UNIT-2

Binary Operations :- ①

Let A be a Non empty set then a function $f : A \times A \to A$ is called a binary operation on A.

The symbol $\times, +, \cdot$ are used to denote binary operations on a set.

$\times$ will be a binary operation on A if and only if

$a \times b \in A \ \forall a, b \in A$ and $a \times b$ is unique.

Exp:- Let $A = \{0, -1, 1\}$. Then addition is not a binary operation because $1+1=2$, $(-1)+(-1) = -2 \notin A$.

but multiplication is binary operation on A.

Exp:-2:- The operation of subtraction $(-)$ is a binary operation on Z whereas it is not a binary operation on Z^+. because $3-5 = -2 \notin Z^+$.

A binary operation on a set A is sometimes called a composition in A.

for a finite set, a binary operation on the set can be defined by a table called the composite table.

Exp:- Let $A = \{0, 1\}$ we define binary operation $\vee$ and $\wedge$ by following table

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

Exp:- $S = \{a, b, c, d\}$. The operation $\star$ can be defined as follows -

$x \star y = x$. construct the table.

$\star$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

Properties of binary operation:

① Closure Property:

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

② Associative law:

$(a \star b) \star c = a \star (b \star c)$

③ Commutative law:-

$a \star b = b \star a$

④ Identity element:

An element 'e' in a set is called identity element w.r.t. to binary operⁿ if for any element a in A.

$\boxed{a \star e = e \star a = a}$

0 for Addition
1 for multiplication

(5) Inverse Element :- Consider a set having the identity element 'e' w.r.t. to binary operation. If corresponding to each element $a \in A$ there exists an element $b \in A$ such that

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

then b is said to be the inverse of 'a' and is usually denoted by a^{-1}.

Algebraic structure (Mathematical structure):

A non empty set G equipped with some operation & some properties is called an algebraic structure.

Groupoid: Closure -

Semi Group: Closure, Associative -

Monoid: Closure, Associative, Identity -

Group: Closure, Associative, Identity, Inverse -

Abelian Group: Closure, Associative, Identity, Inverse, Commutative -

Exp:- $A = \{1, w, w^2\}$, w is cube root of unity ?

is Groupoid, semiGroup, monoid, Group, or Abelian group.

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

ii) ans:- Abelian Group.

(2) $G = [1, i, -1, -i]$ an abelian multiplicative Group.

×	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Transpose of matrix

(3) Show that $\left[\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\right]\left[\begin{matrix}-1 & 0\\ 0 & 1\end{matrix}\right]\left[\begin{matrix}1 & 0\\ 0 & -1\end{matrix}\right]\left[\begin{matrix}-1 & 0\\ 0 & -1\end{matrix}\right]$

form a multiplicative abelian Group.

(4) Set $[0, 1, 2, 3, 4]$ is abelian Group of orders 5

under addition modulo '5' as composite.

Subgroup: Let H be a subset of group G. Then H is called a subgroup of G if H itself is a group under the operation of G.

Simple criteria to determine subgroups follows

(i) the identy element $e \in H$

(ii) if $a, b \in H$ then $a * b \in H$

(iii) if $a \in H$ then $a^{-1} \in H$

$(G, *)$, $(\{e\}, *)$ are improper subgroup.

Exp:- ① $G = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$ under multiplication mod 28 is group.

$\{1\}$, $\{1, 15\}$, $\{1, 27\}$, $\{1, 9, 25\}$, $\{1, 3, 19\}$ are subgroup

$\{1, 3\}$, $\{1, 19\}$ are not subgroup.

Exp:- ② $(1, -1, i, -i)$ is group under multiplication.

then $(1, -1)$ is subgroup or not. (Yes)

$(1, i)$ is subgroup or not (No.

Cyclic group: A group is called cyclic group if for some $a \in G$ every element is of the form a^n, where n is positive integer.

The element a is called generator of G.

Exp:- Multiplicative group $G = [1, -1, i, -i]$ is cyclic or not.

$1, -1, i, -i$ can be written

$(i)^4, (i)^2, (i)^1, (i)^3$ so it is cyclic, i is generator.

or

$1, -1, i, -i$ can be written as

$(-i)^4, (-i)^2, (-i)^3, (-i)^1$ so $(-i)$ is another generator.

Exp:- $G = \{1, 2, 3, 4, 5, 6\}$ under modulo 7 multiplication is G cyclic or not.

$2^1 = 2, 2^2 = 4, 2^3 = 1,$ ~~2~~

$3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$

so it is cyclic. 3 is generator

$4^1 = 4, 4^2 = 2, 4^3 = 1, 4^4 = 4$

$5^1 = 5, 5^2 = 4, 5^3 = 6, 5^4 = 2, 5^5 = 3, 5^6 = 1$

so 5 is another generator.

$6^1 = 6, 6^2 = 1, 6^3 = 6$ — —

Order of group, order of element & subgroup Generated by element:-

No of elements in group is called order of group.

Exp:- $G = \{1, 2, 3, 4, 5, 6\}$ under modulo 7.

(i) Find multiplication table.

(ii) Find $2^{-1}, 3^{-1}, 6^{-1}$

(iii) Find the order & subgroup generated by 2 and 3.

(iv) Is G cyclic. (Yes).

ans:- (i)

X	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

ans:- (ii)

$2^{-1} = 4$

$3^{-1} = 5$

$6^{-1} = 6$

ans:- (iii)

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 1$ order $(2) = 3$ subgrp $= \{1, 2, 4\}$

$3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1$ order $(3) = 6$, sub $\{1, 2, 3, 4, 5, 6\}$

Exp:- ② $G = [1, 2, 4, 7, 8, 11, 13, 14]$ modulo 15 under multiplicity.

(i) Find multiplication table

(ii) find $2^{-1}, 7^{-1}, 11^{-1}$

(iii) find order & subgroup generated by 2, 7 and 11.

(iv) It is cyclic or not.

ans:-(i)

X	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	2	1	14	8	4	2
14	14	13	11	8	7	4	2	1

ans:-(ii)

$2^{-1} = 8$

$7^{-1} = 13$

$11^{-1} = 11$

ans:-(iii) $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 1$, $o(2) = 4$, subg $= [1, 2, 4, 8]$

$7^1 = 7, 7^2 = 4, 7^3 = 13, 7^4 = 1$ $o(7) = 4$, subgr $[1, 4, 7, 13]$

$11^1 = 11, 11^2 = 1$ $o(11) = 2$, subgr $[1, 11]$

16,

KTC

ans:- 4:-

$4^1 = 4, 4^2 = 1$, subgp $[1, 4]$, $o(4) = 2$

$8^1 = 8, 8^2 = 4, 8^3 = 2, 8^4 = 1$ $o(8) = 4$, sub $[1, 2, 4, 8]$

$13^1 = 13, 13^2 = 4, 13^3 = 7, 13^4 = 1$ $o(13) = 4$, subgp $= [1, 4, 7, 13]$

$14^1 = 14, 14^2 = 1$ $o(14) = 2$, subgp: $[1, 14]$

Since no element generates group so it is not cyclic.

5

Ring : Suppose R is a non empty set with two binary operation (addition $+$, multiplication $\cdot$) then the algebraic structure $(R, +, \cdot)$ is called a ring if the following properties are satisfied –

1. R should be an abelian group w.r.t. addition.
2. multiplication is associative ~~and~~ closure (semigroup $(R, \cdot)$)

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3. multiplication is distributed w.r.t. addition

$a(b+c) = ab + ac$ · Left distributed

$(b+c)a = ba + ca$ Right distributed

Exp:- $(0, 2, 4, 6, 8)$ under mod 10

Ring with unity: If in a ring R we have $1 \in R$ such that $1 \cdot a = a \cdot 1 = a \ \forall a \in R$. Then 1 is multiplicative identity and ring is called ring with unity.

~~Ring with~~ **Exp:-** $[0, 1, 2, 3]_4$ with addition mod 4.

Commutative ring:- If ~~in~~ a ring R we have $a \cdot b = b \cdot a \ \forall a, b \in R$ then it is called commutative ring.

Field:- A ring R together with two binary operation (+, ·) is called a field if
1. It is a ring with unity.
2. It is a commutative ring
3. every non zero element $a \in R$ has its multiplicative inverse

Exp:- {0, 1, 2, — n-1) under addition mod n

only if n is prime number.

Permutation:-

Suppose P is a finite set having n distinct element. Then a one-one mapping of P onto itself is called a permutation of order n.

$$P : A \rightarrow A$$

$$P = \begin{pmatrix} a_1 & a_2 & - & \text{———} & a_n \\ b_1 & b_2 & - & \text{———} & b_n \end{pmatrix}$$

Number of distinct Permutation:

Let P be a set with n element then n! distinct Permutation are possible. (3) 3!

Exp: P(1, 2, 3)

$P_1 \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

6

Multiplication of Permutation:-

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$f \cdot g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad g \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Inverse Permutation:-

1, 2, 3

$$f = \boxed{((1,3)(2,2)(3,1)(4,4))}$$

$$f^{-1} = ((3,1), (2,2) (1,3) (2,4))$$

Lagrange's Theorem:

The order of each subgroup of a finite group is a divisor of the order of the group.

Proof: Let G is finite group of order n i.e. $O(G)=n$

i.e. $G=\{a_1, a_2, a_3, \ldots a_n\}$

and H is subgroup of G order m i.e. $O(H)=m$

i.e. $H=\{h_1, h_2, h_3, \ldots h_m\}$

Then right cosets are

$Ha_1=\{h_1 a_1, h_2 a_1, h_3 a_1 \ldots h_m a_1\}$

$Ha_2=\{h_1 a_2, h_2 a_2, h_3 a_2 \ldots h_m a_2\}$

$Ha_3=\{h_1 a_3, h_2 a_3, h_3 a_3 \ldots h_m a_3\}$

$\vdots$

$Ha_n=\{h_1 a_n, h_2 a_n, h_3 a_n \ldots h_m a_n\}$

Suppose there k different cosets among n cosets.

$$\boxed{G = Ha_1 \cup Ha_2 \cup Ha_3 \ldots \cup Ha_k}$$

number of elements in G = number of element in Ha_1 + no. of elements in Ha_2 + ... no. of elements in Ha_k

$n = m + m + m \ldots$ (k times)

$n = km$

$\frac{n}{m} = k$ $\because k$ is integer.

So we can say order of subgroup $O(H)$ divides the order of group $O(G)$.

Coset: Let H be a subgroup of a group $(G, *)$.
Let $a \in G$. Then the set $\{a * h : h \in H\}$ is called left coset of H & is denoted by aH.
Similar set $\{h * a : h \in H\}$ is called Right coset of H & is denoted by Ha.

$aH = \{a * h : h \in H\}$ Left coset
$Ha = \{h * a : h \in H\}$ Right coset

If operato is addition (+) then

$a+H = \{a + h : h \in H\}$ Left coset
$H+a = \{h + a : h \in H\}$ Right coset

Exp:- Z under addition. Let
$H = \{ --- -15, -10, -5, 0, 5, 10, 15, --- \}$

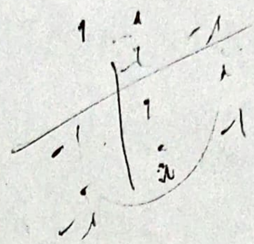
then cosets

$0+H = \{ --- -15, -10, -5, 0, 5, 10, 15 --- \}$
$1+H = \{ --- -14, -9, -4, 1, 6, 11, 16, --- \}$

Normal Subgroup:- A subgroup H of a group G is said to be normal subgroup if $Ha = aH$ for all $a \in G$.
Every subgroup of an abelian group is a normal subgroup

Exp:- additive modulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3



$H = (0,1,4)$, $(0,2,3)$

+	0	1	4
0	0	1	4
1	1	2	0
4	4	0	3

.NO

+	0	2	3
0	0	2	3
2	2	4	0
3	3	0	1

no

Exp:- 2:-
set of Integer with subtraction.

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} A & H \\ [illegible] & 1 \end{bmatrix}$$

A.B [illegible] 3 B.A = 4

7 7

Exp:- $G = \{1, -1, i, -i\}$, is multiplication.
$H = \{1, -1\}$ is a subgroup of G the right cosets are —
$H(1) = \{1 \cdot 1, (-1) \cdot 1\} = \{1, -1\}$
$H(-1) = \{1 \cdot (-1), (-1) \cdot (-1)\} = \{-1, 1\}$
$H(i) = \{i, -i\}$
$H(-i) = \{-i, i\}$

Group Homomorphism and Group Isomorphism:

Let $(G, *)$ and $(G', \odot)$ be two groups. A mapping ~~from~~ $f : G \to G'$ is called group homomorphism from $(G, *)$ to $(G', \odot)$ if for any $(x_1, x_2) \in G$, we have $f(x_1 * x_2) = f(x_1) \odot f(x_2)$.

A group homomorphism is called a monomorphism if the mapping is one to one.

A group homomorphism is called epimorphism if the mapping is onto.

A group homomorphism is called isomorphism if the mapping is one to one and onto.

Exp: ① $(I, +)$, $(2I, +)$ are isomorphic or not (Yes)

$\quad G \qquad\quad G'$

$f : G \to G'$ $\cancel{f(x)}\ 2(x)$.

Ans:- $f(a+b) = 2(a+b)$

$= 2a + 2b$

$= f(a) + f(b)$

f is also one to one and onto so isomorphic.

Exp: ② $(G, +)$, $(G^+, \cdot)$ G real numbers.

$f \to G \to G^+$ $f(x) = 2^x$.

is Homomorphism or not

$f(a+b) = 2^{a+b}$

$= 2^a \cdot 2^b$

$= f(a) \cdot f(b)$

so it is homomorphism.

Exp (3): $f: R^* \to R^*$

$f(x) = x^2$

$f(ab) = (ab)^2$

$= a^2 \cdot b^2$

$= f(a) \cdot f(b)$

Exp (4): $f \quad \underset{G}{(I,+)} \quad \underset{G'}{(I,+)}$

$f: G \to G' = f(x) = a^x$

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

$= a^m \cdot a^n$

$= f(m) \cdot f(n)$

so homomorphism.