UNIT - IV ALGEBRAIC STRUCTURES

PART - B

GROUP, SUBGROUP AND NORMAL SUBGROUP

(1) Show that M_2, the set of all 2×2 non-singular matrices over R is a group under usual matrix multiplication. Is it Abelian [A/M '15]

(2) If $(G, *)$ is an abelian group, show that $(a*b)^2 = a^2 * b^2$ [N/D '10]

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

(i) Find $\langle R, * \rangle$ is a semigroup.

(ii) Find the identity element if it exists?

(iii) Which elements has inverse & what are they. [A/M

(4) If $S = N \times N$, the set of ordered pairs of positive integers with the operation $*$ defined by $(a,b) * (c,d) = (ad + bc, bd)$ and if $f: (S, *) \to (Q, \cdot)$ is defined by $f(a,b) = \frac{a}{b}$, show that f is a semigroup homomorphism. [A/M '15]

(5) Find the left cosets of the subgroup $H = \{[0], [3]\}$ of the group $[Z_6, +_6]$. [M/J '14]

(6) State and prove Lagrange's theorem

[N/D '10] [A/M '11] [M/J '12] [N/D '13] [M/J '14] [A/M

(7) Prove that the order of a subgroup of a finite group divides the order of the group. [N/D '11] [M/J '13]

(8) Find all the subgroups of $(Z_{24}, +_{24})$ [M/J '14]

(9) Prove the theorem: Let $\langle G, * \rangle$ be a finite cyclic group generated by an element $a \in G$. If G is of order n, that is $|G| = n$, then $a^n = e$, so that $G = \{a, a^2, a^3, \ldots, a^n = e\}$. Further more n is a least positive integer for which $a^n = e$

(10) Prove that intersection of any two subgroups of a group $(G, *)$ is again a subgroup of $(G, *)$. [N/D '11] [N/D '13]

(11) Prove that intersection of two normal subgroups of a group $(G, *)$ is a normal subgroup of a group $(G, *)$. [M/J '13]

(12) Show that the union of two subgroups of a group G is a subgroup of G if and only if one is contained in the other. [A/M '15]

(13) Prove that every cyclic group is an ab

(14) Prove that the necessary and sufficient condition for a non empty subset H of a group $\{G,*\}$ to be a subgroup is $a,b \in H \Rightarrow a * b^{-1} \in H$. [N/D'12].

(15) If '*' is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a,b)*(x,y) = (ax,$ Show that $(S,*)$ is a semigroup. Is it commutative? Also find the identity element of S. [N/D'12]

(16) Define the Dihedral group $(D_4, *)$ and give its composite table. Hence find the identity element and inverse of each element. [A/M'20

HOMOMORPHISM AND ISOMORPHISM

(1) Prove that every finite group of order n is isomorphic to a permutation group of order n. [N/D'11] [M/J'13]

(2) State and prove the fundamental theorem of group homomorphism. [N/D'13]

(3) Let $f: G \to G'$ be a homomorphism of groups with Kernel K. Then prove that K is a normal subgroup of G & G/K is isomorphic to the image of f [M/J'12].

(4) Let $(G,*)$ & (H,Δ) be two groups & $g: (G,*) \to (H,\Delta)$ be group homomorphism. Then prove that the kernel of g is normal subgroup of $(G,*)$ [M/J'13].

(5) Show that the Kernel of a homomorphism of a group $\langle G,* \rangle$ into an another group $\langle H,\Delta \rangle$ is a subgroup of

(6) If $f: G \to G'$ is a group homomorphism from $\{G,*\}$ to $\langle G',\Delta \rangle$ then prove that for any $a \in G$, $f(a^{-1}) = [f(a)]^{-1}$ [A/M [N/D'12

(7) If $(Z,+)$ & $(E,+)$ where Z is the set all integers & E is the set all even integers, show that the two semigroups $(Z,+)$ & $(E,+)$ are isomorphic [N/D'10

(8) Let $(S,*)$ be a semigroup. Then prove that there exist a homorphism $g: S \to S^S$ where $\langle SS, \circ \rangle$ is a Semigro of functions from S to S under the operation of (left Composition. [N/D'11]

(9) Let $(M,*)$ be a monoid. Prove that there exists a subset $T \subseteq M^M$ s.t $(M,*)$ is isomorphic to the monoid $(T,\circ)$ here M^M denotes the set of all mappings from M to M & "$\circ$" denotes the composition of mappings [M/J'14

RINGS AND FIELDS

(2)

(1) Show that $(Z, +, \times)$ is an integral domain where Z is the set of all integers. [N|D|2010]

(2) Prove that the set $Z_4 = \{[0], [1], [2], [3]\}$ is a commutative ring w.r.t the binary operation addition modulo 4 & multiplication modulo $+_4, \times_4$. [N|D|12]

UNIT-IV
ALGEBRAIC STRUCTURES

- Algebraic Systems
- Semigroups and Monoids
- Groups
- Subgroups
- Homomorphism
- Cosets
- Lagrange's Theorem.
- Normal Subgroup
- Ring
- Field
- Solved PART-A.
- Expected A/U PART Questions & Answers.

UNIT-IV : ALGEBRAIC STRUCTURES

BINARY OPERATION :

Let A be a non-empty set a function f s.t $f: A \times A \to A$ is called a binary operation on the set A where $A \times A = \{(a,b) \mid a \in A, b \in A\}$

Binary Operation symbols : $+, -, \odot, \oplus, \cdot, \Delta, *, \cap, \cup, \times$ ....

NOTATIONS

- N = The set of natural numbers $= \{0, 1, 2, \ldots\}$
- Z / I = The set of integers $= \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- C = The set of Complex numbers $= \{a+ib \mid a,b \in R\}$
- R = The set of real numbers
- Q = The set of all rational numbers $= \{\frac{a}{b} : a,b \in Z, b \neq 0\}$
- $M_{2\times 2}(R)$ = The set of all 2x2 real matrices
- Z_n = The set of residue classes modulo $n = \{0, 1, 2, \ldots, n-1\}$

ALGEBRAIC SYSTEM : DENOTED BY $[G, *]$

A non empty set G equipped with one or more binary operation, * is called an algebraic system (or) algebraic structure.

Eg: $(N,+)$, $(Z,-)$, $(R,\cdot)$, $(R,+,\cdot)$, $(Q,+)$, $(C,+)$

PROPERTIES OF BINARY OPERATIONS :

Let the binary operation be $* : G \times G \to G$

Then we have the following property

(1) CLOSURE PROPERTY : $a * b \in G$, for all $a,b \in G$

(2) COMMUTATIVITY : $a * b = b * a$, for all $a,b \in G$.

(3) ASSOCIATIVITY : $(a*b)*c = a*(b*c)$, for all $a,b,c \in G$

(4) IDENTITY ELEMENT : $\exists e \in G$ s.t $a*e = e*a = a$, for all $a \in G$

(5) INVERSE ELEMENT : $\exists b \in G$ s.t $a*b = b*a = e$, $\forall a \in G$ then b is called inverse of a & denoted by $b = a^{-1}$

	For all $a,b,c \in G$	$(G,+)$	$(G,\times)$
1.	Associativity	$(a+b)+c = a+(b+c)$	$(a\times b)\times c = a\times(b\times c)$
2.	Commutativity	$a+b = b+a$	$a\times b = b\times a$
3.	IDENTITY ELEMENT	$a+0 = 0+a = a$ — (0 → IDENTITY)	$a\times 1 = 1\times a = a$ — (1 → IDENTITY)
4.	INVERSE ELEMENT	$a+(-a) = (-a)+a = 0$ — ($-a$ → ...)	$a \times \frac{1}{a} = \frac{1}{a} \times a = 1$

SEMIGROUP : $(S, *)$

If a non-empty set S together with the binary operation '$*$' satisfying the following two properties.

- (a) CLOSURE PROPERTY.
- (b) ASSOCIATIVE PROPERTY.

MONOIDS : $(M, *)$

If a non-empty sets M together with the binary operation satisfying the following properties.

- (a) CLOSURE PROPERTY
- (b) ASSOCIATIVE PROPERTY
- (c) IDENTITY PROPERTY.

eg:- (Z_n, t_n), (Z_n, X_n)

GROUP : $(G, *)$

A non empty set G with binary operation $*$ is called a group if the following axioms are satisfied

- (a) ASSOCIATIVE : $(a*b)*c = a*(b*c) \quad \forall a, b, c \in G$.
- (b) IDENTITY : $\exists e \in G$ s.t $a*e = e*a = a \quad \forall a \in G$.
- (c) INVERSE : $\forall a \in G, \exists a^{-1} \in G$ s.t $a*a^{-1} = a^{-1}*a = e$

ABELIAN GROUP / COMMUTATIVE GROUP:

A group $(G, *)$ is called abelian if $a*b = b*a \quad \forall a, b \in G$.

FINITE AND INFINITE GROUP :

If in a group $(G, *)$ the set G consists of a finite number of elements then the group is called a finite group otherwise an infinite group.

ORDER OF A GROUP: $O(G)$ or $|G|$

The number of elements in a finite group is called the order of the group.

ORDER OF AN ELEMENT: $O(a)$

Let $(G, *)$ be a group of any element belonging to G. If there exist a least positive integer 'n' s.t $a^n = e$, where e is the identity element, then the order of 'a' is 'n'.

NOTE:

1. For any group, the identity element is the only element of order 1.
2. To verify an operation is binary it is enough to verify closure property.

ELEMENTARY PROPERTIES OF A GROUP

THEOREM 1 [CANCELLATION LAW]

Let $(G,*)$ be a group. Then for any $a,b,c \in G$

(i) If $a*b = a*c$ then $b=c$ [Left Cancellation]

(ii) If $b*a = c*a$ then $b=c$ [Right Cancellation]

Proof

Let $a \in G$, a^{-1} is the inverse of a and 'e' is the identity element such that $a*a^{-1} = a^{-1}*a = e$ and $a*e = e*a = a$

T.P: LEFT CACELLATION

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

$\Rightarrow a^{-1}*(a*b) = a^{-1}*(a*c)$ [Pre operating a^{-1} on both sides]

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

$\Rightarrow e*b = e*c$ [Inverse]

$\Rightarrow b = c$ [Identity]

T.P: RIGHT CANCELLATION

Now, $b*a = c*a$

$\Rightarrow (b*a)*a^{-1} = (c*a)*a^{-1}$ [Post operating a^{-1} on boths

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

$\Rightarrow b*e = c*e$ [Inverse]

$\Rightarrow b = c$ [Identity].

NOTE:

Converse is not true: Eg: In $(N,+)$ → Right & left cancellation hold But it is not a group.

PROPERTY 2 (2M)

Let $(G,*)$ be a group then identity element of G is unique

PROOF:

Let e_1, e_2 be two identity elements of G

T.P G has unique identity element ie T.P $e_1 = e_2$

$a*e_1 = e_1*a = a \rightarrow (1)$ [$\because e_1$ is the identity elt]

$a*e_2 = e_2*a = a \rightarrow (2)$ [$\because e_2$ is the identity elt]

From (1) & (2) $a*e_1 = a*e_2 \Rightarrow e_1 = e_2$ [By Left Cancellation]

∴ The identity is unique.

PROPERTY 3 (2M)

Let $(G,*)$ be a group. For any $a \in G$, inverse of 'a' is Unique.

PROOF

Let $a \in G$, e be the identity element.

Let $a \in G$ and a_1^{-1} & a_2^{-1} be two inverses of a

T.P G has unique inverse element. ie T.P $a_1^{-1} = a_2^{-1}$.

$\because a_1^{-1}$ is

$\therefore a_2$ be the inverse of $a \Rightarrow a * a_2^{-1} = a_2^{-1} * a = e \rightarrow (2)$

From (1) & (2) $\therefore a * a_1^{-1} = a * a_2^{-1}$

$\Rightarrow a_1^{-1} = a_2^{-1}$ [By Left Cancellation law]

$\therefore$ The inverse is unique

PROPERTY 4:

Let $(G,*)$ be a group. Then for each $a \in G$ $(a^{-1})^{-1} = a$.

PROOF:

Let $a \in G$, e be the identity element & a^{-1} is the inverse of a.

T.P $(a^{-1})^{-1} = a$.

$\because a^{-1}$ is the inverse of $a \Rightarrow a * a^{-1} = a^{-1} * a = e \rightarrow (1)$

$(a^{-1})^{-1}$ is the inverse of $a^{-1} \Rightarrow a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * a = e \rightarrow (2)$

From (1) & (2), $a * a^{-1} = (a^{-1})^{-1} * a^{-1} \Rightarrow a = (a^{-1})^{-1}$ [Right Cancellation]

$\therefore (a^{-1})^{-1} = a$

PROPERTY 5:

Let $(G,*)$ be a group. For any $a,b \in G$ then $(a*b)^{-1} = b^{-1} * a^{-1}$

PROOF:

Let $a,b \in G$, e be the identity elt & a^{-1} & b^{-1} is inverse of a & b

$a * e = e * a = a \rightarrow (1)$ | $a * a^{-1} = a^{-1} * a = e \rightarrow (3)$

$b * e = e * b = b \rightarrow (2)$ | $b * b^{-1} = b^{-1} * b = e \rightarrow (4)$

T.P $(a*b)^{-1} = (b^{-1} * a^{-1}) \Rightarrow \frac{1}{(a*b)} = (b^{-1} * a^{-1})$

i.e T.P (i) $(a*b)*(b^{-1} * a^{-1}) = e$ (ii) $(b^{-1} * a^{-1}) * (a*b) = e$

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

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

$= a * [e * a^{-1}]$ [From (4)].

$= a * a^{-1}$ [Identity].

$\therefore \boxed{(a*b)(b^{-1} * a^{-1}) = e} \rightarrow (A)$ [From (3)]

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

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

$= b^{-1} * [e * b]$ [From (1)]

$= b^{-1} * b$ [From 2]

$\therefore \boxed{(b^{-1} * a^{-1}) * (a*b) = e} \rightarrow (B)$ [From 4]

From (A) & (B) $(a*b)^{-1} = b^{-1} * a^{-1}$

PROPERTY 6 SM(X):

For any group G, if $a^2 = e$ with $a \neq e$ then G is abelian (or) If every element of a group G is its own inverse then G is abelian. $(a*b)^{-1} = b^{-1} * a^{-1}$

PROOF:

Let $a \in G$. Given $a^2 = e$

T.P G is abelian ie T.P $(a*b) = (b*a)$

If $a^2 = e \Rightarrow a = a^{-1}$.

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

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

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

$\therefore a*b = b*a$ $\therefore$ G is abelian.

$a^2 = e$

$a^{-1} * a^2 = a^{-1} *$

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

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

$= a * a$

Every elt its own inverse

Converse Need Not be true

Since $(Z, +)$ is an abelian group. Except 0, there is no element in Z which has its own inverse.

PROPERTY 7: (7) 6M.

A group $(G, *)$ is abelian iff $(a*b)^2 = a^2 * b^2$. [NID'10]

PROOF:

For any $a, b \in G$, G is abelian. $\therefore a*b = b*a$

T.P.T $(a*b)^2 = a^2 * b^2$

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

$= a * [(b*a)*b]$

$= a * [(a*b)*b]$

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

$\therefore (a*b)^2 = a^2 * b^2$

Conversely:

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

T.P.T: G is abelian $\Rightarrow$ T.P $(a*b) = (b*a)$.

$\because (a*b)^2 = a^2 * b^2 \Rightarrow (a*b)*(a*b) = (a*a)*(b*b)$

$\Rightarrow a * [b*(a*b)] = a * [a*(b*b)]$

[left Cancellation] $\Rightarrow b*(a*b) = a*(b*b)$

[Associative] $\Rightarrow (b*a)*b = (a*b)*b$.

[Right Cancellation] $\Rightarrow (b*a) = (a*b)$

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

$\therefore$ G is abelian.

PROPERTY 8: (8) 8M.

If G is an abelian group then for all $a, b \in G$ & all integers n, $(a*b)^n = a^n * b^n$

PROOF:

Case(i): We have $(a*b)^0 = e$

Also $a^0 * b^0 = e * e = e$

Case (ii)

$n>0$, $n=1$ then $(a*b)^1 = a*b = a^1*b^1$

If $n=k$ then: $(a*b)^k = a^k * b^k$ → (1)

T.P $n=k+1$ then $(a*b)^{k+1} = a^{k+1} * b^{k+1}$

Now $(a*b)^{k+1} = (a*b)^k * (a*b)$

$= (a^k * b^k) * (a*b)$ [From (1)]

$= a^k * [b^k * (a*b)]$

$= a^k * [(b^k * a) * b]$

$= a^k * [(a*b^k) * b]$ [∵ G is abelian]

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

$(a*b)^{k+1} = a^{k+1} * b^{k+1}$

Hence by mathematical induction for all $n>0$

$(a*b)^n = a^n * b^n$.

Case (iii)

$n<0$, Let $n=-m$, where m is a +ve integer.

Then $(a*b)^n = (a*b)^{-m} = [(a*b)^m]^{-1} = [a^m * b^m]^{-1}$

$= [b^m * a^m]^{-1}$ [∵ G is abelian]

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

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

$(a*b)^n = a^n * b^n$

∴ Hence $(a*b)^n = a^n * b^n$, $\forall n \in Z$.

PROPERTY 9 (i) QM

In a group the only idempotent element is identity element.

PROOF: $a=e$

Let $a \in G$ is an idempotent element then $a*a=a$

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

$\therefore a=e$

∴ The only idempotent element is identity element.

PROPERTY 10 (i) QM

In a group $(G,*)$ the equation $a*x=b$ & $y*a=b$ have unique solution for the unknown x & y as $x=a^{-1}*b$ and $y=b*a^{-1}$, where $a,b \in G$.

PROOF:

Given $(G,*)$ is a group & let e be identity elt of G & a^{-1} be inverse of

T.P (i) $a*x=b$ has unique solution $x=a^{-1}*b$

(ii) $y*a=b$ has unique solution $y=b*a^{-1}$

(i) Given $a * x = b$

$\Rightarrow a^{-1} * (a * x) = a^{-1} * b$ [Premultiplying by a^{-1}]

$\Rightarrow (a^{-1} * a) * x = a^{-1} * b$ [By associative axiom]

$\Rightarrow e * x = a^{-1} * b$ [By inverse axiom]

$\Rightarrow x = a^{-1} * b$ [By identity axiom].

Thus $x = a^{-1} * b \in G$ is a solution.

We shall now prove the uniqueness:

Suppose $x_1, x_2 \in G$ be two solutions of $a * x = b$

$\therefore a * x_1 = b$ & $a * x_2 = b$

$\Rightarrow a * x_1 = a * x_2$

$\Rightarrow x_1 = x_2$ [By Cancellation Law]

Hence the solution is unique & the unique solution is $x = a^{-1} * b$.

(ii) Now $y * a = b$

$\Rightarrow (y * a) * a^{-1} = b * a^{-1}$ [Postmultiplying by a^{-1}]

$\Rightarrow y * (a * a^{-1}) = b * a^{-1}$ [By associative axiom]

$\Rightarrow y * e = b * a^{-1}$ [By inverse axiom]

$\Rightarrow y = b * a^{-1}$ [By identity axiom]

Thus $y = b * a^{-1} \in G$ is a solution.

We shall now prove the uniqueness:

Let y_1, y_2 be two solutions of $y * a = b$

$\therefore y_1 * a = b$ and $y_2 * a = b$

$\Rightarrow y_1 * a = y_2 * a$

$\Rightarrow y_1 = y_2$ [By Right Cancellation Law].

Hence the solution is unique & the unique solution is $y = b * a^{-1}$.

PROBLEMS ON GROUP [IMP & M]

(1) Let $G = \{1, -1\}$. Prove that G is a group under usual Multiplicat

Sol: Given $G = \{1, -1\}$ & the binary operation $*$ is usual multiplic

Since G is a finite set, we form Cayley table & verify the axioms of a group.

CAYLEY TABLE:

$*$	1	-1
1	1	-1
-1	-1	1

- CLOSURE: The body of the table contains only elements of G. So G is closed under multiplication.
- ASSOCIATIVITY: Since Multiplication is associative in any number set, it is true here also.

Hence associativ

- IDENTITY : I is the identity elt i.e) $a*1 = 1*a = a$ ✓
- INVERSE : Inverse of 1 is 1 & Inverse of -1 is -1. ✓

∴ $(G, \circ)$ is a group.

Further, G is an abelian group, since $\circ$ is commutative

---

(2) Show that M_2, the set of all 2x2 non-singular matrices over R is group under usual matrix multiplication. Is it abelian [A M 15 Refer Pb 7 ⇒]

Let $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$, Show that G is a group under the operation of matrix Multiplication.

Sol: T.P $(G, *)$ is a Group.

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

∴ $G = \{I, A, B, C\}$. Since it is a finite set.

We shall form Cayley table and verify the axioms of a group

I is Identity element.

$A \cdot I = I \cdot A = A$, $B \cdot I = I \cdot B = B$, $C \cdot I = I \cdot C = C$

$A^2 = A \cdot A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

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

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

$B^2 = B \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$C^2 = C \cdot C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

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

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

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

$CB = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = A$.

CAYLEY TABLE

$\circ$	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

$a*e = e*a = a$

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

CLOSURE: The body of the table contains only all the elts of G. So G is closed under matrix multiplication.

ASSOCIATIVE: Since matrix multiplication is associative it is true for G also. So associative axiom is satisfied.

IDENTITY : I is the identity element

INVERSE : $(I)^{-1} = I$, $A = (A)^{-1}$, $B = (B)^{-1}$, $(C)^{-1} = C$ [Inverse of C is

∴ $(G, \circ)$ is group under matrix multiplication.

$(G, \circ)$ is abelian : 'coz elements equi distant from the main

③ Show that the set of all non-zero real numbers is an abelian group under the operation * defd by $a*b = \frac{ab}{2}$. [A/U 07]

Sol: Let G be the set of all non-zero real numbers.

$G = R - \{0\}$, where R is the set of real numbers.

The operation * on G is defd by $a*b = \frac{ab}{2}$ $\forall a,b \in G$.

T.P $(G,*)$ is an abelian group

Closure: $a*b = \frac{ab}{2}$, where a & b are nonzero real no:s and so $\frac{ab}{2}$ is non-zero.

$\therefore \frac{ab}{2} \in G \Rightarrow a*b \in G \ \forall a,b \in G$.

Hence G is closed under *.

ASSOCIATIVITY: For any $a,b,c \in G$.

$$a*(b*c) = a*\frac{bc}{2} = \frac{a(\frac{bc}{2})}{2} = \frac{a(bc)}{4}$$

$$(a*b)*c = \frac{ab}{2}*c = \frac{(\frac{ab}{2})c}{2} = \frac{(ab)c}{4}$$

$\therefore a*(b*c) = (a*b)*c \ \forall a,b,c \in G$. [$\because$ usual multiplicatn is associative]

IDENTITY: Suppose $e \in G$ be the identity, then $a*e = a \ \forall a \in G$

$\Rightarrow \frac{ae}{2} = a \Rightarrow \frac{e}{2} = 1 \Rightarrow \boxed{e = 2}$

$\therefore$ Identity is 2.

INVERSE: Let $a \in G$, suppose a^{-1} is inverse of a ie) $a*a^{-1} = e$

Then $a*a^{-1} = \frac{aa^{-1}}{2} = 2 \Rightarrow a^{-1} = \frac{4}{a} \in G$ [$\because a \neq 0$]

So, for every element $a \in G$ inverse is $\frac{4}{a}$

Thus inverse axiom is satisfied.

COMMUTATIVE: Let a, b be any two elements of G, then.

$a*b = \frac{ab}{2} = \frac{ba}{2} = b*a$ [usual multiplicatn is commutative].

Hence $(G,*)$ is an abelian group.

④ Show that $(R-\{-1\}, *)$ is an abelian group where * is defd by $a*b = a+b+ab$ for all $a,b \in R$.

Sol: Here $R-\{-1\}$ means the set of real numbers except -1.

T.P $(R-\{-1\}, *)$ is an abelian group.

1) CLOSURE PROPERTY:-

Clearly $a*b = a+b+ab \in (R-\{-1\})$ [$a \neq -1, b \neq -1$].

2) ASSOCIATIVE PROPERTY:-

$$(a*b)*c = (a+b+ab)*c = (a+b+ab)+c+(a+b+ab)c$$
$$= a+b+ab+c+ac+bc+abc \quad -(A)$$

$$a*(b*c) = a*(b+c+bc) = a+(b+c+bc)+a(b+c+bc)$$
$$= a+b+c+bc+ab+ac+abc \quad -(B)$$

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

(3) IDENTITY:

Let 'e' be the identity element.

Then, $a*e = a \Rightarrow a+e+ae = a \Rightarrow e(1+a) = 0 \Rightarrow \boxed{e=0}$

Hence '0' is the identity element and $0 \in R-\{1\}$.

(4) INVERSE:

Let the inverse of a be a^{-1}

Then $a*a^{-1} = 0$ (Identity)

$a+a^{-1}+aa^{-1} = 0 \Rightarrow a^{-1}(1+a) = -a \Rightarrow \boxed{a^{-1} = \frac{-a}{1+a}} \in (R-\{1\})$

∴ Inverse element is $\frac{-a}{1+a}$

(5) COMMUTATIVE:

$a*b = a+b+ab = b+a+ba = b*a$

$\therefore a*b = b*a \quad \forall\ a,b \in (R-\{1\})$

∴ $(R-\{1\})$ is an abelian group.

---

(5) Prove that the set $A = \{1, \omega, \omega^2\}$ is an abelian group of order 3 under usual multiplication, where $1, \omega, \omega^2$ are cube roots of unity and $\omega^3 = 1$ [AU '06]

Sol: The following is the composition table of the elements in A with usual multiplication. T.P $(A,\cdot)$ is an abelian Group.

·	1	ω	ω^2
1	(1)	ω	ω^2
ω	ω	ω^2	(1)
ω^2	ω^2	(1)	ω

(1) CLOSURE PROPERTY:

All the elements in the table are the elements of A. Hence A is closed under ·

(2) ASSOCIATIVE PROPERTY:

Since multiplication of Complex numbers are associative.

(3) Identity:

The identity element is (1)

(4) Inverse:

The inverse of 1 is 1

The inverse of ω is ω^2

The inverse of ω^2 is ω

$\omega^4 = \omega^3 \cdot \omega$

$= 1 \cdot \omega$

$= \omega$.

(5) Commutative

From the table, the Commutative property is satisfies.

i.e. $\omega \cdot \omega^2 = \omega^3 = \omega^2 \cdot \omega$ etc.

∴ $(A,\cdot)$ is an abelian Group.

---

(6) Prove that the direct product of two groups is a group [AU '04]

Sol: Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups

Direct Product: $(G_1 \times G_2, *)$

Binary Operation '*' is defd: $(a_1,b_1) * (a_2,b_2) = (a_1 *_1 a_2, b_1 *_2 b_2)$

T.P $(G_1 \times G_2, *)$ is a group.

(I) ASSOCIATIVE OF $*$: $a*(b*c) = (a*b)*c$

Let $a, b, c \in G_1 \times G_2$ and $a=(x_1,y_1)$, $b=(x_2,y_2)$, $c=(x_3,y_3)$ for some $x_1, x_2, x_3 \in G_1$ & $y_1, y_2, y_3 \in G_2$.

Now,

$a*(b*c) = (x_1,y_1) * ((x_2*y_2) * (x_3,y_3))$

$= (x_1,y_1) * (x_2 *_1 x_3, y_2 *_2 y_3)$ [Def of $*$]

$= (x_1 *_1 (x_2 *_1 x_3), y_1 *_2 (y_2 *_2 y_3))$ [Def of $*$]

$= ((x_1 *_1 x_2) *_1 x_3, (y_1 * y_2) *_2 y_3)$ [By Ass Law for $*_1, *_2$]

$= (x_1 *_1 x_2, y_1 *_2 y_2) * (x_3,y_3)$

$= ((x_1,y_1) * (x_2,y_2)) * (x_3,y_3)$

$= (a*b)*c$

So associative axiom is satisfied in G for $*$.

(II) IDENTITY FOR $*$ IN $G_1 \times G_2$

If e_1 and e_2 are identities for G_1 and G_2 resp. then $e=(e_1,e_2)$ is the identity for $G_1 \times G_2$.

Let $a=(x_1,y_1) \in G_1 \times G_2$

$a*e = (x_1,y_1)*(e_1,e_2) = (x_1 *_1 e_1, y_1 *_2 e_2) = (x_1,y_1) = a$.

$e*a = (e_1,e_2)*(x_1,y_1) = (e_1 * x_1, e_2 * y_1) = (x_1,y_1) = a$.

So $a*e = e*a = a$.

Hence $e=(e_1,e_2)$ is the identity element in G.

(III) INVERSE FOR $*$ IN $G_1 \times G_2$

The inverse of an element e in $G_1 \times G_2$ is determined compotentwise, let $a' = (x_1,y_1)' = (x_1', y_1')$.

$a*a' = (x_1,y_1)*(x_1',y_1') = (x_1 *_1 x_1', y_1 *_2 y_1')$ [Def of $*$]

$= (e_1,e_2) = e$.

$a'*a = (x_1',y_1')*(x_1,y_1) = (x_1'*x_1, y_1'*_2 y_1) = (e_1,e_2) = e$

$\therefore a*a' = a'*a = e$

$\therefore G = G_1 \times G_2$ is a group.

---

(7) Prove that the set of all matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ forms an abelian group w.r.t multiplication. [AIM '15]

Sol: Let G be the set of all matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$

T-P $(G, \times)$ is an abelian group

CLOSURE PROD: Let $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G$ & $\begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in G$. Not both a, b zero

$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \in G$

$\therefore$ Closure prop is satisfied in G, $\therefore$ G is cld under $*$

$x^2+y^2 = (ac-bd)^2 + (ad-bc)^2 = a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd$
$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = a^2(c^2+d^2) + b^2(c^2+d^2) = (a^2+b^2)(c^2+d^2)$

INVERSE PROPERTY:

The inverse Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G$. where $a^2+b^2 \neq 0$.

Suppose $A' = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ be the inverse then $A * A' = I$.

$\Rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} * \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} ax-by & ay+bx \\ -bx-ay & -by+ax \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$

$\therefore ax-by = 1 \rightarrow (1)$ & $ay+bx = 0 \Rightarrow (2)$

$(1) \times a \Rightarrow a^2x - aby = a$

$(2) \times b \Rightarrow b^2x + aby = 0$

$+ \quad (a^2+b^2)x = a \Rightarrow x = \frac{a}{a^2+b^2}$ $[\because a^2+b^2 \neq 0]$.

$(2) \Rightarrow ay = -bx \Rightarrow y = -\frac{b}{a} \cdot \frac{a}{a^2+b^2} = -\frac{b}{a^2+b^2}$.

$\therefore$ Inverse $A' = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}$. $x^2+y^2 = \frac{1}{a^2+b^2}$

Now $x^2+y^2 = \frac{a^2}{(a^2+b^2)^2} + \frac{b^2}{(a^2+b^2)^2} = \frac{a^2+b^2}{(a^2+b^2)^2} = \frac{1}{a^2+b^2} \neq 0$

$\therefore A' \in G$ Hence Inverse exist.

(3) **Associativity**: W.K.T matrix multiplication is associative Hence it is true in G also.

(4) **Identity**:

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in G be the identity element.

$\therefore A * I = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} * \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = A$.

$I * A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} * \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = A$.

(5) **Commutative**:

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in G$, $a^2+b^2 \neq 0$ & $c^2+d^2 \neq 0$ we

$A * B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} * \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix}$

$B * A = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} * \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix}$

$\therefore A * B = B * A \quad \forall A, B \in G$.

Hence $(G, *)$ is an abelian group.

PROBLEMS UNDER SEMIGROUPS

① Let $S = \mathbb{Q} \times \mathbb{Q}$, be the set of all ordered pairs of rational numbers and given that $(a,b) * (x,y) = (ax, ay+b)$.

(i) Check $(S,*)$ is a semigroup. Is it Commutative?

(ii) Also find the identity element of S & inverse element of S.

Sol: (i) T.P $(S,*)$ is a semigroup.

(a) closure property : obviously $*$ satisfies closure Property.

(b) Associative Property:

$$[(a,b)*(x,y)]*(c,d) = [(ax, ay+b) * (c,d)]$$
$$= [axc, adx + ay + b] \rightarrow (1)$$
$$(a,b) * [(x,y) * (c,d)] = [(a,b) * (xc, xd+y)]$$
$$= [axc, a(xd+y)+b]$$
$$= [acx, adx, ay+b] \rightarrow (2)$$

$\therefore [(a,b)*(x,y)] * (c,d) = (a,b) * [(x,y) * (c,d)]$

$\therefore (S,*)$ is a associative.

$\therefore (S,*)$ is a semigroup.

(c) T-P $(S,*)$ is commutative

$$(a,b)*(x,y) = (ax, ay+b). \rightarrow (3)$$
$$(x,y)*(a,b) = (xa, ya - xb + y) = (ax, bx+y) \rightarrow (4)$$

From (3) & (4) $(a,b)*(x,y) \neq (x,y)*(a,b)$

$\therefore (S,*)$ is not Commutative.

(ii) TO FIND: IDENTITY ELEMENT OF S

Let (e_1, e_2) be the identity element of $(S,*)$

Then for any $(a,b) \in S$

$$(a,b) * (e_1, e_2) = (a,b)$$
$$(ae_1, ae_2 + b) = (a,b)$$
$$\Rightarrow ae_1 = a \text{ \& } ae_2 + b = b$$
$$e_1 = 1 \text{ \& } e_2 = \frac{b-b}{a} = 0, a \neq 0$$

The identity element $= (e_1, e_2) = (1,0)$

TO FIND: INVERSE ELEMENT OF S

Let $(a,b) \in S$ & (a^{-1}, b^{-1}) is the inverse such that

$$(a,b) * (a^{-1}, b^{-1}) = (e_1, e_2) = (1,0)$$
$$\Rightarrow (aa^{-1}, ab^{-1} + b) = (1,0)$$
$$\Rightarrow aa^{-1} = 1 \text{ \& } ab^{-1} + b = 0$$
$$\boxed{a^{-1} = \frac{1}{a}} \text{ \& } \boxed{b^{-1} = \frac{-b}{a}}, a \neq 1$$

Hence the element (a,b) has an inverse if $a \neq 0$ & its inverse is $(\frac{1}{a}, -b/a)$.

If $*$ is a binary operation on the set R of real numbers defined by $x * y = x + y + 2xy$.

(i) Find $\langle R, * \rangle$ is a semigroup

(ii) Find the identity element if it exists.

(iii) Which elements has inverse

I TO PROVE $\langle R, * \rangle$ is a semigroup

(a) CLOSURE PROPERTY:

$\because x, y \in R \Rightarrow x+y \in R \;\&\; xy \in R$

$\therefore x+y+2xy \in R$

$x * y \in R$

$\therefore$ '$*$' satisfies closure Property.

(b) ASSOCIATIVE PROPERTY:

$$(x*y)*z = (x+y+2xy)*z$$
$$= (x+y+2xy)+z+2(x+y+2xy)z$$
$$= x+y+2xy+z+2xz+2yz+4xyz$$
$$= x+y+z+2xy+2yz+2xz+4xyz \rightarrow (1)$$
$$x*(y*z) = x*(y+z+2yz)$$
$$= x+(y+z+2yz)+2x(y+z+2zy)$$
$$= x+y+z+2yz+2xy+2xz+4yzx \rightarrow (2)$$

$\because (x*y)*z = x*(y*z)$

$\therefore *$ is a associative.

Hence $\langle R, * \rangle$ is a semigroup

II: TO FIND IDENTITY ELEMENT:

If identity element exist, let it be 'e'. For any $a \in R$.

$$a*e = a \Rightarrow a+e+2ae = a \Rightarrow e(1+2a) = a-a = 0 \Rightarrow \boxed{e=0}$$

$e = 0 \in R$ $\quad [1+2a \neq 0]$

$\therefore$ Identity element exist

III: TO FIND INVERSE ELEMENT:

Let a^{-1} be the inverse of an element $a \in R$. Then

$$a * a^{-1} = e \Rightarrow a+a^{-1}+2aa^{-1} = e \Rightarrow a^{-1}(1+2a) = e-a = 0-a \quad [\because e=$$

$$\boxed{a^{-1} = \frac{-a}{1+2a}}, \quad a \neq -\frac{1}{2}, \; a^{-1} \text{ exist}.$$

(5) Show that the binary operation $*$ defd $\langle R, * \rangle$ where $x*y = \max(x,$ is associative (or) P.T $(R, *)$ is a semigroup.

Sol: T.P $\langle R, * \rangle$ is a semigroup.

(a) CLOSURE PROPERTY

Let $x, y \in R$ then $\max\{x,y\} \in R$

$\Rightarrow x*y \in R$.

$\therefore$ closure Property is satisfied.

(b) ASSOCIATIVE PROPERTY

$$(x*y)*z = \max\{x*y, z\}$$
$$= \max\{\max\{x,y\}, z\}$$
$$= \max\{x,y,z\} \rightarrow (1)$$
$$x*(y*z) = \max\{x, y*z\}$$
$$= \max\{x, \max\{y,z\}\}$$
$$= \max\{x,y,z\} \rightarrow (2)$$

$\because (x*y)*z = x*(y*z)$

Hence From (a) & (b)

$(*)$ is a semigroup

PROBLEMS UNDER MONOIDS

(1) If the set N of natural numbers is a semigroup under the operation $x * y = \max\{x, y\}$. Is it a Monoid? [AU: Dec 02]

Sol: Given: $(N, *)$ is a semigroup, $N = \{0, 1, 2, \ldots\}$.

To check: $(N, *)$ is a Monoid.

IDENTITY:

$0 \in N$ is the identity

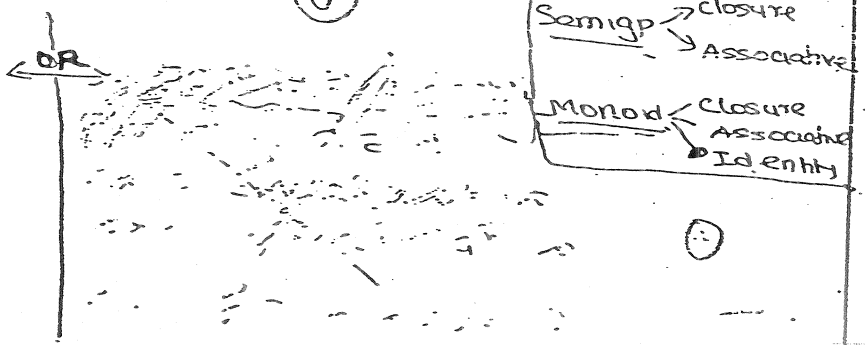
For any $a \in N$,

$a * 0 = \max\{a, 0\} = a$

$0 * a = \max\{0, a\} = a$

$\therefore a * 0 = 0 * a = a \quad \forall a \in N$

Hence $(N, *)$ is a Monoid.



(2) If Z_6 is the set of equivalence classes generated by the equivalence relation "Congruence modulo 6", prove that (Z_6, X_6) is a monoid where the operation X_6 on Z_6 is defined on $[j] X_6 [k] = [(j \times k) \bmod 6]$ for any $[j], [k] \in Z_6$

Sol: We know $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$ [AU: Dec 08]

From: Composition table / $[j] X_6 [k] = [(j \times k) \bmod 6]$

T.P: $\langle Z_6, X_6 \rangle$ is a Monoid

(a) CLOSURE PROPERTY

The body of the table contains only all the elements of Z_6.

So, Z_6 is closed under 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]	[0]	[5]	[4]	[3]	[2]	[1]

(b) ASSOCIATIVITY PROPERTY

$\therefore [a] X_6 ([b] X_6 [c]) = [a] X_6 (bc \bmod 6)$

$= abc \bmod 6$

Here X_6 depends on associativity of usual multiplication

$\therefore X_6$ is associative.

$i +_n j = i + j$

$i \times_n j = ij$ if value is $\geq n$ take rem value

$[5] X_6 [5] = [(5 \times 5) \bmod 6] = [25 \bmod 6]$

$25 = 1 \bmod 6$ write

(c) IDENTITY:

From the table we find $[1] X_6 [a] = [a]$ for all $[a] \in Z_6$.

$\therefore [1]$ is the identity element.

Multiple of identity is 1 Hence (Z_6, X_6) is a Monoid.

of 11 is 0

INVERSE:- To find the inverse of an elt P_i, find P_1 [The 1st elt in the gn set] in the row through P_i, the column head of P_1 is the inverse of P_i ie $\Rightarrow P_i^{-1}$.

③ Show that the set $G = \{1,2,3,4,5\}$ is not a monoid or semigroup or group under addition Modulo 6.

Sol) Gn: $G = \{1,2,3,4,5\}$ 2M

T-P: $\langle G, +_6 \rangle$ is not a monoid, semigp or Group.

CLOSURE PROPERTY

All the entries in the Composition table do not belong to G.

In particular $0 \notin G$.

$\therefore$ G is not closed w.r.t $+_6$.

Hence $\langle G, +_6 \rangle$ is not a monoid, Semigroup or group. group, semigp. monoid.

Composition Table $+_6$

$+_6$	[1]	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4.

$i +_6 j \equiv [(i+j) \text{ Mod } n]$

④ Prove that the set $\{0,1,2,3,4\}$ is a monoid and hence a finite abelian group of order 5 under addition modulo 5

(or)

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

Sol: Let $G = \{0,1,2,3,4\}$

I: T-P $\langle Z_5, +_5 \rangle$ is a monoid.

→ CLOSURE PROPERTY

∵ All the entries in the Composition table belongs to G ✓

Z_5 is Closed in $+_5$.

→ ASSOCIATIVE PROPERTY.

$+_5$ depends on associativity of usual addition Eg $(2+_5 3)+_5 4 = 0+_5 4 = 4$.

$\therefore$ $+_5$ is associative. $2+_5(3+_5 4) = 2+_5 2 = 4$

Composition table

$+_5$	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	2

$3+_5 2 = 5 \equiv 0 \text{ Mod } 5$

$4+_5 3 = 7 \equiv 2 \text{ Mod } 5$

→ IDENTITY PROPERTY

0 is the identity element.

$\therefore$ $\langle Z_5, +_5 \rangle$ is a Monoid.

∵ $0+_5[a] = [a]$ $\forall a \in G$

$0+_5 1 = 1$ | $0+_5 3 = 3$ | $0+_5 5 =$

$0+_5 2 = 2$ | $0+_5 4 = 4$ |

II T-P $\langle Z_5, +_5 \rangle$ is a abelian group.

→ INVERSE PROPERTY

The inverse of 0,1,2,3,4 are 0,4,3,2,1 resp

→ COMMUTATIVE PROPERTY

$+_5$ depends on commutativity of usual addition

$\therefore$ $+_5$ is commutative.

ie, the gn set is a finite abelian group of order 5 under $+_5$.

SUBGROUP

SUBGROUP:

Let $(G,*)$ be a group. Let e be the identity element in G and Let $H \subseteq G$. If H itself is a group with the same operam * and the same identity element e. , (or)

Let $(G,*)$ be a group & $H \subseteq G$. $(H,*)$ is called a subgroup of $(G,*)$ if H itself is a group w.r.t $*$.

Eg: $(Q,+)$ is a subgroup of $(R,+)$.

TRIVIAL SUBGROUP / IMPROPER SUBGROUP

For any group $(G,*)$, $\{\{e\},*\}$ & $(G,*)$ are subgroups, called trivial subgroups.

NON-TRIVIAL SUBGROUP / PROPER SUBGROUP

All other subgroups other than $\{\{e\},*\}$ & $(G,*)$ are called non-trivial subgroup.

CONDITION FOR A NON-EMPTY SUBSET H TO BE A SUBGROUP OF G.

$(H,*)$ is said to be a subgroup of $(G,*)$ if

(i) H is closed for the operation $*$. $\forall a,b \in H$, $a*b \in H$.

(ii) H contains the identity elt e. i.e) $e \in H$ where e is the identity of G

(iii) For any $a \in H$, $a^{-1} \in H$.

NECESSARY AND SUFFICIENT CONDITION FOR A SUBGROUP:

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

PROOF

NECESSARY CONDITION:

Let H be a subgroup of a group G and $a,b \in H$

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

Since H is a subgroup and $b \in H$, b^{-1} must exist & $b^{-1} \in H$.

Now $a \in H$, $b^{-1} \in H \Rightarrow a*b^{-1} \in H$ [By closure Prop].

SUFFICIENT CONDITION:

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

T-P H is a subgroup of G.

(i) IDENTITY:

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

Hence the identity element, $e \in H$.

ii) INVERSE:

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

e) Every element 'a' of H has its inverse a^{-1} is in H

iii) CLOSURE:

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

(iv) ASSOCIATIVE :-

Now $H \subseteq G$ and the associative law holds good for G as G is a Group. Hence it is true for the elements of H.

Thus all axioms for a group are satisfied for H. Hence H is a subgroup of G.

THEOREM 2 (X) 8M (X) U-Q.

The intersection of two subgroups of a group $(G, *)$ is also a subgroup of $(G, *)$.

PROOF:

Let H & K are subgroups of $(G, *)$. T.P $H \cap K$ is subgp of $(G, *)$

We have $H \cap K \neq \phi$ [$\because$ atleast identity elt is common to both H & K].

Let $a, b \in H \cap K \Rightarrow a \in H \cap K$ & $b \in H \cap K$

$a \in H \cap K \Rightarrow a \in H$ & $a \in K$

$b \in H \cap K \Rightarrow b \in H$ & $b \in K$

Now, $a \in H, b \in H \Rightarrow a * b^{-1} \in H$ [H is a subgp, THM1].

$a \in K, b \in K \Rightarrow a * b^{-1} \in K$ [K is a subgp, THM1].

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

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

$H \cap K$ is a subgroup of G [By thm].

NOTE: The union of two subgroups need not be a subgroup.

Eg: Let $(Z, +)$ is a group

Let H & K are subgp of $(Z, +)$

where $H = \{\ldots -4, -2, 0, 2, 4, 6, \ldots\} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$

$K = \{\ldots -6, -3, 0, 3, 6, 9, \ldots\} = \{0, \pm 3, \pm 6, \pm 9 \ldots\}$

$H \cup K = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \ldots\}$

$3, 8 \in H \cup K$ but $3 + 8 = 11 \notin H \cup K$.

$\therefore H \cup K$ is not closed w.r.t addition.

$\therefore H \cup K$ is not a subgp of G.

THEOREM 3 (X) 8M.

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

PROOF:

Assume H & K are two subgroups of G & $H \subseteq K$ or $K \subseteq H$.

T.P $H \cup K$ is a subgroup.

$\because H$ & K are subgroup & $H \subseteq K \Rightarrow H \cup K = K$

(or) H & K are subgroup & $K \subseteq H \Rightarrow H \cup K = H$.

$\therefore H \cup K$ is a subgroup.

Converse:

Suppose $H \cup K$ is a subgroup.

T.P one is contained in the other i.e. $H \subseteq K$ or $K \subseteq H$.

Suppose $H \not\subseteq K$ or $K \not\subseteq H$.

Then $\exists$ elts a, b s.t. $a \in H$ & $a \notin K$ $\rightarrow$ (1)

$b \in K$ & $b \notin H$ $\rightarrow$ (2)

Clearly $a, b \in H \cup K$.

Since $H \cup K$ is a subgroup of G, $ab \in H \cup K$

Hence $ab \in H$ or $ab \in K$.

Case 1: Let $ab \in H$. $\because a \in H, a^{-1} \in H$

Hence $a^{-1}(ab) = b \in H$, $\Rightarrow\Leftarrow$ (2).

Case 2: Let $ab \in K$. $\because b \in K, b^{-1} \in K$

Hence $b^{-1}(ab) = a \in K$, $\Rightarrow\Leftarrow$ (1)

$\therefore$ our assumption is wrong.

$\therefore H \subseteq K$ or $K \subseteq H$.

PROBLEMS

(1) Let $(H, \circ)$ be a subgroup of $(G, \circ)$. Let $N = \{x / x \in G, xHx^{-1} = H\}$. Show that $(N, \circ)$ is a subgroup of G.

Sol: Let $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$ when $h_1, h_2 \in H$.

Now $(xh_1x^{-1})(xh_2x^{-1})^{-1} = (xh_1x^{-1})[(x^{-1})^{-1} h_2^{-1} x^{-1}]$

$= x h_1 (x^{-1} (x^{-1})^{-1} h_2^{-1} x^{-1})$

$= x h_1 e h_2^{-1} x^{-1} = x h_1 h_2^{-1} x^{-1}$

$\in xHx^{-1}$ [$\because h_1 h_2^{-1} \in H$].

$\therefore H$ is a subgroup.

xHx^{-1} is a subgroup of G.

$O(H) = 2$

$\{0, x\}$

$\{0, 1, x\}$

$\{0, 1, 0x, 1x\}$

(2) Find all the non-trivial subgroups of $(Z_6, +_6)$ [AU '06]

Sol: $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$ if H is subgroup of Z_6 then $o($

Hence $o(H) = 1, 2, 3$ or 6

$o(H) = 1 \Rightarrow H = [0]$.

$o(H) = 2 \Rightarrow H = \{[0], [x]\} \Rightarrow \therefore H = \{[0], [3]\}$

$[x] + [x] = 0 \Rightarrow x = 3$

$o(H) = 3 \Rightarrow H = \{[0], [x], [2x]\} \Rightarrow$

$\therefore H = \{[0], [2], [4]\}$.

$o(H) = 6 \Rightarrow H = \{Z_6, +_6\}$.

$+_6$	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

③ Check whether $H_1 = \{0, 5, 10\}$ & $H_2 = \{0, 4, 8, 12\}$ are subgroups of Z_{15} w.r.t $+_{15}$.

Sol

$H_1 = \{0, 5, 10\}$

$+_{15}$	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

$(H_1, +_{15})$
Table 1

$H_2 = \{0, 4, 8, 12\}$

$+_{15}$	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

$(H_2, +_{15})$.
Table 2

Table 1 : $(H_1, +_{15})$: All the entries in the addition table for H_1 are the elements of H_1.

$\therefore$ **H_1 is a subgp of Z_{15}**

Table 2 : $(H_2, +_{15})$: All the entries in the addition table for H_2 are not the elements of H_2

$\therefore$ **H_2 is not a subgroup of Z_{15}**

---

④ Find all the subgroups of $(Z_9, +_9)$.

Sol $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$,

$\frac{O(H)}{O(G)} = O(H)/9$

Hence $O(H) = 1, 3$

$O(H) = 1 \Rightarrow H = \{0\}$ → 0 is fixed bcz 0 is identity of $+$

$O(H) = 3 \Rightarrow H = \{0, 3, 6\}$

$+_9$	0	3	6
0	0	3	6
3	3	6	0
6	6	0	3

$+_9$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

$H = \{0, 1, 2\}$. (try for many values).

$+_9$	0	1	2
0	0	1	2
1	1	2	3
2	2	3	4

→ not subgp elements bcz 3, 4 is present.

find trivial means tell identity + coholeset
non-trivial → not that 2 tell others.

CYCLIC GROUP

CYCLIC GROUP

A group $(G,*)$ is called the cyclic group if there exist an element $a \in G$ s.t every element $x \in G$ is expressed as $\boxed{x = a^m}$ or ma for any integer m.

- 'a' is called the generator of the cyclic group G.
- $G = \langle a \rangle$ denote the cyclic group G generated by the element a.

Eg:

① Consider the group $G = \{1, -1, i, -i\}$ under multiplication.

→ G can be generated by i, $\langle a \rangle = \{i^1, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$

$[\because i = i,\ i^2 = -1,\ i^3 = i^2 \cdot i = -i,\ i^4 = i^2 \cdot i^2 = 1]$.

→ G can be generated by $-i$, $\langle a \rangle = \{-i^1, -i^2, -i^3, -i^4\} = \{-i, -1, i, 1\}$

$[\because -i = -i,\ -i^2 = -(-1) = 1,\ -i^3 = -(i^2) \cdot i = -(-1) \cdot i = i,\ -i^4 = -[i]^2[i]^2 = -1]$

② Consider the group $G = \{1, \omega, \omega^2\}$ under multiplication

→ G can be generated by ω, $\langle \omega \rangle = \{\omega, \omega^2, \omega^3\} = \{1, \omega^2, \omega^3\}$

$[\because \omega = \omega,\ \omega^2 = \omega^2,\ \omega^3 = 1 \quad \because \omega^3 = 1]$

→ G can be generated by ω^2, $\langle \omega^2 \rangle = \{\omega^2, \omega^4, \omega^6\} = \{\omega^2, \omega, 1\} = G$

$[\because \omega^2 = \omega^2,\ \omega^4 = \omega^3 \cdot \omega^1 = 1 \cdot \omega = \omega,\ \omega^6 = \omega^3 \cdot \omega^3 = \omega^3 = 1]$

③ In the group $(Z_{12}, +_{12})$, $\{[0], [3], [6], [9]\}$ is the cyclic subgp generated by $[3]$.

$\because \langle [3] \rangle = \{0, 6, 9, 0\} = \{0, 6, 9\}$.

THEOREM 1

Every cyclic group is abelian.

PROOF

Let $(G, *)$ be a cyclic group with 'a' as a generator.

Then $G = \{a^n \mid n \in Z\}$

Let $x, y \in G \Rightarrow x = a^{m_1}$, $y = a^{m_2}$ for some $m_1, m_2 \in Z$

$$x * y = a^{m_1} * a^{m_2} = a^{m_1 + m_2} = a^{m_2 + m_1} = a^{m_2} * a^{m_1} = y * x$$

$\therefore x * y = y * x$.

$\therefore G$, cyclic group is abelian.

NOTE

Converse of the above theorem need not be true

Eg $(\mathbb{Q}, +)$ is an abelian group but not a cyclic group

THEOREM: Let $(G,*)$ be a finite cyclic group generated by an element $a \in G$. If $O(G)=n$ then $a^n=e$ & so $G=\{a, a^2, a^3, a^{n-1}, a^n=e\}$. Further $O(a)=n$. That is n is the least positive integer such that $a^n=e$ [A/O/N]

PROOF

Given $(G,*)$ is a finite cyclic group generated by a.

1st I-P: $a^m=e$ is not possible for $m<n$.

Assume, it is possible ie $a^m=e$, $m<n$.

$\because$ G is a cyclic group generated by a

$\Rightarrow$ Any elt $x \in G$ is an integral power of a

$\Rightarrow x=a^k$ for some integer k.

Now for the integers m, k, by Euclidian division Algorithm we can find integers q & r s.t $k=mq+r$, $0 \le r < m$.

$\therefore x = a^k = a^{mq+r} = a^{mq} * a^r = e * a^r = a^r$

Thus any element of G is a^r for $r<m$.

This means the no: of elements of a is atmost m.

$\therefore O(G)=m<n \Rightarrow \Leftarrow$ [$\because O(G)=n$]

Hence $a^m=e$ is not possible for $m<n$.

$\therefore a^n=e$.

2nd I-P: The elements $a, a^2, a^3, \ldots a^n$ are all distinct.

Suppose it is not true, then there are repetitions

ie $a^s=a^r$, $0<r<s \le n$.

$\Rightarrow a^s * a^{-r} = a^r * a^{-r}$

$a^{s-r} = a^0 = e$ $\quad 0<s-r<n$

$\Rightarrow \Leftarrow$ to 1st part.

$\therefore$ All the elements are distinct.

Hence $a, a^2, a^3, \ldots, a^n=e$ are all distinct.

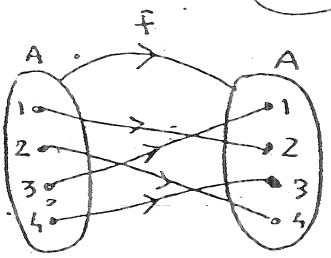
$\because O(G)=n$, it follows $G=\{a, a^2, a^3, \ldots, a^n=e\}$ & $a^n=e$

So $O(a)=n$.

PERMUTATION GROUPS. (S_n)

PERMUTATION:

Let A be a finite set. A bijection (1-1 & onto) from A onto itself i.e) $f: A \to A$ is called Permutation on A.



If $A = \{a_1, a_2, \ldots, a_n\}$ then permutation on A is $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ where row $b_1, b_2, \ldots, b_n$ is just a rearrangement of the elts of $a_1, a_2, \ldots, a_n$

SYMMETRIC SET:

If S is a finite set having 'n' distinct elements then we shall have n! distinct permutations of the sets. The set of all distinct permutations of degree n defined on the set S is denoted by S_n called Symmetric set of permutations of degree n.

NOTE $O(S_n) = n!$

PROBLEMS

① List all the elements of the symmetric set S_3, where $S = \{1,2,3\}$ & prove that $(S_3, \circ)$ is a non abelian group.

Sol :- Given $S = \{1, 2, 3\}$

Total no: of permutation on $S = 3! = 6$.

Elements of symmetric set $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$.

where $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$; $P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$; $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$;

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

The operation 'o', product of permutations defined on the set $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ is gn in the table.

o	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_1	P_4	P_3	P_6	P_5
P_3	P_3	P_5	P_1	P_6	P_4	P_2
P_4	P_4	P_6	P_2	P_5	P_1	P_3
P_5	P_5	P_3	P_6	P_1	P_4	P_2
P_6	P_6	P_4	P_5	P_2	P_3	P_1

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

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

$P_2 \circ P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_4$

$P_2 \circ P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_3$

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

$P_3 \circ P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_5$

$P_3 \circ P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1$

1	2	3
↓	↓	↓
1	2	3
↓	↓	↓
1	3	2

$P_3 \circ P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_6$; $P_3 \circ P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$; $P_3 \circ P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_4$

$P_4 \circ P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_6$; $P_4 \circ P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$; $P_4 \circ P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_5$

$P_4 \circ P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1$; $P_5 \circ P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_3$; $P_5 \circ P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_6$

$P_5 \circ P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1$; $P_5 \circ P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

T-P $(S_3, \circ)$ is a non-abelian group.

(i) CLOSURE:

Since the body of the table contains only the elements of S_3. $\therefore (S_3, \circ)$ is closed.

(ii) ASSOCIATIVITY

We know composition of function's is associative and so it is true in S_3 also. $\therefore (S_3, \circ)$ is associative.

i.e: $P_1 \circ (P_3 \circ P_4) = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \circ \left[\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right]$

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

$(P_1 \circ P_3) \circ P_4 = \left[\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right] \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = P_6$

$\therefore P_1 \circ (P_3 \circ P_4) = (P_1 \circ P_3) \circ P_4.$

(iii) IDENITY:

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

(iv) INVERSE:- From the table.

$P_1^{-1} = P_1$; $P_2^{-1} = P_2$; $P_3^{-1} = P_3$; $P_4^{-1} = P_5$; $P_5^{-1} = P_4$; $P_6^{-1} = P_6$.

Thus: inverse exists for every element.

Hence inverse axiom is verified.

$\therefore (S_3, \circ)$ is a Group.

T-P $(S_3, \circ)$ is non-abelian group.

From the table; $P_3 \circ P_4 = P_6$ & $P_4 \circ P_3 = P_2$.

$\therefore P_3 \circ P_4 \neq P_4 \circ P_3$

Hence the group is not commutative/abelian

DIHEDRAL GROUP (D_n) (8M.)

DIHEDRAL GROUP : $D_n \rightarrow n^{th}$ DIHEDRAL GROUP

The group of symmetries of a regular polygon of n sides is called a dihedral group $(D_n, *)$, where the transformations are n rotations about its centre through angles $\frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \frac{2n\pi}{n}$ in the anticlockwise sense.

NOTE:

① By considering the symmentries of a regular polygon of n sides, we obtain a set of permutations and the set of these Permutations form a group w.r.t the product of Permutations.

② This Permutation group is called the Dihedral gp $(D_n, \circ)$.

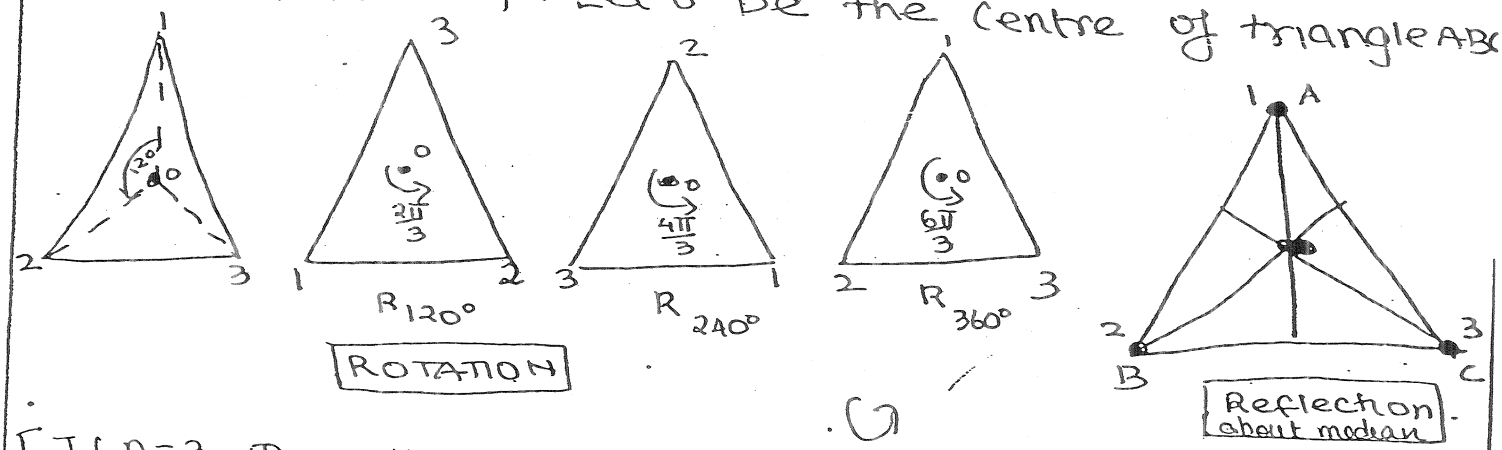
The Dihedral group $(D_n, \circ)$ is a subgp of the Symmetric gp $(S_n, \circ)$ whose elements are ~~[illegible]~~

Problems on Dihedral Groups :-

① List all the elements of dihedral gp $(D_3, 0)$ & form the Composition table

Sol: The elements of $(D_3, 0)$ are the permutations obtained by considering the symmetries of an equilatral triangle

Consider an equilateral triangle, vertices A, B, C are labelled 1, 2, 3 resp. Let o be the centre of triangle ABC



[If $n=3$, D_3 is the group of symmetries of an equilateral $\triangle$le

Since regular polygon of 3 sides is the equilateral $\triangle$le]

The symmetries are the rotations about the centre o & the reflections R_1, R_2, R_3 about the altitudes through the vertices 1, 2, 3 resp.

The Rotations are :-

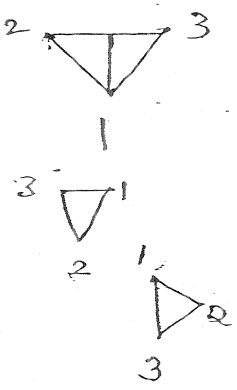
$P_1 = R_{120°} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; $P_2 = R_{240°} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$; $P_3 = R_{360°} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

The Reflections through median A, B, C resp

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

Composition table for Dihedral Gp $(D_3, 0)$

o	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_3	P_1	P_5	P_6	P_4
P_3	P_3	P_1	P_2	P_6	P_4	P_5
P_4	P_4	P_6	P_5	P_1	P_3	P_2
P_5	P_5	P_4	P_6	P_2	P_1	P_3
P_6	P_6	P_5	P_4	P_3	P_2	P_1

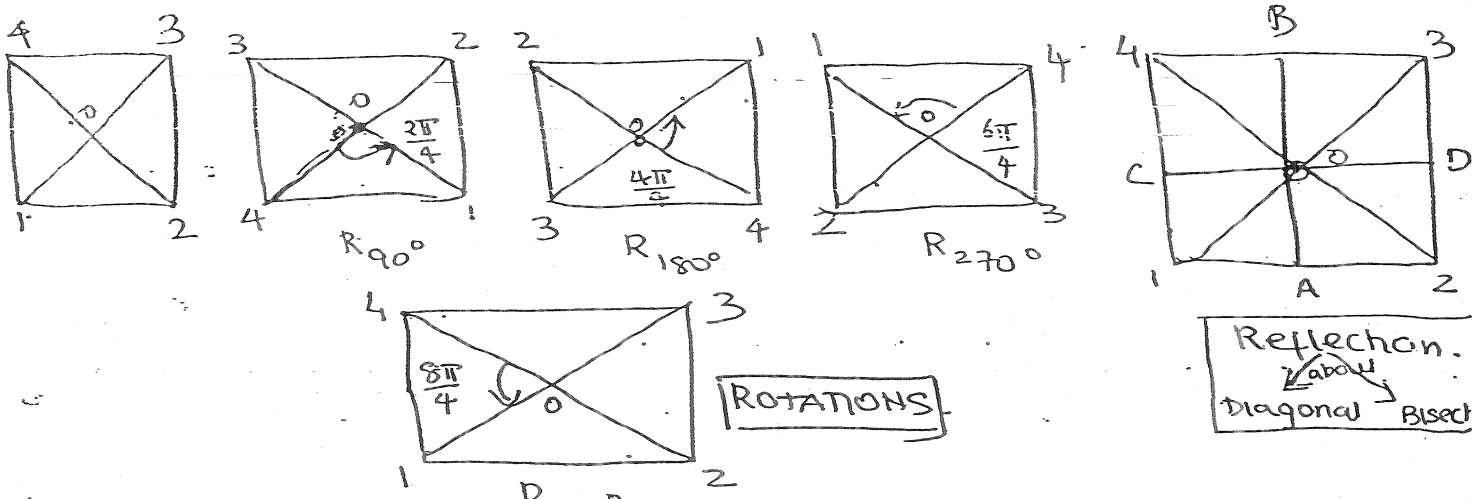


NOTE : $D_3 = S_3$ ∵ S_3 is permutation gp D_3 is also permuta gp ∵ the 3 rotations & 3 reflections are the symmetries of the

② List the elements of the Dihedral gp $(D_4, \circ)$.

Sol: If $n=4$, D_4 is the dihedral group of symmetries of a regular polygon with 4 sides, which is a square.

Let 1,2,3,4 are the vertices of the square.



ROTATIONS

Reflection about Diagonal / Bisect

The symmetries are the rotations about the centre through 90°, 180°, 270°, 360° and the reflections about the diagonals and the bisectors of the sides.

The Rotations are

$P_4 = R_{90°} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$; $P_3 = R_{180°} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$; $P_2 = R_{270} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

$P_1 = R_{360°} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

The Reflections through the diagonals & the bisectors are

$P_5 = R_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$; $P_6 = R_{24} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ → About Diag

$= R_{AB} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$; $P_8 = R_{CD} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ → About Bisect

$\therefore$ D_4 Consists of 8 symmetries of the square.

NOTE

Permutation group, $S_4 = \{1, 2, 3, 4\}$.

$(S_4) = 4! = 24$ elements.

Dihedral group, $D_4 = 8$ elements.

$\therefore$ D_4 is a subset of S_4.

Indeed D_4 is a Subgroup of S_4

Hence D_4 is a permutation group.

CYCLIC PERMUTATIONS

CYCLIC PERMUTATION:

The permutation f defined on $S=\{a_1, a_2, \ldots, a_n\}$ is said to be cyclic if $f(a_1)=a_2$, $f(a_2)=a_3$, ..., $f(a_{r-1})=a_r$ & $f(a_r)=a_1$ & $f(b)=b$ for all other elements.

Eg: $f=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix}$ → CYCLIC PERMUTATION

Represented by a cycle: (1 3 2). $1\to3\to2\to1$.

DISJOINT CYCLES:

Two cycles are said to be disjoint if they have no elements in common. Any permutation can be expressed as a pt of disjoint cycles.

Eg: (1 3 6) & (2 4 5) → Disjoint Cycles

TRANSPOSITION:

A cycle of length two is called a transposition.

Eg: (1,3) ; (2 5 3) → (2,3) (2,5).

EVEN AND ODD PERMUTATIONS:

A permutation is said to be an even permutation if it is expressed as a product of even number of transposition otherwise it is said to be and odd permutation.

PROBLEMS:

① Express $\theta=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&4&5&1&6&7&9&8\end{pmatrix}$ in SQ as a product of disjoint cycles. Decide its order & test it is even or odd

SQ $\theta=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&4&5&1&6&7&9&8\end{pmatrix}$ $1\to2\to3\to4\to5\to1$, $8\to9\to8$, 6 & 7 are fixed - Ignore.

CYCLE, $\theta=(1\,2\,3\,4\,5)(8\,9)$

ORDER, $\theta=$ l.c.m $\{5,2\}=10$.

TRANSPOSITION, $\theta=(1\,2)(1\,3)(1\,4)(1\,5)(8\,9)$ is a ptd of 5 transposition

∴ θ is a odd Permutation.

② Compute the product (12) (24) (36) as a permutation on $\{1,2,3,4,5,6\}$. Determine (i) It is even or odd (ii) Its order

SQ: Let $\sigma=(12)(24)(36)$

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

Permutation, $\sigma=\begin{pmatrix}1&2&3&4&5&6\\4&1&6&2&5&3\end{pmatrix}$ as permutation.

CYCLE $\sigma=(1\,4\,2)(3\,6)$.

ORDER $\sigma=$ l.c.m $\{3,2\}=6$.

TRANSPOSITION $\sigma=(1\,4)(1\,2)(3\,6)$, ptd of 3 transposition.

∴ σ is an odd permutation.

COSETS AND LAGRANGE'S THEOREM

Let $(H,*)$ be a subgroup of $(G,*)$

LEFT COSET: $a*H = \{a*h : h \in H\}$, for any $a \in G$

RIGHT COSET: $H*a = \{h*a : h \in H\}$, for any $a \in G$

NOTE:

1. If H is a subgroup of G then H itself is a Left coset as well as right coset.
2. If $a \in H*b$ then $H*a = H*b$
3. If $a \in b*H$ then $a*H = b*H$
4. The union of all left or right cosets of H is equal to G.

EXAMPLE 2(1)

(1) Let $(Z_4, +_4)$ be a group and $H = \{0,2\}$ be a subgroup of Z_4.

Sol: $Z_n = \{0,1,\cdots,n-1\}$; $Z_4 = \{0,1,2,3\}$

Left coset:

$0+H = \{0,2\} = H$

$1+H = \{1,3\}$

$2+H = \{2,0\} = H$

$3+H = \{3,1\} = 1+H$

$\therefore$ $0+H$ and $1+H$ are distinct Left Coset in Z_4.

(2) Let $G = \{1,-1,i,-i\}$ is a group under multiplication & $H = \{1,-1\}$ is a subgroup of G.

Sol Left Coset:

$1 \times H = \{1,-1\} = 1H = H$

$-1 \times H = \{-1,1\} = H$

$i \times H = \{i,-i\} = iH$

$-i \times H = \{-i,i\} = iH$

H & iH are distinct Left cosets of H in G.

RIGHT COSET:

$H \times 1 =$

(3) Let $G = \{1, a, a^2, a^3\}$ $(a^4 = 1)$ is a group & $H = \{1, a^2\}$ is a subgroup of G under multiplication.

Sol Left Coset:

$1 \times H = \{1, a^2\} = 1H$

$a \times H = \{a, a^3\} = aH$

$a^2 \times H = \{a^2, 1\} = 1H$

$a^3 \times H = \{a^3, a\} = aH$

$\therefore$ 1H & aH are distinct Left Cosets

RIGHT COSET:

THEOREM 1

Any right (or left) cosets of H in G are either disjoint or Identical

PROOF:

Let H be a subgroup of a group G.

For any $a, b \in G$ then $H*a$ & $H*b$ be two right cosets of H

I-P Either $(H*a) \cap (H*b) = \phi$ (D: disjoint, $A \cap B = \phi$)

(or)

$H*a = H*b$

Suppose $(H*a) \cap (H*b) \neq \phi \Rightarrow \exists : x \in (H*a) \cap (H*b)$

$\Rightarrow x \in (H*a)$ and $x \in (H*b)$

Now, $x \in H*a$ then $H*x = H*a \rightarrow (1)$

$x \in H*b$ then $H*x = H*b \rightarrow (2)$ [By the note]

From (1) & (2) $H*a = H*b$.

∴ Any two right coset of H in G are either disjoint or identical

THEOREM: 2

If $(H,*)$ is a subgroup of a group $(G,*)$ & $H*a$ is any right coset of H in G, then there exist a 1-1 correspondence (bijective mapping) between the elements of H and $H*a$

(or)

$O(H) = O(H*a)$

PROOF: Define a map $f: H \rightarrow H*a$ by $f(h) = h*a$ for any $a \in G$

(i) TO PROVE: f is 1-1.

For any $h_1, h_2 \in H \Rightarrow f(h_1) = f(h_2)$

$h_1 * a = h_2 * a$

$\Rightarrow h_1 = h_2$

∴ f is 1-1

(ii) TO PROVE: f is onto

For every $h*a \in H*a$

$\exists : h \in H$ s.t $f(h) = h*a$

∴ f is onto

∴ There is a 1-1 correspondence between H & $H*a$ ie) $O(H) = O(H*a)$

LAGRANGE'S THEOREM (Compulsory write THEOREM) (always)

Let G be a finite group of order 'n' & H be any subgroup of G. Then the order of H divides the order of G ie) $O(H) \mid O(G)$

(or)

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

PROOF:

Let $(G,*)$ be finite group of order 'n' · ie) $O(G) = n$.

Let $(H,*)$ be a subgroup of $(G,*)$ with m distinct elts ie) $O(H) = m$

$H = \{h_1, h_2, \cdots, h_m\}$

Let $a \in G$ and $H*a$ is the right coset of H in G.

$H*a = \{h_1*a, h_2*a, \cdots, h_m*a\}$

Since there is 1-1 correspondence between the elements of H. There are 'm' distinct elements in $H*a$.

W.K.T Any right coset of H in G are either disjoint or identical

Then no: of distinct right cosets of H in G is finite (say k).

The 'k' distinct right cosets are $H*a_1, H*a_2, \cdots, H*a_k$

The union of these k distinct right cosets of H in G is equal to G

ie) $G = (H*a_1) \cup (H*a_2) \cup (H*a_3) \cdots (H*a_k)$

$\therefore O(G) = O(H*a_1) + O(H*a_2) + \cdots + O(H*a_k)$

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

Since k is an integer m is the divisor of n
∴ m/n which gives o(H) | o(G).

THEOREM:

If G is a finite group of order n, then $a^n = e$ for any $a \in G$

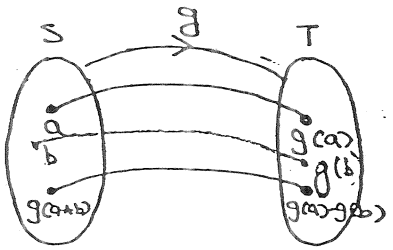
PROOF:

Let G be a finite group of order n.
Let $a \in G$ be an element of order m.
Then the order of 'a' is same as the order of cyclic group
By Lagrange's thm,
The order of the subgroup $\langle a \rangle$ divides the order of G.
Hence $m/n \Rightarrow n = km$
If 'm' is the order of 'a' then $a^m = e$
Now $a^n = a^{km} = (a^m)^k = e^k = e$
$\therefore a^n = e$.

HOMOMORPHISM OF SEMIGROUPS

SEMIGROUP HOMOMORPHISM

Let (S, *) & (T, o) be two semigroups.
A mapping $g: S \to T$ is called a semigroup homomorphism if $g(a*b) = g(a) \circ g(b)$ $\forall a, b \in S$



SEMIGROUP MONOMORPHISM:

If g is 1-1, then $g: S \to T$ is called Semigroup Monomorphism

SEMIGROUP EPIMORPHISM:

If g is onto, $g: S \to T$ is called semigroup epimorphism.

SEMIGROUP ISOMORPHISM

If g is both 1-1 & onto, then $g: S \to T$ is called Semigroup Isomorph

PROPERTY 1 (*) 2M

A Semigroup homomorphism preserves the property of associativity

PROOF:

Let $a, b, c \in S$
$g[(a*b)*c] = g(a*b) \circ g(c) = [(g(a) \circ g(b)) \circ g(c)] \to (1)$
$g[a*(b*c)] = g(a) \circ g(b*c) = g(a) \circ (g(b) \circ g(c)) \to (2)$
But in S,
$(a*b)*c = a*(b*c)$ $\forall a, b, c \in S$
$g[(a*b)*c] = g[a*(b*c)]$
$\Rightarrow [g(a) \circ g(b)] \circ g(c) = g(a) \circ [g(b) \circ g(c)]$
$\therefore$ The Property of associativity is Preserved.

PROPERTY 2 (*) 2M

A Semigroup homomorphism preserves Idempotency

PROOF:

Let $a \in S$ be an idempotent element.

$\therefore a * a = a$

$\therefore g(a*a) = g(a)$

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

This shows that $g(a)$ is an idempotent element in T.

PROPERTY 3: (8) 2M.

A semigroup homomorphism preserves commutativity.

PROOF

Let $a, b \in S$. Assume that $a*b = b*a$

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

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

This means that the operation '$\circ$' is commutative in T

$\therefore$ The semigroup homomorphism preserves commutativity

PROBLEMS

① If $(Z,+)$ and $(E,+)$ where Z is the set all integers & E is the set all even integers, show that the two semigroups $(Z,+)$ & $(E,+)$ are isomorphic [AU '10]

Sol

Let $f: (Z,+) \to (E,+)$ be defined by $f(x) = 2x \quad \forall x \in Z$

(i) T.P f is homomorphism.

$f(x+y) = 2(x+y) = 2x+2y = f(x)+f(y)$

$\therefore f(x+y) = f(x) + f(y)$ $\therefore$ f is homomorphism.

(ii) T.P f is 1-1 ie T.P $f(x) = f(y) \Rightarrow x = y$.

Assume $f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$ $\therefore$ f is 1-1

(iii) T.P f is onto ie T.P $\forall y \in E$, $\exists x \in Z$ s.t $f(x) = y$

Now $f(x) = y \Rightarrow 2x = y \Rightarrow x = \frac{y}{2}$

$\therefore \forall y \in E$, the corresponding premage is $\frac{y}{2} \in Z$

$\therefore$ f is onto.

Since $f: (Z,+) \to (E,+)$ is bijective & homomorphism

$\therefore (Z,+) \cong (E,+)$

Property 4:-

② Let $(S,*)$ be a semigroup. Then there exists a homomorphism $g: S \to S^S$, where $(S^S, \circ)$ is a semigroup of functions from S to S under the operation of (left) composition. [AU '10].

Sol T.P $g: S \to S^S$ is a Homomorphism.

ie $g(a*b) = g(a) \circ g(b)$ for all $a, b \in S$

We define $g: S \to S^S$ by $g(a) = f_a$ for $a \in S$

where $f_a: S \to S$ s.t $f_a(b) = a*b$ for $b \in S$.

Since $a*b \in S$, $g(a*b) = f_{a*b}$ for $a, b \in S$

T.P $f_{a*b} = f_a \circ f_b$

Consider $f_{a*b}(c) = (a*b)*c = a*(b*c)$ [* is ass]

$= a * f_b(c)$

$= f_a[f_b(c)]$

$= (f_a \circ f_b)(c)$

$\therefore f_{a*b} = f_a \circ f_b \quad \forall a,b \in S.$

T.P g is homomorphism.

Consider $g(a*b) = f_{a*b} = f_a \circ f_b = g(a) \circ g(b) \quad \forall a,b \in S$

Hence $g: S \to S^S$ is a homomorphism.

---

③ If $S = N \times N$, the set of ordered pairs of positive integers with the operation * defined by $(a,b)*(c,d) = (ad+bc, bd)$ & If $f: (S,*) \to (Q,+)$ is defd by $f(a,b) = \frac{a}{b}$ then show that f is a semigroup homomorphism. [Aug 08] [Aug 09]

Sol: T.P: $(S,*)$ is semigroup

$\{(a,b)*(c,d)\}*(e,f) = (ad+bc, bd)*(e,f)$

$= \{(ad+bc)f + bde, bdf\}$

$= (adf + bcf + bde, bdf)$

$(a,b)*\{(c,d)*(e,f)\} = (a,b)*(cf+de, df)$

$= \{adf + b(cf+de), bdf\}$

$= (adf + bcf + bde, bdf)$

S is associative w.r.t '*' and hence it is a semigroup

T.P f is homomorphism

$f((a,b)*(c,d)) = f(ad+bc, bd) = \frac{ad+bc}{bd} = \frac{a}{b} + \frac{c}{d} = f(a,b) + f(c,d)$

$f: (S,*) \to (Q,+)$ is a semigroup homomorphism.

MONOID HOMOMORPHISM

Monoid Homomorphism

Let $(M,*,e)$ and $(T,\circ,e)$ be any two monoids. * mapping $g: M \to T$ is called a monoid homomorphism if

(i) $g(a*b) = g(a) \circ g(b)$, $a,b \in M$ (ii) $g(e) = e$,

Monoid Monomorphism:

If f is 1-1, then $g: M \to T$ is called Monoid Monomorphism

Monoid Epimorphism:

If f is onto, then $g: M \to T$ is called Monoid Epimorphism.

Monoid Isomorphism:

If f is 1-1 & onto, then $g: M \to T$ is a monoid Isomorphism.

① Show that monoid homomorphism preserves the property of invertibility [AU 1.07] (10)

Sol:- Let $(M,*)$ & $(M',\circ)$ be two monoids with identity e & e' respectively.

Let $g: M \to M'$ be a homomorphism.

Let $a \in M$ be an element with inverse a^{-1}.

T.P $g(a^{-1}) = [g(a)]^{-1}$

$\because a^{-1}$ is the inverse of a, we have $a*a^{-1} = a^{-1}*a = e$

Now $a*a^{-1} = e \Rightarrow g(a*a^{-1}) = g(e) = e' \Rightarrow g(a)\cdot g(a^{-1}) = e'$

Also $a^{-1}*a = e \Rightarrow g(a^{-1})\cdot g(a) = e' \Rightarrow \boxed{g(a)\cdot g(a^{-1}) = g(a^{-1})\cdot g(a) = e'}$

Hence $g(a^{-1})$ is the inverse of $g(a)$. i.e. $g(a^{-1}) = [g(a)]^{-1}$

② Let $(M,*)$ be a monoid. Then there exists a subset $T \subseteq M^M$ s.t $(M,*)$ is isomorphic to the monoid $(T,\circ)$ where M^M is the set of all functions from M to M & $\circ$ is the operation composition of function [A/U ii,4].

Sol:

For any element $a \in M$, let $g(a) = f_a$ where $f_a \in M^M$ is defd by $f_a(b) = a*b$ for any $b \in M$.

Clearly g is a function from M to M^M

Now $g(a*b) = f_{a*b}$ where $f_{a*b}(c) = (a*b)*c = a*(b*c)$ [Ass]

$= f_a(b*c) = (f_a \circ f_b)(c)$

$\therefore \boxed{f_{a*b} = f_a \circ f_b}$

Hence $g(a*b) = f_{a*b} = f_a \circ f_b = g(a)\circ g(b) \Rightarrow \boxed{g(a*b) = g(a)\circ g(b)}\ \forall a,b$

$\therefore g: M \to M^M$ is Homomorphism

Corresponding to an element $a \in M$, the function f_a is completely determined from the entries in the row corresponding to the element a in the composition table of $(M,*)$

Since $f_a = g(a)$, every row of such a table determine the image of b under the homomorphism g.

Let $g(M)$ be the image of M under the homomorphism g such that $g(M) \subseteq M^M$.

Let for $a,b \in M$, then $g(a) = f_a$ & $g(b) = f_b$ are element in $g(M)$. Also $f_a \circ f_b = f(a*b) \in g(M)$ $\because a*b \in M$.

$\therefore g(M)$ is closed under the operation, composition of func

The mapping $g: M \to g(M)$ is onto since $(M,*)$ is a monoid & no two elements of the composition table can be identical.

∴ The mapping $g: M \to g(M)$ is 1–1 & onto.

∴ $g: M \to g(M)$ is an isomorphism. If e is the identity elem of M then we define $f_e(a) = a \; \forall \; a \in M$.

Clearly, this function $f_e \in T = g(M)$.

Now $f_e = g(e)$. Also $f_a \circ f_e = g(a) \circ g(e) = g(a * e) = g(a)$

∴ $f_a \circ f_e = g(a) = f(a)$

Thus shows that f_e is the identity element of $T = g(M)$

∵ $f_a, f_b \in T$, $f_a \circ f_b \in T$

∴ T is closed for the operation Composition of functio

∴ $T = g(M)$ is a monoid.

Further $g: M \to T$ is a isomorphism.

Hence $(M, *)$ is isomorphe to the monoid $(T, \circ)$

GROUP HOMOMORPHISM (X) (X) (X) 8M.

Group Homomorphism

Let $(G, *)$ and $(G_1, \circ)$ be two groups. A mapping $g: G \to G_1$, is called a group homomorphism if $g(a * b) = g(a) \circ g(b) \; \forall \; a, b \in G$.

PROPERTIES OF GROUP HOMOMORPHISM.

A group homomorphism preserves identities, inverses and Subgps

THEOREM1:

Homomorphism Preserves Identities. (or) $f(e) = e_1$, where (e) & (e_1) are the identity elements of (G) & (G_1) resp. e & e_1

PROOF:

Let $a \in G$, then $a * e = e * a = a \Rightarrow f(a * e) = f(a) \Rightarrow f(a) \circ f(e) = f($ [Let

$\boxed{f(e) = e_1}$ ∵ f Preserves Identities [f is ho

(0)

THEOREM2

Homomorphism Preserves inverse (or) $f(a^{-1}) = [f(a)]^{-1}$ [Alu|10] [Au

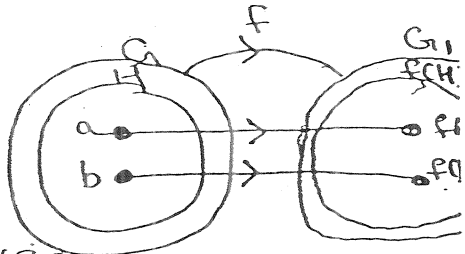
PROOF

Let $a \in G$ then $a^{-1} \in G \Rightarrow a * a^{-1} = a^{-1} * a = e$

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

$f(a) \circ f(a^{-1}) = e_1$ [f is homomorphism]

$\Rightarrow \boxed{f(a^{-1}) = [f(a)]^{-1}}$ ∴ f Preserves Inverse.



THEOREM3

Homomorphism Preserves Subgroup (or) If H is a subgroup of G then f(H) is a Subgroup of G_1. [AU Y12]

PROOF:

Let H be a subgroup of G ⇒ For $a, b \in H$, $a * b^{-1} \in H$ [∵ His sub

Let $f(a) \in f(H)$ & $f(b) \in f(H)$.

I.P $f(a) \circ [f(b)]^{-1} \in f(H)$

Consider $f(a) \circ [f(b)]^{-1} = f(a) \circ f(b^{-1}) = f(a*b^{-1}) \in f(H)$ [$\because a*b^{-1} \in$

$\Rightarrow f(a) \circ [f(b)]^{-1} \in f(H)$ $\forall$ $f(c) \in f(H)$ & $f(b) \in f(H)$

$\therefore f(H) \subseteq G_1$ is a subgp of G_1 ✓

THEOREM 4

Let $f: G \to G'$ be a group homomorphism and H is a subgroup of G' then $f^{-1}(H)$ is a subgroup of G.

PROOF:

Let $f^{-1}(H) = \{ a = f^{-1}(c) \in G,\ f(a) = c \in H \}$

Clearly $f^{-1}(H)$ will be a non-empty subset of G. [$\because$ H is a subg of G].

Now let us Consider

$a = f^{-1}(c) \in f^{-1}(H)$ & $b = f^{-1}(d) \in f^{-1}(H)$

for $c, d \in H$ with $f(a) = c$ & $f(b) = d$.

Let $a, b \in f^{-1}(H) \Rightarrow f(a) f(b) \in H$ [$\because$ H is a subgp]

$\Rightarrow f(a) * [f(b)]^{-1} \in H$

$\Rightarrow f(a) * f(b^{-1}) \in H$.

$\Rightarrow f(a*b^{-1}) \in H$. [f is homomorphism]

$\Rightarrow a*b^{-1} \in f^{-1}(H)$

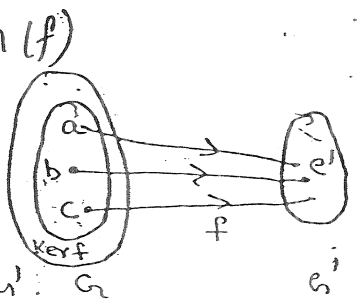
$\therefore a, b \in f^{-1}(H) \Rightarrow a*b^{-1} \in f^{-1}(H)$

Hence $f^{-1}(H)$ is a subgp of G'

$f: G \to G'$

2.M KERNEL OF A HOMOMORPHISM

Let $f: G \to G'$ be a group homomorphism. The set of elements of G which are mapped into e' (identity in G') is called the kernel of f & denoted by $\ker(f)$.



$\ker(f) = \{ x \in G \mid f(x) = e' \}$, e' identity in G'.

Then $\ker(f) = \{a, b, c\}$

THEOREM 1 V.V. (X)

If $f: G \to G'$ is a homomorphism then $\ker f = \{e\}$ iff f is 1-1 [AU Oct]

PROOF:

Assume f is 1-1. Then $f(e) = e'$ $\therefore \ker f = \{e\}$

Conversely

Assume $\ker f = \{e\}$

Now $f(x) = f(y) \Rightarrow f(x)[f(y)]^{-1} = e' \Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \ker f \Rightarrow x^{-1}y \in e \Rightarrow x = y$. [$\because$ f is homomorphism]

$\therefore f(x) = f(y) \Rightarrow x = y$.

① Let $f: G \to G'$ be a homomorphism of groups with Kernel K. Then P.T K is a normal subgp of G & G/K is isomorphic to the image of f.

Sol: T-P (i) K is a normal subgp of G:

V.I.Q (ii) $G/K \cong G'$

FUNDAMENTAL THEOREM OF GROUP HOMOMORPHISM

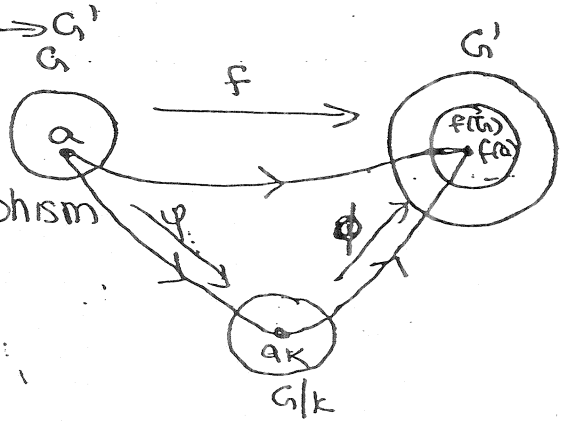
Let $(G, *)$ & $(G', \circ)$ be two groups. Let $f: G \to G'$ be a homomorphism of groups with Kernel K. Then G/K is homomorphic to $f(G) \subseteq G'$ [AU 10s]

PROOF: Let f be homomorphism $f: G \to G'$ let G' be the homomorphic image of a group G.

Let K be the Kernel of this homomorphism

Clearly K is a normal subgp of G.

[Refer Pg: ___ for pf].



T-P $G/K \cong G'$

Define $\phi: G/K \to G'$ by $\phi(K*a) = f(a)$ for all $a \in G$.

① ϕ is well defined:

We have $K*a = K*b \Rightarrow a*b^{-1} \in K$

$\Rightarrow f(a*b^{-1}) = e'$ [e' – identity in G']

$\Rightarrow f(a) \circ f(b^{-1}) = e'$ [f – homomorphism]

$\Rightarrow f(a) \circ [f(b)]^{-1} = e'$

$\Rightarrow f(a) \circ [f(b)]^{-1} \circ f(b) = e' \circ f(b)$

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

$\Rightarrow \phi(K*a) = \phi(K*b)$

$\therefore \phi$ is well defined.

② ϕ is 1-1

T-P $\phi(K*a) = \phi(K*b) \Rightarrow K*a = K*b$.

W.K.T $\phi(K*a) = \phi(K*b) \Rightarrow f(a) = f(b)$

$\Rightarrow f(a) \circ f(b^{-1}) = f(b) \circ f(b^{-1})$

$= f(b*b^{-1})$ [f-Homo]

$= f(e)$

$\Rightarrow f(a) \circ f(b^{-1}) = e'$

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

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

$\Rightarrow K*a = K*b$ $\therefore \phi$ is 1-1.

(3) ϕ is onto

Let $y \in G'$. $\because f$ is onto, $\exists\ a \in G$ s.t $f(a) = y$

Hence $\phi(k*a) = f(a) = y$.

$\therefore \phi$ is onto. //

(4) ϕ is homomorphism

Now $\phi(k*a*k*b) = \phi(k*a*b) = f(a*b) = f(a)*f(b) = \phi(k*a)*\phi(k*b)$

$\therefore \phi(k*a*k*b) = \phi(k*a) * \phi(k*b)$

$\therefore \phi$ is a homomorphism.

$\therefore$ Since ϕ is 1-1, onto & homomorphism between G/K & G'. $\therefore \phi$ is an isomorph. $\therefore G/K \cong G'$

---

(2) The Kernel of a homomorphism f from a group $(G,*)$ to $(G',*)$ is a subgroup of G. (XX) UQ. [AU '07] [AU '09]

Proof

W.K.T $\ker f = \{x \in G \mid f(x) = e'\}$

$\because f(e) = e'$ is always true, atleast $e \in \ker f$

In other words $\ker(f)$ is not empty in G.

Let the two elements $a, b \in \ker(f)$.

$\therefore f(a) = e'$ & $f(b) = e'$

Now, $f(a*b^{-1}) = f(a) * f(b^{-1})$ [f is homomorphism]

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

$= e' * e'$

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

$\Rightarrow a*b^{-1} \in \ker f$.

i.e. $a, b \in \ker(f) \Rightarrow a*b^{-1} \in \ker f$.

$\therefore \ker(f)$ is a subgroup of G.

(XX) 8M

THEOREM : CAYLEY'S THEOREM OR CAYLEY'S REPRESENTATION THM

Every finite group of order n is isomorphic to a permutation group of degree n. We shall find a set B' of [AU '04] [AU '01]

PROOF Step1:- permutation.

Let $a \in G$ be any element. Corresponding to a we define a map $f_a : G \to G$ by $f_a(x) = a*x \ \forall x \in G$.

Then f is 1-1, for $f_a(x) = f_a(y) \Rightarrow a*x = a*y$.

$\Rightarrow x = y$ [Left Cancell]

Now $y \in G$ (codomain), then $a^{-1}*y \in G$ such that

$f_a(a^{-1}*y) = a*(a^{-1}*y) = (a*a^{-1})*y = e*y = y$ $\therefore f_a$ is onto

Thus f_a is a 1-1 & onto function from $G \to G$ & so it is a permutation on G.

Since G has n elements f_a is a permutation on n symbols (or) a permutation of degree n

~~Step: Prove G' is a group.~~

Let $G' = \{f_a \mid a \in G\}$. We shall prove G' is a group.

We verify axioms of the group.

Let $f_a, f_b \in G'$ by any two elements

$\because f_a, f_b$ are functions from $G \to G$.

Then $(f_a \cdot f_b)(x) = f_a(f_b(x)) = f_a(b*x) = a*(b*x) = (a*b)*x$

$= f_{a*b}(x) \quad \forall x$

$\therefore \boxed{f_a \cdot f_b = f_{a*b}}$ — (1)

Since $a, b \in G$, $a*b \in G$ & so $f_{a*b} \in G' \Rightarrow f_a f_b \in G'$.

Hence G' is closed under composition of function operation.

$f_e \in G'$ is the identity element. $f_{a^{-1}}$ is the inverse of $f_a \in G'$

So G' is a group.

Finally we prove $G \cong G'$

Let $\phi : G \to G'$ be defined by $\phi(a) = f_a \ \forall \ a \in G$

Now for any $a, b \in G$, $\phi(a*b) = f_{a*b} = f_a \cdot f_b = \phi(a) \cdot \phi(b)$.

$\therefore \phi$ is homomorphism

Suppose $\phi(a) = \phi(b)$, then $f_a = f_b$.

$\Rightarrow f_a(x) = f_b(x) \quad \forall x \in G$.

$\Rightarrow a*x = b*x$

$\Rightarrow a = b$ [By right Cancellation law]

$\therefore \phi$ is 1-1.

Now let $f_a \in G'$ be any elt with $a \in G$.

Then $\phi(a) = f_a$ and so ϕ is onto.

Thus ϕ is an isomorphism of G onto G' $\therefore G \cong G'$.

---

⑤ Let $f : (R, +) \to (R^+, \cdot)$ defd by $f(x) = e^x \ \forall x \in R$. S.T f is isomorphic

Sol: Gn $f : R \to R^+$ defd by $f(x) = e^x, \forall x \in R$.

T-P f is isomorphism : Homomorphis, 1-1, onto.

T-P: f is homomorphism : $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$.

T-P: f is 1-1 : Assume $f(x) = f(y) \Rightarrow e^x = e^y \Rightarrow e^{x-y} = 1 \Rightarrow e^{x-y} = e^0$

$\Rightarrow x - y = 0 \Rightarrow \boxed{x = y}$ $\therefore f$ is 1-1

T-P: f is onto : Let $y \in (R^+, \cdot)$. Then $\exists \log_e y \in R$ s.t.

$f(\log_e y) = e^{\log y} = y$, $\log_e y$ is the preimage of y. $\therefore f$ is

NORMAL SUBGROUP

DEFINITION:

A subgroup $(H,*)$ of $(G,*)$ is called a Normal Subgroup of G if $aH = Ha \ \forall a \in G$ (or) If $x*h*x^{-1} \in H$ i.e. $x*H*x^{-1} \subseteq H$, $\forall x \in G, h \in H$

NOTE:

(1) $aH = Ha \Rightarrow a*h = h_1*a$

$\Rightarrow a*h = h_1*a$, for some $h, h_1 \in H$

(2) If H is a normal subgroup, then $Ha = aH, \forall a \in G$ & some may simply called them cosets.

THEOREMS UNDER NORMAL SUBGROUP

① A subgroup H of a group G is normal iff $x*h*x^{-1} = H \ \forall x \in G$.

Proof: Let $x*h*x^{-1} = H$

T.P H is a normal subgroup of G.

$\because x*h*x^{-1} = H \Rightarrow x*h*x^{-1} \subseteq H$

$\therefore H$ is a normal subgroup of G [By def of N.S]

Conversely

Let us assume that H is a normal subgroup of G

T.P $x*h*x^{-1} = H$ i.e. T.P $x*h*x^{-1} \subseteq H$ & $H \subseteq x*h*x^{-1}$

$\because H$ is a normal subgp of $G \Rightarrow \boxed{x*h*x^{-1} \subseteq H} \rightarrow ①$ [By def of NS]

Now, $x \in G \Rightarrow x^{-1} \in G$

i.e. $x^{-1}*H*(x^{-1})^{-1} \subseteq H$, for all $x \in G$

$\Rightarrow x^{-1}*H*x \subseteq H$

$\Rightarrow x*(x^{-1}*H*x)*x^{-1} \subseteq x*H*x^{-1}$

$\Rightarrow x^{-1}*x*H*x*x^{-1} \subseteq x*H*x^{-1}$

$\Rightarrow e*H*e \subseteq x*H*x^{-1}$

$\Rightarrow \boxed{H \subseteq x*H*x^{-1}} \rightarrow ②$

From ① & ② $x*H*x^{-1} = H, \forall x \in G$.

② The intersection of any two normal subgroups of a group is a normal subgroup (or) If H & K are normal subgroups of a group G, then $H \cap K$ is also a normal subgroup.

Proof: Gn: H & K are normal subgroups [M.U '13]

T.P: $H \cap K$ is a normal subgroups

Given H and K are normal subgroups $\Rightarrow H$ & K are subgroups of G

$\Rightarrow H \cap K$ are subgroups [Already proved, Pg ⑧, Thm: 2]

Now **T.P** $H \cap K$ is normal

Let $x \in G$ & $h \in H \cap K$

i.e. $x \in G$ & $h \in H$ & $h \in K$

i.e.

$\Rightarrow x*h*x^{-1} \in H \rightarrow (1)$ and $x*h*x^{-1} \in K \rightarrow (2)$

$\therefore$ From (1) & (2) $x*h*x^{-1} \in H \cap K$ [$\because$ H & K are Normal Subgps]

$\Rightarrow H \cap K$ is a normal subgroup of G.

---

(3) Let G & G' be any two groups with identity element e and e' respectively. If $f: G \to G'$ be a homomorphism, then Ker(f) is a normal subgroup. [M/J '13]

Proof: Given e is an identity in G and e' is an identity in G'

Let $K = \text{Ker}(f) = \{x \in G \mid f(x) = e'\}$

W.K.T Ker(f) is a subgroup of G [Already proved]

T.P Ker(f) is normal.

For, Let $x \in G$ and $h \in K$

$\therefore f(x*h*x^{-1}) = f(x*h) * f(x^{-1}) = f(x) * f(h) * f(x^{-1})$

$= f(x) * e' * f(x^{-1})$ [$\because$ f is homomorphism]

$= f(x) * f(x^{-1})$ [$\because h \in K = \text{Ker}(f)$]

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

$= f(e)$

$\boxed{f(x*h*x^{-1}) = e'}$

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

$\therefore$ For $x \in G, h \in K$, we have $x*h*x^{-1} \in K$

$\therefore K = \text{Ker}(f)$ is a normal subgroup of G

---

(4) Every subgroup of an abelian group is normal. (M/J '13) (2M)

Proof: Let G be an abelian group & H be a subgroup of G

$\therefore x*H*x^{-1} = x*(H*x^{-1})$, $x \in G, h \in H$.

$= x*(x^{-1}*H)$ [G is abelian, $\therefore x^{-1}*H = H*x^{-1}$]

$= (x*x^{-1})*H$

$= e*H$

$= H$

$\therefore$ For $x \in G$ & $h \in H$, we have $x*H*x^{-1} = H$

$\therefore H$ is a normal subgroup of G.

ALGEBRAIC SYSTEMS WITH TWO BINARY OPERATIONS

RING:

An algebraic system $(R,+,\cdot)$ is said to be Ring if

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

(ii) '$\cdot$' is associative i.e. $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ $\forall\ a,b,c \in R$

(iii) The operation $\cdot$ is distributive over $+$, for any $a,b,c \in$

$a\cdot(b+c) = a\cdot b + a\cdot c$ [Left distributive Law]

$(b+c)\cdot a = b\cdot a + c\cdot a$ [Right distributive Law]

DEF: COMMUTATIVE RING

The ring $(R,+,\cdot)$ is called a Commutative ring, if $ab=ba$, for $a,b \in$

Eg: $(\mathbb{Z},+,\cdot)$, $(R,+,\cdot)$, $(Q,+,\cdot)$.

DEF: RING WITH IDENTITY

The ring is said to be a ring with identity if there exists an elem $e \in R$ such that $a*e = e*a = a$ $\forall\ a \in R$

DEF: BOOLEAN RING:

A ring R is said to be a Boolean ring if $a^2=a$ $\forall\ a \in R$.

DEF: ZERO DIVISOR:

Let $(R,+,\cdot)$ be a ring. A non zero element $a \in R$ is called a zero divisor if there exist an element $b \in R$, $b\neq 0$ s.t $a\cdot b = b\cdot a = 0$. Then b is called the zero divisor of 'a'.

Eg: Consider the ring $(\mathbb{Z}_6,+_6,\times_6)$, $\because \bar{2}\times_6\bar{3}=\bar{0}$.

DEF: WITHOUT ZERO DIVISORS:

If in a Commutative ring $(R,+,\cdot)$ if for any $a,b \in S$ s.t $a\neq 0, b\neq 0$ $\Rightarrow ab\neq 0$ then the ring is without zero-divisors.

NOTE: In a ring without zero divisors $a\cdot b=0 \Rightarrow a=0$ or $b=0$

DEF: INTEGRAL DOMAIN: V.V.IMP 2m CIE

A Commutative ring $(R,+,\cdot)$ with identity & without zero-divisor is called an integral domain.

Eg: $(\mathbb{Z}_n,+_n,\cdot_n)$ is an Integral domain if n is a prime number

DEF: FIELD CIE

A Commutative ring $(R,+,\cdot)$ with identity in which every non-zero element has multiplicative inverse is called a field

Eg: $(Q,+,\cdot)$ & $(R,+,\cdot)$ are field but $(\mathbb{Z},+,\cdot)$ is not a field.

Example of a Commutative ring without identity:

The algebraic system $(E,+,\times)$ where E is the set of all even integers is an example of Commutative ring without identity.

PROBLEMS IMP & SM.

1) Prove that the set $\mathbb{Z}_4=(0,1,2,3)$ is a Commutative ring with respect to the binary operation $+_4$ & $\times_4$. END 1/27

Sol: Composition table: Addition Modulo 4 and Multiplication Modulo 4

t_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

X_4

X_6	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

T-P $(Z_4, +_4, X_4)$ is a Commutative Ring.

① CLOSURE PROPERTY

All the etries in both the tables belong to Z_4. Hence Z_4 is closed under t_4 & X_4.

② COMMUTATIVE PROPERTY

The entries in the first row are the same as those of the first column in both as those of the first column in both tables. Hence Z_4 is commutative w.r.t both t_4 and X_4.

③ ASSOCIATIVE PROPERTY: If $a,b,c \in Z_4$.

→ $(a +_4 b) +_4 c = a +_4 (b +_4 c)$. Consider $a=1, b=2, c=3$

$(1+_4 2)+_4 3 = 3 +_4 3 = 2$ & $1 +_4 (2 +_4 3) = 1 +_4 1 = 2$

→ $(a X_4 b) X_4 c = a X_4 (b X_4 c)$

$(1 X_4 2) X_4 3 = 2 X_4 3 = 2$ & $1 X_4 (2 X_4 3) = 1 X_4 2 = 2$

Thus, associative Law is satisfied for t_4 & X_4 by Z_4.

④ IDENTITY PROPERTY

→ Additive identity of Z_4: 0 $[0 +_4 a = a +_4 0 = a \ \forall \ a \in Z_4]$

→ Multiplicative identity of Z_4: 1 $[1 X_4 a = a X_4 1 = a \ \forall \ a \in Z_4]$

⑤ INVERSE PROPERTY: FROM THE TABLE.

→ Additive inverse: 0, 1, 2, 3 are 0, 3, 2, 1 resp

→ Multiplicative inverse: 1, 2, 3 are 1, 2, 3 resp. [non-zero element]

⑥ DISTRIBUTIVE PROPERTY: X_4 is distributive over t_4 in Z_4.

→ $a X_4 (b +_4 c) = (a X_4 b) + (a X_4 c)$ & $(b +_4 c) X_4 a = (b X_4 a) + (c X_4 a)$

Consider $a=2, b=3, c=1$

$2 X_4 (3 +_4 1) = 2 X_4 0 = 0$; $(2 X_4 3) +_4 (2 X_4 1) = 2 +_4 2 = 0$

Hence $(Z_4, +_4, X_4)$ is a Commutative ring with identity.

---

② Show that $(Z, +, X)$ is a Integral domain where Z is the set of I

Sol: T-P $(Z, +, X)$ is a Integral domain [MD '10]

(i) T-P $(Z, +)$ is an abelian group

→ closure Prop: $a+b \in Z$, for any $a,b \in Z$

→ Associative property

$(a+b)+c = a+(b+c)$, $a,b,c \in Z$

→ Identity element: $0 \in Z$.

$0+a = a+0 = a$, $\forall \ a \in Z$.

→ INVERSE element: $-a \in Z$.

$a+(-a) = (-a)+a = 0$, $\forall \ a \in Z$

→ Commutative: $a+b = b+a$, $a,b \in Z$

$\therefore (Z, +)$ is an abelian gp.

(ii) T-P (R, X) is a Monoid

→ CLOSURE PROP: $ab \in Z$, $\forall \ a,b \in Z$

→ ASSOCIATIVE PROP: for any $a,b,c \in Z$

$(a X b) X c = a X (b X c)$

→ IDENTITY ELT: $1 \in Z$ is the Identity

→ Commutative: $ab = ba$, $\forall \ a,b \in Z$

(iii) T-P DISTRIBUTIVE PROP:

$a X (b+c) = a X b + a X c$ $\forall, a,b,c \in Z$

Hence $(Z, +, X)$ is a commutative ring with

(iv) T-P Z has no zero divisor

If $a \neq 0$, $b \neq 0$ in $Z \Rightarrow ab \neq 0$

Hence $(Z, +, X)$ is an Integral Domain

UNIT - IV - ALGEBRAIC STRUCTURES

PART - A

(1) Define a semigroup. Give an example.

Sol: SEMIGROUP: $(S,*)$: If a non-empty sets together with the binary operation '$*$' satisfying the following two properties
(i) CLOSURE PROP (ii) ASSOCIATIVE PROP
Eg: $(2\mathbb{Z},+)$ & $(\mathbb{Z},\cdot)$ are semigroups.

(2) Define a Monoid. Give an example.

Sol: MONOID: $(M,*)$: If a non-empty set M together with the binary operation $*$ satisfying the following properties
(i) Closure prop (ii) Associative Prop (iii) Identity Property.
Eg: $(\mathbb{N},\times)$ is a Monoid with identity 1.

(3) Define a Group. Give an example

Sol: GROUP: $(G,*)$: A non-empty set G with binary operation $*$ is called a group if the following properties satisfies:
(i) Associative Prop (ii) Identity Property (iii) Inverse Property
Eg (1) $(\mathbb{R},+)$, $(\mathbb{R},\cdot)$, $(I,+)$ are groups.
(2) $M_2(\mathbb{R})$, the set of all 2×2 matrices is a group w.r.t '$\times$'.

(4) State any two properties of Group [AU/2010]

Sol: In a Group $(G,*)$ (i) Identity elt is Unique (ii) Inverse elt is Unique

(5) When is a group $(G,*)$ called abelian [AU/11]

Sol: The group $(G,*)$ is called abelian if $a*b=b*a$, $\forall a,b\in G$

(6) In a group G if $a^2=e$ $\forall a\neq e$, then P.T G is abelian. [AU/06] [AU/05]

Sol: T.P G is abelian $\Rightarrow$ T.P $a*b=b*a$

Gn $a^2=e$ $\forall a\in G$
$\therefore a^{-1}*a^2=a^{-1}*e$
$(a^{-1}*a)*a=a^{-1}*e$
$e*a=a^{-1}*e$
$\boxed{a=a^{-1}}$

Let $a,b\in G \Rightarrow a*b\in G$ & Gn Every element has its own inverse $\Rightarrow a=a^{-1}$ & $b=b^{-1}$
& $(a*b)=(a*b)^{-1}=b^{-1}*a^{-1}=b*a$
$\therefore (a*b)=(b*a)$
$\therefore$ G is abelian

(7) In an abelian group $(G,*)$, P.T $(a*b)^2=a^2*b^2$ $\forall a,b\in G$

Sol: Let $a,b\in G$ be any two elements. [AU/10]
$(a*b)^2=(a*b)*(a*b)=a*(b*a)*b=a*(a*b)*b$ [$\because$ G is abelian]
$=(a*a)*(b*b)=a^2*b^2$.
$\therefore (a*b)^2=a^2*b^2$

(8) Give an example of a non-abelian finite group.

Sol: S_3 is a non-abelian group

(9) State the minium order of a non-abelian group.

Sol: S_3 is the smallest non abelian group. $O(S_3)=3!=6$.

(10) Give an example of a cyclic group.

Sol: The fourth roots of unity $\{1,-1,i,-i\}$ under usual multiplication.

(11) P.T every idempotent element of a group is its identity element. [AU '10]

Sol:- Idempotent element: An elt $a \in G$ is said to be idempotent w.r.t $*$ if $a*a = a$

Identity element: An element $e \in G$ is said to be identity elt s.t $e*a = a*e = a$, for every $a \in G$.

In a group the identity element e only satisfies the idempotent condition $e*e = e$

(12) If a and b are the elements of a group $(G, *)$. S.T $(a*b)^{-1} = b^{-1}*a^{-1}$ [AU '04]

Sol Let $a, b \in G \Rightarrow a*b \in G$ [closure axiom].

By the existence of inverse elements axiom, $a^{-1}, b^{-1}, (a*b)^{-1} \in G$

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

Closure prop, $b^{-1}, a^{-1} \in G \Rightarrow b^{-1}*a^{-1} \in G$.

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

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

By (1) & (2) we get.

$(a*b)(b^{-1}*a^{-1}) = (b^{-1}*a^{-1})*(a*b) = e$ [i.e) $a*a^{-1} = a^{-1}*a = e$]

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

(13) Give an example of sub semigroup [AU '07]

Sol: For the semigroup $(N, +)$, the set E of all even non-negative integers is a sub semigroup $(E, +)$ of $(N, +)$

(14) Give ane example of semigroup but not a monoid [AU

Sol Let $D = \{\ldots -4, -2, 0, 2, 4 \ldots\}$. Then $(D, *)$ is a semigp but not Mo

~~Let $N = \{1, 2, 3, \ldots\}$ Then $(N, +)$ is a semigp not Monoid~~ [does not contain additive identity e

(15) Let $E = \{2, 4, 6, 8, \ldots\}$. S.T $\{E, +\}$ & $\{E, *\}$ are semigp but not Mon [AU '10]

Sol Let $E = \{2, 4, 6, 8, \ldots\}$ be the set of all even no:. Then $(E, +)$ is Semi

But $(E, +)$ is not a monoid since the additive identity elt $0 \notin E$. Also $(E, \times)$ is a semigroup.

But $(E, \times)$ is not a monoid, since multiplicative identity elt $1 \notin E$

(16) Define Cyclic monoid [AU '08]

Sol: A monoid $(M, *)$ is said to be cyclic, if every elt of M is of the form a^n, $a \in M$ & n is an integer i.e) $x = a^n$

Such a cyclic monoid $(M, *)$ is said to be generated by the elt 'a'. Here 'a' is called the generator of the cyclic Monoid

(17) Prove that every cyclic monoid is commutative [AU '09]

Sol Let $(M, *)$ be a cyclic monoid whose generator is $a \in M$

Then for $x, y \in M$. We have $x = a^n$, $y = a^m$, m, n - integers.

Now, $x*y = a^n * a^m = a^{n+m} = a^{m+n} = a^m * a^n = y*x$

$\therefore (M, *)$ is a commutative or abelian

(18) If 'a' is a generator of a cyclic gp G, S.T a^{-1} is also a generator of G.

Sol: $(a^{-1}) = \{(a^{-1})^n : n \in Z\} = \{a^{-n} ; n \in Z\} = \{a^m : m \in Z\} = (a)$

$\therefore (a^{-1}) = a$.

(19) Give an example of a monoid which is not a group. [AU '10]

Sol: $(Z^+, \cdot)$ is a monoid which is not a group [$\because a \in G \Rightarrow \frac{1}{a} \notin G$]

(19) Let $\langle M, *, e_M \rangle$ be a monoid and $a \in M$. If a invertible then show that its inverse is unique.

Sol: Let b and c be elements of a Monoid M s.t $a*b = b*a = e$ and $a*c = c*a = e \rightarrow (1)$

Now $b = b*e = b*(a*c) = (b*a)*c = e*c = c \Rightarrow b = c$

$\therefore$ Inverse is unique (2.5)

(20) Give an example of a semigroup which is not a group

Sol: $(\mathbb{Z}, \cdot)$ is a semigroup, but is not a group. $\because$ in $\mathbb{Z}$ inverse element does not exist.

(21) If P(S) is the power set of non-empty set S, P.T $(P(S), \cap)$ is a monoid [Alu 10].

Sol Let $A, B \in P(S)$. Then A & B are subsets of S

$\therefore A \cap B$ is a subset of $S \Rightarrow A \cap B \in P(S) \Rightarrow$ closure P.

W.K.T intersection of sets is associative.

Further $A \cap S = A \ \forall \ A \in P(S) \Rightarrow S$ is the identity elt in P(S)

$\therefore (P(S), \cap)$ is a monoid.

(22) $G = \{1, -1, i, -i\}$ is a group under usual multiplication. $H = \{1, -1\}$ is a subset of G. Is H a subgroup of G? Is H a normal subgp?

Sol: $H = \{1, -1\}$ is a finite subset of G.

Since H is closed under multiplication, H is a subgroup of G

$\because \frac{O(G)}{O(H)} = \frac{4}{2} = 2$, H is of index 2 in G. $\rightarrow 2(1)$ i.e. prime no

So.

·	1	-1
1	1	-1
-1	-1	1

Hence H is a normal subgp of G. $\leftarrow$

(23) P.T every subgroup of an abelian group is normal.

Sol: Let $(G, *)$ be an abelian group & H be a subgroup of G. Let $a \in G$ be any element, then

$a*H = \{a*h \mid h \in H\} = \{h*a \mid h \in H\}$, since G is abelian $\forall a \in G$

$a*H = H*a \ \forall \ a \in G$ $\therefore$ H is normal in G $a*H = H*a$

(24) Find a subgroup of order two of the gp $(Z_8, +_8)$ [Alu 08]

Sol: $Z_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$.

$\because Z_8$ is a cyclic group, there is a unique subgp of order 2.

The subgp of order 2 is $\{[0], [4]\}$.

(25) Find all non-trivial subgroups of $(Z_6, +_6)$.

Sol: $(Z_6, +_6)$ is a cyclic group. The non-trivial subgps are of orders 2 and 3, which are divisors of $O(Z_6) = 6$ where

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

The subgps are $H_1 = \{[0], [3]\}$, $H_2 = \{[0], [2], [4]\}$.

(26) Find all the subgps of $(Z_{12}, +_{12})$.

Sol: $\because Z_{12}$ is cyclic of order 12, there is a unique subgp corresponding to each divisor of 12. So there are 6 subgps of order 1, 2, 3, 4, 6..

$H_1 = \{[0]\}$ [illegible]

(27) P.T the identity of a subgp is the same as that of the grp

Sol: Let G be a group. Let H be a subgroup of G.
Let e & e' be the identity elements in G & H.
Now if $a \in H$, then $a \in G$ & $ae = a$ [$\because$ e is the identity elt in G]
Again if $a \in H$, then $ae' = a$ [$\because$ e' is the identity elt in H].
$\therefore ae = ae' \Rightarrow e = e'$

(28) Show that the set of all elements 'a' of a group $(G, *)$ st $a * x = x * a$ for every $x \in G$ is a subgp of G

Sol Clearly $ex = xe = x \ \forall x \in G$.
$\therefore e \in H$ & H is non-empty
Now, Let $a, b \in H$. Then $ax = xa$ & $bx = xb$.
Now, $bx = xb \Rightarrow b^{-1}(bx)b^{-1} = b^{-1}(xb)b^{-1}$
$\Rightarrow b^{-1}b(xb^{-1}) = b^{-1}x(bb^{-1})$
$\Rightarrow \boxed{xb^{-1} = b^{-1}x} \rightarrow (1)$
Now $(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1}$
$\therefore (ab^{-1})x = x(ab^{-1})$ $= x(ab^{-1})$
$\therefore ab^{-1} \in H$ $\therefore$ H is a subgroup.

(29) Test whether the subset $\{[0], [2]\}$ is a normal subgp of $(Z_4, +_4)$

Sol : Let $H = \{[0], [2]\}$. Since the finite subset H is closed under $+_4$, H is a subgroup of $G = Z_4$.
Further $\frac{O(G)}{O(H)} = \frac{4}{2} = 2$. H is of index 2 in G.
So H is a normal subgp.

$+_4$	[0]	[2]
[0]	[0]	[2]
[2]	[2]	[0]

(30) Find the orders of the elements of the multiplicative group $\{1, -1, i, -i\}$.

Sol: We know $i^2 = -1$ $\therefore i^4 = 1$ $\therefore O(i) = 4$
$(-1)^2 = 1$ $O(-1) = 2$

(31) In the group $(Z_{12}, +_{12})$ find the order [6].

Sol: $2[6] = [12] = [0]$, so $O([6]) = 2$

(32) Prove that any group of prime order is cyclic.

Sol Let $(G, *)$ be group of prime order P.
Let $a \neq e$ be an element of G.
Since G is finite, the cyclic subgroup H generated by a is finite.
By Lagrange's theorem $O(H) \mid O(G) \Rightarrow O(H) \mid P$.
$\because$ P is a prime $O(H) = 1$ or P
$\because a \neq e$, $O(H) \neq 1$
$\therefore O(H) = P$, then $H = G$ & hence G is cyclic.

(33) State Lagranges theorem for finite groups [A/D]

Sol Lagrange's theorem : The order of a subgp H of a finite group G divides the order of the group.

(34) Find all right cosets of $\{[0],[2]\}$ in the group $(Z_4, +_4)$

Sol: Let $H = \{[0],[2]\}$, $Z_4 = \{[0],[1],[2],[3]\}$

$\because [0],[2] \in H$, $H+[0] = H$, $H+[2] = H$,

$H+[1] = \{[1],[3]\}$, $H+[3] = \{[3],[1]\}$

(35) If H is a subgroup of G, among the right cosets of H in G Prove that there is only one subgroup viz H. [AU 10]

Sol: Given H is a subgroup of $(G, \cdot)$.

Let $a \in G$ be any element $(a \neq e)$ and so Ha is a right coset of H in G. Clearly Ha is a subset of G.

If $x, y \in Ha$ then $x = h_1 a$; $y = h_2 a$ for some $h_1, h_2 \in H$

$\therefore xy = h_1 a \cdot h_2 a \notin Ha$. So Ha is not closed under multiplication. So the subset Ha is not a subgroup if $a \neq e$

If $a = e$ then the right coset is $He = \{he \mid h \in H\} = \{h \mid h$

So H is the only right coset, which is a subgroup.

(36) Show that $H = \{[0],[4],[8]\}$ is a subgroup of $(Z_{12}, +_{12})$. Also find the left cosets of H in $(Z_{12}, +_{12})$. [AU 10]

Sol: Since H is finite it is enough to verify closure

$\therefore$ H is a subgroup.

$\because [0],[4],[8] \in H$.

$+_{12}$	[0]	[4]	[8]
[0]	[0]	[4]	[8]
[4]	[4]	[8]	[0]
[8]	[8]	[0]	[4]

$[0]+H = H$, $[4]+H = H$, $[8]+H = H$

$[1]+H = \{[1],[5],[9]\}$; $[2]+H = \{[2],[6],[10]\}$

$[3]+H = \{[3],[7],[11]\}$; $[5]+H = \{[5],[9],[1]\}$

$[6]+H = \{[6],[10],[2]\}$; $[7]+H = \{[7],[11],[3]\}$; $[9]+H = \{[9],[1],[5]\}$

$[10]+H = \{[10],[2],[6]\}$; $[11]+H = \{[11],[3],[7]\}$.

(37) Find all the cosets of the subgroup $H = \{1,-1\}$ in $G = \{1,-1,i,-i\}$ with the operation multiplication [AU 10]

Sol: Let us find the right cosets of H in G.

$H(1) = \{1,-1\} = H$, $H(-1) = \{-1,1\} = H$, $H(i) = \{i,-i\}$

$H(-i) = \{-i,i\} = Hi$; $H1 = H = H-1 = \{1,-1\}$ & $Hi = H-i = \{i,-i\}$ are 2 distinct right cosets of H in G.

Similarly find the left cosets of H in G.

(38) Find the left cosets of $\{[0],[3]\}$ in the addition modular group $(Z_6, +_6)$. [AU 10]

Sol: Let $Z_6 = \{[0],[1],[2],[3],[4],[5],[6]\}$ be a group & $H = \{[0],[3]\}$ be a subgroup of Z_6 under $+_6$ (addition mod 6)

The left cosets of H are

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

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

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

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

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

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

$\therefore [6]+H = [3]+H = H$

(39) Give an example for left cosets & right cosets.

Sol Let us consider the group $G = \{1, -1, i, -i\}$ which consists of the 4th root of unity under multiplication. The subset $H = \{i, -i\}$ is a subgroup of G.

The various cosets of H in G are.

$1H = \{1, -1\} = H = H1$ | $iH = \{i, -i\} = Hi$

$-1H = \{1, -1\} = H = H(-1)$ | $-iH = \{i, -i\} = iH = H(-i)$.

Here there are two left cosets H, iH & similarly there are two right cosets H, Hi.

Infact $1H = H1$ and $iH = Hi$

---

(40) Consider the group $Z_4 = \{[0], [1], [2], [3]\}$ of integers modulo 4. Let $H = \{[0], [2]\}$ be a subgroup of Z_4 under $+_4$ Caddition Mod 4. Find the left cosets of H [AU '08] [AU'0

Sol: Then the left cosets of H are

$[0]+H = \{[0], [2]\} = H$

$[1]+H = \{[1], [3]\}$

$[2]+H = \{[2], [4]\} = \{[2], [0]\} = \{[0], [2]\} = H$

$[3]+H = \{[3], [5]\} = \{[3], [1]\} = \{[1], [3]\}$
$= [1]+H.$

$[0]+H = [2]+H = H$
& $[1]+H = [3]+H$ are the two distinct left cosets of in Z_4

---

(41) Define homomorphism & isomorphism between to algebraic system.

Sol: Let $(A, *)$ and $(B, \circ)$ be two algebraic systems. A mapping $f: A \to B$ is called a homomorphism if $f(a*b) = f(a) \circ f(b)$ $\forall a, b \in A$.

If the homomorphism f is 1-1 & onto, then f is called an isomorphism.

---

(42) Show that semigroup homomorphism preserves the property of idempotency? [AU 107]

Sol: Let $a \in S$ be an idempotent element

$\therefore a * a = a$

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

$\therefore g(a)$ is an idempotenent element in T

---

(43) If f is a homomorphism of a group G into a a group G', then P.T a group homomorphism preserves identities. [AU 106]

Sol: Let $a \in G \Rightarrow a*e = e*a = a$. $a*e = e$ ...

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

$f(a) \circ f(e) = f(a) \circ e$, $[e_1 \in G_1, f(a) \in G_1$

$\therefore f(e) = e_1$ [L.C.L]

---

(44) When do you call a homomorphism of a semigroup into itself

Sol: A homomorphism of a semigroup into itself is called a semigroup endo morphism.