1} = -j,\quad (-j)^{-1} = j,\quad (k)^{-1} = -k,\quad (-k)^{-1} = k$

(It is clear from the table.)

Thus G is group under the multiplication of symbols defined above.

Example

Let G be the set of all 2×2 non-singular real matrices. Prove that G is group under the usual multiplication of matrices.

Solution

Closed (I) Let $A, B \in G$ (i.e. A and B non-singular matrices of order 2)

Then AB is also a non singular matrix of order 2.

i.e. $AB \in G$.

Thus multiplication is closed over G.

Associative (II) Let $A, B, C \in G$

Then $(AB)C = A(BC);\quad \forall\, A, B, C \in G$.

($\because$ Associative law w.r.t. "multiplication" holds in matrices)

Identity (III) Let "I" be the identity matrix of order 2. i.e. $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Since $\det(I) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 - 0 = 1 \neq 0$

So, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is a non singular matrix of order 2. i.e. $I \in G$.

Let $A \in G$ $\quad$ Then $AI = IA = A$

Hence "I" is an identity element of G w.r.t multiplication.

(IV) Let $A \in G$

i.e. A is a non-singular matrix of order 2. $\therefore A^{-1}$ exists.

Since $(A^{-1})^{-1} = A$ i.e. $(A^{-1})^{-1}$ exists.

Hence A^{-1} is a non-singular matrix of order 2. i.e. $A^{-1} \in G$

Thus G is a group under multiplication of matrices.

Note

The set G of all non-singular real matrices is non-abelian group under multiplication of matrices. $\because AB \neq BA;\ \forall A, B \in G$

Example

Let $S = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ be the set of residue classes modulo 5. Show that S is a group under the addition modulo 5.

Solution

Let $\bar{a}, \bar{b} \in S$ then $\bar{a} + \bar{b} = \bar{r}$, where $\bar{r}$ is the remainder obtained after the division of $\bar{a} + \bar{b}$ by 5 when $\bar{a} + \bar{b}$ equals or exceed 5.

e.g $\bar{3} + \bar{1} = \bar{4}$

& $\bar{3} + \bar{4} = \bar{2}$

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

(I) Addition modulo 5 is closed over S

i.e. $\bar{a} + \bar{b} \in S;\ \forall \bar{a}, \bar{b} \in S$

(It is clear from the table.)

(II) Addition modulo 5 is associative over S.

i.e. $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})\ ; \forall\ a, b, c \in S$

Let $\bar{2}, \bar{3}, \bar{4} \in S$

$(\bar{2} + \bar{3}) + \bar{4} = \bar{0} + \bar{4}$ $\qquad$ $\bar{2} + (\bar{3} + \bar{4}) = \bar{2} + \bar{2}$

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

Similarly by taking any three elements of S we can prove the associative property.

(III) $\bar{0}$ is an identity element of S.

$\because \bar{0} + \bar{a} = \bar{a} + \bar{0} = \bar{a}\ ; \forall\ \bar{a} \in S$

(It is clear from the table.)

(IV) $(\bar{0})^{-1} = \bar{0}$, $(\bar{1})^{-1} = \bar{4}$, $(\bar{2})^{-1} = \bar{3}$, $(\bar{3})^{-1} = \bar{2}$, $(\bar{4})^{-1} = \bar{1}$

(It is clear from the table.)

Thus S is a group under the addition modulo 5.

Example

Let $G = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ be a set of non-zero residue classes modulo 5. Show that G is a group under the multiplication modulo 5.

Solution

Let $\bar{a}, \bar{b} \in G$ then $\bar{a} \bullet \bar{b} = \bar{r}$, where $\bar{r}$ is the remainder obtained after the division of $\bar{a} \bullet \bar{b}$ by 5 when $\bar{a} \bullet \bar{b}$ equals or exceed 5.

e.g $\bar{3} \bullet \bar{1} = \bar{3}$

& $\bar{3} \bullet \bar{4} = \bar{2}$

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

(I) Multiplication modulo 5 is closed over G
i.e. $\bar{a} \bullet \bar{b} \in G$; $\forall a, b \in G$
(It is clear from the table.)

(II) Multiplication modulo 5 is associative over G.
i.e. $(\bar{a} \bullet \bar{b}) \bullet \bar{c} = \bar{a} \bullet (\bar{b} \bullet \bar{c})$; $\forall a, b, c \in G$
Let $\bar{2}, \bar{3}, \bar{4} \in G$

$(\bar{2} \bullet \bar{3}) \bullet \bar{4} = \bar{1} \bullet \bar{4} = \bar{4}$ $\qquad$ $\bar{2} \bullet (\bar{3} \bullet \bar{4}) = \bar{2} \bullet \bar{2} = \bar{4}$

Similarly by taking any three elements of G we can prove the associative property.

(III) $\bar{1}$ is an identity element of G.
$\because \bar{1} \bullet \bar{a} = \bar{a} \bullet \bar{1} = \bar{a}$; $\forall \bar{a} \in G$
(It is clear from the table.)

(IV) $(\bar{1})^{-1} = \bar{1}$, $(\bar{2})^{-1} = \bar{3}$, $(\bar{3})^{-1} = \bar{2}$, $(\bar{4})^{-1} = \bar{4}$
(It is clear from the table.)

Thus G is a group under the ~~addition~~ multiplication modulo 5.

Theorem (The Cancellation Laws)

For any three elements a, b, c in G

(i) $ab = ac \Rightarrow b = c$ (*Left cancellation Law*)

(ii) $ba = ca \Rightarrow b = c$ (*Right cancellation Law*)

Proof:

For a, b, c in G

$$ab = ac$$
$$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$$
$$\Rightarrow (a^{-1}a)b = (a^{-1}a)c \quad \text{(By associative law)}$$
$$\Rightarrow eb = ec$$
$$\Rightarrow b = c$$

Thus the left cancellation law is satisfied.

Similarly we can prove the right cancellation law.

Theorem (Solutions of Linear Equations)

For any two elements a, b in a group G, the equations

$ax = b$ and $xa = b$

have unique solutions.

Proof: G be a group So inverse of each element of G exist in G

For a, b in a group G, let a^{-1} be inverse.

$$ax = b$$
$$\Rightarrow a^{-1}(ax) = a^{-1}b$$
$$\Rightarrow (a^{-1}a)x = a^{-1}b \quad \text{(By associative law)}$$
$$\Rightarrow ex = a^{-1}b$$
$$\Rightarrow x = a^{-1}b \quad \text{is the solution of } ax = b$$

To see that the solution is unique, we suppose that x_1, x_2 in G are two solutions of $ax = b$

Then $ax_1 = b$ and $ax_2 = b$

Thus $ax_1 = ax_2$

$\Rightarrow \quad x_1 = x_2$ (By left cancellation law)

Hence the solution is unique.

The case for the solution of $xa = b$ is similar.

Theorem

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

Proof:

Since $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$

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

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

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

$\Rightarrow$ $(ab)^{-1} = b^{-1}a^{-1}$ as required.

Note

Also for $a_1, a_2, a_3, \ldots, a_k$ in G

$(a_1a_2a_3 \ldots a_k)^{-1} = a_k^{-1}a_{k-1}^{-1} \ldots a_2^{-1}a_1^{-1}$

Order of a Group

The number of elements in a group G is called the *order of group* and is denoted by $|G|$ or $O(G)$.

A group G is said to be finite if G consists of only a finite number of elements. Otherwise G is said to be an infinite group.

Order of an element of a Group

Let a be an element of a group G. A least positive integer n is said to be the order of a if $a^n = e$

The order of an element $a \in G$ is denoted by $|a|$ or $O(a)$.

Theorem

Let G be a group. Let $a \in G$ have order n. Then, for any integer k, $a^k = e$ if and only if $k = qn$, where q is an integer.

Proof:

Let G be any group and $a \in G$ such that $O(a) = n$

We have to prove that $a^k = e, k \in Z \Leftrightarrow k = qn$, where q is an integer.

Suppose $a^k = e$

Since $O(a) = n$ i.e. n is the smallest positive integer such that $a^n = e$.

$\therefore k > n$ Thus by Euclids Theorem there exists unique integers q, r such that $k = qn + r, 0 \le r < n$.

Now $a^k = a^{nq+r}$

$e = a^{nq}.a^r \quad (\because a^k = e)$

$= (a^n)^q.a^r$

$= (e)^q.a^r \quad (\because a^n = e)$

$= e.a^r$

$= a^r$

Thus $a^r = e$ where $0 \le r < n$. which is contradiction unless $r = 0$

Now $k = qn + r$

$\Rightarrow k = qn$ Hence the proof.

Conversely suppose that $k = qn$

Now $a^k = a^{qn}$

$= (a^n)^q$

$= e^q$

$= e$ As required.

Example

Show that the set $S = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ is a group under multiplication modulo 8. Find the orders of each element of S.

Solution

Let $\bar{a}, \bar{b} \in S$ then $\bar{a} \bullet \bar{b} = \bar{r}$, where $\bar{r}$ is the remainder obtained after the division of $\bar{a} \bullet \bar{b}$ by 8 when $\bar{a} \bullet \bar{b}$ equals or exceed 8.

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

e.g. $\bar{3} \bullet \bar{1} = \bar{3}$

& $\bar{3} \bullet \bar{5} = \bar{7}$

Multiplication modulo 8 is closed over S.

i.e. $\bar{a} \bullet \bar{b} \in S;\ \forall a, b \in S$

(It is clear from the table.)

(I) Multiplication modulo 8 is associative over S.

i.e. $(\bar{a} \bullet \bar{b}) \bullet \bar{c} = \bar{a} \bullet (\bar{b} \bullet \bar{c})\ ;\ \forall\ a, b, c \in S$

Let $\bar{1}, \bar{3}, \bar{5} \in S$

$(\bar{1} \bullet \bar{3}) \bullet \bar{5} = \bar{3} \bullet \bar{5} = \bar{7}$ $\qquad$ $\bar{1} \bullet (\bar{3} \bullet \bar{5}) = \bar{7} \bullet \bar{7} = \bar{7}$

Similarly by taking any three elements of S we can prove the associative property.

(II) $\bar{1}$ is an identity element of S.

$\because \bar{1} \bullet \bar{a} = \bar{a} \bullet \bar{1} = \bar{a}\ ;\ \forall\ \bar{a} \in S$

(It is clear from the table.)

(III) $(\bar{1})^{-1} = \bar{1}$, $(\bar{3})^{-1} = \bar{3}$, $(\bar{5})^{-1} = \bar{5}$, $(\bar{7})^{-1} = \bar{7}$

(It is clear from the table.)

Thus S is a group under the ~~addition~~ multiplication modulo 8.

From the table it is clear that

$\bar{3} \bullet \bar{3} = \bar{1} \Rightarrow (\bar{3})^2 = \bar{1} \Rightarrow O(\bar{3}) = 2$

& $\bar{5} \bullet \bar{5} = \bar{1} \Rightarrow (\bar{5})^2 = \bar{1} \Rightarrow O(\bar{5}) = 2$

Also $\bar{7} \bullet \bar{7} = \bar{1} \Rightarrow (\bar{7})^2 = \bar{1} \Rightarrow O(\bar{7}) = 2$

But $O(\bar{1}) = 1$

Associative
$(3\times5)\times7 = 3\times(5\times7)$
$7\times7 = 3\times3$
$1 = 1$
Identity $e = 1$
$1\times7 = 7, 1\times5 = 5, 1\times3 = 3, 1\times1 = 1$
Inverse For each element $\exists$ s there exist inverse element
as $1\times1 = 1$
$3\times3 = 1$
$5\times5 = 1$
$7\times7 = 1$

Example

Let G be a group, and $a, b \in G$. Show that

(i) The orders of a and a^{-1} are equal.

(ii) The orders of ab and ba are equal.

(iii) The orders of a and bab^{-1} are equal.

Solution

(i) Let $O(a) = m$ and $O(a^{-1}) = n$

We shall prove that $m = n$

Since $O(a) = m$

$\Rightarrow \quad a^m = e$

$\Rightarrow \quad a^{-m}.\, a^m = a^{-m}e$

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

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

But $O(a^{-1}) = n \quad \therefore \; n|m \; \ldots\ldots \; (1)$

[By the theorem if $O(a) = m$, and $a^n = e$ then $m|n$]

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

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

$\Rightarrow \quad a^{-n} = e$

$\Rightarrow \quad a^{-n}.\, a^n = e.\, a^n$

$\Rightarrow \quad e = a^n$

i.e. $a^n = e$

But $O(a) = m \quad \therefore \; m|n \; \ldots\ldots \; (2)$

From (1) and (2) we get $m = n$ i.e. $O(a) = O(a^{-1})$

(ii) Let $O(ab) = m$

$\Rightarrow \quad (ab)^m = e$

$\Rightarrow \quad ab.ab.ab \ldots\ldots\ldots ab$ (m-times)$= e$

$\Rightarrow \quad b.ab.ab \ldots\ldots\ldots ab = a^{-1}.e$

$\Rightarrow \quad ba.ba.ba \ldots\ldots b = a^{-1}$

$\Rightarrow \quad ba.ba.ba \ldots\ldots\ldots ba = a^{-1}a$

$\Rightarrow \quad ba.ba.ba \ldots\ldots\ldots ba$ (m-times)$= e$

$\Rightarrow \quad (ba)^m = e$

$\Rightarrow \quad O(ba) = m$

(iii) Let $O(a) = m$ and $O(bab^{-1}) = n$

i.e. $(a)^m = e$ & $(bab^{-1})^n = e$

$(bab^{-1})^m = (bab^{-1})(bab^{-1})(bab^{-1}) \ldots\ldots\ldots (bab^{-1})$ (m-times)

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

$= baeaea \ldots\ldots\ldots ab^{-1}$

$= baaa \ldots\ldots\ldots ab^{-1}$

$= ba^m b^{-1}$

$= beb^{-1} \quad (\because a^m = e)$

$= bb^{-1}$

$= e$

But $O(bab^{-1}) = n \quad \therefore \; n|m \; \ldots\ldots\ldots \; (1)$

Since $(bab^{-1})^n = e$

$\Rightarrow$ $(bab^{-1})(bab^{-1})(bab^{-1}) \dots\dots\dots (bab^{-1})$ (n-times) $= e$

$\Rightarrow$ $ba(b^{-1}b)a(b^{-1}b)a \dots\dots\dots ab^{-1} = e$

$\Rightarrow$ $baeaea \dots\dots\dots ab^{-1} = e$

$\Rightarrow$ $baaa \dots\dots\dots ab^{-1} = e$

$\Rightarrow$ $ba^nb^{-1} = e$

$\Rightarrow$ $(ba^nb^{-1})b = eb$

$\Rightarrow$ $ba^n(b^{-1}b) = b$

$\Rightarrow$ $ba^ne = b$

$\Rightarrow$ $b^{-1}(ba^n) = b^{-1}b$

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

$\Rightarrow$ $ea^n = e$

$\Rightarrow$ $a^n = e$

But $O(a) = m$ $\therefore$ $m|n$ ……… (2)

From (1) and (2) we get $m = n$ i.e. $O(a) = O(bab^{-1})$

Example

In a group of even order, prove that there is at least one element of order 2.

Solution

Let G be a group of even order. Then non-identity elements in G are odd in number. Also the inverse of each element of G belongs to G and that $e^{-1} = e$

There occur pairs each consisting of some non-identity element x and x^{-1} in G such that $x^{-1} \neq x$. as there are odd number of non-identity elements in G, after pairing off such non-identity elements for which $x^{-1} \neq x$, we must have at least one element $a\ (\neq e) \in G$ such that

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

$$\Rightarrow aa = aa^{-1}$$

$$\Rightarrow a^2 = e$$

$$\Rightarrow O(a) = 2$$ As required.

Example

Let G be a group and x be an element of odd order in G. Then there exist an element y in G such that $y^2 = x$

Solution

For some non-negative integer m, let for $x \in G$, $O(x) = 2m + 1$

Then $x^{2m+1} = e$

Clearly $x, x^2, x^m, x^{m+1}, \dots\dots\dots x^{2m} \in G$

Let $y = x^{m+1}$

Then $y^2 = x^{2m+2}$

$= x^{2m+1}.x$

$= e.x$ $(\because x^{2m+1} = e)$

$= x$

EXERCISE 2.1

Q. No.1

Which of the following sets are groups and why?

(i) The set of all positive rational numbers under multiplication.

Solution

Let $\mathbf{Q}^+$ be the set of all positive rational numbers.

(I) Since $a \bullet b \in \mathbf{Q}^+, \forall\, a, b \in \mathbf{Q}^+$

($\because$ product of two positive rational numbers is a rational number.)

$\therefore$ " $\bullet$ " is closed over $\mathbf{Q}^+$

(II) Since $(a \bullet b) \bullet c = a \bullet (b \bullet c);\ \forall\, a, b, c \in \mathbf{Q}^+$

($\because$ Associative law w.r.t. " $\bullet$ " holds in the set of rational numbers.)

$\therefore$ " $\bullet$ " is associative over $\mathbf{Q}^+$.

(III) "1" is the identity element in $\mathbf{Q}^+$ w.r.t. " $\bullet$ ".

$\because\ 1 \bullet a = a \bullet 1 = a, \quad \forall\, a \in \mathbf{Q}^+$

(IV) If $a \in \mathbf{Q}^+$, then $\frac{1}{a} \in \mathbf{Q}^+$

Further $a.\frac{1}{a} = 1 \Rightarrow a^{-1} = \frac{1}{a} \in \mathbf{Q}^+$

Hence $(\mathbf{Q}^+, \bullet)$ is a group.

(ii) The set of all complex numbers z such that $|z| = 1$, under multiplication.

Solution

Let C' be the set of all complex numbers z such that $|z| = 1$

(I) If $z_1, z_2 \in C'$ then $|z_1| = 1$ and $|z_2| = 1$

Now $|z_1 \bullet z_2| = |z_1| \bullet |z_2| = 1.1 = 1 \quad \therefore\ z_1 \bullet z_2 \in C'$

Hence " $\bullet$ " is closed over C'

(II) Let $z_1, z_2, z_3 \in C'$

Then $(z_1 \bullet z_2) \bullet z_3 = z_1 \bullet (z_2 \bullet z_3)$

($\because$ Associative law w.r.t. " $\bullet$ " holds in the set of complex numbers.)

$\therefore$ " $\bullet$ " is associative over C'

(III) Since $1 = 1 + 0i$ and $|1| = |1 + 0i| = \sqrt{1^2 + 0^2} = 1$

Thus $1 \in C'$ further $1 \bullet z = z \bullet 1 = z, \quad \forall\, z \in C'$

Hence 1 is the identity element of C'

(IV) Let $z \in C'$ then $|z| = 1$

Since z is a complex number, $\therefore \frac{1}{z}$ is also a complex number.

And $\left|\frac{1}{z}\right| = \frac{|1|}{|z|} = \frac{1}{1} = 1 \quad \therefore\ \frac{1}{z} \in C'$

Further $z \bullet \frac{1}{z} = 1 \Rightarrow z^{-1} = \frac{1}{z} \in C'$

Hence $(C', \bullet)$ is a group.

(iii) The set Z of integers under binary operation "$\circ$" defined by $a \circ b = a - b \ \forall\, a, b \in Z$

Solution

$(Z, \circ)$ is not a group.

$\because$ "$\circ$" is not associative over Z

For example, $2,3,4 \in Z$

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

$2 \circ (3 \circ 4) = 2-(3-4)$
$= 2+1$
$= 3$

Thus $(2 \circ 3) \circ 4 \neq 2 \circ (3 \circ 4)$

(iv) The set Q' of all irrational numbers under multiplication.

Solution

$(Q', \bullet)$ is not a group.

$\because$ "$\bullet$" is not closed over Q'

For example $\sqrt{2} \in Q'$ But $\sqrt{2} \bullet \sqrt{2} = 2 \notin Q'$

Q. No.2

Let G be a group such that $(ab)^n = a^n b^n$ for three consecutive natural numbers n and all a, b in G. Show that G is abelian.

Solution Let $a, b \in G$

Let $n, n+1, n+2$ be three consecutive integers

Such that $(ab)^n = a^n b^n$ .... (1)

$(ab)^{n+1} = a^{n+1} b^{n+1}$ .... (2)

$(ab)^{n+2} = a^{n+2} b^{n+2}$ .... (3)

We are to show that G is abelian. i.e. $ab = ba$

From (2) $(ab)^n(ab) = a^n a\, b^n b$

$\Rightarrow a^n b^n ab = a^n a\, b^n b$ [By (1)]

$\Rightarrow b^n a = a\, b^n$ .... (4) [By left and right cancellation laws]

From (3) $(ab)^n (ab)^2 = a^n a^2 b^n b^2$

$\Rightarrow a^n b^n abab = a^n a^2 b^n b^2$ [By (1)]

$\Rightarrow b^n abab = a^2 b^n b^2$ [By left cancellation law]

$\Rightarrow ab^n bab = aab^n bb$ [By (4)]

$\Rightarrow b^n ba = b^n ab$ [By left and right cancellation laws]

$\Rightarrow ba = ab$

Hence G is an abelian group.

Q. No. 3

Show that the set $\{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ under multiplication modulo 9 is a group.

Solution Let $S = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$

Let $\bar{a}, \bar{b} \in S$ then $\bar{a} \bullet \bar{b} = \bar{r}$, where $\bar{r}$ is the remainder obtained after the division of $\bar{a} \bullet \bar{b}$ by 9 when $\bar{a} \bullet \bar{b}$ equals or exceed 9.

e.g. $\bar{2} \bullet \bar{4} = \bar{8}$ & $\bar{5} \bullet \bar{7} = \bar{8}$

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

(I) Multiplication modulo 9 is closed over S. i.e. $\bar{a} \bullet \bar{b} \in S$; $\forall\, a, b \in S$
(It is clear from the table.)

(II) Multiplication modulo 9 is associative over S.

$\because (\bar{a} \bullet \bar{b}) \bullet \bar{c} = \bar{a} \bullet (\bar{b} \bullet \bar{c})\ ;\ \forall\ a,b,c \in S$

Let $\bar{4}, \bar{5}, \bar{7} \in S$

$(\bar{4} \bullet \bar{5}) \bullet \bar{7} = \bar{2} \bullet \bar{7} = \bar{5}$ $\qquad$ $\bar{4} \bullet (\bar{5} \bullet \bar{7}) = \bar{4} \bullet \bar{8} = \bar{5}$

Similarly by taking any three elements of S we can prove the associative property.

(III) $\bar{1}$ is an identity element of S.

$\because \bar{1} \bullet \bar{a} = \bar{a} \bullet \bar{1} = \bar{a}\ ;\ \forall\ \bar{a} \in S$

(It is clear from the table.)

(IV) $(\bar{1})^{-1} = \bar{1},\ (\bar{2})^{-1} = \bar{5},\ (\bar{4})^{-1} = \bar{7},\ (\bar{5})^{-1} = \bar{2},\ (\bar{7})^{-1} = \bar{4},\ (\bar{8})^{-1} = \bar{8}$

(It is clear from the table.)

Thus S is a group under the ~~addition~~ multiplication modulo 9.

Q. No. 4

Is $(Z,\circ)$ a group? Where $\circ$ is defined by $a \circ b = 0,\ \forall\ a,b \in G$

Solution

$(Z,\circ)$ is not a group, because $(Z,\circ)$ has no identity element.

If possible then suppose that e is the identity of $(Z,\circ)$.

$\therefore\quad a \circ e = a\ \ \forall\ a \in Z$

But $a \circ e = 0$

Thus $\quad a = 0,\ \forall\ a \in Z.\quad$ This is wrong.

Hence $(Z,\circ)$ is not a group.

Q. No. 5

Show that if a group G is such that $x.x = e$, for all $x \in G$, where e is the identity element of G, then G is an abelian group.

Solution

Since $\ x.x = e,\quad \forall\ x \in G$

$\Rightarrow\quad (x.x).x^{-1} = e.x^{-1}$

$\Rightarrow\quad x.(x.x^{-1}) = x^{-1}$

$\Rightarrow\quad x.e = x^{-1}$

$\Rightarrow\quad x = x^{-1}\quad \forall\ x \in G\ \ldots\ldots\ (1)$

Let $\ a,b \in G\qquad \therefore\ ab \in G$

Using (1) on $a, b, ab\ \in G\ $ we get

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

$b = b^{-1}$ .... (2)

$ab = (ab)^{-1}$ .... (3)

We Know that $\ (ab)^{-1} = b^{-1}a^{-1}$

$\Rightarrow\qquad ab = ba\qquad$ [By (1), (2), (3)]

Hence G is an abelian group.

Q. No. 6

If a group G has three elements, show that it is abelian.

Solution

Let $G = \{e, a, b\}$ be a group with identity element "e".

Since $a, b \in G \quad \therefore \quad ab \in G$

Then $ab = a$ or $ab = b$ or $ab = e$

Now $ab \neq a \quad \because \quad b \neq e$ and $ab \neq b \quad \because a \neq e$

$\therefore \quad ab = e \quad \Rightarrow \quad a = b^{-1}$ or $b = a^{-1}$

Now $ab = aa^{-1} = e = a^{-1}a = ba$

$\Rightarrow \quad ab = ba \quad \therefore$ G is an abelian group.

Q. No. 7

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

Solution

It is given that $x^{-1} = x \quad \forall\, x \in G$ .... (1)

Let $a, b \in G \quad \therefore \quad ab \in G$

Using (1) on $a, b, ab \in G$

We get $a^{-1} = a$ .... (2)

$b^{-1} = b$ .... (3)

$(ab)^{-1} = ab$ .... (4)

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

$\Rightarrow \quad ab = ba$

Hence G is an abelian group.

Q. No. 8

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

Solution

For all non identity elements $x \in G \quad \Rightarrow \quad x^2 = e$ .... (1)

Let $a(\neq e), b(\neq e) \in G \;\Rightarrow\; ab, ba \in G$ [By closure property in G]

Thus $a^2 = e,\ b^2 = e,\ (ab)^2 = e$, etc. [By (1)]

Since $(ab)^2 = e$

$\Rightarrow \quad ab.ab = e$

$\Rightarrow \quad a(ba)b = e$ (By associative law)

$\Rightarrow \quad aa(ba)b = ae$ (By pre-multiplication with a)

$\Rightarrow \quad a^2(ba)b = a$

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

$\Rightarrow \quad (ba)bb = ab$ (By post-multiplication with b)

$\Rightarrow \quad (ba)\,b^2 = ab$

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

$\Rightarrow \quad ba = ab$

Thus G is an abelian group.

Q. No. 9

Answer *true* or *false*. Justify your answer.

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

Answer

False The identity element in a group is unique.

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

Answer

False The identity element must belong to the set but there is no element belonging to null set.

(iii) There may e groups in which cancellation law fails.

Answer

False On contrary if there exist a group in which cancellation law fails then existence of inverses and identity play no role. Hence there does not exist a group in which cancellation law fails.

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

Answer

False The inverse of additive identity element "0" in the groups of real numbers or complex numbers under addition does not exist under multiplication.

$R-\{0\}$ and $C-\{0\}$ are groups under multiplication but they are not groups under addition since additive identity element "0" does not exist in each case.

(v) The set R of all real numbers is a group w.r.t subtraction.

Answer

False The associative law with respect to subtraction does not hold in R.

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

Answer

False ~~The inverses of all non-zero integers except 1,1 does not exist.~~ Associative law w.r.t division does not hold in Z

(vii) To each element of a group, there does not correspond an inverse element.

Answer

False The inverse of each element must exist and is to be unique.

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

True The inverse of each element of a group is unique.

(ix) To each element of a group, there corresponds more then one inverse element.

Answer

False The inverse of each element of a group is unique.

Shahzad Ahmad Khan
Lecturer (Mathematics)
Govt.College Kot Sultan
District Layyah.

Q. No. 10

Show that the matrices $I = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$, $A = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$, $B = \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}$, $C = \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}$ **form a group under matrix multiplication.**

Solution

Let $G = \{I, A, B, C\}$

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

Here $IA = AI = A,\ IB = BI = B,\ IC = CI = C$

Thus I is the identity element of G.

•	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

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

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

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

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

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

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

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

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

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

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

Identity: $I\cdot I = I$
$I\cdot A = A$
$I\cdot B = B$
$I\cdot C = C$

(I) $\because\ \forall X, Y \in G \Rightarrow XY \in G$
$\therefore$ "." is closed over G.
(It is clear from the table.)

(II) $\because (XY)Z = X(YZ);\ \forall X, Y, Z \in G$
[$\because$ Associative Law w.r.t multiplication holds in matrices]
$\therefore$ "." is associative over G

(III) I is the identity element of G $\because\ IX = XI = X,\ \forall X \in G$.
(It is clear from the table.)

(IV) Here $(I)^{-1} = I,\quad (A)^{-1} = A,\quad (B)^{-1} = B,\quad (C)^{-1} = C$
(It is clear from the table.)

$I\cdot I = I,\ A\cdot A = I,\ B\cdot B = I,\ C\cdot C = I$

Thus G is a group under multiplication of matrices.

Q. No. 11

Prove that the set of complex valued functions I, f, g and h defined on the set $C-\{0\}$ of non-zero complex numbers by $I(z)=z,\ f(z)=-z,\ g(z)=\frac{1}{z},\ h(z)=-\frac{1}{z},\ z\in C-\{0\}$ form a group under composition of functions defined by

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

Solution

Let $G=\{I,f,g,h\}$

Then, $(f\circ f)(z)=f\big(f(z)\big)=f(-z)=z=I(z)$

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

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

$(g\circ f)(z)=g\big(f(z)\big)=g(-z)=-\frac{1}{z}=h(z)$

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

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

$(h\circ f)(z)=h\big(f(z)\big)=h(-z)=\frac{1}{z}=g(z)$

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

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

∘	I	f	g	h
I	I	f	g	h
f	f	I	h	g
g	g	h	I	f
h	h	g	f	I

(I) "$\circ$" is closed over G.
(It is clear from the table.)

(II) "$\circ$" is associative over G.
For example if we take $f,g,h\in G$

$(f\circ g)\circ h(z)=(f\circ g)(h(z))$
$=(f\circ g)(-\frac{1}{z})$
$=f(g(-\frac{1}{z}))$
$=f(z)$
$=+z$

$f\circ(g\circ h)(z)=f((g\circ h)(z))$
$=f(g(h(z))$
$=f(g(-\frac{1}{z}))$
$=f(z)$
$=+z$

Clearly $(f\circ g)\circ h=f\circ(g\circ h)$
Similarly by taking any three elements of G we can prove the associative property.

(III) "I" is the identity element of G
$\because\ I\circ\alpha=\alpha\circ I=\alpha;\quad\forall\,\alpha\in G$
(It is clear from the table.)

(IV) Here $(I)^{-1}=I,\quad (f)^{-1}=f,\quad (g)^{-1}=g,\quad (h)^{-1}=h$
(It is clear from the table.)

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

Q. No. 12

Show that the set $G = \{2^k : k = 0, \pm1, \pm2, \ldots\ldots\}$ is a group under multiplication.

Solution

(I) Let $2^m, 2^n \in G$, where $m, n \in Z = \{0, \pm1, \pm2, \ldots\ldots\}$
Then $2^m \bullet 2^n = 2^{m+n} \in G \quad \because m+n \in Z$
Thus " $\bullet$ " is closed over G

(II) Let $2^l, 2^m, 2^n \in G$, where $l.m, n \in Z$
Then $2^l \bullet (2^m \bullet 2^n) = 2^l \bullet 2^{m+n} = 2^{l+m+n}$ $\qquad (2^l \bullet 2^m) \bullet 2^n = 2^{l+m} \bullet 2^n = 2^{l+m+n}$

Clearly $2^l \bullet (2^m \bullet 2^n) = (2^l \bullet 2^m) \bullet 2^n$
Thus " $\bullet$ " is associative over G

(III) $2^0 = 1$ is the identity element in G
$\because 2^0 \bullet 2^k = 2^k \bullet 2^0 = 2^k \quad \forall\, 2^k \in G.$

(IV) Let $2^k \in G$ Then $2^{-k} \in G$
Further $2^k \bullet 2^{-k} = 2^0$ and $2^{-k} \bullet 2^k = 2^0$
i.e. $2^k \bullet 2^{-k} = 2^{-k} \bullet 2^k = 2^0$
Thus $(2^k)^{-1} = 2^{-k}$
Hence $(G, \bullet)$ is a group.

Q. No. 13

In a group G, let a, b and ab all have order 2, then $ab = ba$

Solution

Since $O(a) = 2$	Since $O(b) = 2$	Since $O(ab) = 2$
$\therefore\ a^2 = e$	$\therefore\ b^2 = e$	$\therefore\ (ab)^2 = e$
$\Rightarrow\ a.a = e$	$\Rightarrow\ b.b = e$	$\Rightarrow ab.ab = e$
$\Rightarrow (a)^{-1} = a \ldots.$ (1)	$\Rightarrow\ (b)^{-1} = b \ldots.$ (2)	$\Rightarrow (ab)^{-1} = ab \ldots.$ (3)

We know that $(ab)^{-1} = b^{-1}a^{-1}$
$\Rightarrow \quad ab = ba \qquad$ [By (1), (2) and (3)]

Q. No. 14

Show that in a group G

(i) The identity element is unique.

(ii) The inverse of each element is unique.

Solution

(i) Suppose e_1, e_2 are two identities in G (Group)
Since e_1 is identity element in G and $e_2 \in G$
$$\therefore\ e_1.e_2 = e_2.e_1 = e_2 \ldots\ldots\ldots (1)$$
Since e_2 is identity element in G and $e_1 \in G$
$$\therefore\ e_2.e_1 = e_1.e_2 = e_1 \ldots\ldots\ldots (2)$$
From (1) and (2), we get $e_1 = e_2$
Hence identity element in a group G is unique.

(ii) Suppose $a^{-1} = b$ and $a^{-1} = c \ \forall a \in G$ (Group)

Since $a^{-1} = b \quad \because \ ab = ba = e$ .... (1)

Also $a^{-1} = c \quad \therefore \ ac = ca = e$ .... (2)

Since $a, b, c \in G$

$\therefore \ (ba)c = b(ac)$ [Associative Law holds in groups]

$\Rightarrow \quad ec = be$

$\Rightarrow \quad c = b$

Hence inverse of each element in a group G is unique.

Q. No. 15

Let G be a group, show that G is abelian if and only if

$$(ab)^2 = a^2b^2 \quad \forall a, b \in G$$

Solution

Suppose G is an abelian group.

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

$\Rightarrow \quad aab = aba$ [By pre-multiplication with a]

$\Rightarrow \quad aabb = abab$ [By post-multiplication with b]

$\Rightarrow \quad a^2b^2 = (ab)^2$

Or $\quad (ab)^2 = a^2b^2 \quad \forall \ a, b \in G$

Conversely let $(ab)^2 = a^2b^2 \quad \forall \ a, b \in G$

$\Rightarrow \quad abab = aabb$

$\Rightarrow \quad ba = ab$

Hence G is an abelian group.

Q. No. 16

If G is an abelian group, show that $(ab)^n = a^nb^n \quad \forall a, b \in G$

Solution

We have to prove that $(ab)^n = a^nb^n \ \forall a, b \in G$ and $n \in Z$ ...... (1)

We shall prove (1) by principle of mathematical induction.

Case-I When n is positive integer.

Put $n = 1$ in (1)

L.H.S $= (ab)^n = (ab)^1 = a^1b^1 = a^nb^n =$ R.H.S

Suppose (1) is true for $n = k$

i.e. $\quad (ab)^k = a^kb^k \ \forall a, b \in G$ and $k \in Z$ ...... (2)

We shall prove that (1) is true for $n = k + 1$

i.e. $\quad (ab)^{k+1} = a^{k+1}b^{k+1} \ \forall a, b \in G$ and $k \in Z$

L.H.S $= (ab)^{k+1}$

$= (ab)^k(ab)$

$= (a^kb^k)(ab)$ [By (2)]

$= a^k\left(b^k(ab)\right)$ [By associative Law]

$= a^k\left((b^k a)b\right)$ [By associative Law]

$= a^k\left((ab^k)b\right)$ [$\because$ G is an abelian group]

$= a^k\left(a(b^k b)\right)$ [By associative Law]

$= a^k(ab^{k+1})$

$= (a^k a)\, b^{k+1}$ [By associative Law]

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

$=$ R.H.S

<u>*Case-II*</u> <u>When $n = 0$</u>

Put $n = 0$ in (1)

L.H.S $= (ab)^n = (ab)^0 = e = e.e = a^0b^0 = a^nb^n =$ R.H.S

<u>*Case-III*</u> <u>When $n = -m$ where m is a positive integer.</u>

L.H.S $= (ab)^n$

$= (ab)^{-m}$

$= [(ab)^{-1}]^m$

$= (b^{-1}a^{-1})^m$ [$\because (ab)^{-1} = b^{-1}a^{-1}$]

$= (a^{-1}b^{-1})^m$ [$\because$ G is an abelian group]

$= (a^{-1})^m(b^{-1})^m$ [By case-I $\because$ m is positive integer]

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

$= a^nb^n$

$=$ R.H.S

Q. No. 17

Let G be a group. Suppose that G has only one element of order 2. Show that $ax = xa$ for all $x \in G$

Solution

Let G be a group. Suppose $a \in G$ such that $O(a) = 2 \Rightarrow a^2 = e$

Now $(xax^{-1})^2 = xax^{-1}.xax^{-1}$

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

$= xaeax^{-1}$

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

$= xex^{-1}$ [$\because a^2 = e$]

$= xx^{-1}$

$= e$

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

But a is the only element of G of order 2

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

$\Rightarrow$ $(xax^{-1})x = ax$ [By post-multiplication with x]

$\Rightarrow$ $xa(x^{-1}x) = ax$ [By associative Law]

$\Rightarrow$ $xae = ax$

$\Rightarrow$ $xa = ax$ Hence the proof.