MA253 Unit : 5 Abstract Algebra

Date
Page

28/07/21

* Set :- A set is a collection of well-defined elements.

* Function :- Let $A, B \neq \phi$, If each elements of set A is uniquely associates with the elements of set B, then that relation is known as a function.

* Cartesian Product :-

→ Let $A, B \neq \phi$, then the cartesian product of A and B is denoted by $A \times B$ and defined as $A \times B = \{ (a,b) : a \in A, b \in B \}$.

e.g. 1) Let $A = \{1, 2\}$, $B = \{a, b\}$

→ Then $A \times B = \{ (1,a), (1,b), (2,a), (2,b) \}$

2) Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$

→ Then number of elements in $A \times B = n(A) \cdot n(B)$

$= 3 \cdot 3 = 9$.

Note :- Number of subsets, if $A \times B = 2^{n(A) \cdot n(B)}$

$= 2^{2 \cdot 2} = 2^4$

* Binary Operation / Binary Composition :-

→ A binary composition or binary operation on a non empty set A is a mapping $f : A \times A \to A$.

Suppose $a, b \in A$ then the image of (a,b) under a binary composition / operation $*$ defined by $a * b$ has to be in A.

$f : A \times B \to A$

$f(a,b) = a * b$

Ex:-01 Let us consider N. $+ : N \times N \to N$ defined $+(a,b) = a+b$. Check whether '+' is binary operation on N or not.

→ $1, 2 \in N$, $+(1,2) = 1+2 = 3 \in N$.
∴ '+' is a binary operation on N.

Ex:-02 N. $- : N \times N \to N$, $-(a,b) = a-b$.

→ e.g. $1, 2 \in N$, $-(1,2) = 1-2 = -1 \notin N$.
∴ '−' is not a binary operation on N.

Ex:-03 N. $\cdot : N \times N \to N$, $\cdot(a,b) = a \cdot b$.

→ e.g. $1, 2 \in N$, $\cdot(1,2) = 1 \cdot 2 = 2 \in N$.
∴ '·' is a binary operation on N.

Ex:-04 N. $\div : N \times N \to N$, $\div(a,b) = a \div b$.

→ e.g. $1, 2 \in N$, $\div(1,2) = 1/2 \notin N$.
∴ '÷' is not a binary operation on N.

Ex:-05 Binary or Not:

	$+ : Z \times Z \to Z$	$- : Z \times Z \to Z$
	Yes	Yes
	$\cdot : Z \times Z \to Z$	$\div : Z \times Z \to Z$
	Yes	No

Ex:-06
Q → +, −, ÷, ·
R → +, −, ÷, ·
All the basic arithmatic operations are binary.

* Alegbraic structure :-

→ A non empty set G with one or more binary operations is called an algebraic structure. Suppose * is a binary operation on G. Then (G, *) is an algebraic structures.

→ e.g: (N, +), (Z, +), (Q, +), (R, +),
(N, -), (Z, -), (Q, -), (R, -),
(N, ·), (Z, ·), (Q, ·), (R, ·),
(N, /), (Z, /), (Q, /), (R, /).

03/08/21

* GROUP :-

* Identity element :-

→ There exist an element $e \in G$ such that

$$a * e = a = e * a \quad , \forall\, a \in G$$

The element e is called the identity element.

* Inverse element :-

→ There exist an element $a^{-1} \in G$ such that

$$a * a^{-1} = e = a^{-1} * a \; ; \forall\, a \in G$$

Here, a^{-1} is called the inverse element.

* GROUP :-

Let G be a non-empty set with a binary operation denoted by *. Then this algebraic structure (G, *) is a group, if the binary * satisfies the following properties :

1) Closure property : $a * b \in G$, $\forall a, b \in G$

2) Associativity : $(a * b) * c = a * (b * c)$
$\forall a, b, c \in G$

* 3) Existence of Identity :
There exist an identity element $e \in G$ such that $a * e = a = e * a$, $\forall a \in G$

* 4) Existence of Inverse :
Each element of G possess inverse.
i.e., $a * a^{-1} = e = a^{-1} * a$; $\forall a \in G$

* ABELIAN GROUP :-
A group is said to be abelian or commutative if in addition to the above four properties the following property is also satisfied.
i.e.

5) $a * b = b * a$; $\forall a, b \in G$
[Commutative property or Abelian property]

* Finite group and infinite group :-

→ If in a group G the underlying set G consists of a finite number of distinct elements then the group is called a finite group otherwise an infinite group.

* Composition table :-

→ Modulo n set (Z_n) :- $n \to$ positive integer. [$n \in N$.]

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

$Z_3 = \{0, 1, 2\}$

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

→ Addition modulo n : '$+_n$'

→ Let a, b. Then $a +_n b = r \leftarrow$ remainder

$$n \overline{)\, a+b}$$
$$r$$

Ex: $3 +_3 7 = 1$

$-3 +_4 5 = 2$

→ Multiplication modulo n : '$\cdot_n$'

$$n \overline{)\, a \cdot b}$$
$$r$$

Ex: $3 \cdot_5 2 = 1$

$3 \cdot_4 5 = 3$

* Composition table :-

A binary composition (operation) on the non empty finite set A can be defined by table is called a composition table.

Example :- The composition table for multiplication modulo 7 on the set $G = \{0, 1, 2, 3, 4, 5, 6\}$. $[Z_7, \times_7)$ is an algebraic structure.

← a →

$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
↑ 1	0	1	2	3	4	5	6
b 2	0	2	4	6	1	3	5
↓ 3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

* $(Z_7, +_7)$ The comp. table for addition modulo 7.

$+_7$	0	1	2	3	4	5	6
0	0	01	02	03	04	05	06
1	01	2	3	4	5	6	0
2	02	3	4	5	6	0	1
3	03	4	5	6	0	1	2
4	04	5	6	0	1	2	3
5	05	6	0	1	2	3	4
6	06	0	1	2	3	4	5

* Examples of Group :-

Ex:- Show that the set z of all integers $z = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$ is a group with respect to the operation of addition of integers. $(z, +)$

→ We are given $z = \{\dots, -2, -1, 0, 1, 2, \dots\}$ and $+$ is provided as a binary operation.

1) Closure property :

→ We know that the sum of two integers is also an integer.

i.e. $a+b \in z$. Thus, z is closed with respect to addition.

2) Associativity :

→ We know that addition of integers is an associative

$a + (b+c) = (a+b)+c \quad , \forall\, a, b, c \in z.$

3) Existence of Identity : $a + \square = a$

→ Here, $a + 0 = a = 0 + a \; ; \; a \in z$ and $0 \in z$.

Therefore, 0 is the identity element.

4) Existence of Inverse : $a + \square = 0$

→ Here, $a + (-a) = 0 = (-a) + a \; ; \; a \in z$ and $-a \in z$. Therefore, every integer possess additive inverse.

→ Therefore, z is a group with respect to addition. Since, addition of integer is a commutative operator

Extra : 1) $(N, -)$ → No group 1) $1 - 3 = -2 \notin N$.

2) $(N, +)$ → No group 3) $0 \notin N$.

3) $(N, /)$ → No group 1) $1/2 \notin N$.

4) $(N, \cdot)$ → group Satisfies all (4) properties

Ex:- Show that the set of all positive rational number forms an abelian group under the composition defined by $a * b = \frac{ab}{2}$.

→ Let $\mathbb{Q}_+$ denote the set of all positive rational number. To show : $(\mathbb{Q}_+, *)$ is a group.

1) Closure property :

→ We know that multiplication and division of two rational numbers is a rational number therefore $\frac{ab}{2}$ is a rational number.

Thus for every $a, b \in \mathbb{Q}_+ \Rightarrow a * b \in \mathbb{Q}_+$.

→ Thus, $\mathbb{Q}_+$ is closed with respect to the binary operation $*$.

2) Associativity :

→ Let $a, b, c \in \mathbb{Q}_+$.

To prove associativity, we must get,

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

→ L.H.S $= a * (b * c)$

$$= a * \left[\frac{bc}{2}\right]$$

$$= \frac{a\left(bc/2\right)}{2}$$

$$= \frac{abc}{4}$$

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

$$= \left[\frac{ab}{2}\right] * c$$

$$= \frac{\left(\frac{ab}{2}\right)c}{2}$$

$$= \frac{abc}{4}$$

$\therefore$ L.H.S. = R.H.S.

Therefore, $*$ is associative.

3) Existence of Identity :

→ Let e be the identity element in $\mathbb{Q}^+$.

Now, by the definition of an identity element,

$$a * e = a$$

$$\Rightarrow \frac{ae}{2} = a$$

$$\Rightarrow e = 2 \quad (\because a \in \mathbb{Q}^+)$$

and $e * a = a$

$$\Rightarrow \frac{ea}{2} = a \quad (\because a \neq 0)$$

$$\Rightarrow e = 2$$

$\therefore$ 2 is an identity element.

4) Existence of Inverse :

→ Let a be any element of $\mathbb{Q}^+$. and 'b' be the inverse of 'a'.

$\therefore$ By the definition of inverse,

$$a * b = e$$

$$\Rightarrow \frac{ab}{2} = e$$

$$\Rightarrow ab = 4 \quad (\because e = 2)$$

$$\Rightarrow b = \frac{4}{a} \in \mathbb{Q}^+ \quad (\because a \neq 0)$$

→ Now, $a * \frac{4}{a} = 2 = \frac{4}{a} * a$.

Therefore $\frac{4}{a}$ is inverse of a.

Thus each element of $\mathbb{Q}_+$ is invertible.
Hence, $(\mathbb{Q}_+, *)$ is a group.
Since it satisfies the abelian condition we can also call it as an abelian group.

Ex:- Check whether the set $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is group with respect to addition or not.

→ Let x, y be any two elements of G.
$\therefore \quad x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$

1) Now, $x + y = a + b\sqrt{2} + c + d\sqrt{2}$
$= (a + c) + (b + d)\sqrt{2}$
$= A + B\sqrt{2}$

Since, $a + c$ and $b + d$ are the elements of $\mathbb{Q}$, therefore $(a + c) + (b + d)\sqrt{2} \in G$
$A + B\sqrt{2} \in G \quad \forall A, B \in \mathbb{Q}$

Thus $x + y \in G$, $\forall x, y \in \mathbb{Q}$.
$\therefore$ G is closed with respect to addition.

2) Associativity :
→ The elements of G are all real numbers and addition of real numbers is associative. Hence, associative holds true.

3) Existence of Identity :
→ Observe that $0 + 0\sqrt{2} \in G$ since $0 \in \mathbb{Q}$.

If $a+b\sqrt{2}$ is any element of G, then

$(a+b\sqrt{2}) + (0+0\sqrt{2})$

$= (a+b\sqrt{2})$

$= (0+0\sqrt{2})+(a+b\sqrt{2})$

$\therefore (0+0\sqrt{2})$ is an identity element.

4) Existence of Inverse:

→ Since, $a, b \in \mathbb{Q} \Rightarrow -a, -b \in \mathbb{Q}$.

$\therefore$ if $a+b\sqrt{2} \in G \Rightarrow (-a)+(-b)\sqrt{2} \in G$

Now, $a+b\sqrt{2} + (-a+(b\sqrt{2})) = 0+0\sqrt{2}$

and $(-a)+(-b)\sqrt{2} + a+b\sqrt{2} = 0+0\sqrt{2}$

Therefore, $(-a)+(-b)\sqrt{2}$ is the inverse element

→ Thus, the set $G = \{ a+b\sqrt{2} : a, b \in \mathbb{Q} \}$ is a group with respect to addition.

Ex:- Show that the set of all matrices of the form $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$, where x is a non-zero real number, is a group of singular matrices for multiplication. Find the identity and inverse of an element.

1) Closure property :

→ Let $G = M = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} : x \text{ is a non-zero real number.} \right\}$

and let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in M$,

$B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in M$, where x and y are non-zero real numbers.

Now, $AB = \begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} y & y \\ y & y \end{bmatrix} = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in M$,

because $2xy$ is non-zero real number.

2) Associativity :

→ We know that Matrix multiplication is always associative. (i.e. $(AB)C = A(BC)$).

3) Existence of Identity :

→ For $A \in M$, let $E = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$ be such that

$E \cdot A = A$.

→ Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in M$.

$$E \cdot A = A \Rightarrow \begin{bmatrix} e & e \\ e & e \end{bmatrix}\begin{bmatrix} x & x \\ x & x \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 2ex & 2ex \\ 2ex & 2ex \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$$

$$\Rightarrow 2ex = x$$

$$\Rightarrow e = \frac{1}{2} \quad (\because x \neq 0)$$

and $A \cdot E = A \Rightarrow \begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} e & e \\ e & e \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$

$$\Rightarrow \begin{bmatrix} 2ex & 2ex \\ 2ex & 2ex \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$$

$$\Rightarrow 2ex = x$$

$$\Rightarrow e = \frac{1}{2} \quad (\because x \neq 0)$$

$\therefore E \cdot A = A = A \cdot E$

and $E = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \in M$ as $1/2 \neq 0$ and $A \in M$.

4) Existence of Inverse :

→ If $C = \begin{bmatrix} c & c \\ c & c \end{bmatrix}$ be the inverse of A then,

$C \cdot A = E \quad , \quad \forall \; A \in M.$

→ Now, let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in M.$

$\therefore C \cdot A = E \Rightarrow \begin{bmatrix} c & c \\ c & c \end{bmatrix} \begin{bmatrix} x & x \\ x & x \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 2cx & 2cx \\ 2cx & 2cx \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$

$\Rightarrow c = \frac{1}{4x} \neq 0 \quad (\because x \neq 0)$

and $A \cdot C = E \Rightarrow \begin{bmatrix} x & x \\ x & x \end{bmatrix} \begin{bmatrix} c & c \\ c & c \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 2cx & 2cx \\ 2cx & 2cx \end{bmatrix} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$

$\Rightarrow c = \frac{1}{4x} \neq 0 \quad (\because x \neq 0)$

Thus, $C = \begin{bmatrix} 1/4x & 1/4x \\ 1/4x & 1/4x \end{bmatrix} \in M$ as $x \neq 0$

such that $C \cdot A = E = A \cdot C \; , \; \forall \; A \in M.$

$\therefore C = \begin{bmatrix} 1/4x & 1/4x \\ 1/4x & 1/4x \end{bmatrix} \in M$ is the inverse of A.

→ Hence, M is a group with respect to the matrix multiplication.

Ex:- Check whether the set S of all ordered pairs (a, b) of real numbers for which $a \neq 0$ with respect to the operation $*$ $(\cdot)$ defined by $(a, b) \cdot (c, d) = (ac, bc + d)$ is a group w.r.t $\cdot$ or not.

1.) Closure property :

→ Let (a, b) and (c, d) be any two element of S. where $a \neq 0$ and $c \neq 0$.

Now, $(a, b) \cdot (c, d) = (ac, bc + d) \in S$

because $a \neq 0$ and $c \neq 0$ → any real num.

$\Rightarrow ac \neq 0$.

→ Hence, S is closed w.r.t the given composition (binary operation.)

2.) Associativity :

→ Let (a, b), (c, d), (e, f) be any three elements of S.

∴ To prove the associativity we must get,

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

Now, L.H.S. $= [(a, b) \cdot (c, d)] \cdot (e, f)$.

$= (ac, bc + d) \cdot (e, f)$

$= (ace, (bc + d)e + f)$

$= (ace, bce + de + f)$

and R.H.S. $= (a, b) \cdot [(c, d) \cdot (e, f)]$

$= (a, b) \cdot [ce, de + f]$

$= (a, b) \cdot (ce, de + f)$

$= (ace, bce + de + f)$

$=$ L.H.S.

Hence, the given composition $\cdot$ is associative.

3) Existence of Identity:

→ Let, (x,y) be the identity element of S such that $(a,b)\cdot(x,y) = (a,b) = (x,y)\cdot(a,b)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad e$

Now, $(a,b)\cdot(x,y) = (a,b)$

$\Rightarrow (ax, bx+y) = (a,b)$

$\Rightarrow ax = a$ and $\Rightarrow bx+y = b$

$\Rightarrow \boxed{x = 1}$ $\qquad\qquad \Rightarrow b+y = b$

$\Rightarrow \boxed{y = 0}$

$\therefore$ The identity element is $(x,y) = (1,0)$.

and for $(x,y)\cdot(a,b) = (a,b)$

$\Rightarrow (xa, ya+b) = (a,b)$

$\Rightarrow xa = a$ and $\Rightarrow ya+b = b$

$\Rightarrow \boxed{x = 1}$ $\qquad\qquad \Rightarrow \boxed{y = 0}$

$\therefore$ The identity element is $(1,0)$.

4) Existence of inverse :

→ Let $(c,d) \in S$, $c \neq 0$ be the inverse of $(a,b) \in S$.

$\therefore (a,b)\cdot(c,d) = (1,0) = (c,d)\cdot(a,b)$

→ Now, $(a,b)\cdot(c,d) = (1,0)$

$\Rightarrow (ac, bc+d) = (1,0)$

$\Rightarrow ac = 1$ and $\Rightarrow bc+d = 0$

$\Rightarrow \boxed{c = \frac{1}{a}}$ ⊛ $\qquad\qquad \Rightarrow d = -bc$

$\Rightarrow \boxed{d = -\frac{b}{a}}$ $(\because$ ⊛$)$

and $(c,d)\cdot(a,b) = (1,0)$

$\Rightarrow (ca, da+b) = (1,0)$

$\Rightarrow ca = 1$ and $\Rightarrow da + b = 0$

$\Rightarrow \boxed{c = \frac{1}{a}}$ $\Rightarrow \boxed{d = -\frac{b}{a}}$

$\therefore$ The inverse of (a, b) is given by $\left(\frac{1}{a}, \frac{-b}{a}\right)$.

→ Hence, the set S of all ordered pairs (a, b) of real numbers for which $a \neq 0$ w.r.t. the operation $\cdot$ defined by $(a, b) \cdot (c, d) = (ac, bc + d)$ is a group.

* Groupoid :

→ Suppose G is non-empty set and $*$ is a binary operation then $(G, *)$ is called a groupoid if $*$ is closed in G, that is, given any two elements,

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

* Semi-group :

→ A non-empty set G together with binary operation $*$, $(G, *)$ is a semi group if binary operation $*$ is associative.

* Monoid :

→ A non-empty set G together with a binary operation $*$, $(G, *)$ is called a monoid if it satisfies the following properties :

1) $*$ is closed in $(G, *)$.

2) $*$ is associative in $(G, *)$.

3). There exist an Identity element in $(G, *)$.

Ex:- The set of all integers Z. with operation defined by $a * b = a + b + 1$.

1) Is Z groupoid ?

→ To prove G is groupoid, we need to prove that G is closed w.r.t. *.

→ let $a, b \in Z$, $\therefore a * b = a + b + 1 \in Z$

(∵ The sum of integers is always an integer.)

Hence, $a * b \in G$

∴ G is closed w.r.t. * operation.

Therefore G is groupoid.

2) Is Z semi-group ?

→ To prove z is semi-group, we need to prove that G is associative. w.r.t. *.

→ Now, let $a, b, c \in Z$.

∴ we must get $(a * b) * c = a * (b * c)$

∴ L.H.S. $= (a * b) * c$

$= (a + b + 1) * c$.

$= a + b + 1 + c + 1 = a + b + c + 2$.

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

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

$= a + b + c + 1 + 1 = a + b + c + 2$.

∴ R.H.S. = L.H.S.

∴ $G \in Z$ is associative $\Rightarrow$ Z is semigroup.

3). Is Z. Monoid ?

→ 1) Prove closure property

→ 2) Prove associativity

→ 3) Existence of Identity :

→ let $e \in G$ be the identity element of G.

∴ We must get $a * e = a = e * a$.

Now, $a * e = a$

$\Rightarrow a + e + 1 = a$

$\Rightarrow e = -1 \in G$

and $e * a = a$

$\Rightarrow e + a + 1 = a$

$\Rightarrow e = -1 \in G$

∴ The identity element is -1.

Extra 4) Existence of Inverse :

→ let $b \in G$ be the inverse of $a \in G$.

∴ $a * b = e = b * a$.

∴ $a * b = e$

$\Rightarrow a + b + 1 = e$

$\Rightarrow a + b = -1 - 1 = -2$

$\Rightarrow b = -2 + a = a - 2 \in G \ (\because a \in z)$

and $b * a = e$

$\Rightarrow b + a + 1 = -1$

$\Rightarrow b + a = -2$

$\Rightarrow b = a - 2 \in G \ (\because a \in z)$

∴ The inverse of a is $a - 2$ w.r.t. $*$ binary operation.

5) Commutative property for Abelian group :

→ $a * b = a + b + 1 \in G \ (\because \forall a, b \in G)$

and $b * a = b + a + 1$

$= a + b + 1 = a * b$.

∴ $*$ binary operation satisfies the commutative property, ∴ It is an abelian group.

* Order of Group and Order of Element :-

** Order of a group :

→ The order of the group is defined as the number of element in the group.
It is denoted by $o(G)$.

** Order of an element :

→ Let G be a group with binary operation $*$.
By the order of an element $a \in G$ is meant the least positive integer n, if one exists, such that $a^n = e$ [the identity of G].
It is denoted by $o(a)$.

* Remarks :

1. If there does not exist any positive integer n such that $a^n = e$, then we say that a is of infinite ~~number~~ order.

2. The order of the identity element is always 1.

Ex:- Find the order of each element of the multiplicative group $\{1, -1, i, -i\}$.

→ Here, we are given the multiplicative group $\{1, -1, i, -i\}$.
∴ The order of a group is : 4 /* = O(g) */

→ Now, for multiplicative group, the identity element $e = 1$.

→ The order of 1 :

$1^{1} = 1$ ← The identity element.

/* $1^{2} = 1 \cdot 1 = 1$ */ ← least positive integer

$\therefore o(1) = 1$

→ The order of -1 :

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

$(-1)^{2} = (-1)(-1) = 1$ ← The identity element.

$\therefore o(-1) = 2$

→ The order of i :

$(i)^{1} = i$

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

$(i)^{3} = -i$

$(i)^{4} = (-1)(-1) = 1$ ← The identity element.

$\therefore o(i) = 4.$

→ The order of $(-i)$:

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

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

$(-i)^{4} = (-1)(-1) = 1.$ ← The identity element

$\therefore o(-i) = 4.$

Ex:- Find the order of each element of the group $\{0, 1, 2, 3, 4, 5\}$, the composition being addition modulo 6. $(Z_6, +_6)$

→ Since, 0 is the identity element.
Therefore, $o(0) = 1.$

→ $O(1)$:

$1^1 = 1$

$1^2 = 1 +_6 1 = 2$

$1^3 = 1 +_6 1 +_6 1 = 3$

$1^4 = 1 +_6 1 +_6 1 +_6 1 = 4$

$1^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5$

$1^{\boxed{6}} = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0$ ← identity element

1
6 | 6
6
0

$\therefore O(1) = 6.$

→ $O(2)$:

$2^1 = 2$

$2^2 = 2 +_6 2 = 4$

$2^{\boxed{3}} = 2 +_6 2 +_6 2 = 0$ ← identity element.

$\therefore O(2) = 3$

→ $O(3)$:

$3^1 = 3$

$3^{\boxed{2}} = 3 +_6 3 = 0$ ← identity element.

$\therefore O(3) = 2$

→ $O(4)$:

$4^1 = 4$

$4^2 = 4 +_6 4 = 2$

$4^{\boxed{3}} = 4 +_6 4 +_6 4 = 0$ ← identity element

$\therefore O(4) = 3$

→ $O(5)$:

$5^1 = 5$

$5^2 = 5 +_6 5 = 4$

$5^3 = 5 +_6 5 +_6 5 = 3$

$5^4 = 5 +_6 5 +_6 5 +_6 5 = 2$

$5^5 = 5 +_6 5 +_6 5 +_6 5 +_6 5 = 1.$

$5^{\boxed{6}} = 5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0.$ ↑ identity element

$\therefore O(5) = 6$

Ex:- Is multiplicative modulo 6 a group ?
L.6 $(U_6 = \{0, 1, 2, 3, 4, 5\}, *_6)$.
If not, how to make it a group ?
Find the order of all the elements.

→ To check the multiplicative modulo 6 of a given group, we need to generate the composition table for $Z_6 = (U_6, X_6)$

X_6	[0]	[1]	[2]	[3]	[4]	[5]
[0]	0	0	0	0	0	0
[1]	0	1	2	3	4	5
[2]	0	2	4	0	2	4
[3]	0	3	0	3	0	3
[4]	0	4	2	0	4	2
[5]	6	5	4	3	2	1

1) Closure property :

→ Since all the elements of the table lie in the set $U_6 = \{0, 1, 2, 3, 4, 5\}$, we can say that closure property is satisfied.

2) Associative property :

→ For all the elements in the table, it can be verified that $(a *_6 b) *_6 c = a *_6 (b *_6 c)$ $\forall\ a, b, c \in U_6$.

→ For example, let $a = 1$, $b = 2$, $c = 4$.

$\therefore$ L.H.S. $= (1 *_6 2) *_6 4$

$= 2 *_6 4$

$= 2$

& R.H.S. $= 1 *_6 (2 *_6 4)$

$= 1 \times_6 8$

$= 2$

$= L.H.S.$

3) Existence of identity :

→ From the table, it can be observed that 1 will be the identity element as $a *_6 1 = a$, $\forall\ a \in U_6$.

4) Existence of inverse :

→ For only [1] and [5] the condition $(a) *_6 (a^{-1}) = 1$ is satisfied. and there will not be any element from U_6 which will satisfy the above requirement.

→ Hence, inverse element for [0], [2], [3] and [4] does not exist.

→ Therefore, 4th property is not satisfied and we can say that U_6 is not a group.

→ Here, if we remove [0], [2], [3] and [4] from U_6, we get $S_{U_6} = \{[1], [5]\}$ which will satisfy the 4th property which will result in U_6 being a group.

Prove all the 4 pro. again

→ Now, the $O(5) = 2$. (order of group).

and $O(1)$: $1^{(1)} = 1$ (order) $\therefore O(1) = 1$.

and $O(5)$: $5^{1} = 5$

$5^{(2)} = 5 \times_6 5 = 1$ (order) $\therefore O(5) = 2$

→ Non zero rational number : $Q - \{0\}$

Date
Page

Ex :- In the infinite multiplicative group of non-zero rational numbers. Find the order of each number.

→ Since '1' is the identity element therefore $o(1) = 1$.

Now, $o(-1)$: $(-1)^1 = (-1)$

$(-1)^2 = 1$ $\therefore o(-1) = 2$

and $o(2)$: $(2)^1 = 2$

$(2)^2 = 4$

$(2)^3 = 8$. and so on.

∴ There does not exist any positive integer n such that $2^n = 1$. (identity element)

∴ $o(2)$ = infinite.

∴ Similarly, the order of the remaining elements will be infinite.

Ex :- Find the order of each element in the additive group of integers.

→ Here for additive group, the identity element is '0'.

∴ For identity element $o(0) = 1$.

→ Now, $o(1)$: $1^1 = 1$

$1^2 = 1 + 1 = 2$

$1^3 = 1 + 1 + 1 = 3$ and so on.

∴ There does not exist any positive integer n such that $1^n = 0$.

∴ $o(1)$ = infinite.

∴ Similarly, the order of the remaining elements will be infinite.

* Remarks :

1. The order of every element of a finite group is finite and is less than or equal to the order of the group. $O(a) \leq O(G)$

2. The order of an element of a group is same as that of its inverse a^{-1}.

3. In an infinite group, an element can have the finite order as well as the infinite order.

* SUBGROUP :-

→ A non empty subset H of a group G is called a subgroup of G if H itself is a group under the same binary operation as of G.

* Remark : For any group G, $H = \{e\}$ and $H = G$ are always a subgroup of G. [Improper subgroup].

→ Examples : $(\mathbb{Z}, +)$ of $(\mathbb{Q}, +)$ $\quad H \subset G$

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

$(\mathbb{R}, +)$ of $(\mathbb{C}, +)$

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

1. The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$.

2. The additive group of even integers is a subgroup of the additive group of of all integers. [$(2\mathbb{Z}, +)$ of $(\mathbb{Z}, +)$]

3. The multiplicative group of positive rational numbers is a subgroup of the multiplicative of all non-zero rational numbers.
[$(\mathbb{Q}^+, \times)$ of $(\mathbb{Q}, \times)$]

MCQs * Remarks :-

1. Every set is a subset of itself. Therefore if G is a group, then G itself is a group of G. Also, if e is the identity element of G, then the subset of G containing only one element (e) is also a subgroup of G. These two are subgroup of any group. They are called trivial or improper subgroup. A subgroup other than these two is called proper subgroup.

2. The identity of a subgroup is same as that of the group.

3. The inverse of any element of a subgroup is same as the inverse of the same

regarded as an element of the group.

4. The order of any element of subgroup is the same as the order of the element regarded as a member of a group.

✳ CRITERION FOR A NON EMPTY SET TO BE A SUBGROUP :-

* Theorem :- A non empty subset H of a group G is a subgroup of G if and only if,

(i) $a \in H, b \in H \Rightarrow a * b \in H$ (Closure)
(ii) $a \in H \Rightarrow a^{-1} \in H$ (inverse)

* Theorem :- A necessary and sufficient condition for a non empty subset H of a group to be a subgroup is that $a \in H, b \in H \Rightarrow ab^{-1} \in H$ where b^{-1} is the inverse of b in G.

✳ INTERSECTION OF SUBGROUP :-

* Theorem :- If H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

Example: (Prob.)

Proof :- Since H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2 = \phi$, since at least the identity e is common to both H_1 and H_2.

→ In order to prove that $H_1 \cap H_2$ is a subgroup of G, it is sufficient to prove that, $a \in H_1 \cap H_2$, $b \in H_1 \cap H_2$
$\Rightarrow a * b^{-1} \in H_1 \cap H_2$.

Now, $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$
$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

but H_1 and H_2 are subgroups.
therefore, $a \in H_1, b \in H_1 \Rightarrow a * b^{-1} \in H_1$
and $a \in H_2, b \in H_2 \Rightarrow a * b^{-1} \in H_2$

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

Thus, $a \in H_1 \cap H_2$, $b \in H_1 \cap H_2$
$\Rightarrow ab^{-1} \in H_1 \cap H_2$.

Hence, $H_1 \cap H_2$ is a subgroup of G.

* Remark :-

→ The union of two subgroups is not necessarily a subgroup.

Date
Page

** For example :-

(1) → Let G be the additive group of integers.

$H_1 = \{ \ldots, -6, -4, -2, 0, 2, 4, 6, \ldots \}$

$H_2 = \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}$.

Here, H_1 and H_2 are two subgroups of G.

→ $H_1 \cup H_2 = \{ -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9, \ldots \}$

→ Now, $2 \in H_1 \cup H_2$, $3 \in H_1 \cup H_2$

$\Rightarrow 2 * 3 = 2 + 3 = 5 \notin H_1 \cup H_2$.

$\therefore H_1 \cup H_2$ is not closed w.r.t. addition.

$\therefore H_1 \cup H_2$ is <u>not</u> a subgroup w.r. to addition

(2) ** Ex :-

** $H = \{ a + ib : a, b \in \mathbb{Q} \}$

Prove : H is a sub group of $(C, +)$.

→ Let $x, y \in H$. and $x = a + ib$

$y = c + id$.

→ Here, we need to show $x * y^{-1} \in H$

where $x, y \in H$ to prove H is a subgroup

$\therefore$ we must get $x + y^{-1} \in H$

$x + (-y) \in H$.

$x - y \in H$

Now, $x - y = a + ib - c - id$

$= (a - c) + i(b - d)$

$= A + iB \in H$

$\therefore$ H is a subgroup of $(C, +)$.

Ex:- Let G be the additive group of integers. Then prove that the set of all multiples of integers by a fixed integer m is a subgroup of G.

→ Here, G is the additive group of integers.
$\therefore G = \{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \} = \mathbb{Z}$

→ Now, let m be any fixed integer.
$\therefore H = \{ \ldots, -3m, -2m, -1m, 0, 1m, 2m, \ldots \}$.
$\therefore H \subseteq G$. $\quad \therefore H = m\mathbb{Z}$

→ To prove that H is a subgroup, we have to prove that $a * b^{-1} \in H$
$(a \in H$ and $b \in H)$ $\Rightarrow a + b^{-1} \in H$
$\Rightarrow a - b \in H$

→ Let $a = km$ and $b = nm$; $k, n \in \mathbb{Z}$
where, $a, b \in H$.

The inverse of b w.r.t. additive group is given by $b^{-1} = (-n)m = -b$.

Now, $a * b^{-1} = a + b^{-1}$
$= a - b$
$= a + (-n)m$
$= km - nm$
$= (k-n) \cdot m \in H$
(∵ subtraction of integers is an integer.)

Thus, $a \in H, b \in H \Rightarrow ab^{-1} = a - b \in H$.

Therefore, H is a subgroup of G.

Ex:- Let G be a set of all ordered pairs (a, b) of real numbers for which $a \neq 0$. Let a binary operation $\times$ defined by
$(a, b) \times (c, d) = (ac, bc+d)$.
Show that $(G, \times)$ is non-abelian group.
Does the subset H of all those elements of G which are of the form $(1, b)$ form a subgroup of G?

→ To prove that G is a group, we must prove the 4 properties :

1) Closure property :
→ let (a, b) and (c, d) be any two elements of S. where, $a \neq 0$, $c \neq 0$.

Now, $(a, b) * (c, d) = (a, b) \times (c, d)$
$= (ac, bc+d)$

where, $ac \neq 0$ and $bc+d \in S$
∴ S is closed w.r.t. the given binary operation

2) Associative property :
→ let (a, b), (c, d), $(e, f) \in S$.
where, $a, c, e \neq 0$.
→ To prove associative property, we must get,
$[(a, b) * (c, d)] * (e, f)$
$= (a, b) * [(c, d) * (e, f)]$.

Now, L.H.S. $= [(a, b) * (c, d)] * (e, f)$
$= (ac, bc+d) * (e, f)$
$= (ace, e(bc+d)+f)$
$= (ace, bce + de + f)$.

and, R.H.S $= (a*b) * [(c,d) * (e,f)]$

$= (a*b) * (ce, de+f)$

$= (ace, bce + de + f)$

$= L.H.S$

∴ The given composition / binary operation is associative.

3). Existence of identity :

→ Let (x,y) be any identity element of S.

∴ we must get $(x,y) * (a,b) = (a,b)$

where, (a,b) is the element of S.

∴ $(x,y) * (a,b) \Rightarrow (x,y) \times (a,b) = (a,b)$

$\Rightarrow (xa, ya+b) = (a,b)$

$\Rightarrow xa = a$ and $ya+b = b$

$\Rightarrow \boxed{x = 1}$ $(\because a \neq 0)$ $\Rightarrow ya = 0$

$\Rightarrow \boxed{y = 0}$ $(\because a \neq 0)$

∴ The identity element is $(x,y) = (1,0)$.

4). Existence of inverse :

→ Let $(c,d) \in S$; $c \neq 0$ be the inverse of $(a,b) \in S$; $a \neq 0$.

we must get, $(a,b) * (c,d) = (1,0)$

$\Rightarrow (a,b) \times (c,d) = (1,0)$

$\Rightarrow (ac, bc+d) = (1,0)$

$\Rightarrow ac = 1$ and $bc+d = 0$

$\Rightarrow \boxed{c = \frac{1}{a}}$ $\Rightarrow d = -bc$

$\Rightarrow \boxed{d = -\frac{b}{a}}$

∴ The inverse of (a,b) is $(c,d) = \left(\frac{1}{a}, -\frac{b}{a}\right)$.

→ Hence, the set S of all ordered pairs (a, b) of real numbers for which $a \neq 0$ w.r.t. the binary operation $*$ defined by $(a,b) * (c,d) = (ac, bc+d)$ is a group.

→ Now, To check the abelian group,
let $(a,b) \in S$ and $(c,d) \in S$
where, $a \neq 0$, $c \neq 0$.
Now, $(a,b) * (c,d) = (ac, bc+d)$.
and $(c,d) * (a,b) = (ac, ad+b)$
∴ It does not satisfy the commutative property.
Hence, it is not an abelian group.

✱ → To prove H is a subgroup of $(G; *)$:
we are given $H = \{(1,b) : b \in \mathbb{R}\}$

Now, let $x = (1,a) \in H$, $y = (1,b) \in H$.
where, $a, b \in R$.
If H is a subgroup of G, it must satisfies the following property,
$$x * y^{-1} \in H$$
$$(1,a) * (1,b)^{-1} \in H.$$

Now, $(1,a) * (1,b)^{-1} = x * y^{-1}$.
$$\therefore x * y^{-1} = (1,a) * \left(\frac{1}{1}, \frac{-b}{1}\right)$$
$$= (1,a) * (1,-b)$$
$$= (1, a + (-b))$$
$$= (1, a-b) \; ; a-b \in R$$
$$= (1, a-b) \in H$$

→ To prove $a * b^{-1} \in H$, binary operation should be of G. That means both the binary operations of H and G must be same.

∴ $(1, a) * (1, b)^{-1} \in H$

Hence, H is a subgroup of G.

★ Ex:- Let H be the multiplicative group of all positive real numbers and G be the additive group of all real numbers. Is H a subgroup of G ?

$H = (R^+, \cdot)$
$G = (R, +)$

→ Here, the set of all positive real numbers is a subset of the set of G. of all the real numbers.

→ But the group H is not a subgroup of G because the composition / binary operation in H is different from that of the G.

✱ Lagrange's Theorem :-

→ If H is a subgroup of finite group G, then

$$o(H) \mid o(G).$$

In other words, "The order of each subgroup of a finite group is a divisor of the order of the group."

Ex:- $G = \{1, -1, i, -i\}$.

$o(G) = 4 \longrightarrow o(H) = 1, 2, 4$

✱ [There will be 3 subgroups and the order will be 1, 2, 4.]

prime number ; which is divisible by 1 and only itself.

Date
Page

* Note :- Langrange's theorem has very important applications.

→ Suppose G is a finite group of order n. If m is not a divisor of n, then there can be no sub group of order m.

→ Thus if G is a group of order 6, then there can be no group of order 5 or 4.

→ Similarly, if G is a group of prime order p then G can have no proper sub group.

* CYCLIC GROUP :-

→ A group G is called cyclic group if for some $a \in G$, every element of G is of the form a^n, for some integer n. The element 'a' is then called a generator of G and we write $G = \langle a \rangle$.

Ex:- The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic.

→ Here, $G = \{1, -1, i, -i\}$.
we can write it as
$G = \{i^4, i^2, i, i^3\}$
$= \{i, i^2, i^3, i^4\}$
Thus, G is a cyclic group and 'i' is a generator.

$i^1 = i$
$i^2 = -1$
$i^3 = i^2 i = -i$
$i^4 = i^2 i^2 = 1$
will be possible in case of $\langle -i \rangle$ also.

$\omega^3 = 1$

Date
Page

Also we can write $G = \{1, -1, i, -i\}$
as $G = \{(-i)^4, (-i)^2, (-i)^3, (-i)^1\}$
Thus $-i$ is also the generator.

Ex:- The multiplicative group $\{1, \omega, \omega^2\}$ is cyclic. The generators are ω, ω^2. (prove)

→ Here, we are given $G = \{1, \omega, \omega^2\}$.

Now, $\omega^1 = \omega$
$\omega^2 = \omega^2$
$\omega^3 = \omega \cdot \omega^2 \neq 1$
$\omega^4 = \omega^3 \cdot \omega = \omega$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	ω^3	$\omega^4 = \omega^3 \cdot \omega$
		1	$= 1 \cdot \omega$
			$= \omega$

Thus, ω is the generator.

and $(\omega^2)^1 = \omega^{2} = \omega^2$
$(\omega^2)^2 = \omega^4 = \omega$
$(\omega^2)^3 = \omega^6 = \omega^3 \cdot \omega^3 = 1$
Thus, ω^2 is also the generator.

Ex:- Find the generators of a group $A = (\{0, 1, 2, 3, 4, 5\}, +_6)$.
(Prove: the given group is cyclic.)
[We can also generate a composition table and prove.]

→ Here, we are given $A = \{0, 1, 2, 3, 4, 5\}$, with the binary operation addition modulo 6.

→ Now, for $1^1 = 1$
$1^2 = 1 +_6 1 = 2$
$1^3 = 1 +_6 1 +_6 1 = 3$
$1^4 = 1 +_6 1 +_6 1 +_6 1 = 4$
$1^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5$

and $1^6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0$.

∴ we can write $A = \{0, 1, 2, 3, 4, 5\}$ as a $A = \{1^6, 1^1, 1^2, 1^3, 1^4, 1^5\}$.

Thus 1 is the generator.

→ Now, for $5^1 = 5$

$5^2 = 5 +_6 5 = 4$

$5^3 = 5 +_6 5 +_6 5 = 3$

$5^4 = 5 +_6 5 +_6 5 +_6 5 = 2$

$5^5 = 5 +_6 5 +_6 5 +_6 5 +_6 5 = 1$

$5^6 = 5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0$

∴ we can write A as $A = \{5^6, 5^5, 5^4, 5^3, 5^2, 5^1\}$.

Thus 5 is also a generator.

* Remark :-

→ Every cyclic group is an abelian.

→ If 'a' is a generator of a cyclic group G, then a^{-1} is also generator of G.

→ If 'a' is a generator of an infinite cyclic group G, then the order of 'a' must be infinite. If the order of 'a' is finite, then the cyclic group generated by 'a' is of finite order. Therefore, the order of the cyclic group is equal to order of its generating element.

L:8 28:00 → If G is a cyclic group of order n then total number of generators of G will be equal to the number of integers less than n and prime to n. i.e. $\phi(n)$. (Euler's ϕ function)

For example, if 'a' is generator of a cyclic group G of order 8, then a^1, a^3, a^5, a^7 will be the only generators of G. Since 4 is not prime to 8 therefore a^4 cannot be generator of G. Similarly, a^2, a^6, a^8 cannot be the generators of G.

→ If a finite group of order n contains an element of order n, then group must be cyclic.

$$o(G) = n = o(a) \Rightarrow \text{cyclic group}$$

Ex:- Show that the group $(\{1,2,3,4,5,6\}, \times_7)$ is cyclic. How many generators are there?

→ Let $G = \{1,2,3,4,5,6\}$. If there exists an element $a \in G$ such that $o(a) = 6$. i.e. the order of the group G then the group G will be cyclic group and 'a' will be a generator of G.

→ For 3, $3^1 = 3$

$3^2 = 3 \times_7 3 = 2$

$3^3 = 3 \times_7 3 \times_7 3 = 6$.

$3^4 = 3 \times_7 3 \times_7 3 \times_7 3 = 4$

$3^5 = 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 = 5$

$3^6 = 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 = 1$ ← identity element

$\therefore o(3) = 6$.

→ For 5, $5^1 = 5$

$5^2 = 5 \times_7 5 = 4$

$s^3 = s \times_7 s \times_7 s = 6.$

$s^4 = s \times_7 s \times_7 s \times_7 s = 2.$

$s^5 = s \times_7 s \times_7 s \times_7 s \times_7 s = 3$

$s^6 = s \times_7 s \times_7 s \times_7 s \times_7 s \times_7 s = 1$ (identity element)

$\therefore o(s) = 6.$

→ Thus, 3 and 5 are the generators of a cyclic group a_4.

∴ There are two generators.

* PERMUTATION GROUP :-

* Definition :

Suppose S is a finite set having n distinct elements. Then a one-one mapping of S onto itself is called a permutation of degree n.

→ The permutation set is denoted by 'S_n'.

→ The number of elements in the finite set S is known as the degree of permutation.

* ~~The total number of elements in the finite set S is known as the degree~~

→ Total number of distinct permutations of degree n is $n!$.

→ If a permutation mapping form a group with respect to the composition of mapping then it

is called a permutation group of degree n.

For example,

Let $S = \{1, 2, 3\}$.

The total number of permutations $= 3! = 6$.

$\therefore f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Ex:- Write the permutations for $S = \{1, 2, 3, 4\}$ (atleast 10)

$\therefore S = \{1, 2, 3, 4\} \Rightarrow$ The total number of permutations $= 4! = 24$

$\therefore f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $f_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$, $f_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$

$f_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, $f_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, $f_9 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$

$f_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$, $f_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, $f_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

$f_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $f_{14} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$, $f_{15} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

$f_{16} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, $f_{17}, \ldots, f_{24}$.

* Equality of two permutation :-

→ Two permutations f and g of degree n is said to be equal if we have, $f(a) = g(a)$, $\forall\ a \in S$.

Ex:- $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

Here, $f(1) = 2$ and $g(1) = 2$
$f(2) = 3$ $g(2) = 3$
$f(3) = 4$ $g(3) = 4$
$f(4) = 1$ $g(4) = 1$.

=> f and g are two equal permutations.

* Product or Composition of two permutations :-

→ The product or composition of two permutations f and g of degree n is denoted by fog, is obtained by first carrying out the operation defined by f and then by g. Similarly, gof.

Ex:- Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ be two permutations of degree 3.

→ Here, we are given,

$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

→ Product of two permutations need not to be commutative.

∴ $fog = f \cdot g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2)$

and $gof = g \cdot f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1, 3)$

* Identity permutation :-

The image of the element is the element itself.

Ex:- $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. Here, $f(1) = 1$, $f(2) = 2$, $f(3) = 3$

∴ f is an identity element / permutation.

Ex:- Show that the set S_3 of all permutations on three symbols 1, 2, 3 is a finite non-abelian group of order 6 with respect to permutation multiplication as composition.

↳ Product of permutations

→ Here, we are given $S_3 = \{1, 2, 3\}$.

∴ The total number of permutations = $3! = 6$.

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Now, generating the composition table,

Composition	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

1) Closure property:

→ Since all the entries in the table are the permutations of S_3, therefore S_3 is closed with respect to multiplication of permutation.

2) Associative Property :

→ We know that composition of permutation is always associative.

3) Existence of Identity :

→ From the table, we can observe that f_1 is the identity element / permutation.

4) Existence of Inverse : (All have different inverses)

→ Here, there exists the inverse of the total 6 permutations,

$(f_1)^{-1} = f_1$, $(f_2)^{-1} = f_3$, $(f_3)^{-1} = f_2$

$(f_4)^{-1} = f_4$, $(f_5)^{-1} = f_5$, $(f_6)^{-1} = f_6$

Thus inverse of each element exists.

→ Since S_3 satisfies all the conditions, therefore S_3 is a group with respect to the permutation multiplication / Composition.

→ We know that the product of two permutations are not commutative. Therefore, the given S_3 group is not an abelian group.

— Ryshik Rathod
20DCS103

——— X ———