Date 20/12/23

UNIT ⇒ IV

Binary operation on a set :-

Let 'G' be a non-empty set. Then $G \times G = \{a, b\}: a \in G, b \in G\}$.

If o (operation) : $G \times G \to G$ then 'o' is said to be a binary operation on the set 'G'. Then image of ordered pair (a, b) under the function 'o' is denoted by aob. Often we use symbols $+, \times, \cdot, o, *, \oplus, \cup, \cap, \wedge, \vee$ etc to denote binary operations on a set.

Thus '+' will be a binary operations on 'G' iff $a+b \in G, \forall a, b \in G$ and $a+b$ is unique.

A binary operation on a set 'G' is some times also called a Binary Composition in this set 'G'.

If '*' is a binary operation in 'G', then $a*b \in G, \forall a, b \in G$. Therefore G is closed with respect to composition denoted by '$*$'.

Example.

① Addition '+' is a binary operation on the set N of natural numbers. The some of two natural no. is also a natural number. ~~Therf~~ Therefore N is closed with respect to addition i.e. $a+b \in N, \forall a, b \in N$.
This operation of addition is binary over the sets I, Q, R and C also.

② The usual operation of subtraction '$-$' is a binary operation over the set I, Q, R and C but it is not binary in N because
$6-9=-3 \notin N$ whereas $6 \in N$, $9 \in N$.
Thus N is not closed with respected to subtraction.

Algebraic Structurs :-

A non-empty set G equipped with 1 or more binary operation is called an algebric structure.
Let symbals $*, +, \cdot, o, \oplus, \cup, \cap, \wedge, \vee$ etc denote binary operation on a set 'G'. Then $(G,*)$, $(G,\oplus)$, $(G,*,o,\wedge,\vee)$ etc are algebric structures.
Example:-
$(N,+)$, $(I,+)$, $(I,-)$, $(R,+)$ are all algebric structure. Addition $(+)$ and multiplication $(\cdot)$ are both binary operations on the set R of real numbers. Therefore $(R,+,\cdot)$ is an algebric structure, equiped with two operations.

21/12/23

Types of Algebric structure:→

Semi-Group:-

Let 'G' be a non-empty set and $*$ be a binary operation on $(G,*)$ is said to be semi group of the operation $*$ is associative.

OR

$(G,*)$ is a semi group, if

(i) $x*y \in G, \forall x,y \in G$ (closure)

(ii) $(x*y)*z = x*(y*z), \forall x,y,z \in G$ (Associative)

Identity Element :→

Let $*$ be a binary operation on a non-empty set G. An element $e \in G$ is said to be an identity element for the operation $*$, If $a*e = e*a = a, \forall a \in G$

$G = \{0,1,2,3,4,5\}$

$(G,+)$

$G = \{$

Monoid :→

A Semigroup $(M,*)$ with an identity element with the operation $*$ is called monoid.

OR

An algebric structure $(M,*)$ is called a monoid, if -

(i) $x*y \in M \; \forall x,y \in M$

(ii) $(x*y)*z = x*(y*z) \; \forall x,y,z \in M$

Example:→

Ex- $(I, \times)$ is a monoid.

$(-7) \times (+7) = -49 \in I, -7 \in I, 7 \in I$

$(2\times3)\times5 = 2\times(3\times5), 2, 3, 5 \in I$

$e = 1 \in I$

Group :-

An algebric structure $(G, *)$ where G is a non-empty set and $*$ is a binary operation define on G, is called a group, if the binary operation $*$ satisfied the following properties:

(i) Closure Property :→

If $a \in G, b \in G$ then $a*b \in G \; \forall a, b \in G$

(ii) Existence of Identity :-

If a, There exist an element $e \in G$

$\therefore a*e = e*a = a \; \forall a \in G$

The element e is called identity element

(iii) Associative Property :→

If $a, b, c \in G$ then $(a*b)*c = a*(b*c), \forall a, b, c \in G$

(iv) Existence of Inverse :→

For each element $a \in G$, there exists an element of G called the inverse of 'a' denoted and denoted by a^{-1} such that

$a \to a^{-1} = a^{-1} * a = e$, where $e \in I$

$G = [(-\infty, \infty), +]$

$e = 0$ | $1 \in G$

$2.5 \in G$

$\cancel{e=}(G\{(-\infty,\infty), \times)$

$e = 1$

$a = 2, a^{-1} = 1/2 \in R$

A group with addition binary operation is known ~~as~~ additive and that with multiplication with binary operation is known as multiplicative group.

Abelian group :-

A group $(G, *)$ is said to be abelian or commuatative if in addition to four group property. The following property is also satisfied.

(V) Commutative property :-

The primary operation $*$ is commutative in 'G' i.e,

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

An abelian group under addition is sometime called "Module". A group which is not abelian is called non-abelian.

Q: Prepare the composition table for multiplication table on the element in the set $A = \{1, \omega, \omega^2\}$, where ω is the cube root of unity. Show that multiplication satisfied the closure property, Associative law, commutative law, and 1 is the identity element write down the multiplicative inverse of each element.

Sol: Since ω is a cube root of unity, i.e. $\omega = \sqrt[3]{1}$

Therefore $\omega^3 = 1$

we can operate on various elements and prepare the composition table as below –

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

If $x^2 = 1$ then $x = \pm 1$

If $x^3 = 1$ then $x = 1, \omega, \omega^2$

$\{\because \omega^4 = \omega \times \omega^3 = \omega$

from the composition table we can conclude that

(i) Closure Property:- Since all the entries in the composition table are in A so closure property is satisfied.

(ii) Associative law:-
$(x \times y) \times z = x \times (y \times z)$ $\forall$ $x, y, z \in A$

eg:- $1, \omega, \omega^2 \in A$

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

(iii) Commutative law:-
$x \times y = y \times x$, $\forall$ $x, y \in A$

From the composition table table, it is clear that element in each row are the same as elements in the corresponding column so that $x \times y = y \times x$

(iv) <u>Identity element :-</u>

$1 \in A$ is the identity element

$x \times 1 = 1 \times x = x \ \forall \ x \in A$

It can be seen from the first row and first column of the composition table.

(v) <u>Inverse :-</u>

Clearly $(1)^{-1} = 1$, $\omega^{-1} = \omega^2$, $(\omega^2)^{-1} = \omega$

$\left\{ \begin{array}{l} a \times a^{-1} = e \\ \omega \times \omega^2 = 1 \end{array} \right.$

Q) Prove that the 4th root of unity $1, -1, i, -i$ from an abelian multiplication group.

<u>Sol</u>:- Let $G = \{1, -1, i, -i\}$

we from the composition table

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\{ \because i^2 = -1$

If $x^2 = 1$, then $x = \pm 1$
If $x^3 = 1$, then $x = 1, \omega, \omega^2$
If $x^4 = 1$, then $x = 1, -1, i, -i$

(i) Closure property :- Since all the entries in the composition table are the element of G and hence G is closed with respect to multiplication.

(ii) Associative property :-

$$(a \times b) \times c = a \times (b \times c), \forall a, b, c \in G$$

for example-

$$1, -1, i \in G$$

$$[1 \times (-1)] \times i = -i = 1 \times [(-1) \times i]$$

(iii) Existence of Identity :-

~~EX~~ $1 \in G$ is identity element as

$$a \times 1 = 1 \times a = a, \forall a \in G$$

~~It~~ Can be seen from the first row & first column of the composition table.

(iv). Existence of Inverse :-

$$\because 1 \times 1 = 1$$

$$(-1) \times (-1) = i \times (-i) = (-i) \times i,$$

the inverse of $1, -1, i, -i$ are $1, -1, -i, i$ respectively and all those belong to G.

(v). Commutative law :-

$$a \times b = b \times a, \forall a, b \in G$$

From the composition table it is clear that element in each row are the same as elements in the corresponding column so that $a \times b = b \times a$

Hence, it follows that G is an abelian multiplication group.

Proved

Show that set $Z_6 = \{0, 1, 2, 3, 4, 5\}$ forms a group with respect to addition modulo 6.

Sol: Here, $Z_6 = \{0, 1, 2, 3, 4, 5\}$

The operation addition modulo 6 is denoted by '$+_6$' we can operate $+_6$ on the element in Z_6 and prepare the composition table as.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\{\because a +_6 b = r\}$
For $0 = 6 \times 0 + 0$
For $1 = 6 \times 0 + 1$
For $6 = 6 \times 1 + 0$

Since all the entries in the composition table are the element of Z_6 and Z_6 is closed with respect to $+_6$.

(ii) Associative law:-

$$(a +_6 b) +_6 c = a +_6 (b +_6 c), \ \forall a, b, c \in Z_6$$

For example-

$$1, 2, 3 \in Z_6$$
$$(1 +_6 2) +_6 3 = 3 +_6 3 = 0$$
$$1 +_6 (2 +_6 3) = 1 +_6 5 = 0$$
$$\therefore (1 +_6 2) +_6 3 = 1 +_6 (2 +_6 3)$$

(iii) Existence of Identity :-

$0 \in Z_6$ is identity element as

$a +_6 0 = 0 +_6 a = a \quad \forall \; a \in Z_6$

In can be seen from the first row and first column of the composition table.

(iv) Existence of Inverse :-

Since, $0 +_6 0 = 0$, $1 +_6 5 = 0$, $2 +_6 4 = 0$

$3 +_6 3 = 0$, $4 +_6 2 = 0$, $5 +_6 1 = 0$

The inverse of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively and all those belong to Z_6

Hence it follow that Z_6 is a group with respect to $+_6$.

2021

Q2 Show that set of all integers Z from a group w.r.t binary operation $*$ defined as $a * b = a + b + 1$, where $a, b \in Z$

Sol:- ① Closure property :-

If $a, b \in Z$ then

$a * b = a + b + 1 \in Z \;\forall\; a, b \in Z$

therefore Z is closed w.r.t binary operation $*$.

$$\left\{ \begin{aligned} Z &= [-\infty, \infty] \\ &= -\infty \cdots -3, -2, -1, 0, 1, 2, \cdots \infty \\ 2 * (-3) &= 2 + (-3) + 1 \\ &= 0 \in Z \end{aligned} \right\}$$

② Associative law :-

If $a, b, c \in Z$ then

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

Evergreen
Page No.
Date: / /20

$= (a+b+c+2)$

and $a*(b*c) = a*(b+c+1) = a+(b+c+1)+1$
$= a+b+c+2$

$\therefore (a*b)*c = a*(b*c), \forall a,b,c \in Z$

③ Existence of Identity :-
$e \in Z$ will be the identity

if
$a*e = e*a = a, \forall a \in Z$

Now,
$a*e = a$
$\Rightarrow a+e+1 = a$
$\Rightarrow e = -1$

and $e*a = a$
$\Rightarrow e+a+1 = a$
$\Rightarrow e = -1$
$\therefore e = -1 \in Z$ is identity element.

④ Existence of Inverse :-
If $a \in Z$ then $a^{-1} \in Z$
will be the inverse of a if
$a*a^{-1} = a^{-1}*a = e$

Now,
$a*a^{-1} = e$
$\Rightarrow a+a^{-1}+1 = -1$
$\Rightarrow a^{-1} = -2-a$

and $a^{-1}*a = e$
$\Rightarrow a^{-1}+a+1 = -1$
$\Rightarrow a^{-1} = -2-a$

$\therefore a^{-1} = -2-a \in Z$ is the inverse of a.

$Z = -\infty \cdots -3,-2,-1,0,1,2,3 \cdots$
$a^{-1} = -2-(-3)$
$= -2+3$
$= 1 \in Z$

Hence set of all integers Z is a group w.r.t. given binary operation '*'.

01/02/2024

Page No.
Date: / /20

Q3 Prove that Set $G = \{1, 2, 3, 4, 5, 6\}$ forms an abilian group with respect to multiplication modulo 7.

Sol: Here $G = \{1, 2, 3, 4, 5, 6\}$ the operation multiplication modulo 7 is denoted by $*_7$. We can operate $*_7$ on the elements in G and prepare the composition table as –

$*_7$	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

(i) **Closure property:-**

Since all the entries in the ~~mult~~ composition table are the element of G ~~and~~

Hence G is closed with respect to $*_7$.

(ii) **Associative law:-**

$(a *_7 b) *_7 c = \cancel{a *_7} (b \times_7 c), \forall a, b \in G.$

For ex-

$1, 2, 3 \in G$

$(1 \times_7 2) \times_7 3 \Rightarrow 2 \times_7 3$

$= 6$

$1 \times_7 (2 \times_7 3) = 1 \times_7 6$

$= 6$

Evergreen
Page No.
Date : / /20

(iii) **Existence of Identity :-**

~~$1 \times_7 1 = 1,\ 2 \times_7 6$~~

$1 \in G$ is identity element as-

$a \times_7 1 = 1 \times_7 a = a,\ \forall\ a \in G$

it can be seen from the first row and first column of the composition table.

(iv) **Existence of Inverse :-**

Since
$$1 \times_7 1 = 1$$
$$2 \times_7 4 = 1$$
$$3 \times_7 5 = 1$$
$$4 \times_7 2 = 1$$
$$5 \times_7 3 = 1$$
$$6 \times_7 6 = 1$$

The inverse of 1, 2, 3, 4, 5, 6 are 1, 4, 5, 2, 3, 6 respectively and all those belong to G.

(v) **Commutative law :-**

$$a \times_7 b = b \times_7 a,\ \forall\ a, b \in G$$

For ex-

$4, 5 \in G$

Now,

$4 \times_7 5 = 6 \Rightarrow 5 \times_7 4 \Rightarrow 6$

Hence it follow that G is an abelian group with respect to $\times_7$.

Date 02/01/2024

Property of group :-

Q→ If $(G, *)$ is a group and a, b, c are in G, then prove that.

(i) $a*b = a*c \Rightarrow b = c$ (Left cancellation law)

(ii) $b*a = c*a \Rightarrow b = c$ (Right cancellation law)

Sol:→ If $a \in G$, then there exist $a^{-1} \in G$ such that $a*a^{-1} = a^{-1}*a = e$, where e is the identity element.

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

$a^{-1}*(a*b) = a^{-1}(a*b) = a^{-1}(a*c)$ {operate both side a^{-1} on the left side with $*$}

$\Rightarrow (a^{-1}*a)*b = (a^{-1}*a)*c$ {by Associative law}

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

$\Rightarrow \boxed{b = c}$ {$\because$ e is identity element}

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

$\Rightarrow (b*a)a^{-1} = (c*a)*a^{-1}$ {operate both side a^{-1} on the right side with $*$}

$\Rightarrow b*(a*a^{-1}) = c*(a*a^{-1})$ {by Associative law}

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

$\Rightarrow \boxed{b = c}$

Q→ In a group $(G, *)$, prove that (i) $(a^{-1})^{-1} = a$ or the inverse of the inverse of an element is equal to the element.

(ii) $(a*b)^{-1} = b^{-1}*a^{-1}$ OR The inverse of the product of two elements is the product of the ~~to~~ inverse in the reverse order.

Evergreen
Page No.
Date: / /20

Sol→ (i) Let e be the identity element for $*$ in G.
Then we have $a * a^{-1} = e$ —(1), where $a^{-1} \in G$
Also, $(a^{-1})^{-1} * a^{-1} = e$ —(2)
from eqn (1) & (2), we get

$$(a^{-1})^{-1} * a^{-1} = a * a^{-1}$$
$\boxed{(a^{-1})^{-1} = a}$ { by right cancellation law }

(ii) Since G is a group for $*$ and let $a, b \in G$, then
$a * b \in G$ { By closure property }
Therefore, $(a*b)^{-1} * (a*b) = e$ —(1)
Let a^{-1} and b^{-1} be the inverse of a and b respectively, then $a^{-1}, b^{-1} \in G$
Now,
$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$$ { by Associative law }

$= b^{-1} * (e * b)$ { $\because a^{-1} * a = e$ }
$= b^{-1} * b$ { $\because e * b = b$ }
$\Rightarrow (b^{-1} * a^{-1}) * (a * b) = e$ —(2)
from (1) and (2), we get
$\boxed{(a * b)^{-1} = b^{-1} * a^{-1}}$ { By right cancellation law }

Q3 Show that if a, b are arbitrary element of a group $(G, \cdot)$, then $(a \cdot b)^2 = a^2 \cdot b^2$ iff G is abelian.

Sol→ Here, a and b are arbitrary element of a group $(G, \cdot)$
Let $(a \cdot b)^2 = a^2 \cdot b^2$ then we have to prove that G is abelian.

Now,

$$(a \cdot b)^2 = a^2 \cdot b^2$$

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

$\Rightarrow a \cdot (b \cdot a) \cdot b = a \cdot (a \cdot b) \cdot b$ {By Associative law}

$\Rightarrow (b \cdot a) \cdot b = (a \cdot b) \cdot b$ {by left cancellation law}

$\Rightarrow b \cdot a = a \cdot b$ {By right cancellation law}

Hence G is abelian.

Conversely :-

Let G is abelian then we have to show that $(a \cdot b)^2 = a^2 \cdot b^2$

Since G is abelian, therefore

$$a \cdot b = b \cdot a, \forall a, b \in G$$

Now,

$(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b)$

$= a \cdot (b \cdot a) \cdot b$ {By Associative law}

$= a \cdot (a \cdot b) \cdot b$ {$\because b \cdot a = a \cdot b$}

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

$(a \cdot b)^2 = a^2 \cdot b^2$

2022

Q) What do you mean by order of an element in a group?

Find the Order of each element of the multiplicative group $g = \{1, -1, i, -i\}$

Sol:- Order of an element in a group :-

Suppose G is a group and the composition has been denoted multiplicatively. 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)

$$\Rightarrow O(a) = n$$

If there exist no positive integer n such that $a^n = e$, then we say that a is of infinite order or of zero order.

We shall use the symbol $o(a)$ to denote the order of a.

Now,

we will find the order of each element of the given multiplicative group.

Since 1 is the identity element. Therefore,

$(1)^1 = 1 = e$

$\boxed{o(1) = 1}$

Now,

$(-1) = -1$

$(-1)^2 = 1 = e$

$\therefore \boxed{o(-1) = 2}$

Again,

$(i) = i$

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

$(i)^3 = i^3 = i^2 . i = (-1).i = -i$

$(i)^4 = i^4 = i^2 . i^2 = (-1).(-1) = 1 = e$

$\therefore \boxed{o(i) = 4}$

Finally,

$(-i)^1 = -i$

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

$(-i)^3 = -i^3 = -i^2 . i = -(-1).i$
$= i$

$(-i)^4 = i^4 = i^2 . i^2 = (-1).(-1) = 1$
$= e$

$\therefore \boxed{o(-i) = 4}$

2021

Q. Find the order of each element in the group $(\{1,-1\},\cdot)$

Sol: We form the composition table as:

$\cdot$	1	-1
1	1	-1
-1	-1	1

From the composition table '1' is the identity element.

Now,

$(1)^1 = 1 = e$

$\therefore o(1) = 1$

and $(-1)^1 = -1$

$(-1)^2 = 1 = e$

$\therefore \boxed{o(-1) = 2}$

Q. Prove that the identity element in a group is unique.

Sol: Suppose e and e' are two identity element of a group $(G, *)$.

We have,

$e * e' = e$ —①, if e' is identity.

and $e * e' = e'$ —②, if e is identity

from eqn ① & ②, we get

$e = e'$

Hence the identity element is unique.

2020

Q. Prove that the inverse of every element of a group is unique.

Sol:- Let a be any element of a group $(G,*)$. and let e be the identity element. Supose b and c are two inverses of a, i.e.

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

and $a*c = c*a = e$

Now,

$$a*c = e$$

$\Rightarrow b*(a*c) = b*e$ {operate both side b on the left with * }

$\Rightarrow b*(a*c) = b$ — ① {∵ e is identity element}

and

$$b*a = e$$

$\Rightarrow (b*a)*c = e*c$ {operate both side c on the right with * }

$(b*a)*c = c$

$b*(a*c) = c$ — ② { by associative law }

from eqn ① & ②, we get

$$\boxed{b = c}$$

Hence the inverse of every element of a group is unique.

Q3 Find the order of every element in the multiplicative group $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$

Sol:- The identity element of the given group is $a^6 = e$.

Now,

$$(a)^1 = a$$
$$(a)^2 = a^2$$
$$(a)^3 = a^3$$

Date 05/01/2024

$(a)^4 = a^4$

$(a)^5 = a^5$

$(a)^6 = a^6 = e$

$\therefore \boxed{o(a) = 6}$

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

$(a^2)^2 = a^4$

$(a^2)^3 = a^6 = e$

$\therefore \boxed{o(a^2) = 3}$

$(a^3)^1 = a^3$

$(a^3)^2 = a^6 = e$

$\therefore \boxed{o(a^3) = 2}$

$(a^4)^1 = a^4$

$(a^4)^2 = a^8 = a^6 \cdot a^2 = e \cdot a^2 = a^2$

$(a^4)^3 = a^{12} = a^6 \cdot a^6 = e \cdot e = e$

$\boxed{o(a^4) = 3}$

$(a^5)^1 = a^5$

$(a^5)^2 = a^{10}$

$(a^5)^3 = a^{15}$

$(a^5)^4 = a^{20}$

$(a^5)^5 = a^{25}$

$(a^5)^6 = a^{30} = (a^6)^5 = (e)^5 = e$

$\therefore \boxed{o(a^5) = 6}$

$(a^6)^1 = a^6 = e$

$\therefore \boxed{o(a^6) = 1}$

2020 Q.3 Show
$G =$
to a
Sol:
(i) closu
$x =$
Now,
Ther
Thus
(ii) Associ
real
numb
(a
(iii) Exist
is
(a+
and
$\therefore$ (a+
Thus o

Page No.
Date: / /20

2020

Q. Show that Set :
$G = \{a + \sqrt{2}b : a, b \in Q\}$ is a group with respect to addition.

$\frac{p}{q}$ rational no.
$q \neq 0$

Sol :-
(i) closure property :-
Let $x, y \in G$. Then
$x = a + \sqrt{2}b$, $y = c + \sqrt{2}d$, where $a, b, c, d \in Q$

Now,
$$x + y = (a + \sqrt{2}b) + (c + \sqrt{2}d)$$
$$= (a + c) + (b + d)\sqrt{2} \in G \quad \{\because a + c \in Q \ \& \ b + d \in Q\}$$

Therefore $x + y \in G$
Thus G is closed with respect to addition

(ii) Associative law :-
The elements of G are all real number's and the addition of real number is associative.
$$(a + b) + c = a + (b + c), \ \forall a, b, c \in R$$

(iii) Existence of identity :-
$0 + 0\sqrt{2} \in G \ \{\because 0 \in Q\}$
is identity element as
$$(a + \sqrt{2}b) + (0 + \sqrt{2}) = (a + 0) + (b + 0)\sqrt{2}$$
$$= a + b\sqrt{2}$$
and $(0 + 0\sqrt{2}) + (a + \sqrt{2}b) = (0 + a) + (0 + b)\sqrt{2}$
$$= a + b\sqrt{2}$$
$\therefore (a + \sqrt{2}b) + (0 + 0\sqrt{2}) = (0 + 0\sqrt{2}) + (a + \sqrt{2}b)$
$= a + b\sqrt{2}, \ \forall a + \sqrt{2}b \in G$

Thus $0 + 0\sqrt{2}$ is the identity element.

Date 09/01/24

Existence of Inverse :-

$$a+\sqrt{2}\,b \in G$$

$$\Rightarrow (-a) + \sqrt{2}(-b) \in G \quad \left\{ \begin{array}{l} \because a, b \in Q \\ \therefore -a, -b \in Q \end{array} \right.$$

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

and $[(-a) + \sqrt{2}(-b)] + [a+\sqrt{2}\,b] = (-\cancel{a}+\cancel{a}) + (-\cancel{b}+\cancel{b})\sqrt{2}$

$\therefore (-a) + \sqrt{2}(-b)$ is the inverse of $a+\sqrt{2}b$.
Hence G is a group with respect to addition.

Subgroup :-

A non-empty subset H of a group G is said to be a subgroup of G if the composition in G is also a composition in H and for this composition H itself is a group. Now every set is subset of itself. There fore if G is a group then G itself is a subgroup of G. Also if e is the identity of G then the subset of G containing only one element, that is e is also a sub group of G. These two G and $\{e\}$ are sub groups of any group. They are called trival or Improper Sub groups. A Sub group other than these two is called non-trival or proper subgroups.

Exampl-

Let $G = \{1, -1, i, -i\}, \cdot\}$ is a group.
~~w.r.f the composition table~~

$$H \subset G$$

i.e, $H = \{1, -1\}$ as

we form the composition table.

$\cdot$	1	-1
1	1	-1
-1	-1	1

Since all the properties of group are satisfied therefore H itself a group.
Hence H is a Subgroup of G with respect to multiplication.

Q) Prove that the necessary and sufficent condition for a non-empty subset H of a group $(G, *)$ to be a subgroup is:
$a \in H,\ b \in H \Rightarrow a * b^{-1} \in H$, where b^{-1} is the inverse of b in G.

Sol. The condition is necessary :-

~~The condition~~

Supose H is a subgroup of G.
Let $a \in H,\ b \in H$
Now, each element of H must possess inverse because H itself is a group.
$\therefore b \in H \Rightarrow b^{-1} \in H$
Further, H must be closed with respect to $*$, i.e. the composition in G.
Therefore, $a \in H,\ b^{-1} \in H \Rightarrow a * b^{-1} \in H$

The condition is sufficient :-

Now, It is given that $a \in H, b \in H \Rightarrow a * b^{-1} \in H$
we have to prove that H is a subgroup of G.

Page No.
Date : / /20

Existence of Identity :-

we have

$a \in H, a \in H \Rightarrow a * a^{-1} \in H$ {By the given Condition}

$\Rightarrow e \in H$

Thus the ~~...~~ identity e is an element of H.

Existence of Inverse :-

Let $a \in H$

Now, $e \in H, a \in H \Rightarrow e * a^{-1} \in H$ {By given condition}

$\Rightarrow a^{-1} \in H$

Thus each element of H possesses inverse.

Closure Property :-

Let $a, b \in H$. Then as shown above $b \in H \Rightarrow b^{-1} \in H$

Now, $a \in H, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H$ {By the given condition}

$= a * b \in H$

Therefore H is closed with respect to $*$ in G.

Associative law :-

The element of H are also the element of G. The composition in G is Associative therefore it must also be associative in H.

Hence H itself is a group for the composition in G.

Therefore H is a subgroup of G.

Cyclic group :-

A group G is called cyclic if there is an element $a \in G$ such that

$$G = \{a^n : n \in Z\}$$

i.e.,

Every element of G is of the form a^n where n is sum integer
Here, The element a is called genrator of G and it is denoted as $G = \{a\}$ or $G = (a)$

Ex-1 - The multiplicative group $G = \{1, \omega, \omega^2)$ is cyclic with genrator ω.

As $(\omega)^3 = \omega^3 = 1$ $\{\because \omega^3 = 1\}$

$(\omega)^1 = \omega$

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

Hence every element of G can be expresed as sum integral power of ω.

Also, ω^2 is a genrator of G.

As $(\omega^2)^3 = \omega^6 = \omega^3 \cdot \omega^3 = 1 \cdot 1 = 1$

$(\omega^2)^2 = \omega^3 \cdot \omega = 1 \cdot \omega = \omega$

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

Example-2 - The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic with genrator i.

As $(i)^4 = i^4 = i^2 \cdot i^2 = (-1) \cdot (-1) = 1$ $\{\because i^2 = -1\}$

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

$(i)^1 = i$

$(i)^3 = i^2 \cdot i = -i$

Hence every element of the given group can be expressed as some integral power of i.

Also; $(-i)$ is a genrator of G

As $(-i)^4 = i^4 = 1$

$(-i)^2 = -1$

$(-i)^3 = -i^3 = -i^2 \cdot i = -(-1) \cdot i = i$

10/1/24 $(-i)^1 = 1$

2021

Ques What is the generator of Cyclic-group.

Soln: Generator of Cyclic group:

A group G is called cyclic if there is an element $a \in G$ such that

$G = \{a^n : n \in Z\}$

i.e, Every element of G is of the form of a^n, where n is sum intiger.

Here, ~~The element of G is of the form~~ a^n

The element of a is called genrator of G and it is denoted as $G = \{a\}$ or $G = (a)$

→ Properties of cyclic group:

Q Prove that every cyclic group is abelian

Soln Let $G = \{a\}$ be a cyclic group genrated by a.

Let x, y be any two elements of G. So, there must exist integers r and s such that -

Thus. $x = a^r \quad , \quad y = a^s$

$$x \cdot y = \cancel{y \cdot x}\ a^r \cdot a^s$$
$$= a^{r+s}$$
$$= a^{s+r}$$
$$= a^s \cdot a^r$$
$$x \cdot y = y \cdot x \ \forall\ x, y \in G$$

$\therefore$ G is an abelian group.

Ques If a is a generator of G then prove that a^{-1} is also a generator of G, where a^{-1} is the inverse of a in G.

Soln: Cyclic group defination:

Let $G = [a]$ be a cyclic ~~by a~~ group generated by a.
Let x be any arbitrary element of G.
So, there must exist integer ~~are~~ r such that $x = a^r$
$\Rightarrow x = (a^{-1})^{-r}$, where $-r$ is also an integer

$\Rightarrow a^{-1}$ is also a generator of G, where a^{-1} is the inverse of a in G.

Ques 2022 Show that $G = [0, 1, 2, 3, 4]$ is a cyclic group under addition modulo 5.

Soln We see that –
$(1)^1 = 1$
$(1)^2 = (1)^1 +_5 (1)^1$

Evergreen Page No. Date: / /20

5)2(0 2 ... 5)3(1 ...

$= 1 +_5 1$

$\boxed{(1)^2 = 2}$

$\Rightarrow (1)^3 = (1)^2 +_5 (1)^1$

$= 2 +_5 1$

$\boxed{(1)^3 = 3}$

$\Rightarrow (1)^4 = (1)^3 +_5 (1)^4$

$= 3 +_5 1$

$\boxed{(1)^4 = 4}$

$\Rightarrow (1)^5 = (1)^4 +_5 (1)^1$

$= 4 +_5 1$

$\boxed{(1)^5 = 0}$

Thus, $G = \{(1)^5, (1)^1, (1)^2, (1)^3, (1)^4\}$

Hence, G is a cyclic group and 1 is a generator.

Similarly,

4 is also a genrator.

As $(4)^1 = 4$

$(4)^2 = (4)^1 +_5 (4)^1$

$= 4 +_5 4$

$\boxed{(4)^2 = 3}$

$(4)^3 = (4)^2 +_5 (4)^1$

$= 3 +_5 4$

$= 4$

$\boxed{(4)^3 = 2}$

$(4)^4 = (4)^2 +_5 (4)^2$

$= 3 +_5 3$

$\boxed{(4)^4 = 1}$

$(4)^5 = (4)^4 +_5 (4)^1$
$= 1 +_5 4$
$\boxed{(4)^5 = 0}$

Hence, $G = \{0, 1, 2, 3, 4\}$ is a cyclic group under addition module 5 with generators 1 and 4.

Q→ Show that $G = \{1, 2, 3, 4, 5, 6\}$ is a cyclic group where multiplication modulo 7.

Sol→ We see that $(3)^1 = 3$

$(3)^2 = (3)^1 \times_7 (3)^1$
$= 3 \times_7 3$
$= (3)^2 = 2$
$(3)^3 = (3)^2 \times_7 (3)^1$
$= 2 \times_7 3$
$= (3)^3 = 5$
$(3)^4 = (3)^3 \times_7 (3)^1$
$= 6 \times_7 3$

$(3)^4 = 4$
$(3)^5 = (3)^4 \times (3)^1$
$= 4 \times_7 3$
$= (3)^5 = 5$
$(3)^6 = 3^5 \times (3)^1$
$(3)^6 = 1$

∴ G is a cyclic group with genrator and similarly 5 is also a generator.

MPTL

As $(5)^1 = 5$

$(5)^2 = (5)^1 \times_7 (5)^1$

$= 5 \times_7 5$

$(5)^2 = 4$

$(5)^3 = (5)^2 \times_7 (5)^1$

$= 4 \times_7 5$

$= (5)^3 = 6$

$(5)^4 = (5)^3 \times_7 (5)^1$

$= 6 \times_7 5$

$= 2$

$(5)^5 = 5^4 \times_7 (5)^1$

$= 2 \times_7 (5)^1$

$= 2 \times_7 5$

$= 3$

$(5)^6 = 5^5 \times_7 (5)^1$

$= 3 \times_7 (5)^1$

$= 3 \times_7 5$

$= 1$

Since, $G = \{1, 2, 3, 4, 5, 6\}$ is a cyclic group under multiplication modulo 7 with genrator 3 & 5.

Q> In a group (G, o), a is an element of order 30.
Find the order of a^5.

Sol:- It is given that $O(a) = 30$

$= a^{30} = a^n = e$ —— (1), where e is an identity element.

let $O(a^5) = n$

$\Rightarrow (a^5)^n = e$

$\Rightarrow a^{5n} = e$ —— (2), where n is the last fasitive integer.

from eqn 1 and 2

$$a^{5n} = a^{30}$$

$$5n = 30$$

$$\boxed{n = 6}$$

$$\boxed{O(a^5) = 6}$$

Cosets :-

Suppose G is a group and H is any subgroup of G. Let a be any element of G.

Then the set $Ha = \{ha : h \in H\}$ is called a right cost of H ~~in~~ G genrated by a.

Similarly, the set $aH = \{ah : h \in H\}$ is called left coset of H ~~is~~ in G genrated by a.

If e is the identity element of G, then $e \in H$ and $He = eH = H$.
Theryare H itself is a right coset as well as a left coset.

Example :-
let $[G = \{----, -3, -2, -1, 0, 1, 2, 3, ---\}, +]$ be a group and $[H = \{----, -15, -10, -5, 0, 5, 10, 15, ---\}, +]$ be a subgroup of $(G, +)$.

we from the set.

$1 + H = \{---, -14, -9, -4, 1, 6, 11, 16, ---\} = H_1$

$2 + H = \{---, -13, -8, -3, 2, 7, 12, 17, ---\} = H_2$

$3 + H = \{----, -12, -7, -2, 3, 8, 13, 18, ---\} = H_3$

$4 + H = \{----, -11, -6, -1, 4, 9, 14, 19, ----\} = H_4$

$5+H = \{ ----, -10, -5, 0, 5, 10, 15, 20 ---- \} = H_5 = H$
$6+H = \{ -----, -9, -4, 1, 6, 11, 16, 21, --- \} = H_6 = H_1$

The Sets 1+H, 2+H, 3+H, 4+H, 5+H, 6+H, and so on are left cosets of H in G. Similarly Right cosets H+1, H+2, H+3, ---- May be formed.
Furthure, we observed that in 1+H, 2+H, 3+H, 4+H, 5+H, 6+H, ----, The sets are either disjoint or identical.
Also it may be observe that union of disjoint cosets is the group G.

For example ⇒
If $G = \{ ---, -3, -2, -1, 0, 1, 2, 3 --- \}(G, +)$ is a group. and $H = \{ ---, -6, -4, -2, 0, 2, 4, 6, --- \}$ is a subgroup of (G, +).
Then there are two disjoint cosets 1+H and 2+H.
Now,
$1+H = \{ ----, -5, -3, -1, 1, 3, 5, 7, - --- \} = H_1$
and $2+H = \{ ----, -4, -2, 0, 2, 4, 6, 8, --- \} = H_2 = H$
$\therefore (1+H) \cup (2+H) = \{ ----, -3, -2, -1, 0, 1, 2, 3 --- \}$

$\Rightarrow \boxed{(1+H) \cup (2+H) = G}$

2022

Permutation groups :→

A one-one mapping of a finite set S onto itself is called a permutation.

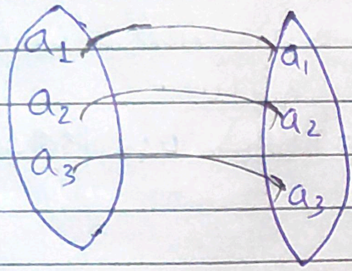
Let f : X → Y be a mapping then.
one-one mapping → distinct element of X have distinct images under f.
onto mapping → each element of Y is the image of some element of X.

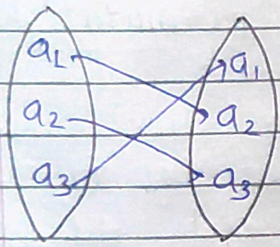
Example :→

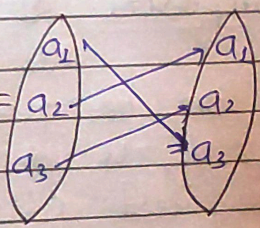
Let $S = \{a_1, a_2, a_3\}$

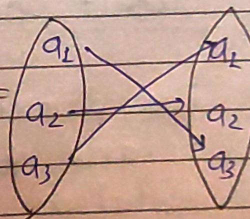
{∵ Permutation = no. of elements ?

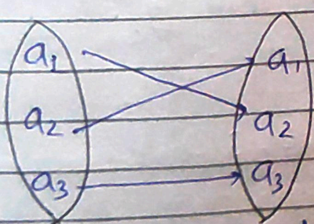
$\lfloor 3 = 3 \times 2 \times 1 = 6$

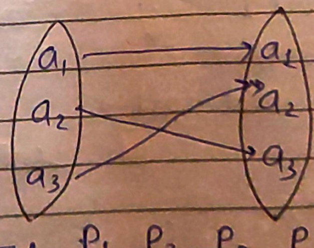
$P_1 =$


$P_2 =$


$P_3 =$


$P_4 =$


$P_5 =$


$P_6 =$


Hence, permutation are $P_1, P_2, P_3, P_4, P_5, P_6$
these written as

$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I_S$, $P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

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

$$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Thus, if $S = \{a_1, a_2, a_3, \cdots a_n)$ then in general a permutat is

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & --- & a_n \\ b_1 & b_2 & b_3 & --- & b_n \end{pmatrix}$$

where $b_1, b_2, b_3, \cdots, b_n$ are again element of S in some different value. such that $b_1 = f(a_1)$, $b_2 = f(a_2)$, $b_3 = f(a_3)$, ..., $b_n = f(a_n)$

Product or Composite of two permutations

The product or composite of two permutation f and g of degree n denoted by fg, is obtained by first carrying out the operation defined by f and then by g.

For example →, Let $S = \{1, 2, 3\}$

If

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ and } P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

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

$$\Rightarrow P_4 P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_3$$

$\left(\because a * a^{-1} = e \right)$

Evergreen
Page No.
Date : / /20

2022
Q. If $A = \{1, 2, 3, 4, 5\}$ then find:
$(1,3) \circ (2,4,5) \circ (2,3)$.

Sol. $(1,3) \circ (2\,4\,5) \circ (2,3) = \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} \right.$

$\left. \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \right] \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$

$\boxed{(1\,3) \circ (2\,4\,5) \circ (2,3) = (1\;2\;4\;5\;3)}$

Q. Find the inverse of the permutation $\longrightarrow \underline{|5} = 5 \times 4 \times 3 \times 2 \times 1 = 120$
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

Sol. Let the inverse of the given permutation
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}$

Then, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ b & c & a & e & d \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

Date 17/01/24

$\therefore a = 3, b = 1, c = 2, d = 5, e = 4$

Hence the required inverse is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

2021 **Ring :-**

Let R be a no-empty set then $(R, +, \cdot)$ is said to be a ring. If the following property are satisfied

(I) $(R, +)$ is an abelian group.

(II) $(R, \cdot)$ is a semi group (closure of Associative laws hold)

(III) Distributive laws :-

let $a, b, c \in R$

(a) Left distributive law →

$a \cdot (b + c) = a \cdot b + a \cdot c, \forall a, b, c \in R$

(b) Right distributive law-

$(a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in R$

Hence $(R, +, \cdot)$

Example.

The set of all real number is a ring with respect to addition and multiplication.

Commutative Ring ⇒

A Ring are is said to be a commutative Ring. If

$a \cdot b = b \cdot a, \forall a, b \in R$

Example -

The Set of all real numbers is a Commutative Ring with respect to addition and multiplication.

Q.) Define the Commutative Ring with unity.

Sol.) Commutative Ring with unity :-

A Ring R is said to be a commutative Ring with unity if in addition, it satisfied the following property:

$e \cdot a = a \cdot e, \forall a \in R$

Obviously e is the multiplicative identity of R.

Example ⇒

The set of all integers is a commutative Ring with unity element with respect to addition and multiplication.

Q.) Define the Characteristic of a Ring.

Characteristic of a Ring :-

Let R be a Ring with 0 (zero) element and suppose there exist a positive integer n such that

$na = a + a + \cdots$ upto n terms $= 0, \forall a \in R$.

The smallest such positive integer n is called the characteristic of the Ring.

If there exist know such positive integer, then, R is said to be characteristic 0 or ∞.

Evergreen
Page No.
Date: / /20

Example -

If $Z_6 = \{0, 1, 2, 3, 4, 5\}$, then the ring $(Z_6, +_6, \times_6)$, i.e. the Ring of intigers madulo 6 has characteristic 6 since
$6x = x+x+x+x+x+x = 0, \forall x \in Z_6$

2021. Field :->

A Ring are with atleast two elements is called a field if it,
(i) is commutative,
(ii) has unity
(iii) is such that each ~~I~~ non-zero element possess multiplicative inverse.

Example -
The set of real numbers $(R, +, \cdot)$ is a field.

2017->
Q.3 Let $A = \{1, 2, 3, 4, 5, 6\}$. Compute $(4, 1, 3, 5) \circ (5, 6, 3)$

Sol:- We have

$$(4, 1, 3, 5) \circ (5, 6, 3) = \overset{\mathrm{I}}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix}}$$

$$\circ \overset{\mathrm{II}}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix}$$

~~Ans~~ $= (1, 5, 4) \circ (2) \circ (3, 6)$

Q.3