Page No.
Date :

Unit - 03

Algebraic structures

* **Binary composition on a set or binary operation on a set →**

Let G be any non-empty set and $G \times G = \{(a,b) : a,b \in G\}$

Then a function $* : G \times G \to G$

defined by $*(a,b) = a * b \in G$ is called a binary operation on the set G.

Ques The operation '.' on the set of real number is a binary operation.

$\cdot : R \times R \to R$

$\cdot(a,b) = a.b \in R$

$R \times R = \{(1,1), (1,2), (2,3) \ldots\}$

$\cdot(1,1) = 1 \in R$

$\cdot(1,2) = 2 \in R$

Ques The operation '+' on the set of natural number N is a binary operation.

$+ : N \times N \to N$ such that $+(a,b) : a+b \in N$

$+(2,3) = 5 = \in N$ $\quad \forall a,b \in N$

$+(2,5) = 2+5 = 7 \in N$

Ques The operation '−' on the set of natural number is not a binary operation.

$- : N \times N \to N$ such that $-(a,b) : a-b \notin N \quad \forall a,b \in N$

eg :- $-(2,3) = 2-3 = -1 \notin N$

\# **Closure property :-** If '*' is a binary operation on the set G then $* : G \times G \to G$ such that $*(a,b) = a*b \in G$ $\forall a,b \in G$.

⇒ G is closed under the binary operation '*'.

[i.e. G satisfy closure property under '*']

Page No.
Date :

Algebraic structure :- A non-empty set G together with one or more binary operation is called a algebraic structure.

for ex :- $(N,+)$ ✓ , $(N,-)$ ✗ , $(Z,+)$ ✓ , $(R,+)$ ✓ , $(R,\cdot)$ ✓

* Groupoid or Quasi-group :-

Let G be a non-empty set and '*' be a binary operation on the set G. Then $(G,*)$ is ~~said~~ said to be groupoid or quasi group if it satisfies following postulates :-

① closure law :-

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

(* : operation)

$\Rightarrow$ G is closed under operation '*'.

Que Prove that the set of natural number N under operation addition '+' is a quasi-group.

Ans $N = \{1,2,3,4,\ldots\}$

closure law :- ~~$\forall$~~ $(a,b) \in N$

$\Rightarrow a+b \in N \Rightarrow (N,+) \in N$

$\Rightarrow$ G is closed under the operation '+' & hence it is a groupoid or quasi group.

* Semi-group :- Let G be an non-empty set and '*' be a binary operation on the set G.

Then $(G,*)$ is said to be semi-group if it satisfies the following properties :-

① closure law :- $\forall a,b \in G \Rightarrow a*b \in G$

$\Rightarrow$ G is closed under the operation '*'.

② Associative law :- $\forall a,b,c \in G \Rightarrow (a*b)*c = a*(b*c)$

$\Rightarrow$ G is closed under the opeⁿ '*'.

Que Prove that the set of all +ve even integers is a semi group under the binary composition addition.

Soln $E = \{2,4,6,8,10\ldots\}$

To show :- $(E,+)$ is a semi-group.

closure law :- $\forall a,b \in E \Rightarrow a+b \in E$

$\therefore$ E ~~is a semi group~~ satisfies the closure law under operation '+'.

Page No.
Date:

(2) Associative law :- $\forall a,b,c \in E$

$a+(b+c) = (a+b)+c \in E$

eg :- 2, 4, 6

$2+(4+6) = (2+4)+6$

$2+10 = 6+6$

$12 = 12 \in E$

$\therefore$ E is a semi-group under E as it satisfies both closure & associative law.

* Monoid :- Let G be a non-empty set and '*' be any binary operation on set G.

Then $(G,*)$ is called Monoid if it satisfies the following properties :-

(1) closure law :- $\forall a,b \in G$

$\Rightarrow a*b \in G$

(2) Associative law :- $\forall a,b,c \in G$

$\Rightarrow (a*b)*c = a*(b*c) \in G$

(3) Identity law :- $\forall a \in G$

$\exists$ an $e \in G$ such that $a*e = a = e*a \in G$

Then e is the identity element of G.

Ques Prove that $(N, \cdot)$ is a Monoid, where '$\cdot$' is the multiplication as a binary oper^n on the set of natural numbers.

Soln $N = \{1, 2, 3, \ldots\}$

(1) closure law :- $\forall a,b \in N$

$\Rightarrow a \cdot b \in N$

$\therefore$ closure law is satisfied.

(2) Associative law :- $\forall a,b,c \in N$

$\Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c) \in N$

$\therefore$ Associative law is satisfied

(3) Identity law :- $\forall a \in N$

$\exists$ an element $e = 1$ such that $a \cdot 1 = a = 1 \cdot a \in N$

$\therefore$ Identity law is satisfied

Page No.
Date

Hence $(N, \cdot)$ is a monoid.

* Group :- Let G be a non-empty set and '*' is a binary operation on the set G.
Then $(G, *)$ is a group if it satisfies the following properties :-

① Closure law :- $\forall a, b \in G$
$\Rightarrow a * b \in G$

② Associative law :- $\forall a, b, c \in G$
$\Rightarrow (a * b) * c = a * (b * c) \in G$

③ Existence of Identity :- $\forall a \in G$
$\exists$ an element e such that $a * e = a = e * a \in G$

④ Existence of inverse :- $\forall a \in G$
$\exists$ an element $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a \in G$

* Abelian group or commutative group :- A group $(G, *)$ is said to be an abelian group it satisfies commutative law.

• Commutative law :- $\forall a, b \in G$
$a * b = b * a \in G$

Order of a group :- The number of elements in a group G is called the order of a group G. It is denoted by $O(G)$.

Note :- If $O(G)$ is finite then G is a finite group.
If $O(G)$ = infinite then G is a infinite group.

Ques Set of integers under addition is a group?
$(Z, +)$

① closure property :- $\forall a, b \in Z$
$\Rightarrow a + b \in Z$
∴ It satisfies closure property

② Associative property :- $\forall a, b \in Z$
$\Rightarrow (a + b) + c = a + (b + c) \in Z$
∴ It satisfies associative property

③ Identity property :- $\forall a \in Z$
$\exists$ an element e such that $a + e = a = e + a \in Z$
$e = 0$

④ Inverse property :- $\forall a \in Z$

$\exists$ an element a^{-1} such that $a+a^{-1} = e = a^{-1}+a$

$\forall a \in Z$

$a+a^{-1} = 0 = a^{-1}+a \in Z$

∴ It is satisfies inverse property.

Hence it is a group.

Ques set of rational number opern addition?

$(Q, +)$

① closure property :- $\forall \frac{p}{q}, \frac{a}{b} \in Q$ such that $q \neq 0$ & $b \neq 0$

$\Rightarrow \frac{p}{q} + \frac{a}{b} \in Q$

② Associative property :- $\forall \frac{p}{q}, \frac{a}{b}, \frac{c}{d} \in Q$ such that

$q, a, b \neq 0$

$\Rightarrow \left(\frac{p}{q} + \frac{a}{b}\right) + \frac{c}{d} = \frac{p}{q} + \left(\frac{a}{b} + \frac{c}{d}\right) \in Q$

③ Identity property :- $\forall \frac{p}{q} \in Q$ such that $q \neq 0$

$\exists$ an element $\boxed{e=0}$ such that $\frac{p}{q} + 0 = \frac{p}{q} = 0 + \frac{p}{q}$

④ Inverse property :- $\forall \frac{p}{q} \in Q$ such that $q \neq 0$

$\exists$ an element $\left(\frac{-p}{q}\right)$ such that $\frac{p}{q} + \left(\frac{-p}{q}\right) = 0 \in Q$.

Hence it is a group.

\# $(R, +)$, $(N, +)$, $(W, +)$, $(Z, -)$, ~~$(Z, \cdot)$~~ $(Z, \cdot)$, $(R, \cdot)$, $(R^*, \cdot)$, $(Q^*, \cdot)$, $(Q, \cdot)$, $(S, \cdot)$

Imp ⇒ S is a set of irrational numbers

* closure property :- $\forall a, b \in S$

$\sqrt{2} \times \sqrt{2} = 2 \notin S$

Hence it is not a group.

⇒ R^* includes set of all real numbers except 0.

$\frac{1}{a} \times a$ is not a group for $\boxed{a=0}$

Page No.
Date

Ques Show that the set I of all integers i.e. $I = \{-4, -3, -2, -1, 0, 1, 2, 3 \ldots\}$ is an infinite abelian group with respect to the operation '+'.

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

Closure law :- $\forall a, b \in I$

$\Rightarrow a + b \in I$

Associative law :- $\forall a, b, c \in I$

$\Rightarrow (a+b)+c = a+(b+c) \in I$

Existence of Identity law :- $\forall a \in I$

$\Rightarrow \exists$ an element $\boxed{e = 0}$ such that $a + 0 = a = 0 + a \in I$

existence of inverse :- $\forall a \in I$

$\exists$ an element a^{-1} such that $a + a^{-1} = 0 = a^{-1} + a \in I$

~~Hence~~ # Commutative law :- $\forall a, b \in I$

$\Rightarrow$ ~~XX~~ $a + b = b + a \in I$

$\therefore$ It is an abelian group.

Ques Prove that the set of all non-zero real numbers is an abelian group wrt '.' as a binary operation.

Soln closure :- $\forall a, b \in R^*$

$\Rightarrow a \cdot b \in R^*$

Associative :- $\forall a, b, c \in R^*$

$\Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c) \in R^*$

Existence of Identity :- $\forall a \in R^*$

$\exists$ an element $\boxed{e = 1}$ such that ~~XX~~ $a \cdot 1 = a = 1 \cdot a \in R^*$

Existence of inverse :- $\forall a \in R^*$

$\exists$ an element a^{-1} such that ~~XX~~ $a \neq 0$ and $a a^{-1} = 1 = a^{-1} a \in R^*$

commutative :- $\forall a, b \in R^*$

$\Rightarrow a \cdot b = b \cdot a \in R^*$

Hence it is an abelian group.

Ques Prove that the set of all non-zero rational numbers is an abelian group under '.' as a binary opern.

It is an abelian group.

Page No.
Date :

Ques Prove that set of all non-zero integers is an abelian group under '$\cdot$'.

It is not an abelian group because for the existence of inverse $a \times \frac{1}{a} = 1 = \frac{1}{a} \times a \in I$

but $\frac{1}{a} \notin I$ Hence existence of inverse does not exist.

Ques Show that the set of all integers I forms an abelian group with respect to binary operation '$*$' defined by $a * b = a + b + 1 \quad \forall a, b \in I$.

Sol

① closure law :- $\forall a, b \in I$

Then $a * b = a + b + 1 \in I$

$\because \forall a, b \in I \Rightarrow a * b \in I$

I is closed under $*$.

② Associative law :- $\forall a, b, c \in I$

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

$= a + b + 1 + c + 1$

$= a + b + c + 2 \in I$

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

$= a + b + c + 2 \in I$

$(a * b) * c = a * (b + c) \in I$

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

③ Existence of identity :- $\forall a \in I$

Let e be the identity of I under $*$

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

$\Rightarrow a * e = a + e + 1$

$\Rightarrow a = a + e + 1$

$\Rightarrow e + 1 = 0$

$\Rightarrow \boxed{e = -1}$

$a * (-1) = a + (-1) + 1 = a$

Page No.
Date :

④ Existence of inverse :- let $b \in I$ be the inverse of $a \in I$ under $*$.

then $a * b = e$

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

$\Rightarrow e = a + b + 1$

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

$\Rightarrow \boxed{-2 - a = b}$

$(-2-a)$ is the inverse of $a \in I$ under $*$.

⑤ commutative law :- $\forall a, b \in I$

$a * b = b * a$

$a + b + 1 = b + a + 1$

Hence $a * b$ is an abelian group under $* \; a, b \in I$

Ques consider an algebraic structure $(\mathbb{Q}, *)$ where $\mathbb{Q}$ is the set of rational numbers and $*$ is a binary operation defined by $a * b = a + b - ab \; \forall a, b \in \mathbb{Q}$. Determine whether $(\mathbb{Q}, *)$ is a group.

Ans ① closure property :- $\forall a, b \in \mathbb{Q}$

then $a * b = a + b - ab \in \mathbb{Q}$

$\therefore \forall a, b \in I \Rightarrow a * b \in \mathbb{Q}$

$\therefore$ It is closed under $*$.

② Associative law :- $\forall a, b, c \in \mathbb{Q}$

then $(a * b) * c = (a + b - ab) * c$

$= (a + b - ab) + c - (a + b - ab)c$

$= a + b + c - ab - ac - bc + abc$

$a * (b * c) = a * (b + c - bc)$

$= a + b + c - bc - a(b + c - bc)$

$= a + b + c - bc - ab - ac + abc$

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

$\therefore$ It is closed under '$*$'.

(3) Existence of Identity :- Let e be the identity of Q under $*$.

Then $\forall a \in Q$ we have $a * e = a$

$\Rightarrow a + e - ae = a$

$\Rightarrow e - ae = 0$

$\Rightarrow e(1-a) = 0$

$\Rightarrow \boxed{e = 0}$ $\because a \neq 1$ ~~$a = 0$~~ ~~$a \neq 0$~~

(4) Existence of Inverse :- Let b be the inverse of a under $*$.

$\Rightarrow a * b = e$

$\Rightarrow a + b - ab = 0$

$\Rightarrow b = ab - a$

$\Rightarrow b - ab = -a$

$\Rightarrow b(1-a) = -a$

$\Rightarrow b = \frac{-a}{1-a}$ or $\boxed{b = \frac{a}{a-1}} \in Q$

$\therefore \frac{a}{a-1} \in Q$ is the Inverse of a under $*$

(5) commutative law :- $\forall a, b \in Q$

$a * b = b * a$

$a + b - ab = b + a - ba$

$a + b + ab = a + b - ab$

$a * b = a + b - ab$

$= b + a - ba$

$= b * a$

Hence it is an abelian group.

Ques Consider an algebraic structure $(G, *)$ where G is the set of all non-zero real numbers and $*$ is a binary operation defined by $a * b = \frac{ab}{4}$. Show that $(G, *)$ is an abelian group.

Page No.
Date :

Sol^n (1) Closure law :- let $a, b \in R^*$

$\Rightarrow ab \in R^*$

$\Rightarrow \frac{ab}{4} \in R^*$

$\Rightarrow a * b \in R^*$

$\therefore \forall a, b \in R^* \Rightarrow a * b \in R^*$

(2) Associative law :- $\forall a, b, c \in R^*$

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

$= \left(\frac{ab}{4}\right) * c = \frac{ab * c}{16} \in R^*$

$a * (b * c) = a * \frac{bc}{4} = \frac{abc}{16} \in R^*$

$(a * b) * c = a * (b * c) \in R^*$

$\forall a, b, c \in R^* \Rightarrow (a * b) * c = a * (b * c) \in R^*$

(3) Existence of Identity :- $\forall a \in R^*$

Let e be the Identity of R^*.

Then $a * e = a$

$a * e = \frac{ae}{4}$

$\Rightarrow a = \frac{ae}{4} \Rightarrow e = 4 \Rightarrow \boxed{e = 4}$

(4) Existence of Inverse :- let b be the inverse of $a \in R^*$

then $a * b = e$

$\Rightarrow a * b = 4$

$\Rightarrow \frac{ab}{4} = 4$

$\Rightarrow ab = 16 \Rightarrow \boxed{b = \frac{16}{a}} \in R^*$

$\therefore \frac{16}{a}$ is the inverse of $a \in R^*$.

(5) commutative law :- $\forall a, b \in R^*$

$\Rightarrow a * b = \frac{ab}{4} = \frac{ba}{4} = b * a$

$\Rightarrow a * b = b * a \quad \forall a, b \in R^*$

$\therefore (R^*, *)$ is an abelian group.

Ques Let z be the group of integers with binary operation * defined by

$a * b = a + b - 2 \quad \forall a, b \in z$

Find the identity element of the group $(z, *)$

Ans $a * b = a + b - 2$

Let e be the identity of $(z, *)$

$\Rightarrow a * e = a \quad \forall a \in z$

$\Rightarrow a + e - 2 = a$

$\Rightarrow e - 2 = a - a$

$\Rightarrow e - 2 = 0 \Rightarrow \boxed{e = 2}$ Ans

Ques Show that set $G = \{a + \sqrt{2}b : a, b \in Q\}$ is an abelian group under '+'.

Ans (1) closure law :- $a_1 + \sqrt{2}b_1$ & $a_2 + \sqrt{2}b_2 \in G$

Now, $(a_1 + \sqrt{2}b_1) + (a_2 + \sqrt{2}b_2)$

$= (a_1 + a_2) + \sqrt{2}(b_1 + b_2) \in Q$

$= c_1 + \sqrt{2}c_2 \in G$

(2) Associative law :- $\alpha = a_1 + \sqrt{2}b_1$, $\beta = a_2 + \sqrt{2}b_2$,

$\gamma = a_3 + \sqrt{2}b_3 \in G$

$(\alpha + \beta) + \gamma = [(a_1 + \sqrt{2}b_1) + (a_2 + \sqrt{2}b_2)] + \gamma$

$= [(a_1 + a_2) + \sqrt{2}(b_1 + b_2)] + \gamma$

$= (a_1 + a_2 + a_3) + \sqrt{2}(b_1 + b_2 + b_3)$

$= \boxed{c_1 + \sqrt{2}c_2}$

$\alpha + (\beta + \gamma) = \alpha + (a_2 + a_3) + \sqrt{2}(b_2 + b_3)$

$= (a_1 + a_2 + a_3) + \sqrt{2}(b_1 + b_2 + b_3)$

$= \boxed{c_1 + \sqrt{2}c_2}$

$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

(3) Existence of identity :- Let $0 = 0 + \sqrt{2}\,0 \in G$

$\therefore \forall\ a + \sqrt{2}\,b \in G$ we have

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

(4) Existence of inverse :- $\forall\ a+\sqrt{2}\,b \in G \ \forall\ a, b \in \mathbb{Q}$ and $-a, -b \in \mathbb{Q}$

$\forall\ a+\sqrt{2}\,b$ ∃ an element $(-a)+\sqrt{2}(-b) \in G$ such that

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

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

$= 0 + \sqrt{2}\,0 = e$

$(-a)+\sqrt{2}(-b)$ is a inverse of $a+\sqrt{2}\,b$

(5) commutative law :- Let $a_1+\sqrt{2}\,b_1$ & $a_2+\sqrt{2}\,b_2 \in G$

Now $(a_1+\sqrt{2}\,b_1) + (a_2+\sqrt{2}\,b_2)$

$= (a_1+a_2) + \sqrt{2}(b_1+b_2)$

$= (a_2+a_1) + \sqrt{2}(b_2+b_1)$

$= (a_2+\sqrt{2}\,b_2) + (a_1+\sqrt{2}\,b_1)$

$\therefore$ G is an abelian group under '+'.

Ques Show that the set of matrices

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}, \ \alpha \in R$$ forms abelian group under matrix multiplication.

Soln Let $G = \left\{ A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}, \ \alpha \in R \right\}$ Then to show that $(G, \cdot)$ is an abelian group.

(1) closure property :- $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$, $A_\beta = \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$

$$\Rightarrow A_\alpha \cdot A_\beta = \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ +\sin\alpha\cos\beta + \cos\alpha\sin\beta & \sin\beta\sin\alpha + \cos\alpha\cos\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} \in G$$

$$= A_{(\alpha+\beta)} \in G$$

(2) Associative law :- $A_\alpha, A_\beta, A_\gamma \in G$, $\alpha, \beta, \gamma \in R$

$(A_\alpha \cdot A_\beta) \cdot A_\gamma = A_{\alpha+\beta} \cdot A_\gamma = A_{(\alpha+\beta)+\gamma}$

$= A_{\alpha+(\beta+\gamma)}$

$= A_\alpha \cdot A_{(\beta+\gamma)}$

$= A_\alpha \cdot (A_\beta \cdot A_\gamma)$

(3) Existence of identity :-

$\therefore \forall A_\alpha \in G$ $\exists$ an element $A_0 = I \in G$ such that

$A_\alpha A_0 = A_\alpha = A_0 \cdot A_\alpha$

(4) Existence of inverse :-

Let $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \in G$, $\alpha \in R$.

$\sin\alpha \in R$, $-\alpha \in R$

$\therefore \forall A_\alpha \in G$ $\exists$ an element $A_{(-\alpha)} \in G$

such that

$A_\alpha \cdot A_{(-\alpha)} = A_{\alpha-\alpha} = A_0 = A_{(-\alpha)} \cdot A_\alpha$

(5) Commutative law :- Let $A_\alpha, A_\beta \in G$

Then $A_\alpha \cdot A_\beta = A_{\alpha+\beta} = A_{\beta+\alpha} = A_\beta \cdot A_\alpha \in G$

$A_\alpha \cdot A_\beta = A_\beta \cdot A_\alpha$

$\therefore (G, \cdot)$ is an abelian group.

Ques Let $G = \{(a,b) \mid a,b \in R \ a \neq 0\}$. Define on a binary operation '$*$' on G by $(a,b) * (c,d) = (ac, bc+d)$ $\forall$ $(a,b), (c,d) \in G$. Show that $(G, *)$ is a group.

Soln (1) closure law :- Let $(a,b), (c,d) \in G$

$a,b,c,d \in R$ & $a \neq 0$, $c \neq 0$

$\Rightarrow (a,b) * (c,d) = (ac, bc+d) \in G$

$- [ac, bc+d \in R$ & $a \neq 0, c \neq 0$

$\Rightarrow ac \neq 0]$

(2) Associative law :-

The operation $*$ satisfies associative law as the associative law hold on the set of real number.

Let $(a,b), (c,d), (e,f) \in G$

then

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

(3) Existence of Identity :- Let $(a,b) \in G$ & an element $(1,0) \in G$ $(a \neq 0,\ a,b \in R)$ such that

$(a,b) * (1,0) = (a \cdot 1, b \cdot 1 + 0)$

$= (a,b)$

(4) Existence of Inverse :- Let (c,d) is the Inverse of (a,b)

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

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

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

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

$\therefore \left(\frac{1}{a}, -\frac{b}{a}\right)$ is the Inverse of (a,b)

$\therefore$ It is a group.

Ques Show that the set of cube root of unity is an abelian group w.r.t '.'.

Or

Show that the set of cube root of unity $\{1, w, w^2\}$ form a finite abelian group under '.'.

Soln $w^3 = 1$

.	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

$w^4 = w^3 \cdot w = 1 \cdot w = w$

* Closure property :- since all the elements in the ~~combine~~ composition table $\in G$.

$\Rightarrow G$ is closed under '.'.

* Associative property :- since all the elements of G are complex numbers & complex number are associative always $\Rightarrow G$ is satisfies associative law.

* **Existence of identity** :- from the composition table we see that $\forall a \in G$ $\exists$ an element $1 \in G$ such that $1 \times a = a = a \times 1$.

* **Existence of inverse** :- from the composition table $1 \cdot 1 = 1$, $w \cdot w^2 = w^3 = 1$, $w^2 \cdot w = w^3 = 1$
$\therefore \forall a \in G$ $\exists$ an element $b \in G$ such that $a \cdot b = 1 = b \cdot a$

* **commutative law** :- since in the composition table, each row & corresponding column are equal.
$\Rightarrow$ commutative law holds.
i.e. $\forall a, b \in G$
$$\boxed{a \cdot b = b \cdot a}$$
$\therefore (G, \cdot)$ is a finite abelian group ~~of~~ of order 4

Ques Show that the set of four fourth roots of unity namely $1, -1, i, -i$ forms an abelian group w.r.t '.'.

Soln $i^2 = -1$

$\cdot$	1	-1	i	$-i$
1	(1)	-1	i	$-i$
-1	-1	(1)	$-i$	i
i	i	$-i$	-1	(1)
$-i$	$-i$	i	(1)	-1

* **closure property** :- ✓
* **Associative property** :- ✓
* **Existence of identity** :- ✓
* **Existence of inverse** :- ✓
* **commutative law** :- ✓

Ques Show that the set of n-nth roots of unity forms a finite abelian multiplicative group of order n.

Soln

Page No.
Date :

$1^{1/n} = (1+i0)^{1/n}$

$= (\cos 0 + i\sin 0)^{1/n}$

$= (\cos 2k\pi + i\sin 2k\pi)^{1/n}$

$= \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$

$= e^{i2k\pi/n} = w^k$

$G = \{1, w, w^2, w^3 \ldots, w^{n-1}\}$

① Closure law :- $w \cdot w^2 = w^3$

$w^4 \cdot w^5 = w^9$

$\therefore \forall a, b \in G \Rightarrow a \cdot b \in G$

② Associative law :- Since the elements of G are complex number & the set of complex numbers are associative.

$\forall a, b \in G$

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

③ Existence of identity :- $\forall a \in G$ $\exists$ an element $1 \in G$ such that $a \cdot 1 = a = 1 \cdot a$

④ Existence of inverse :- Let $a = w^k$, $b = w^{n-k}$

$a \cdot b = w^k \cdot w^{n-k}$ $\quad 0 \le k \le n-1$

$= w^{k+n-k}$

$= w^n$

$= 1$

$\Rightarrow a \cdot b = 1$

⑤ Commutative law :- $\forall a, b \in G$ $\exists$ we have $\boxed{a \cdot b = b \cdot a}$

$\therefore (G, \cdot)$ is a finite abelian group of order n.

* Addition modulo m :- If a and b are any two integers then the operation of addition modulo m is defined as the least non-negative remainder when ordinary sum of a & b divided by m. i.e. $a \oplus_m b = r$ where r is the non-negative remainder when $a+b$ is divided by m.

Page No.
Date :

ex $5 \oplus_3 3 = 2$

* Additive group of integer modolo m :- The set of $Z_m = \{0, 1, 2, 3 \ldots, m-1\}$ of first m non-negative integers is a group w.r.t the composition addition modolo m i.e. $\oplus_m$.

Ques Prove that the set $Z_6 = \{0, 1, 2, 3, 4, 5\}$ is a finite abelian group of order 6 wrt addition modolo 6.

Soln

$\oplus_6$	0	1	2	3	4	5
0	(0)	1	2	3	4	5
1	1	2	3	4	5	(0)
2	2	3	4	5	(0)	1
3	3	4	5	(0)	1	2
4	4	5	(0)	1	2	3
5	5	(0)	1	2	3	4

* Closure property :- since all the elements in the composition table $\in Z_6$.

$\forall\ a, b \in G = a \oplus_6 b \in Z_6$

* Associative property :- since all the elements in the composition table $\in Z_6$ and integers are associative in nature.

* Existence of identity :- $\forall\ a \in Z_6$

$\exists$ an element 0 such that

$$a \oplus_6 0 = a = 0 \oplus_6 a$$

* Existence of inverse :- from the composition table $\forall\ a \in G$ i.e. Z_6 $\exists$ an element $b \in G$ such that $a \oplus_6 b = 0$

* commutative law :- since in the composition table each row is equal to its corresponding column i.e. $a, b \forall G$ i.e. Z_6

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

$\therefore$ Z_6 is an abelian group under $\oplus_6$.

* Multiplication modolo m :- If a & b are any two integers then the operation of multiplication modolo m is defined as non-negative remainder when the ordinary product of a & b is divided by m.

i.e. $a \otimes_m b = r$

where r is the least non-negative remainder.

* Multiplicative group of integer modolo p :- The set $Z_p = \{1, 2, 3 \ldots\}$ of $(p-1)$ integers (where p is a prime integer) is a finite abelian group of order $(p-1)$ with respect to multiplication modolo p $(\times_p)$.

Ques Prove that the set $G = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group of order 6 under the multiplication modolo 7.

Soln

$\otimes_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$\therefore Z_7$ is an abelian group under $\otimes_7$.

Ques $G = \{1, 2, 3\}$ under $\otimes_4$

$\otimes_4$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	2

It is not a group because 0 is the element i.e. not present in G. $\therefore$ closure property $\notin$ G.

Page No
Date :

Theorem 1 :- Cancellation law :-

Suppose a, b, c are arbitrary elements of a group G.

Then

$ab = ac \Rightarrow b = c$ (left cancellation law)

$ba = ca \Rightarrow b = c$ (right cancellation law)

Proof :- Let e be the identity element of a group G.

and let $a, b, c, d \in G$.

Now $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$ [$\because a \in G \Rightarrow a^{-1} \in G$]

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ [By associative law]

$\Rightarrow eb = ec$ [$\because a^{-1}a = e$]

$\Rightarrow \boxed{b = c}$ [$ae = a$]

left cancellation law.

&

$= ba = ca$ ($\because a \in G \Rightarrow a^{-1} \in G$)

$= (ba)a^{-1} = (ca)(a^{-1})$

$= b(aa^{-1}) = c(aa^{-1})$ (by associative law)

$\Rightarrow be = ce$

$\Rightarrow \boxed{b = c}$

right cancellation law.

Theorem 2 :- Uniqueness of identity :-

Prove that the identity e in a group is unique.

Proof :- If possible, suppose e & e' are two identity in a group G.

Then $\forall a \in G$, we have

$ae = a = ea$ — (1)

$a = e'a = ae'$ — (2)

from (1) & (2)

$\Rightarrow ae = ae'$ & $ea = e'a \Rightarrow e = e'$ (by right cancellation)

$\Rightarrow e = e'$ (by left cancellation)

$\therefore \boxed{e = e'}$

Hence identity in a group G is unique.

Page No.
Date :

Theorem 3 :- Uniqueness of Inverse :- Prove that the inverse of each element of a group is unique.

Proof :- If possible, let b and c be two inverse of the same element a of a group G. Then

$ab = e = ba$ — (1)

$ac = e = ca$ — (2)

from (1) & (2)

$ab = ac$ $\qquad$ $ba = ca$

$b = c$ (by left cancellation) $\qquad$ $b = c$ (by right cancellation)

$\therefore \boxed{b = c}$

Hence inverse of a is unique.

★ **Theorem 4 :-** Reversal law :- The inverse of a product of two elements of a group G is the product of the inverses taken in the reverse order.

Or

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

Proof :- ~~The Inverse~~ Let a & b are any elements of any group G and a^{-1} & b^{-1} are respectively the inverse of a and b. Then

$aa^{-1} = e = a^{-1}a$ — (1)

$bb^{-1} = e = b^{-1}b$ — (2)

} where e is the identity of group G.

Now,

$(ab)(b^{-1}a^{-1}) = [(ab)(b^{-1})]a^{-1}$ (by associative law)

$= [a(bb^{-1})]a^{-1}$ (by associative law)

$= [ae]a^{-1}$ (from (2))

$= aa^{-1}$ (∵ $ae = a$) (by identity law)

$= e$ (from (1))

$\therefore \boxed{(ab)(b^{-1}a^{-1}) = e}$ — (3)

Page No.
Date :

Similarly, $(b^{-1}a^{-1})(ab) = b^{-1}[a^{-1}(ab)]$ (by asso. law)
$= b^{-1}[(a^{-1}a)b]$ (by asso. law)
$= b^{-1}[eb]$ (from ①)
$= b^{-1}(b)$ (from identity law)
$= \boxed{e}$ (from ②)

$\therefore \boxed{(b^{-1}a^{-1})(ab) = e}$ — ④

from ③ & ④

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

Hence proved!!

Theorem 5 :- If the inverse of an element 'a' in a group is a^{-1}. then the inverse of a^{-1} is a.
or
Prove that $(a^{-1})^{-1} = a$ $\forall a \in G$

Proof :- Let e be the identity element of group G.
Then,

$a^{-1}a = e$ $\forall a \in G$
$\Rightarrow (a^{-1})^{-1}a^{-1}a = (a^{-1})^{-1}e$ [$\because$ multiplying by $(a^{-1})^{-1}$ both sides]
$\Rightarrow [(a^{-1})^{-1}a^{-1}]a = (a^{-1})^{-1}$
$\Rightarrow ea = (a^{-1})^{-1}$ ($\because ae = a$) (by identity & (by associative law])
$\Rightarrow \boxed{a = (a^{-1})^{-1}}$ ($b^{-1}b = e$)

Hence proved!!

Order of an element of a group

⇒ Let e be the identity in a group G and $a \in G$.
If $a^n = e$ (where n be the least +ve integer) i.e. the order of the element a is n.

Note :- (i) $O(e) = 1$
(ii) $O(a) = O(a^{-1})$
(iii) If $a^m = e \Rightarrow O(a) \leq m$

(4) If there does not exist least +ve integer n such that $a^n = e$ then $O(a) = \infty$

Eg :- Let $G = \{1, -1, i, -i\}$ be a multiplicative group. Find the order of every element ?

Soln $\boxed{O(1) = 1}$ $(\because O(e) = 1)$

for $O(-1) \Rightarrow (-1)(-1) = 1 \Rightarrow (-1)^2 = \boxed{1}$

$\boxed{O(-1) = 2}$

for $O(i) \Rightarrow i \times i = i^2 = -1 \times i = -i \times i = -i^2 = \boxed{1}$

$\boxed{O(i) = 4}$

$i \times i = -1$

$i \times i \times i = -i$

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

for $(-i) \Rightarrow -i \times -i = +i^2 = -1$

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

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

$\boxed{O(-i) = 4}$

Ques find the order of each element of the multiplicative group $(\{1, w, w^2\}, \cdot)$.

Soln $O(1) = 1$

for $O(w) \Rightarrow w \times w = w^2$

$w \times w \times w = w^3 = \boxed{1}$

$\boxed{O(w) = 3}$

for $O(w^2) \Rightarrow w^2 \times w^2 = w^4 = w$

$w^2 \times w^2 \times w^2 = w^6 = w^3 \times w^3 = \boxed{1}$

$\boxed{O(w^2) = 3}$

Ques find the order of each element of the group $G = \{0, 1, 2, 3, 4, 5\}$, the composition in G is additive modolo '6'.

Ans $\boxed{O(0) = 1}$

for $O(1) =$ ~~1~~ $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 0$

$\boxed{O(1) = 6}$

for $O(2) = 2 \oplus_6 2 = 4$

$2 \oplus_6 2 \oplus_6 2 = \boxed{0}$

$\boxed{O(2) = 3}$

for $O(3) = 3 \oplus_6 3 = \boxed{0}$, ~~$3 \oplus_6 3 \oplus_6 3$~~

$\boxed{O(3) = 2}$

for $O(4) = 4 \oplus_6 4 = 2$

$4 \oplus_6 4 \oplus_6 4 = \boxed{0}$

$\boxed{O(4) = 3}$

for $O(5) = 5 \oplus_6 5 = 4$

$5 \oplus_6 5 \oplus_6 5 = 3$

$5 \oplus_6 5 \oplus_6 5 \oplus_6 5 = 2$

$5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 = \boxed{1}$

$5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 = 0$

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

Ques Find the order of each element of $(\mathbb{Z}, +)$.

Solⁿ $\therefore O(0) = 1$

& $O(a) = \infty \quad \forall a \in \mathbb{Z}$

as we can't find least non-negative integer.

Theorem :- If an element a of a group G is of order n, then

$a^m = e$ iff n is a divisor of m.

Proof :- suppose n is a divisor of m then to prove $a^m = e$.

Let n is a divisor of m.

Then there exists an integer q such that

$\frac{m}{n} = q \Rightarrow \boxed{m = nq} \quad - (1)$

Now, $a^m = a^{nq} = (a^n)^q = e^q = e$

$\Rightarrow \boxed{a^m = e}$

Conversely :

Suppose $\boxed{a^m = e}$ then to show that n is a divisor of m.

Given $O(a) = n \Rightarrow a^n = e$ (n is the least +ve integer)

Now, $a^m = e \Rightarrow O(a) \leq m$

since m is an integer and n is a +ve integer, then by division algorithm, $\exists$ q & r such that

$m = nq + r$ where $0 \leq r < n$ — (2)

Now $a^m = a^{nq+r}$

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

$= (a^n)^q \cdot a^r$

$= e \cdot a^r$

$\boxed{a^m = a^r}$

But $a^m = e \Rightarrow a^r = e$, $0 \leq r < n$

But $O(a) = n$ so we must have $\boxed{r = 0}$

from (2) $m = nq$

$\frac{m}{n} = q$

$\Rightarrow n$ is a divisor of m.

Theorem 2 :- If a and x are arbitary elements of a group, then order of a is the same as the order of $x^{-1}ax$.

i.e. $O(a) = O(x^{-1}ax)$.

Proof :- Let $O(a) = n$ — (1)

$O(x^{-1}ax) = m$ — (2)

Then to show that $\boxed{n = m}$

Now, $(x^{-1}ax)^2 = (x^{-1}ax)(x^{-1}ax) = x^{-1}a(xx^{-1})ax =$

$= x^{-1}aeax$

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

$\therefore (x^{-1}ax)^2 = x^{-1}a^2x$

Similarly $(x^{-1}ax)^n = x^{-1}a^nx$ — (1)

$= x^{-1}ex$

$= x^{-1}x$

$\Rightarrow (x^{-1}ax)^n = e$ — (3)

$\Rightarrow O(x^{-1}ax) \leq n$

$\Rightarrow m \leq n$ — (4)

$\Rightarrow O(x^{-1}ax) = m$ (from ②)

$\Rightarrow (x^{-1}ax)^m = e$

$\Rightarrow x^{-1}a^m x = e$ (from ③)

$\Rightarrow x^{-1}a^m x = x^{-1}x$ $(x^{-1}x = e)$

$\Rightarrow x^{-1}a^m x = x^{-1}ex$

$\Rightarrow \boxed{a^m = e}$ (by right & left cancellation law)

$O(a^{mn}) \leq m$

$n \leq m$ — ⑤

from ④ & ⑤

$\Rightarrow m = n$

$\Rightarrow \boxed{O(x^{-1}ax) = O(a)}$

Theorem :- If a, b are arbitrary elements of a group G, then

$(ab)^2 = a^2b^2$ iff G is abelian.

Proof :- Let G be a group and $a, b \in G$

Suppose $(ab)^2 = a^2b^2$ $\forall$ $a, b \in G$

Then to show that G is abelian.

Now $(ab)^2 = a^2b^2$ $\forall$ $a, b \in G$

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ (Asso. law)

$\Rightarrow \boxed{ba = ab}$ (by right & left cancellation law)

$\therefore ab = ba$ $\forall$ $a, b \in G$

$\Rightarrow G$ is abelian

Conversely, suppose $ab = ba$ then prove that

$(ab)^2 = a^2b^2$ $\forall$ $a, b \in G$

$\Rightarrow$ Now, $(ab)^2 = (ab)(ab)$

$= a(ba)b$ (by asso. law)

$= a(ab)b$ ($\because G$ is abelian)

$= \boxed{a^2b^2}$ (by asso. law)

$\boxed{(ab)^2 = a^2b^2 \ \forall \ a, b \in G}$

Page No.
Date :

INF

① If G is an abelian group then
$(ab)^n = a^n b^n \quad \forall a, b \in G$ & $\forall n \in I$.

② If every element of a group G is its own inverse, then G is an abelian group.

③ If for every element in a group G,
$a^2 = e \Rightarrow a \cdot a = e$
then G is an abelian group.

④ If G is a group such that
$(ab)^m = a^m b^m$ for three consecutive integers m
then G is abelian.

⑤ Any group of order less than 6 must be abelian.

Subgroup

Let H be a non empty subset of a group G. Then H is called a subgroup of G if H is itself group under the same operation defined on G.

Note → Let G be a group then G and $\{e\}$ both are subgroup of G are called trivial group or improper subgroup of G.
Any subgroup other than these two subgroups are called non-trivial subgroup or proper subgroup of G.

Theorem :- A necessary & sufficient condition that a non-empty subset H of a group G to be a subgroup is
$a \in H, b \in H \Rightarrow ab^{-1} \in H$

Or A non-empty subset H of a group G is a subgroup of G iff $a \in H, b \in H \Rightarrow ab^{-1} \in H$.

Proof :- Let H be a subgroup of G, then to show that
$a \in H, b \in H \Rightarrow ab^{-1} \in H$.

Necessary condition :-
Since H is a subgroup of G then H itself is a group same operation as in G.

Let $a, b \in H$

Now $b \in H \Rightarrow b^{-1} \in H$ (by inverse property)

$\therefore a, b \in H \Rightarrow a, b^{-1} \in H$ (by closure property)

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

Page No.
Date :

Hence $a,b \in H \Rightarrow ab^{-1} \in H$

* Sufficient condition :- Let H be a non-empty subset of G such that $a \in H, b \in H \Rightarrow ab^{-1} \in H$ — (1)

Then to show that H is a subgroup of G.

FOR this we have to show that H is also a group.

(1) existence of identity :- from (1)

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

$\therefore$ the identity e is an element of H.

(2) existence of inverse :- Let $b \in H$ from (1)

$e \in H, b \in H \Rightarrow eb^{-1} \in H \quad [e \cdot b = b]$

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

$\therefore b \in H \Rightarrow b^{-1} \in H$

$\therefore$ each element poses inverse in H.

(3) closure law :- Let $b \in H \Rightarrow b^{-1} \in H$

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

$\Rightarrow a(b^{-1}) \in H \Rightarrow ab \in H$ (from (1))

$\therefore a \in H, b \in H \Rightarrow ab \in H$

H is closed under same operation G.

(4) Associative law :- Since $H \subset G$ Let $a,b,c \in H$

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

$\therefore (a.b).c = a.(b.c) \; \forall \; a,b,c \in H$

Hence H is itself a group.

$\Rightarrow$ H is a subgroup of G.

Ques Prove that $\{1,-1\}$ is a subgroup of group $\{-1,1,i,-i\}$ under multiplication.

Soln Let $H = \{1,-1\}$ & $G = \{-1,1,i,-i\}$

Let $a = 1, b = (-1) \quad H \subset G$

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

$= 1.(-1)$

$= -1 \in H$

$\therefore a \in H, b \in H \Rightarrow ab^{-1} \in H$

Hence H is a subgroup of G.

Page No.
Date :

* for multiplication :-
$a \in H, b \in H \Rightarrow a \cdot b^{-1} \in H$

* for addition :-
$a \in H, b \in H \Rightarrow a + b^{-1} \in H$
$\Rightarrow \boxed{a - b} \in H$

(*) Prove that $H = \{5n : n \in z\}$ is a subgroup of Integers under addition.

Ans Let $a, b \in H$
such that $a = -10$, $b = 5$
& $a - b = -10 - 5 = -15 \in H$
$\therefore \boxed{a \in H \& b \in H \Rightarrow a - b \in H}$

Prof Prove :- Prove that the intersection of two subgroups of a group G, is a subgroup of G.
Or
If H_1 & H_2 are two subgroups of G, then $H_1 \cap H_2$ is also a subgroup of G.

Proof :- Let H_1 & H_2 be any two subgroup of a group G. Then to show that $H_1 \cap H_2$ is a subgroup of G.

Since $e \in H_1$ & $e \in H_2 \Rightarrow e \in H_1 \cap H_2$
$\Rightarrow H_1 \cap H_2 \neq \phi$

Let $a, b \in H_1 \cap H_2$
$\Rightarrow a, b \in H_1$ & $a, b \in H_2$ (since H_1 & H_2 are subgroups of G)
$\Rightarrow ab^{-1} \in H_1$ & $ab^{-1} \in H_2$
$\Rightarrow ab^{-1} \in H_1 \cap H_2$
$\therefore a \in H_1 \cap H_2$, $b \in H_1 \cap H_2 \Rightarrow ab^{-1} H_1 \cap H_2$
Hence $H_1 \cap H_2$ is also a subgroup of G.

Theorem :- Union of two subgroup is not necessarily a subgroup.
Let $H_1 = \{ \ldots\ldots -6, -4, -2, 0, 2, 4, 6 \ldots \}$
& $H_2 = \{ \ldots\ldots -15, -10, -5, 0, 5, 10, 15 \ldots \}$
are subgroup of $(z, +)$.

Then $H_1 \cup H_2 = \{0, \pm 2, \pm 4, \pm 6, \ldots\} \; 0, \pm 5, \pm 10, \pm 15 \ldots$

since $4 \in H_1 \cup H_2$, $5 \in H_1 \cup H_2$

$\Rightarrow 4+5 = 9 \notin H_1 \cup H_2$

Hence closure property does not satisfied.

Hence $H_1 \cup H_2$ is not a group / not a subgroup of $(Z, +)$.

Theorem :- The union of a two subgroup of a group G is a subgroup of G iff one contained in the other.

Proof :- Let H_1 & H_2 be subgroups of a group G.

Suppose $H_1 \subset H_2$ or $H_2 \subset H_1$

Then to show that $H_1 \cup H_2$ is a subgroup of G.

Since $H_1 \subset H_2$ then $H_1 \cup H_2 = H_2$

or $H_2 \subset H_1$ then $H_1 \cup H_2 = H_1$

Since H_1 & H_2 are subgroup of $G \Rightarrow$

$H_1 \cup H_2$ is also a subgroup of G.

conversely, Suppose $H_1 \cup H_2$ is a subgroup of a group G. Then to show that

$H_1 \subset H_2$ or $H_2 \subset H_1$.

If possible, $H_1 \not\subset H_2$ or $H_2 \not\subset H_1$

$H_1 \not\subset H_2 \Rightarrow \exists\, a \in H_1$ such that $a \notin H_2$ — (1)

$H_2 \not\subset H_1 \Rightarrow \exists\, b \in H_2$ such that $b \notin H_1$ — (2)

Now $a \in H_1, b \in H_2 \Rightarrow a, b \in H_1 \cup H_2$

[$\because H_1 \cup H_2$ is a subgroup]

$\Rightarrow ab \in H_1 \cup H_2$

$\Rightarrow ab \in H_1$ or $ab \in H_2$

Now $ab \in H_1$ [$\because a \in H_1 \Rightarrow a^{-1} \in H_1$]

$a^{-1} \in H_1$

$\Rightarrow a^{-1}(ab) \in H_1$

$\Rightarrow (a^{-1}a)\, b \in H_1$

$= b \in H_1$ (which is contradiction)

Page No.
Date :

$\because ab \in H_2$, $b^{-1} \in H_2 \Rightarrow (ab)b^{-1} \in H_2$ [$b \in H_2 \Rightarrow b^{-1} \in H_2$]
$= a(bb^{-1}) \in H_2$
$= a \in H_2$ (which is also a contradiction)

$\therefore$ Our assumption is wrong.

Thus $H_1 \subset H_2$ or $H_2 \subset H_1$.

cyclic group

Let G be any group. If for $a \in G$, every element $x \in G$ can be generated by a such that $x = a^n$, $n \in I$. Then G is called a cyclic group and a is called its generator.
A cyclic group G with generator a is denoted by
$G = \langle a \rangle$ or $G = \{a\}$.

Ques Prove that $G = \{1, -1, i, -i\}$ is cyclic. also find its generator.

Soln $G = \{1, -1, i, -i\}$
or $G = \{i^4, i^2, i^0, i^3\}$
$G = \{i, i^2, i^3, i^4\}$
$\Rightarrow G = \langle i \rangle \Rightarrow$ G is cyclic

$-1 = (i)^2$

* $G = \{1, i, i, -i\}$
or $G = \{(-i)^4, (-i)^2, (-i)^3, -i\}$
$G = \langle -i \rangle \Rightarrow$ G is cyclic

Hence G is a cyclic group & its generator are i & $-i$.

$\Rightarrow$ If a is a generator then a^{-1} is also a generator.

Ques Prove that the multiplicative group of the cube roots of unity $\{1, w, w^2\}$ is a cyclic group. find its generator?

Ans
$G = \{1, w, w^2\}$
$G = \{w^3, w, w^2\}$
or $G = \{w, w^2, w^3\}$ $\quad w \cdot w^2 = \boxed{1}$
or $G = \langle w \rangle \Rightarrow$ G is cyclic
Now, $G = \{1, w, w^2\}$
$G = \{(w^2)^3, (w^2)^2, w^2\}$
$G = \langle w^2 \rangle \Rightarrow$ G is cyclic

Page No.
Date :

Ques Prove that $(G = \{0,1,2,3,4,5\}, \oplus_6)$ is a cyclic group. Find generators?

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

$1^1 = 1$

$1^2 = 1 \oplus_6 1 = 2$

$1^3 = 1 \oplus_6 1 \oplus_6 1 = 3$

$1^4 = 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$

$1^5 = 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 5$

$1^6 = 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 0$

$\therefore G = \{1^1, 1^2, 1^3, 1^4, 1^5, 1^6\}$

$G = \langle 1 \rangle \Rightarrow G$ is cyclic

$1 \oplus_6 5 = 0$

$5^1 = 5$

$5^2 = 5 \oplus_6 5 = 4$

$5^3 = 5 \oplus_6 5 \oplus_6 5 = 3$

$5^4 = 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 = 2$

$5^5 = 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 = 1$

$5^6 = 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 \oplus_6 5 = 0$

$\therefore G = \{5^1, 5^2, 5^3, 5^4, 5^5, 5^6\}$

$G = \langle 5 \rangle \Rightarrow G$ is cyclic.

Ques $G = \{1,2,3,4,5,6\}$ $\times_7$ is cyclic & find its generators?

$G = \{1,2,3,4,5,6\}$

~~$1^1 = 1$~~

~~$1^2 = 1 \otimes_7 1 = 1$~~

~~$1^3 = 1$~~

$2^1 = 2$

$2^2 = 2 \otimes_7 2 = 4$

$2^3 = 2 \otimes_7 2 \otimes_7 2 = 1$

$2^4 = 2 \otimes_7 2 \otimes_7 2 \otimes_7 2 = 2$

$2^6 = 2 \otimes_7 2 \otimes_7 2 \otimes_7 2 \otimes_7 2 \otimes_7 2 =$

Date :

$3^1 = 3$, $3^2 = 3 \otimes_7 3 = 2$, $3^3 = 3 \otimes_7 3 \otimes_7 3 = 6$

$3^4 = 3 \otimes_7 3 \otimes_7 3 \otimes_7 3 = 4$, $3^5 = 3 \otimes_7 3 \otimes_7 3 \otimes_7 3 \otimes_7 3 = 5$

$3^6 = 3 \otimes_7 3 \otimes_7 3 \otimes_7 3 \otimes_7 3 \otimes_7 3 = 1$

$G = \langle 3 \rangle \Rightarrow G$ is cyclic

~~$5^1 = 5$, $5^2 = 5 \otimes_7 5 = 4$, $5^3 = 5 \otimes_7 5 \otimes_7 5 = 6$~~

$5^4 = 5 \otimes_7 5 \otimes_7 5 \otimes_7 5 = 2$, $5^5 = 5 \otimes_7 5 \otimes_7 5 \otimes_7 5 \otimes_7 5 = 3$

$5^6 = 5 \otimes_7 5 \otimes_7 5 \otimes_7 5 \otimes_7 5 \otimes_7 5 = 1$

$G = \{5^1, 5^2, 5^3, 5^4, 5^5, 5^6\}$

$G = \langle 5 \rangle \Rightarrow G$ is cyclic

Properties of cyclic group :-

Theorem 1 :- Prove that every cyclic group is an abelian group.

Proof :- Let $G = \langle a \rangle$ be a cyclic group, generated by a. Then to show that G is an abelian group.

Let $x, y \in G$, then $\exists\ r, s \in I$ such that

$x = a^r$, $y = a^s$

Now, $xy = a^r \cdot a^s$

$= a^{r+s}$

$= a^{s+r}$ [$\because r, s \in I \Rightarrow r+s = s+r$]

$= a^s \cdot a^r$

$= y \cdot x$

$xy = yx \ \forall\ x, y \in G$

Hence G is an abelian group.

Theorem 2 :- If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof :- Let $G = \langle a \rangle$ be a cyclic group with generator a.

Let $x \in G$ then $x = a^r$ [$r \in I$]

Now, $x = a^r = (a^{-1})^{-r}$ [$r \in I, -r \in I$]

$x = (a^{-1})^{-r}$

$\therefore$ every element of G is generated by a^{-1}.

Thus a^{-1} is also generator of group G.

Page No.
Date :

Note : ① Every subgroup of a cyclic group is also cyclic.

② Every group of prime order is cyclic.

Cosets

For multiplication :-

Let G be a group and H is a subgroup of G.

Let $a \in G$, then

$aH = \{ah : h \in H\}$ (left coset of H)

$Ha = \{ha : h \in H\}$ (right coset of H)

For addition :-

$a + H$ (left coset of H)

$H + a = \{h + a : h \in H\}$ (right coset of H)

Que If $G = \{1, -1, i, -i\}$ be a multiplicative group and $H = \{1, -1\}$ is a subgroup of G. Find all distinct left and right coset of H in G.

Soln $G = \{1, -1, i, -i\}$ & $H = \{1, -1\}$

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

$1H = \{1, -1\}$ (left coset of 1)

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

$= \{-1, 1\}$ (left coset of -1)

$H1 = \{1 \cdot 1, -1 \cdot 1\}$

$= \{1, -1\}$ (right coset of 1)

$H(-1) = \{1 \cdot (-1), -1 \cdot (-1)\}$

$= \{-1, 1\}$ (right coset of -1)

$iH = \{i, -i\}$, $Hi = \{i, -i\}$

$-iH = \{-i, i\}$, $H(-i) = \{-i, i\}$

Page No.
Date :

Note → ① If e is the identity of G then
$He = H = eH$

② If $R \in H$, then $\boxed{Hh = H = hH}$

③ The union of all left cosets or right cosets is equal to G.

④ Any two left or right cosets of H is either disjoint or identical.

⑤ $e \in H \Rightarrow ae \in Ha \Rightarrow \boxed{a \in Ha}$

Ques If G is a additive group of all integers and H is additive subgroup of all even integers of G, then find all the cosets of H in G.

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

$H = \{\ldots -4, -2, 0, 2, 4, 6, 8 \ldots\}$

$H+0 = \{\ldots -4, -2, 0, 2, 4, \ldots\} = H$

$H+1 = \{\ldots -3, -1, 1, 3, 5 \ldots\}$

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

$H+3 = \{\ldots -1, 1, 3, 5, 7 \ldots\} = H+1$

$H+4 = \{\ldots 0, 2, 4, 6 \ldots\} = H$

∴ Hence H & H+1 are two distinct cosets of H in G.

Theorem 1 :- If a and b are any two elements of a group G & H is a subgroup of G, then

(i) $Ha = Hb \Leftrightarrow ab^{-1} \in H$

(ii) $aH = bH \Leftrightarrow b^{-1}a \in H$

Proof :- (i) Let H is a subgroup of G such that

$Ha = Hb, \forall a, b \in G$

Then to prove that $ab^{-1} \in H$

since $a \in Ha$ and $a \in Hb$ (from ①)

$\Rightarrow ab^{-1} \in Hb^{-1}$ $[bb^{-1} = e]$

$\Rightarrow ab^{-1} \in He$ $[He = H]$

$\Rightarrow \boxed{ab^{-1} \in H}$

Page No.
Date :

Conversely, let H is a subgroup of G such that
$ab^{-1} \in H, \forall a, b \in G$
Then to show that $Ha = Hb$.
Now $ab^{-1} \in H$
$\Rightarrow Hab^{-1} = H$ $[a \in H \Rightarrow Ha = H]$
$\Rightarrow Hab^{-1}b = Hb$
$\Rightarrow Hae = Hb$
$\Rightarrow \boxed{Ha = Hb}$

(ii) Let H is a subgroup of G such that
$aH = bH, \forall a, b \in G$ — (1)
Then to prove that $b^{-1}a \in H$
since $a \in aH$ and $a \in bH$ (from (1))
$= b^{-1}a \in b^{-1}bH$
$= b^{-1}a \in eH$
$= \boxed{b^{-1}a \in H}$

Conversely, let H is a subgroup of G such that $b^{-1}a \in H, \forall a, b \in G$
Then to show that $aH = bH$.
Now, $b^{-1}a \in H$
$\Rightarrow Hb^{-1}a = H$
$= Hb^{-1}a = Hb$
$\Rightarrow bHb^{-1}a = bH$
$\Rightarrow Hbb^{-1}a = bH$
$\Rightarrow Ha = bH$
$\Rightarrow b^{-1}aH = H$
$\Rightarrow bb^{-1}aH = bH$
$\Rightarrow eaH = bH$
$\Rightarrow \boxed{aH = bH}$

Theorem :- Prove that any two right (left) cosets of a subgroup are either disjoint or identical.

Soln Let H is a subgroup of G and let Ha & Hb be any two right cosets of H in G.

Then to show that $Ha \cap Hb = \phi$ or $Ha = Hb$

Suppose $Ha \cap Hb \neq \phi$

Then ∃ at least one element c such that

$c \in Ha$ and $c \in Hb$

Let $c = h_1 a \in Ha$ & $c = h_2 b \in Hb$ (by right coset) where $h_1 \in H$ & $h_2 \in H$

$\therefore \boxed{h_1 a = h_2 b}$

$\Rightarrow h_1^{-1}(h_1 a) = h_1^{-1}(h_2 b)$ $[h_1 \in H \text{ & } h_1^{-1} \in H]$

$\Rightarrow ea = h_1^{-1} h_2 b$

$\Rightarrow a = (h_1^{-1} h_2) b$ $[h_1 \in H \text{ & } h_2 \in H \Rightarrow h_1^{-1} h_2 \in H]$

Now $Ha = H(h_1^{-1} h_2) b$

$= Hb$ $[h \in H \Rightarrow Hh = H]$ ↓ right coset of H.

$\Rightarrow \boxed{Ha = Hb}$

$\therefore Ha \cap Hb \neq \phi \Rightarrow \boxed{Ha = Hb}$

Lagrange Theorem

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

Proof :- Let G is a finite group of order n & H is subgroup of G of order m. $\therefore O(G) = n$ - (1)

Then to show that $O(H) = m$ - (2)

$O(H) \mid O(G)$ or n/m or $\frac{O(G)}{O(H)}$

Since $a_1 \in G$, then $Ha_1 = \{h_1 a_1, h_2 a_1, \ldots, h_m a_1\}$ be right coset of H in G having m distinct elements

because $h_i a = h_j a$

$= \boxed{h_i = h_j}$, $1 \leq i, j \leq m$

$= O(H) \neq m$ (which is not possible)

$\therefore O(Ha_1) = m$

Page No.
Date :

Therefore, each right coset of H in G have m distinct elements.

Now, suppose, there are k distinct cosets of H in G as

$Ha_1 = \{h_1a_1, h_2a_1, \ldots, h_ma_1\}$.

$Ha_2 = \{h_1a_2, h_2a_2, \ldots h_ma_2\}$.

$Ha_k = \{h_1a_k, h_2a_k \ldots, h_ma_k\}$

We know that the union of all cosets of all left or right cosets of H is equal to the group i.e.

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$$

$$\Rightarrow O(G) = O(Ha_1) + O(Ha_2) + \ldots + O(Ha_k)$$

$$\Rightarrow n = m + m + \ldots + m \ (k \text{ times})$$

$$\Rightarrow n = m \cdot k$$

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

$\Rightarrow O(H)$ is divisor of $O(G)$.

Application :-

Theorem :- Use lagrange theorem to show that any group of prime order can have no proper subgroup.

Proof :- Let $O(G) = P$, where P is prime and H be any subgroup of G.

Then to show that H is improper subgroup of G.

Let $O(H) = m$, then by Lagrange theorem.

$$O(H) \mid O(G)$$

$$\text{i.e. } \frac{O(G)}{O(H)} = \frac{P}{m}$$

Since P is prime number then

$$m = 1 \quad \text{or} \quad m = P$$

$$O(H) = 1 \quad \text{or} \quad O(H) = P = O(G)$$

$$\Rightarrow H = \{e\} \quad \text{or} \quad \boxed{H = G}$$

Improper subgroup.

Date :

Normal subgroup (special type of subgroup)

If left coset of H is a right coset of H. Then subgroup H is called normal subgroup.

Eg :- Let $G = \{1, -1, i, -i\}$ be any group & $H = \{1, -1\}$ is subgroup of G.

Then

$1H = \{1, -1\}$, $H1 = \{1, -1\} \Rightarrow \boxed{1H = H1}$

$-1H = \{-1, 1\}$, $H(-1) = \{-1, 1\} \Rightarrow \boxed{-1H = H(-1)}$

$iH = \{i, -i\}$, $Hi = \{i, -i\} \Rightarrow \boxed{iH = Hi}$

$(-i)H = \{-i, i\}$, $H(-i) = \{-i, i\} \Rightarrow \boxed{-iH = H(-i)}$

Hence H is normal subgroup of G.

⇒ Definition :- A subgroup H of a group G is said to be a normal subgroup if $\boxed{xhx^{-1} \in H, \forall x \in G \text{ \& } \forall h \in H}$

Note :- $\boxed{xHx^{-1} \subset H \ \forall \ x \in G \text{ \& } \forall h \in H}$

Theorem 1 :- Prove that every subgroup of an abelian group is normal.

Soln Let G be an abelian group & H be any subgroup of G.

Now, ~~xhx⁻¹~~ $x \in G$, $h \in H$

$\therefore xhx^{-1} = (xh)x^{-1}$ [G is an abelian group]

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

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

$= he$

$= h \in H$

$xhx^{-1} \in H \ \forall \ x \in G \ \forall h \in H$

$\therefore$ H is a normal subgroup of G.

Theorem :- Prove that the intersection of two normal subgroup of a group is a normal subgroup.

Soln Let H and K be two normal subgroup of a group G. Then to show that $H \cap K$ is also normal.

⇒ We know that the intersection of two subgroup is also a subgroup ⇒ $H \cap K$ is a subgroup of G.

Now, let $x \in G$, $h \in H \cap K$.

$\Rightarrow h \in H$ & $h \in K$

Now, since H is a normal subgroup.

then, $xhx^{-1} \in H \ \forall x \in G$ & $h \in H$

Since K is a normal subgroup then,

$xhx^{-1} \in K$, $\forall x \in G$ & $\forall h \in K$.

Now, $xhx^{-1} \in H$ & $xhx^{-1} \in K$

$\Rightarrow xhx^{-1} \in H \cap K \ \forall x \in G$ & $\forall h \in H \cap K$

Hence $H \cap K$ is a normal subgroup of G.

Theorem :- A subgroup H of a group G is normal iff $xHx^{-1} = H \ \forall x \in G$.

Sol: First suppose that H is normal subgroup of G.

Then to show that $xHx^{-1} = H \ \forall x \in G$

Since H is normal subgroup of G then

$xHx^{-1} \subset H, \forall x \in G$ — (1)

Also, $x \in G \Rightarrow \boxed{x^{-1} \in G}$

$\therefore$ from (1) $x^{-1}H(x^{-1})^{-1} \subset H$

$\Rightarrow x^{-1}Hx \subset H$

$= x(x^{-1}Hx)x^{-1} \subset xHx^{-1}$

$\Rightarrow (xx^{-1})H(xx^{-1}) \subset xHx^{-1}$

$= eHe \subset xHx^{-1}$

$= H \subset xHx^{-1}$ — (2) $\forall x \in G$

from (1) & (2)

$\boxed{xHx^{-1} = H} \ \forall x \in G$

Conversely, suppose $xHx^{-1} = H \ \forall x \in G$ then to show that H is a normal subgroup of G.

Since $xHx^{-1} = H \ \forall x \in G$

$\Rightarrow xHx^{-1} \subset H \ \forall x \in G$

$\therefore$ H is normal subgroup of G.

H is normal $\therefore$ $\boxed{xHx^{-1} = H \ \forall x \in G}$

Page No.
Date :

Theorem :- A subgroup H of a group G is normal iff left coset of H in G is a right coset of H in G.

Soln Let H is a normal subgroup of G then to show that $\boxed{xH = Hx}$ $\forall x \in G$.

Since H is normal, $xHx^{-1} = H \ \forall x \in G$

$\Rightarrow (xHx^{-1})x = Hx \ \forall x \in G$

$\Rightarrow xH(x^{-1}x) = Hx \ \forall x \in G$

$\Rightarrow xHe = Hx \ \forall x \in G$

$\Rightarrow xH = Hx \ \forall x \in G$

conversely, $\boxed{xH = Hx}$ $\forall x \in G$ then to show that H is a normal subgroup.

Now $xH = Hx$

$\Rightarrow (xH)(x^{-1}) = H(xx^{-1}) \ \forall x \in G$

$\Rightarrow xHx^{-1} = He \ \forall x \in G$

$\Rightarrow xHx^{-1} = H \ \forall x \in G$

$\therefore$ H is a normal subgroup of G.

Theorem :- A subgroup H of a group G is a normal subgroup if the product of two right cosets of H in G is again a right coset of H in G.

Proof :- Suppose H is a normal subgroup of G then to show that $(Ha)(Hb) = Hab$.

Now, $(Ha)(Hb) = H(aH)b$

$= HHab$ [since H is normal $aH = Ha$]

$= \boxed{Hab}$. [$\because HH = H$]

$\therefore \boxed{(Ha)(Hb) = Hab}$

* **Index :-** The number of distinct left or right coset of H in G.

Theorem :- If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G.

Proof :- Suppose H is a subgroup of index 2 in a group G, then the number of distinct right

(or left) cosets of H is 2.

Then to show that H is normal.

⇒ Let $x \in G$. Then either $x \in H$ or $x \notin H$.

If $x \in H$, then

$xH = H$ & $Hx = H$ $\forall x \in G$

$\Rightarrow xH = Hx$ $\forall x \in G$

$\Rightarrow$ H is normal subgroup of G.

⇒ If $x \notin H$, then suppose

He & Hx are two distinct right coset of H. (As index of H is 2).

$\therefore G = He \cup Hx = H \cup Hx$ — (1)

If eH & xH are two distinct left coset of H

$\therefore G = eH \cup xH = H \cup xH$ → (2)

from (1) & (2)

$\Rightarrow H \cup Hx = H \cup xH = G$

$\Rightarrow H \cup Hx = H \cup xH$ $\forall x \in G$

$\Rightarrow \boxed{Hx = xH}$ $\forall x \in G$

$\therefore$ H is a normal subgroup.

Permutation Group

Permutation :- Let $S = \{a_1, a_2, a_3 \ldots, a_n\}$ be a finite set with n elements.

Then a mapping $f : S \xrightarrow[\text{onto}]{\text{one-one}} S$

eg :- Let $S = \{a_1, a_2, a_3\}$

then $f = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix}$ ← Pre-image, ← Image

Note :- (1) If $S = \{a_1, a_2, \ldots a_n\}$ be a finite set with n elements then total number of Permutation on the set S is $n!$.

(2) The set of all permutation on the set S is denoted by S_n or P_n.

$S_n = \{f \mid f : S \xrightarrow[\text{onto}]{1-1} S\}$

Product of permutations
or
composition of permutations

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

and $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ & $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ be two permutation of S then

$$fog = fg = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

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

$$gof = gf = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

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

$\therefore fog \neq gof$

Permutation group or symmetric group

Let $S = \{a_1, a_2, \ldots a_n\}$ be a finite set of n elements. Then the set of all permutations

$S_n = \{f \mid f \text{ is a permutation on } S\}$

form a group w.r.t. composition of mapping. The group S_n is called symmetric group or permutation group of order $\lfloor n$. i.e. $\boxed{O(S_n) = \lfloor n}$

Equal permutation :- $fog = gof$

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

$\Rightarrow fog = gof \quad \forall a \in S$

$\Rightarrow f$ & g are equal permutation.

Page No
Date :

Identity Permutation :- Let $S = \{a_1, a_2, \ldots a_n\}$ then $I = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$ is called identity permutation on S.

Inverse of permutation :- If

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

then its inverse permutation is

$$f^{-1} = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

such that

$$f o f^{-1} = f f^{-1} = I$$

$$f^{-1} o f = f^{-1} f = I$$

Ques find the inverse of $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

Soln

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

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

$$AA^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = I$$

Ques How many time $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ be multiplied to itself to produce identity permutation I?

Soln Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$

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

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

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

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

= 3 times | ans

cyclic Permutation :- Let $S = \{a_1, a_2, a_3\}$ be a finite set then the permutation

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix} = (a_1\, a_2\, a_3)$$

is called cyclic permutation

ex :- $S = \{1, 2, 3, 4\}$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\,2\,3\,4) \rightarrow \text{cycle of length 4}$$

Note :- Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be a set

Then permutation $f = (1\ 3\ 4\ 2\ 6) \rightarrow$ cycle of length 5

$$f = \begin{pmatrix} 1 & 3 & 4 & 2 & 6 & 5 & 7 & 8 & 9 \\ 3 & 4 & 2 & 6 & 1 & 5 & 7 & 8 & 9 \end{pmatrix}$$

Transposition :- A cycle of length 2.

eg :- $f = (1, 2)$ & $g = (2, 4)$

Note :- ① Every permutation can be express as the product of cycle permutations.

② Every permutation can be express as the product of transposition.

eg :- $$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 6 & 7 & 8 & 5 \end{pmatrix}$$

$$= (1\,2\,3)\,(4)\,(5\,6\,7\,8)$$

$$= (1\,2)(1\,3)(5\,6)(5\,7)(5\,8) \text{ (into transposition)}$$

Page No.
Date :

Even permutation & odd permutation :-

→ even permutation can be expressed as the product of even number of transposition.

→ odd permutation can be expressed as the product of odd number of transposition.

eg :- $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix}$

$= (1\,7\,2\,3)(4\,8)(5)(6)$

$= (1\,7\,2\,3)(4\,8)$

$= (17)(12)(13)(48)$

= even permutation

Note :- ① $O(S_n) = \lfloor n$

② for $n \neq 2$, the group S_n is abelian, for $n \geq 3$, the group S_n is not abelian.

③ If S_n is a permutation group on n symbols of order $\lfloor n$. Then there are exactly $\frac{\lfloor n}{2}$ even permutation & $\frac{\lfloor n}{2}$ odd permutation.

* Alternating Group :-

Let $A_n = \{ f : f$ is an even permutation$\}$.

Then $O(A_n) = \frac{\lfloor n}{2}$

The set A_n of all even permutation form a group under the composition of permutation is called alternating group of order $\frac{\lfloor n}{2}$.

Ques Let $A = \{1,2,3,4,5\}$

find $(1\,3) \circ (2\,4\,5) \circ (2\,3)$.

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

$(2\,3)$

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

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

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

$$= (1\ 2\ 4\ 5\ 3)$$

Ques find the elements and multiplication table of symmetric group S_3.

soln $O(S_3) = \underline{L3} = 6$

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

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

$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

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

composition table.

Product of Permutation	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

Group Homomorphisms

Homomorphism :- Let $(G, *)$ and (G', o) be any two groups. A mapping f from G to G' i.e. $f : G \to G'$ is called a homomorphism of G to G' if $\boxed{f(a*b) = f(a) \circ f(b) \ \forall\ a, b \in G}$
($*$: G oper^n, $\circ$: G' oper^n)

\# **Homomorphism onto :-** If $f : G \to G'$ is a onto mapping such that $\boxed{f(a*b) = f(a) \circ f(b)}\ \forall\ a, b \in G$ then f is called homomorphism ~~from~~ G onto G'.

\# **Homomorphism into :-** If $f : G \to G'$ is a into mapping such that $\boxed{f(a*b) = f(a) \circ f(b)\ \forall\ a, b \in G}$ then f is called homomorphism G into G'.

Note :- (1) If $(G, +)$ & $(G', +)$ be any two groups. then
$f(a+b) = f(a) + f(b)\ \forall\ a, b \in G$

(2) If $(G, +)$ & $(G', \cdot)$ be any two groups then
$f(a+b) = f(a) \cdot f(b)\ \forall\ a, b \in G$.

example :- Let G be a group of all real numbers under addition & let G' be the group of non-zero real numbers under multiplication and $f : G \to G'$ defined by
$f(a) = 2^a\ \forall\ a \in G$.

Soln Let $a, b \in G$. Then $\left.\begin{matrix} f(a) = 2^a \\ f(b) = 2^b \end{matrix}\right\} \to (1)$

Now, $f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$
$\Rightarrow f(a+b) = f(a) \cdot f(b)$
Hence proved.
Hence f is Homomorphism.

example :- Let G be a group of integers under addition & $G' = G$ and let $f(x) = 3x\ \forall\ x \in G$.

Page No.
Date :

Soln Let $x+y \in G$ Then $f(x) = 3x$
$f(y) = 3y$

$f(x+y) = 3(x+y) = 3x+3y = f(x)+f(y)$
$f(x+y) = f(x)+f(y)$
f is Homomorphism

Ques If for a group G
$f: G \to G$ is given by $f(x) = x^2 \ \forall x \in G$ is a homomorphism, Prove that G is abelian.

Soln Let $x, y \in G$ then $f(x) = x^2$
$f(y) = y^2$ — (1)

f is homomorphism (given)
$f(xy) = (xy)^2$
$= (xy)(xy)$ [$\because f(ab) = f(a) \cdot f(b)$]
$f(x) \cdot f(y) = (xy)(xy)$
$x^2 \cdot y^2 = (xy)(xy)$
$x^2 \cdot y^2 = (xy)(xy)$
$(xx) \cdot (yy) = x(yx)y$
$x(xy)y = x(yx)y$ (by left and right cancellation law)
$\boxed{xy = yx} \ \forall x, y \in G$
$\Rightarrow G$ is an abelian group.

Properties :-

Theorem :- Let f be a homomorphic mapping of a group G into a group G'. Then we have the following important properties :-

(i) The f-image of the identity e of G is the identity of G' i.e. $f(e)$ is the identity of G'.
Or Prove $\boxed{f(e) = e'}$

(ii) The f-image of the inverse of an element a of G is the inverse of the f-image of a i.e.
Or prove $f(a^{-1}) = [f(a)]^{-1}$

(iii) The order of the f-image of an element is the same as the order of the element.

Page No
Date :

Sol^n (i) Let e' be the identity of G & G' respectively.

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

and $e' \cdot f(a) = f(a)$

$= f(ae)$ $(ae = a)$

$= f(a)f(e)$ (f is homomorphism)

$e' \cdot f(a) = f(e) f(a)$ (right cancellation)

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

(ii) If e is the identity of G then $\boxed{f(e) = e'}$ is the identity of G'. If a^{-1} is the inverse of a in G, then

$aa^{-1} = e = a^{-1}a$ — (1)

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

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

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

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

$ab = e$
$b^{-1} = a$
$a^{-1} = b$

$aa^{-1} = e$

$\Rightarrow f(aa^{-1}) = f(e)$

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

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

(iii) Let e be identity of G, then $f(e) = e'$ be the identity of G'.

Let $O(a) = n$ & $n[f(a)] = m$

Then to show that $\boxed{n = m}$

Note :- (i) If $O(a) = n \Rightarrow a^n = e$ and n is least +ve integer

(ii) If $a^m = e \Rightarrow O(a) \leq m$.

Now, $O(a) = n$

$a^n = e$

$\Rightarrow a \cdot a \cdot a \ldots n$ time $= e$

Page No.
Date :

$\Rightarrow f(a \ldots n \text{ times}) = f(e)$

$\Rightarrow f(a) \cdot f(a) \ldots n \text{ times} = e'$

$\Rightarrow [f(a)]^n = e'$

$\Rightarrow o[f(a)] \leq n$

$\Rightarrow \boxed{m \leq n} \quad -(1)$

Also, $o[f(a)] = m$

$\Rightarrow [f(a)]^m = e'$

$\Rightarrow f(a) \cdot f(a) \ldots m \text{ times} = f(e)$

$\Rightarrow f(a \cdot a \ldots m \text{ times}) = f(e)$

$\Rightarrow a^m = e$

$\Rightarrow o(a) \leq m$

$\Rightarrow \boxed{n \leq m} \quad -(2)$

from (1) & (2)

$\boxed{n = m}$

$\therefore \boxed{o(a) = o[f(a)]}$

Date.....

Rings :- A set S under two operations addition & ~~multi~~ multiplication is said to be a ring iff it satisfies the following properties :-

$(S, +, \cdot)$

A1) $a, b \in S \Rightarrow a+b \in S$

A2) $(a+b)+c = a+(b+c)$ $\forall$ $a, b, c \in S$

A3) $\exists$ $0 \in S$ such that $a+0 = 0+a = a$ $\forall a \in S$

A4) $\forall a \in S$ $\exists$ $(-a) \in S$ such that $a+(-a) = (-a)+a = 0$

A5) $a+b = b+a$ $\forall$ $a, b \in S$

M1) $a, b \in S \Rightarrow a.b \in S$

M2) $(a.b).c = a.(b.c)$ $\forall$ $a, b, c \in S$

D1) $a.(b+c) = a.b + a.c$ $\forall$ $a, b, c \in S$

D2) $(a+b).c = a.c + b.c$ $\forall$ $a, b, c \in S$

Field :-

M3) $\exists$ $1 \in S$ such that $a.1 = 1.a = a$ $\forall a \in S$

M4) $\forall a \in S$ $(a \neq 0)$

$\exists$ $a^{-1} \in S$

such that $a.a^{-1} = a^{-1}a = 1$

M5) $a*b = b*a$ $\forall$ $a, b \in S$

Ques $(Z, +, \cdot)$

It is a ring

M4) is not satisfied

$\therefore$ it is not a field

$(1/2) \notin Z$

Ques $(R, +, \cdot)$

It is ring as well as field

Ques $(C, +, \cdot)$

It is ring as well as field

Date.....

Ques $(Q, +, \cdot)$

It is ring as well as field

Ques $(Z_5, \oplus_5, \odot_5)$

Cayley Table

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

It is a field

Ques $(Z_6, \oplus_6, \odot_6)$

Cayley Table

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

It is not a field (MH) $\not\in (Z_6, \otimes_6)$

Note:- Z_p $p \to$ prime $(Z_p, \oplus_p, \odot_p)$ always forms a field.

Spiral