Closure: Let $x, y \in S$, then $x = (a,b)$; $y = (c,d)$

where $a, b, c, d \in R$

Now $x \oplus y = (a,b) \oplus (c,d) = (a+c, b+d)$

Since a, b, c, d are real numbers, $a+c$, $b+d$ are real numbers.

Hence $(a+c, b+d) \in S \Rightarrow x \oplus y \in S$

So, S is closed under $\oplus$

Associativity: Let x, y, z be any three elements in S.

Then $x = (a,b)$, $y = (c,d)$ $z = (p,q)$.

where a, b, c, d, p, q are some real numbers.

Now $x \oplus (y \oplus z) = (a,b) \oplus ((c,d) \oplus (p,q))$

$= (a,b) \oplus (c+p, d+q)$

$= (a + (c+p), b + (d+q))$

$= ((a+c)+p, (b+d)+q) \rightarrow (1)$

[$\because$ usual addition is associative)

and $(x \oplus y) \oplus z = ((a,b) \oplus (c,d)) \oplus (p,q)$

$= (a+c, b+d) \oplus (p,q)$

$= ((a+c)+p, (b+d)+q) \rightarrow (2)$

From (1) and (2)

$x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad \forall x, y, z \in S$.

So associative axiom is satisfied.

Identity:- Let $x = (a,b)$ be any element in S.

Suppose $e = (c,d)$ be the identity element in S,

then $x \oplus e = x$

$\Rightarrow (a,b) \oplus (c,d) = (a,b)$

$\Rightarrow (a+c, b+d) = (a,b)$

$\Rightarrow a+c = a$, $b+d = b$

$\Rightarrow c = 0$, $d = 0$. $\therefore e = (0,0)$ is identity element of S.

Inverse: Let $x = (a,b)$ be any element of S.

Suppose $x' = (c,d)$ be the inverse,

then $x \oplus x' = e$

$\Rightarrow (a,b) \oplus (c,d) = (0,0)$

$\Rightarrow (a+c, b+d) = (0,0)$

$\Rightarrow a+c = 0, \; b+d = 0$

$\Rightarrow c = -a, \; d = -b$

$\therefore x' = (-a,-b)$ is the inverse of x.

So, inverse axiom is satisfied.

Commutativity: Let $x = (a,b)$ and $y = (c,d)$ be any two elements on S.

Now $x \oplus y = (a,b) \oplus (c,d)$

$= (a+c, b+d)$

$= (c+a, d+b)$ [Integer addition is commutative]

$= (c,d) \oplus (a,b)$ [by definition of $\oplus$]

$= y \oplus x$

$\therefore x \oplus y = y \oplus x \quad \forall x, y \in S$

Hence $(S, \oplus)$ is a commutative group.

(ie), $(S, \oplus)$ is an abelian group.

PERMUTATION

Let S be a non-empty set. A bijective function $f: S \to S$ is called a permutation. If S has n elements, then the permutation is said to be of degree n.

Usually we take $S = \{1, 2, 3, \ldots, n\}$

The set of all permutations on a set of n symbols is denoted by S_n.

(17) If $S = \{1, 2, 3\}$, then prove that $(S_3, \cdot)$ is a non-abelian group, where $\cdot$ is composition of function.

Soln: Given $S = \{1, 2, 3\}$. The total number permutation on S is $3! = 6$. The permutations are

$$P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \quad P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \quad P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

Then $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ and the binary operations on S_3 is the composition of functions.

The operation is performed on the left as below.

For example $(1)(P_2 \cdot P_3) = ((1) \cdot P_2) P_3$
$= (1) P_3 = 2$.

i.e $1 \xrightarrow{P_2} 1 \xrightarrow{P_3} 2$

$(1) P_2 \cdot P_3 = 2$

Similarly for other elements.

since $(1) P_1 = 1$, $(2) P_1 = 2$, $(3) P_1 = 3$,

P_1 is the identity element on S.

$P_1 \cdot P_1 = P_1$; $P_1 \cdot P_2 = P_2 \cdot P_1 = P_2$;

$P_1 \cdot P_3 = P_3 \cdot P_1 = P_3$; $P_1 \cdot P_4 = P_4 \cdot P_1 = P_4$;

$P_1 \cdot P_5 = P_5 \cdot P_1 = P_5$; $P_1 \cdot P_6 = P_6 \cdot P_1 = P_6$.

$$P_2 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$

$1 \xrightarrow{P_2} 1 \xrightarrow{P_2} 1$

$2 \xrightarrow{P_2} 3 \xrightarrow{P_2} 2$

$3 \xrightarrow{P_2} 2 \xrightarrow{P_2} 3$

$P_2 \cdot P_2$

$$P_2 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$

$$P_2 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$

$$\begin{array}{cccc} & 1 & 2 & 3 \\ P_2 & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 \\ P_3 & \downarrow & \downarrow & \downarrow \\ & 2 & 1 & 3 \end{array}$$

$P_2 \cdot P_3$.

$$\therefore \quad P_2 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$

$$P_2 \cdot P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = P_3.$$

$$P_2 \cdot P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = P_6$$

$$P_2 \cdot P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5.$$

$$P_3 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = P_6$$

$$P_3 \cdot P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5$$

$$P_3 \cdot P_4 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = P_2.$$

$$P_3 \cdot P_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = P_1.$$

$$P_3 \cdot P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = P_4.$$

$$P_4 \cdot P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = P_5.$$

$$P_4 \cdot P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_6$$

$$P_4 \cdot P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1.$$

$$P_4 \cdot P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2.$$

$$P_4 \cdot P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_3.$$

$$P_5 \cdot P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_4.$$

$$P_5 \cdot P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1.$$

$$P_5 \cdot P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_6$$

$$P_5 \cdot P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_3.$$

$$P_5 \cdot P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$$

$$P_6 \cdot P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_3$$

$$P_6 \cdot P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$$

$$P_6 \cdot P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_5.$$

$$P_6 \cdot P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_4.$$

$$P_6 \cdot P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1.$$

The cayley table is,

$\cdot$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_1	P_4	P_3	P_6	P_5
P_3	P_3	P_6	P_5	P_2	P_1	P_4
P_4	P_4	P_5	P_6	P_1	P_2	P_3
P_5	P_5	P_4	P_1	P_6	P_3	P_2
P_6	P_6	P_3	P_2	P_5	P_4	P_1.

Closure: Since the body of the table contains only the elements of S_3, S_3 is closed with respect to $\cdot$.

Associativity: We know composition of functions is associative and so it is true in S_3 also. So associative axiom is verified.

Identity: $P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ is the identity element of S_3.

Inverse: To find the inverse of an element P_i, find P_1 in the row through P_i, the column head of P_1 is the inverse of P_i ie P_i^{-1}.

$\therefore$ from the table we see that

$P_1^{-1} = P_1$, $P_2^{-1} = P_2$, $P_3^{-1} = P_5$, $P_4^{-1} = P_4$

$P_5^{-1} = P_3$, $P_6^{-1} = P_6$.

Thus inverse exists for every element. Hence inverse axiom is verified. So $(S_3, \cdot)$ is a group.

From the table we find that,

$P_3 \cdot P_4 = P_2$ and $P_4 \cdot P_3 = P_6$.

$\therefore P_3 \cdot P_4 \neq P_4 \cdot P_3$.

Hence the group is not commutative.

GROUP OF RESIDUE CLASSES Mod n

congruence mod n

Let n be a fixed positive integer. Let a and b be integers, we define $a \equiv b \pmod{n}$, if $a-b$ is divisible by n.

For example, $2 \equiv -1 \pmod{3}$, since $2-(-1) = 3$ is divisible by 3.

$25 \equiv 5 \pmod{2}$, since $25-5 = 20$ is divisible by 2.

$-1 \equiv 3 \pmod{2}$, since $-1-3 = -4$ is divisible by 2.

The equivalence class of a is $[a] = \{x \mid x \equiv a \pmod{n}\}$

For eg, the congruence classes mod 4 are

$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$

$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$

$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\}$

$[3] = \{\dots, -5, -1, 3, 7, 11, \dots\}$

$[4] = \{\dots, -8, -4, 0, 4, 8, \dots\} = [0]$

similarly $[5] = [1]$, $[6] = 2$ etc..

$\therefore$ The distinct congruence classes mod 4 are $[0], [1], [2], [3]$.

The set of congruence classes mod 4 is denoted by,

$Z_4 = \{[0], [1], [2], [3]\}$ and is called the set of residue classes mod 4 or residual classes mod 4.

more generally, the set of residue classes mod n is $Z_n = \{[0], [1], [2], \ldots [n-1]\}$.

(9) Let $Z_5^* = \{[1], [2], [3], [4]\}$ be the non-zero elements of Z_5 prove that $(Z_5^*, \cdot_5)$ is an abelian group.

Soln: $Z_5^* : \{[1], [2], [3], [4]\}$

we form the cayley table to verify axioms of a group.

$[2] \cdot_5 [2] = [4]$.

$[2] \cdot_5 [3] = [6] = [1]$ $[\because 6 \equiv 1 \pmod 5]$

ie the remainder when 6 is $\frac{a}{b}$ by 5 is 1,

$[2] \cdot_5 [4] = [8] = [3]$ $[\because 8 \equiv 3 \pmod 5]$

$[3] \cdot_5 [2] = [6] = [1]$ $[\because 6 \equiv 1 \pmod 5]$

$[3] \cdot_5 [3] = [9] = [4]$ $[\because 9 \equiv 4 \pmod 5]$

$[3] \cdot_5 [4] = [12] = [2]$ $[\because 12 \equiv 2 \pmod 5]$

$[4] \cdot_5 [1] = [4]$.

$[4] \cdot_5 [2] = [8] = [3]$ $[\because 8 \equiv 3 \pmod 5]$

$[4] \cdot_5 [3] = [12] = [2]$ $[\because 12 \equiv 2 \pmod 5]$

$[4] \cdot_5 [4] = [16] = [1]$ $[\because 6 \equiv 1 \pmod 5]$

The cayley table is

$\cdot_5$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Closure: The body of table contains only elements of Z_5^*

$\therefore$ Z_5^* is closed w.r.to $\cdot_5$

Associativity: Since usual multiplication is associative, it is true in Z^*_5 also.

Identity: [1] is the identity element, since $[1] \cdot_5 [a] = [a]$ $\forall a \in Z^*_5$

ie $[1]\cdot_5[1] = [1]$; $[1]\cdot_5[2] = 2$,

$[1]\cdot_5[3] = [3]$; $[1]\cdot_5[4] = 4$

Inverse: From the table we note that

inverse of [1] is [1]; inverse of [2] is [3]

inverse of [3] is [2] ; inverse of [4] is [4].

Further, the elements equidistant from the main diagonal are same and so $\cdot_5$ is commutative in Z_5^*. So $(Z_5^*, \cdot_5)$ is an abelian group.

(10) Show that if every element in a group G is its own inverse, then the group G must be abelian.

(or)

In a group G, if $a^2 = e$ $\forall$ $a \in G$, then G is abelian.

Soln: Let $a, b \in G$ be any two elements, then $a * b \in G$. Given every element is its own inverse.

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

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

$\Rightarrow b*a = a*b \quad \forall a, b \in G$

$\therefore$ G is abelian.

<u>note</u>: 1. consider the second part.

Given $a^2 = e \quad \forall a \in G$

$\therefore a^{-1} * a^2 = a^{-1} * e$

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

$\Rightarrow a = a^{-1} \quad \forall a \in G \qquad [\because a^{-1} * a = e]$

ie, every element is its own inverse. How G is abelian by first part.

2. Is the converse true?

<u>ie</u>. If G is abelian, that every element is its own inverse

Ans: No. For example, $(z, +)$ is an abelian group. But inverse of 2 is -2 and not 2.

3. Let $(G, *)$ be a group. An element $a \in G$ is called an independent element if $a^2 = a$

Then $a^{-1} = a^2 = a^{-1} * a \Rightarrow a = e$. So, the only independent element in a group is the identity element.