M T W T F S S

Page No.: YOUVA

Date:

# Unit-IV

## ALGEBRAIC STRUCTURE

2 Marks and definitions | Important 2 marks

1) Group: A non empty set G, together with a binary operation * is said to be in form of group if
   i) closure: $a*b \in G$
   ii) Associative: $(a*b)*c = a*(b*c)$
   iii) Identity: $e*a = a$, $a*e = a$
   iv) Inverse: $a*a^{-1} = e$
2) Abelian group: Also satisfies commutative
3) Semigroup: Satisfies closure, Associative
4) Monoid: closure, Associative, Identity
5) order of group: The number of elements in G is called an order of group
6) Give the example of semi group which is not monoid

   Soln: $(N, +)$ not Monoid

   $(E, \circ)$
7) Give the example of Monoid which is not a group

   Soln: $(W, +)$ is a Monoid
8) Cyclic group: A group G is said to be cyclic group if, for some $a \in G$ every element of G is of the form of $a^n$, where n is some Integer the element e is called a Generator of G

   EX: $G = \{1, -1, i, -i\}$

   $\langle i \rangle = \{i^0, -i^2, -i^3, -i^4\}$

   $G = \{-i, 1, i, 1\}$

   $Z_6 = \{1^6, 1, 1^2, 1^3, 1^4$

   $Z_6 = \langle 1 \rangle$

   is a cyclic group

9) Imaginary unit:

$i^1 = i$

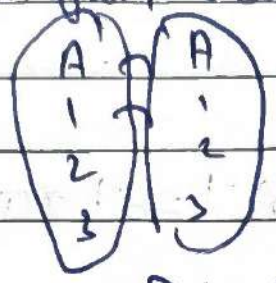
$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

10) Permutation: A bijection from a set A to itself is called a permutation

$A = \{1, 2, 3\}$




$$\left\{ \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \right\} = S_2$$

11) Permutation Group (Symmetric group): The set of all permutation of a set S with n elements form a group under composition is called the permutation group

12) Homomorphism: $f(a*b) = f(a) * f(b)$

13) Normal Group: Let H be a subgroup of the group G. Then H is said to be a normal subgroup of G, for every $x \in H$ and for $g \in G$, if $gxg^{-1} \in H$

Ex: $(H, *)$ is subgroup $(a, *)$

$H * a = a * H \in H$

$a * H = H * a$

14) Ring: An Algebraic system $(R, +, \cdot)$ is called ring if

i) $(R, +)$ is an abelian

ii) $(R, *)$ is a semigroup

iii) The operation is distributive over +

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

Types of Ring: Commutative

Ring with unit: It has identity element

Ring without zero divisors

15) Integral domain:
A Commutative Ring with identity and without zero

16) Field: A Commutative Ring with identity is a field if every non-zero element has a multiplicative inverse

17) Algebraic System: A system consisting of a set and one or more n-ary operations on the set will be called an algebraic system.

18) In a group $(G, *)$ show that $(a*b)^{-1} = b^{-1} * a^{-1} \forall a, b \in G$

Soln:

$(a*b)^{-1} = b^{-1} * a^{-1} \forall a, b \in G$

Let $a, b \in G$ and $a^{-1}, b^{-1} \in G$

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

$b * b^{-1} = b^{-1} * b = e$

Now $(a*b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$

Simply $a*b * (a*b)^{-1} = e$

Therefore $(a*b)^{-1} = b^{-1} * a^{-1}$

19) The Two properties of Group: The identity element of a group is unique
The inverse element is unique

20) Show Identity element in a group is unique:

Soln Let $(G, *)$ is a group

Let $e_1$ and $e_2$ be the identity element

$e_1 * e_2 = e_2 * e_1 = e_2$ if $e_1$ is identity

$e_1 * e_2 = e_2 * e_1 = e_1$ if $e_2$ is identity

Thus

$e_1 * e_2 = e_2 * e_1$

$e_1 = e_2$

∴ They are unique

21) Show that every element of G is self inverse then G is abelian

Ans

Let $(G, *)$ be a group

For $a, b \in G$ we have $a * b \in G$

Given $a = a^{-1}$, $b = b^{-1}$

$(a*b) = (a^{-1} * b^{-1})$

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

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

∴ They are abelian

22) Prove that the Identity element is the only idempotent element

Ans:

Let a be an idempotent element of G then $a*a = a$

Now $a \in G \Rightarrow a^{-1} \in G$

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

$\boxed{a = e}$

23) Prove $a*b = a+b-2$ for all $a, b \in Z$, then find the identity element of the group $(Z, *)$

Ans:

$a = a*e = a+e-2$

$a = a+a-2$

$e-2 = 0$

$\boxed{e = 2}$

24) Show that every cyclic group is abelian

Ans: Let $(G, *)$ be a cyclic with a as generator

$\therefore \forall x, y \in G \Rightarrow x = a^m, y = a^n \therefore x*y = a^m * a^n = a^{m+n} = a^{n+m}$

$= y*x$

$\boxed{x*y = y*x}$

Commutative is true

They are abelian

25) Prove that the Semigroup homomorphism preserves idempotents

Ans:

Let $a \in S$ be an idempotent element

$a * a = a$

$g(a*a) = g(a)$

$g(a) \circ g(a) = g(a)$

This shows that $g(a)$ is an idempotent element in $S'$

26) Homomorphism preserves identity

Ans:

Let $f:(G,*) \to (G',\Delta)$

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

$f(a*e) = f(a)$

$f(a) \Delta f(e) = f(e)$

$f(e)$ is an identity element of $G'$

i.e $f(e) = e'$

27) Find the left cosets of $\{[0],[3]\}$ in a group $(Z_6, +_6)$

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

$H = \{0\ 3\}$

$0+H = \{0,3\} = H$

$1+H = \{1,4\}$

$2+H = \{2,5\}$

$3+H = \{0,3\}$

$4+H = \{4,1\} = \{1,4\} = 1+H$

$5+H = \{5,2\} = \{2,5\} = 2+H$

$0+H$, $1+H$ and $2+H$ are three distinct left cosets of $H$.

(18)

28) Find the idempotent elements of $G = \{1, -1, i, -i\}$ under the binary operation multiplication.

Ans:

Idempotent condition $a*a = a$

$-1 \cdot -1 = 1$

$i \cdot i = i^2 = -1$

$-i \cdot -i = i^2 = -1$

but $1 \cdot 1 = 1$

The idempotent element is 1

End of Important two marks

## Part-B Important

1) Prove $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ forms an abelian under matrix

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

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

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

$$B \cdot C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = A$$

The matrix multiplication table

| X | I | A | B | C |
|---|---|---|---|---|
| I | I | A | B | C |
| A | A | I | C | B |
| B | B | C | I | A |
| C | C | B | A | I |

from the table

1) closure
2) Associative
3) Identity
4) Inverse
5) Commutative

} True ∴ They are abelian

2) Show that a non empty subset of H of a group $(G,*)$ is a subgroup of G if and only if $a*b^{-1} \in H$ for all $a,b \in H$

Soln: Let $(H,*)$ is a subgroup of $(G,*)$

TP $a,b \in H \Rightarrow a*b^{-1} \in H \forall a,b \in H$

Let $b \in H \Rightarrow b^{-1} \in H$ (∵ H is a subgroup)

Let $a,b \in H$ $a,b^{-1} \in H$

$a*b^{-1} \in H$

∴ closure

$a,b \in H$ if $\Leftrightarrow a*b^{-1} \in H$

Sufficient condition

$a,b \in H \Rightarrow a*b^{-1} \in H \forall a,b \in H$

TP $(H,*)$ is a subgroup of $(G,*)$

i) Identity

If $a \in H$, $a*a^{-1} = e \in H$

ii) Inverse

$a,e \in H$ then $a^{-1}*e = a^{-1} \in H$

iii) Closure

$a, b^{-1} \in H$ then $a*(b^{-1})^{-1} = a*b \in H$

iv) Associative:

* is always associative in all

remember!

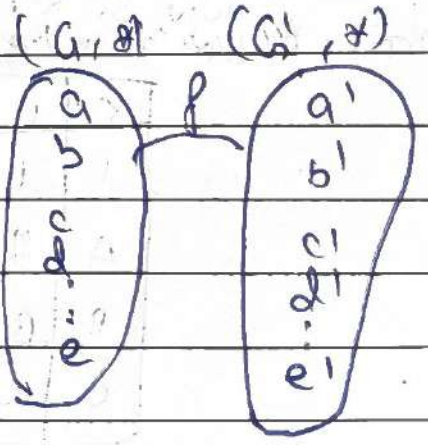
3) Prove that homomorphism preserves identity and inverse

Soln: $f:(G,*) \to (G',*)$ be a homomorphism

$f(a) = a'$

$f(b) = b'$

$f(e) = e'$



i.e $f(e) = e'$ (i)

ie $f(a^{-1}) = a$

ie $(f(a))^{-1} = f(a^{-1})$ (ii)

i) $a \in G \Rightarrow f(a) \in G'$

$f(a) * e' = f(a)$

$= f(a * e)$

$= f(a) * f(e)$

$\Rightarrow e$

$f(a) * e' = f(a) * f(e)$

$f(e) = e'$

∴ Identity is preserved

ii) $(f(a))^{-1} = f(a^{-1})$

To prove $f(a) * f(a^{-1}) = e'$

$f(a * a^{-1}) = e'$

$\boxed{f(e) = e'}$

∴ They are Inverse

4) Prove that Intersection of two Subgroups of a group G is again a Subgroup of G, but their union need not be a Subgroup of G

Soln:

i) Intersection of two ~~Sets~~ Subgroup is again Subgroup

~~Let H and K be two Subgroups~~

Let H and K be two Subgroups of G

Let $a, b \in H \Rightarrow a * b^{-1} \in H$

Let $a, b \in K \Rightarrow a * b^{-1} \in K$

$a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$

ie $a * b^{-1} \in H$ and $a * b^{-1} \in K$

i.e $a * b^{-1} \in H$ and K

$a * b^{-1} \in H \cap K$

∴ $H \cap K$ is a Subgroup of G

ii) Union of two subgroups need not to be a subgroup

Let G = Set of integers (Z, +)
$= \{-3, -2, -1, 0, 1, 2, 3 \ldots\}$

H = 2Z

K = 3Z

clears H and K are subgroup of (Z, +)

$H \cup K = \{2Z \cup 3Z\}$

H∪K is not closed under addition

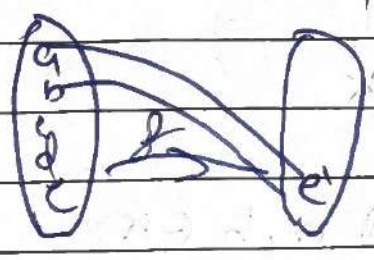
$2, 3 \in H \cup K$ but $2+3 = 5 \notin H \cup K$

H∪K is not a subgroup of (Z, +)

5) Show that the kernal of group homomorphism is a normal subgroup of a Group

Soln Let (G, *) and (H, Δ) be a groups and $f: G \to H$ be a homomorphism. Then the kernal of f is a normal subgroup

**Defn:** Kernal of a group homomorphism
Let (G, *) and (G', *) be two groups with e' as the identity element of G'. Let $f: G \to G'$ be homomorphism Then the kernal of f: $\ker f = \{x \in G \mid f(x) = e'\}$




$\ker f = \{a, b\}$

To prove K is a Normal subgroup
First prove K is a subgroup

To prove $x, y \in K \Rightarrow x * y^{-1} \in K$

TP: $f(x * y^{-1}) = e'$

$= f(x) * f(y^{-1}) = e'$

$= f(x) \Delta (f(y))^{-1}$

$= e' \Delta e'$

$= e'$

i.e $f(x * y^{-1}) = e'$

$\Rightarrow x * y^{-1} \in K$

So K is a subgroup

TP: K normal

$\forall x \in H,\ g \in G$

$g x g^{-1} \in H$

$\forall x \in K \quad g \in G$ s.t $g x g^{-1} \in K$

i.e $f(g * x * g^{-1}) = e'$

LHS: $f(g * x * g^{-1}) = f(g) * f(x) * f(g^{-1})$

$= f(g) \Delta f(x) \Delta f(g^{-1})$

$= f(g) \Delta e' f(g)^{-1}$

$= f(g) \Delta (f(g))^{-1}$

$= e' \in K$

$\therefore f\ g * x * g^{-1} \in K \ \forall\ g, x, g^{-1} \in K$

$\therefore$ Thus K is a Normal subgroup

6) Prove that intersection of any two normal subgroups of a group $(G, *)$ is a normal subgroup of $(G, *)$

Soln:

If H and K are normal subgroups of G
Then $H \cap K$ is also a normal subgroup of G

Proof: If $H \cap K$ is normal
H and K are subgroup G
$\therefore$ Intersection of two subgroup is a subgroup

TP $\forall x \in H \cap K$ $g \in G$
such that $gxg^{-1} \in H \cap K$
then normal
ie $\forall x \in H \Delta x \in K$ and $g \in G$, $gxg^{-1} \in H \cap K$

$x \in H$ and $g \in G \Rightarrow gxg^{-1} \in H$
$x \in K$ and $g \in G \Rightarrow gxg^{-1} \in K$

From both we get
$gxg^{-1} \in H \cap K$
$H \cap K$ is normal

7) State and prove Lagrange's Theorem:

Defn: The G be a finite group of order n and H be a subgroup of G Then for the order of H divides order of G i.e $O(G)/O(H)$ n/m

Proof Let G be a group with order n
Let H be a finite group and its order be M
For $x \in G$, the the Right coset of H is defined by
$Hx = \{h_1 x, h_2 x, h_3 x, \ldots h_m x\}$
Since there is one to one correspondance between H and Hx
the Members of Hx are distinct
Hence each Right coset of H in G has M distinct members
~~Hence each~~
H in G are either identical or disjoint
$Ha = \{h_1 * a, h_2 * a \ldots h_m * a\}$
$Ha$ has M distinct
$\therefore O(H) = O(Ha)$ $a \in G$
Then
$G = [Ha_1] \cup (Ha_2] \cup \ldots [Ha_k]$
$O(G) = O(Ha_1) \ldots + O(Ha_k)$
$n = Mk$

$$k = \frac{n}{M}$$

$n = O(G)$
$M = O(H)$

$$k = \frac{O(G)}{O(H)}$$

→ Lagrange's theorem

8) Prove that every subgroup of a cyclic group is cyclic
Soln:
Let (G, *) be a cyclic group generated by an element 'a'
$\therefore$ every element in G is of the form of $a^n$, n is an integer
Let H be a subgroup of G.
TO Prove H is cyclic
(case i) If H is an Improper subgroup
i.e $H = \{e\}$
$H = G$
Then H is a cyclic subgroup

Case ii) If H is a proper subgroup ($H < G$)

Let $H = \{a^m, a^2, a^3, \ldots\}$

To prove H is cyclic

Let m be the smallest positive int s.t $a^m \in H$

Now to prove H is a cyclic group generated by $a^m$

(i.e) To prove $H = \langle a^m \rangle$

Let $x \in H \Rightarrow x = a^k$, k is an integer

By division algorithm

$k = mq + r \quad ; \quad 0 \leq r < m$

$a^k = a^{mq+r} = a^{mq} \cdot a^r$

$= a^{mq} \cdot a^r$

$(a^{mq})^{-1} a^k = a^r$

i.e $a^r = a^k \cdot (a^{mq})^{-1}$

$a^r \in H$

$r = 0$

$\therefore k = mq + 0$

$= mq$

$x = a^k = a^{mq} = (a^m)^q$

$\therefore H$ is a cyclic subgroup

In a nutshell:

i) Improper cyclic if $H = \{e\}$ it is improper cyclic group

ii) Proper cyclic if $H = \{a^m, a^2, a^3 \ldots\}$

$H = \{any\}$

where m is the smallest +ve int

we need to prove

$x \in H \Rightarrow x = a^k$, k is an integer

$k = mq + r \quad 0 \leq r \leq m$

$a^k = a^{mq} \cdot a^r \Rightarrow a(mq)^{-1} a^k = a^r$

$a^r = a^k \cdot (a^{mq})^{-1}$

$a^r \in H$

r=0

K = Mq + 0

K = Mq

$x = a^K = a^{Mq}$ = (a^M)^q

$a^M$ is cyclic

x is cyclic

9) Prove that the set $Z_4 = \{0,1,2,3\}$ is a commutative ring with respect to the binary op +4

| +4 | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | 0 | 1 | 2 | 3 |
| [1] | 1 | 2 | 3 | 0 |
| [2] | 2 | 3 | 0 | 1 |
| [3] | 3 | 0 | 1 | 2 |

| X4 | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | 0 | 0 | 0 | 0 |
| [1] | 0 | 1 | 2 | 3 |
| [2] | 0 | 2 | 0 | 2 |
| [3] | 0 | 3 | 2 | 1 |

From The Table

i) All the entries in both tables belong to $Z_4$

$Z_4$ is closed under +4 x4

ii) In the both tables, entry in 1st, 2nd, 3rd, 4th rows are equal to entries in 1st 2nd 3rd 4th column respectively

+4 and x4 are commutative

iii) Associative: $0+3 = 3$

$0+1+2 = 3$

Associative true

iv) Inverse

0 is Additive inverse

1 is Multiplicative inverse

v) Additive inverse of 0, 1, 2, 3 are 0, 3, 2, 1

Multiplicative inverse of 1, 3 are 1, 3 respectively

(ii) Commutative is also true

∴ They are Commutative ring

End of Importants

Other Important Items and Theorems

1) If * is a binary operation on the set R of real numbers defined by $a*b = a+b+2ab$

1) Prove that (R, *) is a Semigroup
2) Find the identity element if it exists
3) Which element has inverse and what are they

Soln:

To prove Semigroup:

i) Closure property:

$\forall a,b \in G \quad a*b \in G$ iff $a*b = a+b+2ab$

Closure is true

ii) Associative:

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

$\overbrace{(a+b+2ab)}^{a} \overbrace{*c}^{b} = a*(b*c)$

LHS $= (a+b+2ab)+c+2(a+b+2ab)*c$

$= a+b+2ab+c+2ac+2bc+4bc$

$= a+b+2ab+c+2ac+2bc+4bc$ = RHS

LHS = RHS

∴ Associative is also true

∴ It is Soni

ii) Finding Identity element

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

$$\therefore e * a = a$$
$$e + a + 2ea = a$$
$$e + 2ea = 0$$
$$e(1 + 2a) = 0$$
$$e = \frac{0}{1+2a}$$

$\boxed{e = 0}$ is the identity element

iii) To find $a^{-1}$ inverse element

$$a * a^{-1} = e$$
$$a + a^{-1} + 2(a a^{-1}) = 0 \quad \text{Takes } a \text{ common}$$
$$a^{-1} + 2(a a^{-1}) = a \quad \text{takes } a^{-1} \text{ common}$$
$$a^{-1}(1 + 2a) = a$$
$$\boxed{a^{-1} = \frac{-a}{1+2a}}$$
$$\boxed{a \neq -\frac{1}{2}}$$

2) Show that $(Q^+, *)$ is an abelian group where $*$ is defined by $a * b = \frac{ab}{2} \quad \forall a, b \in Q^+$

Soln:

i) closure $\forall a, b \in Q^+$

$$a * b \in Q^+$$
$$\frac{ab}{2} \in Q^+$$

∴ closure is true

(ii) Associative $\forall a,b,c \in Q^+ \quad (a*b)*c = a*(b*c)$

LHS

$(a*b)*c$

$= \frac{ab}{2} * c$

$= \frac{abc}{2}$

RHS $= a*(b*c)$

$= a * \frac{bc}{2}$

$= \frac{abc}{2}$

LHS = RHS

Associative is true

(iii) Identity

$a*e = a$

$e*a = a$

$\therefore e, a = \frac{ea}{2} = a$

$e = 2 \in Q^+$

(iv) Inverse :

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

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

$aa^{-1} = 4$

$a^{-1} = \frac{4}{a} \in Q^+$

Inverse exist

(v) Commutative $a*b = b*a$

$\frac{ab}{2} = \frac{ba}{2}$

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

$\therefore$ It is true

$\therefore$ They are abelian

determinant $\neq 0$

M T W T F S S
Page No.:
Date:
YOUVA

3) Show that $M_2$, the set of all $2\times2$ non singular matrices over R is a group under usual matrix multiplication is it abelian

Soln $M_2 = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \}$ where $ad - cb \neq 0$ non singular

$(M_2, \cdot)$ is a group if it satisfies all 4 properties and 5 properties for abelian

i) Closure:

Let $A, B \in M_2$

$|A| \neq 0$ , $|B| \neq 0$

To prove

$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$

$B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

$A \cdot B = \begin{bmatrix} a_1a_2 + b_1c_2 & c_1a_2 + d_1c_2 \\ a_1b_2 + b_1d_2 & c_1b_2 + d_1d_2 \end{bmatrix}$

$|AB| = |A| \cdot |B|$

$\neq 0$

$|AB| \neq 0$

$\therefore A \cdot B \in M_2$ closure

ii) Associative:

$A, B, C \in M_2$

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

$A \cdot b \cdot C = A \cdot b \cdot C$

Associative is true

iii) Identity $M_2 = 2 \times 2$

$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $eA = A$, $Ae = A$

$\therefore$ Identity is true

iv) Inverse $M_2 = 2 \times 2$

$AA^{-1} = e$

$A A^{-1} = \frac{1}{|A|} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ $\therefore$ Inverse is true

∴ They are group

v) Commutative $A \cdot B \neq B \cdot A$

∴ Commutative is not true, they are abelian

4) Prove that $(Z_5, +_5)$ is an abelian

$Z_5 = \{0, 1, 2, 3, 4\}$

| $+_5$ | 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 |

i) Closure $a, b \in G$

$a +_5 b \in G$

ii) Associative $a, b, c \in G$

$(a +_5 b) +_5 c = a +_5 (b +_5 c)$

iii) Identity

$0 + 1 = 1$

$e +_5 a = a$

Identity element is 0

∴ Identity exists

iv) Inverse:

$a +_5 a^{-1} = e$

$0^{-1} = 0$

$1^{-1} = 4$

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 1$

∴ Inverse true

v) Commutative

$a +_5 b = b +_5 a$

∴ They are abelian

5) Let a be any element of group G. Suppose $a_1^{-1}$ and $a_2^{-1}$ be two inverse of a

soln:

$a * a_1^{-1} = e \quad \& \quad a_1^{-1} * a = e \quad | \quad a * a_2^{-1} = e \quad a_2^{-1} * a = e$

$a_1^{-1} = a_1^{-1} * e$

$= a_1^{-1} * (a_2^{-1} * a_2)$

$= (a_1^{-1} * a) * a_2^{-1}$

$= e * a_2^{-1}$

LHS = RHS

$a_1$ & $a_2$ are two inverse of a

6) In a group $(G, *)$, the left and right ~~tail~~ cancellation laws are true that is $a*b = a*c \Rightarrow b = c$ (left cancellation)

$b*a = c*a \Rightarrow b = c$ (Rish cancellation)

Sol:

Left cancellation proof

$a*b = a*c \Rightarrow b = c$

LHS

$a*b = a*c$ Multiply by $a^{-1}$

$a^{-1} * a * b = a^{-1} * a * c$

$\boxed{b = c}$ Left

RHS

$a*b = a$.

$b * a = c * a$ Multiply by $a^{-1}$

$b * a * a^{-1} = c * a * a^{-1}$

$b = c$

∴ left and righ are true

7) If a and b are two elements of a group $(G, *)$ then show that G is an abelian group if and only if $(a*b)^2 = a^2 * b^2$

Sol:

If $(G, *)$ is a group then
i) closure
ii) Associative
iii) Identity
iv) Inverse are true

All are true

TP $(a*b)^2 = a^2 * b^2$

$(a*b)(a*b)$

$(a*b)*a)((a*b*)b)$

$= a^2 * b^2 = RHS$

To prove they are abelian

$a*b = b*a$

For that lets take

$(a*b)*(a*b) = (a*a)*(b*b)$ Ass

LHS $= a*(b*(a*b)) = a*(a*(b*b))$

$= a*b$

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

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

LHS = RHS

∴ They are abelian

**Idempotent element : $a * a = a$**

8] Show that the semigroup with more than one idempotents cannot be a group Give an example of semigroup which can not be a group

Sol: Let $(S, *)$ be a semigroup
$a \& b$ are the two idempotent elements
$a * a = a$ & $b * b = b$
To P $(S, *)$ not a group (contradiction method)
we try to prove they are group
Let take associative prop
$(a * a) * a^{-1} = a * (a * a^{-1})$

$e = a$

Let take b
$(b * b) * b^{-1} = b * (b * b^{-1})$
$b * b^{-1} = b * e$
$b = e$

$e_1 \neq e_2$

Thus Identity are not true
so this can never be a group
Ex of semigroup which is not a group
Let $A = 0, 1, -1$

| * | 0 | 1 | -1 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | -1 |
| -1 | 0 | -1 | 1 |

i) closure is True
ii) Associative is True
iii) Identity and inverse are false
∴ They are not a group

9) For any commutative monoid $(M, *)$ the set of all idempotent elements of M forms a sub monoid

Soln:

If its monoid

i) closure is true

ii) Associative is true

iii) identity is true

Also commutative since it is a commutative monoid

TP $(S, *)$ is a sub monoid

let $a, b \in S$

$a*a = a \wedge b*b = b$

TP $(a*b) \in S$

i.e $(a*b)*(a*b) = (a*b)$

$= (a*b)$ is an idempotent

i) closure

ii) Associative is true

iii) Identity

$e*e = e$

Identity is true

iv) commutative

$a*b = b*a$

∴ They are also a commutative submonoid

10) Let $(G, *)$ be a group. Then $(H, *)$ is said to be a subgroup of $(G, *)$ if $H \subseteq G$ and $(H, *)$ itself a group under the operation $*$

Soln.

Example: $(Z, +)$ group

abelian

semi.

monoid

ex $N \subset W \subset Z \subset Q \subseteq R \subset C$

$(\mathbb{Z}, +)$
$(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$
$(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{C}, +)$
proper and improper subgroup:

for any $(G, *)$
(i) The subgroup of $(G, *)$ is $\{e\}$ are called improper subgroup
(ii) Any other group than $\{e\}$ is said to be proper subgroup
Ex: $(Z_6, +_6)$ is a group
subgroup $\{1, 2, 3, 6\}$
$H_1 \{0\}$, $H_2 \{0, 1, 2, 3, 4, 5\}$

↓
improper subgroup

They are semigroup

(ii) The identity element of a subgroup is same as that of group
Sol:
Let $(H, *)$ be a subgroup of $(G, *)$
Let $e_1$ be the identity element of $G$ & $e_2$ be identity element of $H$
Lets say
$H \subseteq G$
Then
$a \in H$ and $a \in G$
$a * e_2 = a$ or $e_1 = a$
$a * e_2 = a * e_1$
$\boxed{e_2 = e_1}$
$\therefore$ Hence proved

M T W T F S S
Page No.: YOUVA
Date:

b) The union of two subgroups of group G is a subgroup iff one is contained in the other

Sol:

Let H and K be two subgroups of a group G. Then-
HUK is a subgroup iff either $H \subseteq K$ or $K \subseteq H$
let $H \subseteq K$ or $K \subseteq H$
To prove HUK is a subgroup

$H \subseteq K \Rightarrow H \cup K = K \wedge K \subseteq H \Rightarrow H \cup K = H$
$\therefore H \cup K$ is a subgroup

Converse: Assume HUK is a subgroup of G
TP $H \subseteq K$ or $K \subseteq H$

Contradiction let $H \not\subseteq K$ or $K \not\subseteq H$
$a \in H \Rightarrow a \notin K \wedge b \in K \Rightarrow b \notin H$
Since HUK is a subgroup
$\Rightarrow a * b \in H \cup K$
$\Rightarrow a * b \in H$ or $a * b \in K$
(or) $a * b \in H$
$\therefore a^{-1} * (a * b) \in H$
$a^{-1} * a * b \in H$
$b \in H$ $b \notin H$ is not true
Case ii) $a * b \in K$
$b^{-1} * b * a \in K$
$a \in K$
$\therefore a \notin K$ is not true
Thus HUK is a subgroup if and only if $H \subseteq K$

13) Show that the set of all elements 'a' of a group $(G, *)$ such that $a * x = x * a$ for every $x \in G$ is a subgroup of $G$

Soln:

Let $(G, *)$ be a group

$$H = \{ a \mid a \in G, \ a * x = x * a \ \forall \ x \in G \}$$

Subgroups of $(G, *)$

1) $H \subseteq G$
2) $H$ is a group

Clearly $H \subseteq G$ and associative law satisfies under $*$

i) closure property:

$a, b \in H$

$a * b \in H \Rightarrow a * x = x * a \quad \text{--} (1)$

$b * x = x * b \quad \text{--} (2)$

To $a * b \in H$

$(a * b) * x = x * (a * b)$

LHS $(a * b) * x = a * (b * x)$

$= a * (x * b)$

$= a * x * b$

$= x * a * b$

$= x * (a * b) = RHS$

closure is true

ii) Identity element:

$e \in H$

$x * e = x$

$\Rightarrow e * x = x * e$

$\Rightarrow e \in H$

iii) Inverse

$a \in H \Rightarrow a * x = x * a$

$a^{-1} \in H \Rightarrow a^{-1} * x = x * a^{-1}$ (Just by some theorem)

$\therefore$ Inverse is also true

14) Find the subgroups of $(Z_8, +_8)$

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$\langle 0 \rangle = \{0\} \subset Z_8$

$\langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Find all

15) Let $A = \{1, 2, 3, 4, 5, 6\}$ and $p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{bmatrix}$ be a permutation of A

(1) write p as product of distinct

(2) State that p is odd permutation

(3) compute $p^{-1}$

(4) compute $p^2$

$p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{bmatrix} = [(1,5)(263)]$ Transpose

$263 = (26)(23)$

$= (15)(26)(23)$

Permutation is odd

$p^{-1} = \begin{bmatrix} 5 & 6 & 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 1 & 3 \end{bmatrix}$

$p^2 = pop = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{bmatrix} o \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{bmatrix}$

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

Find the period of permutation $P = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{bmatrix}$

$P^2 = I$

$P^2 = P \circ P = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 5 & 2 \end{bmatrix}$

$P^2 \circ P = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} = I$

16) Obtain the composition table for $(S_3, \Delta)$. Show that $(S_3, \Delta)$ is a group, check whether $(S_3, \Delta)$ is an abelian group. Justify the answer.

$S_3, \Delta = \{ P_0 \; P_1 \; P_2 \; P_3 \; P_4 \; P_5 \}$

$P_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ $P_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$ $P_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$ $P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$

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

$S_3, \Delta = \{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \}$

Let's obtain the table

| $\circ$ | $P_0$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ |
|---|---|---|---|---|---|---|
| $P_0$ | $P_0$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ |
| $P_1$ | $P_1$ | $P_0$ | $P_3$ | $P_2$ | $P_5$ | $P_4$ |
| $P_2$ | $P_2$ | $P_4$ | $P_0$ | $P_5$ | $P_1$ | $P_3$ |
| $P_3$ | $P_3$ | $P_5$ | $P_1$ | $P_4$ | $P_0$ | $P_2$ |
| $P_4$ | $P_4$ | $P_2$ | $P_5$ | $P_0$ | $P_3$ | $P_1$ |
| $P_5$ | $P_5$ | $P_3$ | $P_4$ | $P_1$ | $P_2$ | $P_0$ |

i) Closure is True
ii) Associative True
iii) Inverse True
iv) Identity True
v) Commutative is not true
Not abelian

M T W T F S S

Page No.: YOUVA

Date:

[7] State and prove cayley's theorem on permutation groups
(or)
Prove that every finite group of order n is isomorphic to a permutation group of degree n

Sol: ~~Proof~~

Isomorphism: Let $G$ & $G'$ be two groups A map $f: G \to G'$ is said to be isomorphism if $f$ is a bijection and $f$ is homomorphism.

If $f$ is a bijection and $f$ is a homomorphism
1-1 onto

one to one, onto homomorphism is called isomorphism

Soln:

we shall prove in 3 steps
1) First find a set $G'$ of permutation
2) prove $G'$ is a group
3) To prove $\phi: G \to G'$ is isomorphism

Step 1: Find a permutation set $G'$

Let $G' = \{f_a \mid a \in G\}$
define a function $f_a: G \to G$ by $f_a(x) = ax$ where $x \in a$, $a \in G$

TP $f_a$ is well defined:

$x = y \iff ax = ay$

$f_a(x) = f_a(y)$

~~TP $f_a$ is one to one~~ $\therefore f_a$ is well defined

TP $f_a$ is a one to one $f_a(x) = f_a(y) \Rightarrow x = y$

$f_a(x) = f_a(y)$

$ax = ay$

$x = y$

To $f_a$ is onto

$f_a(a^{-1}, y) = a(a^{-1}, y) = ey = y$

& $a(a^{-1}y) = a(a^{-1}y)$

$= ey$

$= y$

∴ They are onto

do the same for x

Step 2: To prove G' is a group

Closure: Let $f_a, f_b \in G'$

TP $f_a \circ f_b \in G'$

$f_a \circ f_b(x) = f_a(f_b(x) = f_a(bx)$

$= a(bx)$

$= f_{ab}(x)$

$f_a \circ f_{(b)} x = f_{ab}(x)$

$f_a \circ f_{(b)} \in G'$

∴ G' is closure

Association:

is always true in composition and ∀

Identity:

Let e be the identity element of G

the $f_e$ is for G'

∴ Identity element exists

Inverse

$f_a \in G_1 = a \in G$

$\therefore a^{-1} \in G$

Now $f_a \cdot f_{a^{-1}} = f_{aa^{-1}}$

$= f_e$

Inverse is true

$G'$ is a group

Step 2 : To prove $\varphi : G \to G'$ is isomorphism

① well define $\boxed{a=b}$

$\varphi(a) = \varphi(b)$

② one to one

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

$ax = bx \Rightarrow f_a = f_b$

$= \varphi(a) = \varphi(b)$

③ onto : $\varphi$ is onto

④ $\varphi$ is homomorphism : $\varphi(ab) = \varphi(a) \circ \varphi(b)$

① TP $\varphi$ is well defined

$a=b$

$\Leftrightarrow ax = bx$

$f_a = f_b$

$\varphi(a) = \varphi(b)$

∴ They are well defined

② They are one to one

$a=b$

$ax = bx$

$f_a = f_b$

$\varphi_a = \varphi_b$

$\varphi$ is 1-1

③ onto: Since $f_a$ is onto

$\varphi$ is onto

④ $\varphi(a,b) = f_{ab} = f_a \circ f_b$

$= \varphi(a) \varphi(b)$

∴ $\varphi$ is a homomorphism

$f : G \to G'$ is isomorphic (isomorphism

18) If $a \in Hxb$ then $Hxa = Hxb$ and if $a \in bxH$ then $axH = bxH$

Sol Let $a \in Hxb$

Post Mul by $b^{-1}$

$axb^{-1} \in Hxe$

$axb^{-1} \in H$

$Hxaxb^{-1} = H$ x by b

$Hxaxb^{-1}xb = Hxb$

$\boxed{Hxa = Hxb}$

Let $a \in bxH$

$axH = bxH$

$a \in bxH$ x by $b^{-1}$

$axb^{-1} \in bxHxb^{-1}$

$axb^{-1} \in H$

$Hxaxb^{-1} = H$ x by b

$Hxaxe = Hxb$

$Hxa = Hxb$

$\boxed{axH = bxH}$

19) Any two Right or left cosets of H in G are either disjoint or identical

Sol : G be a group & subgroup

Let $a, b \in G$

To $(Hxa) \cap (Hxb) = \phi$ or $Hxa = Hxb$

$(Hxa) \cap (Hxb) \neq \phi$ To $Hxa = Hxb$

Thus $\exists x \in (Hxa) \cap (Hxb)$

$x \in Hxa$ & $x \in Hxb$

$Hxx = Hxa$

$Hxx = Hxb$

$\boxed{Hxa = Hxb}$

LHS : RHS

$\therefore$ They are identical

M T W T F S S

Page No.: YOUVA

Date:

## Pending and left overs

1) Left Cosets: Let $(H,*)$ be a subgroup of $(G,*)$ for any $a \in G$ the left coset of $H$, denoted by $a*H$, is the set $a*H = \{a*h : h \in H\}$ for all $a \in G$

2) Rings: $(H, *, \circ)$

3) Fundamental theorem on Homomorphism of Groups

Statement: Every homomorphic image of a group $G$ is isomorphic to some quotient group of $G$

or

Let $f: G \to G'$ be an onto homomorphism with kernel $K$ Then $G/K \cong G'$

Proof: Let $f: G \to G'$ be an onto homomorphism

Let $K$ be the kernel of this homomorphism

$\therefore K$ is a a normal subgroups of $G$.

Now to prove i) $f$ is well defined

ii) $f$ is 1-1

iii) $f$ is onto

iv) $f$ is homomorphism

i) To prove $f$ is well defined

TP $K*a = K*b$

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

$K*a = K*b$

$a*b^{-1} \in K$

$f(a*b^{-1}) = e'$

$f(a) * f(b^{-1}) = e'$

$\therefore f(a) * f(b)^{-1} = e' * f(b)$

$\Rightarrow f(a) * e' = f(b)$

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

There are well defined one to one

$\forall$

$f(k*a) = f(k*b) \Rightarrow f(a) = f(b)$

$k*a = k*b$

$f(a) = f(b)$

$f(a) * (f(b))^{-1} = f(b) * (f(b))^{-1}$

$f(a) * f(b^{-1}) = e'$

$f(a*b^{-1}) = e'$

$\Rightarrow a*b^{-1} \in k$

$k*a = k*b$

$f$ is $1$-$1$

TP $f$ is onto

since $f$ is onto func.

$\therefore f$ is also onto

TP $f$ homomorphism

i.e TP $f((k*a) * (k*b)) = f(k*a) * f(k*b)$

$f((k*a) * (k*b))$

$= f(a*b)$

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

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

$\therefore LHS = RHS$

The theorem is proved.