Date / /
Page
MY BEST BOOK

Unit-2

Permutation Groups & isomorphisms

Important Questions for pass Aspirants

(5) State and prove Fermats little theorem

(1) cayley's theorem

(2) Lagranges theorem

(3) ST Set of even permutations in S_n forms a subgroup of S_n

(4) State and prove orbit stabilizer Theorem

Remaining important Questions

(1) PT a group of prime order is cyclic

(2) Define cosets and their properties

(3) Find cosets of Subgroup 4Z of Z
Z is is group of integers

(4) prove that order of Subgroup divides order of G and PT $a^{|G|} = e$
add to Lagrange

(5) PT for $n > 1$ Alternating group A_n has order $\frac{n!}{2}$

(6) Let $\alpha, \beta \in S_6$ and $\alpha = (1\ 2\ 4\ 5\ 3\ 6)$
$\beta = (1\ 4\ 3\ 2\ 5\ 6)$ ⇒ find $\alpha, \beta, \alpha\beta^{-1}, \alpha^2$

(7) Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}$
find $\alpha^{-1}, \beta\alpha, \alpha\beta$

(8) if $\sigma \in S_6$ ⇒ $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{bmatrix}$ ⇒ find σ^{2014}

Permutation:-

A set A defined as function $f: A \to A$ which is both one-to-one and onto is called permutation.

one to one & onto is also called bijections.

$$f = \begin{bmatrix} a_1 & a_2 & a_3 \dots a_i \dots a_n \\ a_{i_1} & a_{i_2} & a_{i_3} \dots a_{i_j} \dots a_{i_n} \end{bmatrix}$$

$f: A \to A$

f is permutation with.

$$f(a_j) = a_{ij} \quad \text{for } j = 1, 2, \dots n$$

where,

$i_1, i_2, \dots i_n$ is a permutation of $\{1, 2, 3, \dots n\}$

Q56. **State and prove Lagrange's theorem on groups.** (MGU) July/Aug.-22, Q10

OR

State the prove Lagrange's theorem for groups. (OU) Jan.-21, Q11

OR

State and prove Lagrange's theorem.

[(OU) Sep./Oct.-21, Q16 | (KU) PP-1, Q10(a) | (KU) May/June-18, Q3(b) | (OU) May/June-18, Q10(a)(i) | (OU) May/June-19, Q3]

Answer :

Statement

If 'G' is a finite group and 'H' is a subgroup of 'G', then $|H|$ divides $|G|$.

Proof

Let, 'G' be a finite group and 'H' be the subgroup of G.

– 1, 0, 1, 2, 3, 4, ...}
nt in G

– 12, – 8, – 4, 0, 4, 8,

ht coset of H in G
[$\because$ G is abelian]
where $a \in G$
8, – 4, 0, 4, 8, 12, 16,

7, – 3, 1, 5, 9, 13, 17,

6, – 2, 2, 6, 10, 14,

– 1, 3, 7, 11, 15, 19,

4, – 0, 4, 8, 12, 16,

1, 5, 9, 13, ...}
2, 6, 10, 14, 18, ...}

..... = 0 + H
..... = 1 + H
..... = 2 + H
..... = 3 + H
are disjoint sets
ment between them
$+ H) \cup (3 + H) = G$
$H) \cup (1 + H) \cup (2 +$

ge's theorem on
(OU) July/Aug.-22, Q10

ge's theorem for
(OU) Jan.-21, Q11

ge's theorem.
16 | (KU) PP-1, Q10(a) |
May/June-18, Q10(a)(i) |
(OU) May/June-19, Q3]

Let the order of G and H be 'n' and 'm' respectively

$\Rightarrow$ $|G| = n$

$\Rightarrow$ $|H| = m$

Let, $a_1H, a_2H, \ldots a_kH$ be distinct left cosets of H in G, then,

For $a \in G$, $aH = a_iH$ for some i and from properties of cosets, $a \in aH$

$\therefore$ Each member of G belongs to one of the cosets a_iH

i.e., $a_1H \cup a_2H \cup \ldots \cup a_kH = G$

Applying modulus on both sides,

$$|a_1H \cup a_2H \cup \ldots \cup a_kH| = |G|$$

$$\Rightarrow |a_1H| + |a_2H| + \ldots + |a_kH| = |G| \quad \ldots(1)$$

From the properties of cosets,

$$|aH| = |H| = m \text{ for each } a \in G$$

Substituting the corresponding values in equation (1),

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

$$\Rightarrow mk = n$$

$$\Rightarrow k = \frac{n}{m} \text{ (an integer)} \quad \ldots(2)$$

It can be seen from equation (2) that m divides n.

$\therefore$ $|H|$ divides $|G|$.

Q57. Prove that a group of prime order is cyclic. **[(OU) Sep./Oct.-21, Q6 | (OU) Jan.-21, Q12]**

OR

Show that every group of prime order is cyclic. **(OU) May/June-18, Q10(a)(ii)**

OR

State Lagrange's theorem in groups. Using Lagrange's theorem prove that every group of prime order is cyclic.

Answer : **[March/April-16, Q10(a) | Oct.-12, Q10(a)]**

Statement

If 'H' is a subgroup of a finite group 'G', then the order of H divides the order of G. i.e., $|H|$ divides $|G|$.

Proof

Let 'G' the group and prime number 'p' is the order of the group.

i.e., $|G|$

Since

Thus element $a \in G$ such that $a \neq e$.

The

Let the order of G and H be 'n' and 'm' respectively

$\Rightarrow \quad |G| = n$

$\Rightarrow \quad |H| = m$

Let, $a_1H, a_2H, \ldots\ldots a_kH$ be distinct left cosets of H in G, then,

For $a \in G$, $aH = a_iH$ for some i and from properties of cosets, $a \in aH$

$\therefore$ Each member of G belongs to one of the cosets a_iH

i.e., $a_1H \cup a_2H \cup \ldots\ldots \cup a_kH = G$

Applying modulus on both sides,

$$|a_1H \cup a_2H \cup \ldots\ldots \cup a_kH| = |G|$$

$$\Rightarrow \quad |a_1H| + |a_2H| + \ldots. + |a_kH| = |G| \qquad \ldots (1)$$

From the properties of cosets,

$$|aH| = |H| = m \text{ for each } a \in G$$

Substituting the corresponding values in equation (1),

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

$$\Rightarrow \quad mk = n$$

$$\Rightarrow \quad k = \frac{n}{m} \text{ (an integer)} \qquad \ldots (2)$$

It can be seen from equation (2) that m divides n.

$\therefore$ $|H|$ divides $|G|$.

OFF Prove that a group of prime order is

Q27. In a finite group, the order of each element of the group divides the order of the group.

Answer :

Let G be a finite group and the orders of G is n

i.e., $|G| = n$

Let $a \in G$

and the order of an element $a \neq e \in G$

$|a| = m$ then

$|H| = < a >$ is a subgroup of G

and $|H| = m$

$\Rightarrow$ $|H|$ divides $|G|$

$\therefore$ $|a|$ divides $|G|$

29. Suppose G is a finite group and let $a \in G$. Then prove that $a^{|G|} = e$.

Answer : **(OU) June/July-22, Q6**

Let, 'G' be a finite group and 'H' be the subgroup of G.

Let the order of G and H be 'n' and 'm' respectively.

$\Rightarrow \quad |G| = n$

$\Rightarrow \quad |H| = m$

If $a_1 H, a_2 H, \ldots\ldots a_k H$ are distinct left cosets of H in G, then

$$a_1 H \cup a_2 H \cup \ldots\ldots \cup a_k H = G$$

Applying modulus on both sides,

$$|a_1 H \cup a_2 H \cup \ldots\ldots \cup a_k H| = |G|$$

$$\Rightarrow \quad |a_1 H| + |a_2 H| + \ldots\ldots + |a_k H| = |G| \qquad \ldots (1)$$

From the properties of cosets,

$$|aH| = |H| = m$$

Substituting the corresponding values in equation (1),

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

$$\Rightarrow \quad mk = n$$

$$\Rightarrow \quad k = \frac{n}{m} \qquad \ldots (2)$$

It can be seen from equation (2) that m divides n.

$\therefore \quad |H|$ divides $|G|$.

Now, $|G| = |a|\, k$ for some positive integer k.

Thus, $a^{|G|} = a^{|a|k} = e^k = e$

$\therefore \quad a^{|G|} = e$

State and prove Cayley's Theorem

(or)

Define group isomorphism and ST every group is isomorphics to a group of permutations.

Group 'Isomorphism' :-

An isomorphism ϕ from a group G to a group $\bar{G}$ is a one-one and onto mapping from G to $\bar{G}$ that preserves all group operations

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

Cayleys Theorem Statement

Every finite group G is isomorphic to a permutation group

proof :-

Isomorphism లో ϕ function ab అనేటప్పుడు axb లాగా వస్తుంది

so ⇒ proof లో

G లోని a, x లను తీసుకొని

ఇక్కడ function $f_a : G \to G$

$f_a(x) = ax$ $\forall x \in G$ అవుతుంది

↙ ↓ ↘

Permutation group ϕ is Isomorphism

prove చేయాలి now,

Proof

Let 'G' be a finite group

If $a \in G$ then for every $x \in G$, there exists a product $ax \in G$.

Consider,

A function $f_a : G \to G$ defined as

$$f_a(x) = ax \; \forall \; x \in G$$

f_a is One-One

$x, y \in G$

$\Rightarrow \quad f_a(x) = f_a(y)$

$\Rightarrow \quad ax = ay$

$\Rightarrow \quad x = y$

$\therefore \quad f_a$ is one-one

f_a is Onto

If $x \in G$, then there exists $a^{-1} x \in G$ such that

$$f_a(a^{-1}x) = a\,(a^{-1}x)$$
$$= (aa^{-1})x$$
$$= ex$$
$$= x \quad [\because e \text{ is an identity element}]$$

$\Rightarrow \quad f_a\,(a^{-1}x) = x$

$\therefore \quad f_a$ is onto

As f_a is one-one and onto,

f_a is a permutation on G.

Let,

$$G' = \{f_a : a \in G\}$$

To prove G' is a group with respect to product of two functions.

Closure

$a, b \in G$

Let, $f_a, f_b \in G'$

$\Rightarrow \quad (f_a\, f_b)\,(x) = f_a\,[f_b(x)]$
$= f_a(bx)$
$= a(bx)$
$= (ab)\,x$
$= f_{ab}\,(x)$

$\therefore \quad f_a f_b = f_{ab} \; \forall \; x \in G$

$f_{ab} \in G'$ since $ab \in G$

$\therefore \quad G'$ is closed under multiplication.

Associativity: $a, b, c \in G$

Let, $f_a, f_b, f_c \in G'$

$\Rightarrow \quad f_a(f_b f_c) = f_a\, f_{bc}$
$= f_{a(bc)}$
$= f_{(ab)c}$
$= f_{ab}\, f_c$
$= (f_a f_b)\, f_c$

$\therefore \quad f_a(f_b f_c) = (f_a \cdot f_b)\, f_c$

$\therefore \quad G'$ is associative.

Existence of Identity: The identity element, $e \in G$

$\Rightarrow \quad f_e \in G'$

$\therefore \quad f_e f_a = f_{ea}$

$= f_a$

$f_a f_e = f_{ae}$

$= f_a$

$\therefore \quad f_e$ is the identity element in G'

Existence of Inverse: As $a \in G$

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

$\therefore \quad f_{a^{-1}} f_a = f_{a^{-1}a} = f_e$

$f_a f_{a^{-1}} = f_{aa^{-1}} = f_e$

$\therefore \quad f_{a^{-1}}$ is the inverse of f_a in G.

$\therefore \quad G'$ is a group

Consider,

A function $\phi : G \to G'$ defined as,

$\phi(a) = f_a \; \forall \; a \in G$

ϕ is One-one

$a, b \in G$

$\Rightarrow \quad \phi(a) = \phi(b)$

$\Rightarrow \quad f_a = f_b$

$\Rightarrow \quad f_a(x) = f_b(x)$

$\Rightarrow \quad ax = bx$

$\Rightarrow \quad a = b$

$\therefore \quad \phi$ is one-one

ϕ is Onto

$f_a \in G'$

For $a \in G$

$f(a) = f_a$

$\therefore \quad \phi$ is onto

ϕ is a Homormophism

If $a, b \in G$

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

$\Rightarrow \quad ab \in G$

Then, $\phi(ab) = f_{ab}$

$= f_a f_b$

$= \phi(a)\phi(b)$

$\therefore \quad \phi$ is homomorphism

Since, ϕ is one-one, onto and homomorphism, is an isomorphism from $G \to G'$.

$\therefore \quad G \cong G'$.

State and prove fermat's little theorem.

Statement:-

For every integer a and every prime p

$$a^p = a \bmod p$$

Proof:-

Let a be an integer and p be prime

Now,

By division algorithm

i.e

there are integers m and r which $a = pm + r \quad 0 \le r < p$

$\Rightarrow a \equiv r \bmod p \quad -(1)$

r is remainder

where $r = 0$, the result obtained is trival i.e both sides zero.

when $r \neq 0$

$r \in U(p)$

where $U(p) = \{1, 2, 3, \ldots p-1\}$ is a finite group under multiplication modulo p

The order of $U(p) = |U(p)| = p-1$

$$r^{|U(p)|} = r^{p-1}$$

or

if G is any finite group with $a \in G$ then

$$a^{|G|} = e$$

$$r^{|u(p)|} = 1$$

$$r^{p-1} = 1.$$

$$r^{p-1} = 1 \bmod p$$

$$\frac{r^p}{r} = 1 \bmod p$$

$$r^p = r \bmod p$$

if r is replaced by a then

$$a^p = a \bmod p$$

Tip/Hint

Ex:- modulo operation = X_6 then 6 divisions లో remainder రాబట్టడం

$12 X_6 = 0$

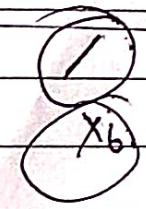
$13 X_6 = \frac{13}{6} = 1$

$15 X_6 = \frac{15}{6} = 3$

$16 X_6 = \frac{16}{6} = 4$

$18 X_6 = \frac{18}{6} = 0$

వచ్చిన group under X_6 లో మొదటిది మొత్తం group కి element & X_6 ని operate చేస్తే రావాల్సిన



ఇలా Step చేసినా వచ్చే remainders లో X_6 మొదట వచ్చిన get same

i.e

$1 X_6 = 1$

$3 X_6 = 3$

$4 X_6 = 4$

$0 X_6 = 0$

State and prove Orbit-Stabilizer theorem.

Answer :

Statement

Let G be a finite group of permutations of a set S. Then for any i from S,

$$|G| = |\text{Orb}_G(i)|\,|\text{Stab}_G(i)|$$

Proof

Let G be a finite group of permutations of a set S.

Let H represents the stabilizer of i in G

$$\Rightarrow \quad \text{Stab}_G(i) = H \qquad \ldots (1)$$

Let K represents the orbit of i under G

$$\Rightarrow \quad \text{Orb}_G(i) = K \qquad \ldots (2)$$

$\text{Stab}_G(i)$ is a subgroup of G as it satisfies the properties of a subgroup.

$\Rightarrow$ H is a subgroup of G

According to Lagrange's theorem,

$\frac{|G|}{|H|}$ represents the number of distinct left cosets of H in G.

There exists one-one correspondence between left cosets of H and the elements of K

$$\Rightarrow \quad \frac{|G|}{|H|} = K \qquad \ldots (3)$$

Let, a function T given as

$$T : \{\alpha H : \alpha \in G\} \rightarrow \{\phi(i) : \phi \in G\}$$

$$[\because T(\alpha H) = \phi(i)]$$

'T' is said to be one-one correspondence if it satisfies the following conditions

(i) 'T' is well defined

(ii) 'T' is one-one

(iii) 'T' is onto

(i) Let, the group G has permutations α and β

Let, $\alpha H = \beta H$

$\Rightarrow \quad \alpha^{-1}\beta \in H$

[$\because$ Using the properties of cosets]

$\Rightarrow \quad \alpha^{-1}\beta(i) = i$

$\Rightarrow \quad \alpha\alpha^{-1}\beta(i) = \alpha(i)$

$\Rightarrow \quad e\beta(i) = \alpha(i)$ [$\because \alpha\alpha^{-1} = e$]

$\Rightarrow \quad \beta(i) = \alpha(i)$ [$\because e = 1$]

$\Rightarrow \quad T(\beta H) = T(\alpha H)$

(or)

$\Rightarrow \quad T(\alpha H) = T(\beta H)$

$\Rightarrow$ If $\alpha H = \beta H$, then $T(\alpha H) = T(\beta H)$ ... (4)

$\therefore$ T is well defined.

(ii) Consider,

$T(\alpha H) = T(\beta H)$

$\Rightarrow \quad \alpha(i) = \beta(i)$

$\Rightarrow \quad \alpha^{-1}\alpha(i) = \alpha^{-1}\beta(i)$

$\Rightarrow \quad ei = \alpha^{-1}\beta(i)$

$\Rightarrow \quad i = \alpha^{-1}\beta(i)$ for each i in S

$\Rightarrow \quad \alpha^{-1}\beta \in H$

$\Rightarrow \quad \alpha H = \beta H$ ... (5)

[$\because$ From properties of cosets]

$\therefore$ T is one-one function.

(iii) Let, j be an element of K.

If $j \in K$, then

$j = \alpha(i)$ for some $\alpha \in G$ and $i \in S$

$\Rightarrow \quad j = \alpha(i) = T(\alpha H)$

$\Rightarrow \quad j = T(\alpha H)$ ... (6)

$\therefore$ T is an onto function.

From equations (4), (5) and (6), T is a one-one correspondence between the left cosets of H and elements of K.

$\therefore \quad \frac{|G|}{|H|} = |K|$ [$\because$ From equation(3)]

$\Rightarrow \quad |G| = |H|\,|K|$ ... (7)

Substituting equations (1) and (2) in equation (7),

$= |\text{Orb}_G(i)|\,|\text{Stab}_G(i)|$

$\therefore \quad |G| = |\text{Orb}_G(i)|\,|\text{Stab}_G(i)|$.

Q41. Show that the set of even permutations in S_n forms a subgroup of S_n.

Answer : **(KU) July/Aug.-21, Q3**

Let, A_n be the set of even permutations in S_n.

and α, β be any two elements in A_n i.e., $\alpha, \beta \in A_n$.

From, two-step subgroup test,

Let G be a group and H be a non-empty subset of *if* G, $ab \in H \; \forall \; a, b \in H$ and $a^{-1} \in H \; \forall \; a \in H$, then H is a subgroup of G.

From the definition of Even permutations,

α is expressed as product of an even number of 2-cycles.

and β is also expressed as product of an even number of 2-cycles.

$\Rightarrow$ $\alpha\beta$ is also a product of even numbers of 2-cycles.

$\Rightarrow$ $\alpha\beta \in A_n$ ... (1)

[even x even = even]

Since,

$$(a_i a_j)^2 = e$$

$\Rightarrow$ $(a_i a_j)^{-1} = (a_i a_j)$

[$a^r = e \Rightarrow aa = e$

$\bar{a}^1 aa = e\bar{a}^1$

$a = \bar{a}^1$]

i.e., inverse of product of an even number of 2-cycles is also a product of an even number of 2-cycles.

Then α^{-1} is also a product of an even number of 2-cycles.

$\Rightarrow$ $\alpha^{-1} \in A_n$ ... (2)

$\therefore$ From equations (1) and (2),

$$A_n \leq S_n$$

i.e., The set of even permutations in S_n forms a subgroup of S_n.

2 Step Subgroup Test :- H is SG if

(1) $a, b \in H \Rightarrow ab \in H$

(2) $a^{-1} \in H \quad \forall a \in H$

Date ___/___/___
Page ___
MY BEST BOOK

Set of even permutations of S_n forms a SG of S_n

ఎలా use చేస్తారు —

$\downarrow$

$(a_i a_j)^2 = e$ ⟶ Identity as product of even permutations

$(1\ 2)(2\ 1)$

$1 \to 2$, $2 \to 1$ ⇒ and on ! on !

(or)

$(1\ 2\ 3)(3\ 2\ 1)$

$(1\ 3)(1\ 2) \quad (3\ 1)(3\ 2)$

$(1)(2)(3)$

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

$\Rightarrow (a_i a_j)^2 = e$

$(a_i a_j)(a_i a_j) = e$

$(a_i a_j)^{-1}(a_i a_j)(a_i a_j) = e\,(a_i a_j)^{-1}$

$(a_i a_j) = (a_i a_j)^{-1}$

Date ___/___/___
Page ___
MY BEST BOOK

Remaining Questions.

Q5-1) prove that a group of prime order is cyclic.

A:- proof

Let "G" the group and prime number "p" is the order of the group.

i.e., $|G| = p$

since $p > 1$,

Thus, there is an element $a \in G$ such that $a \neq e$.

The cyclic subgroup $\langle a \rangle$ generated by 'a' is a subgroup of "G" and it has atleast two elements "a" and "e"

According to Lagrange's theorem. The order of $\langle a \rangle$ i.e. $|\langle a \rangle|$ divides the prime 'p' Let $|\langle a \rangle| = q$

But, 'p' is a prime number.

$\therefore q = 1$ or $q = p$

[$\because$ 1 and p are only divisors of p]

Since, $a \neq e$

$\Rightarrow |\langle a \rangle| \neq 1$

$\Rightarrow |\langle a \rangle| > 1$

if $q = 1 \Rightarrow |\langle a \rangle| = 1$

$\Rightarrow \langle a \rangle = \{a\}$

$a = e \Rightarrow$ q is not a group of prime order

Date / /
Page
MY BEST BOOK

$\Rightarrow |\langle a \rangle| = p$

$\Rightarrow \langle a \rangle = |G|$

$\Rightarrow \langle a \rangle = G$

$\Rightarrow \langle a \rangle$ is cyclic group and G is gr
of poime order.

Therefore, every group of poime
is cyclic.

(2) Define Cosets and mention the properties of Cosets

$\Rightarrow \quad h_1 = h_2$

$\Rightarrow \quad ah_1 = ah_2$

$\Rightarrow \quad f$ is one-one

Also,

$bh' \in bH$

$\Rightarrow \quad h' \in H$

$\Rightarrow \quad ah' \in aH$

$\Rightarrow \quad bh' = f(ah')$

$\Rightarrow \quad f$ is onto

$\Rightarrow \quad f: ah \to bh$ is one-one and onto

$\therefore \quad |aH| = |bH|$.

7. **aH is a subgroup of G, if and only if a $\in$ H.**

Let aH be the subgroup of G

$\Rightarrow \quad e \in aH \qquad [\because e \in G]$

Also $e \in eH$

$\Rightarrow \quad aH \cap eH \neq 0$

$\Rightarrow \quad aH = eH = H$

$\Rightarrow \quad aH = H \qquad [\because aH = H \Rightarrow a \in H]$

$\Rightarrow \quad a \in H$

Let, $a \in H$

$\Rightarrow \quad aH = H$

8. $\bigcup_{a \in G} aH = G$

Let,

$a_1H, a_2H, \ldots\ldots a_kH$ be the different left cosets of H in G.

For each $a \in G$,

$\Rightarrow \quad aH = a_iH$ where $1 \leq i \leq k$

$a \in aH$

Each $a \in G$ must belong to $a_iH_i \in a_iH_i$ for $1 \leq i \leq k$

$\therefore \quad a_1H \cup a_2H \cup \ldots\ldots \cup a_kH = G.$

(3) Define cosets and Find all cosets of subgroup 42 of Z {Z is group of integers}

Cosets ಗೆ ಇಲ್ಲಿ ಇರುವ definition ಅಂದರೆ

Cosets of Subgroup 42 of Z:

⇒ let G be additive group of integers

i.e., $G = \{\ldots\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\ldots\}$

0 is the identity element in G

$\therefore$ G is abelian.

Let H be the subset of G

$H = <4> = 4Z = \{\ldots\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\ldots\}$

$\Rightarrow$ $H \leq G$

The left coset of H in G = Right coset of H in G

[$\because$ G is abelian]

Cosets of H in G are $a + H$ where $a \in G$

$0 + H = \{\ldots\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\ldots\}$

$1 + H = \{\ldots\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\ldots\}$

$2 + H = \{\ldots\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\ldots\}$

$3 + H = \{\ldots\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\ldots\}$

$4 + H = \{\ldots\ldots, -12, -8, -4, -0, 4, 8, 12, 16, \ldots\ldots\}$

$5 + H = \{\ldots\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\ldots\}$

$6 + H = \{\ldots\ldots, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\ldots\}$

It can be observed that,

$4 + H = 8 + H = 12 + H = \ldots\ldots = 0 + H$

$5 + H = 9 + H = 13 + H = \ldots\ldots = 1 + H$

$6 + H = 10 + H = 14 + H = \ldots\ldots = 2 + H$

$7 + H = 11 + H = 15 + H = \ldots\ldots = 3 + H$

$0 + H, 1 + H, 2 + H, 3 + H$ are disjoint sets

i.e., there is no common element between them

And $(0 + H) \cup (1 + H) \cup (2 + H) \cup (3 + H) = G$

$\therefore$ The cosets are, $(0 + H) \cup (1 + H) \cup (2 + H) \cup (3 + H)$.

Q43. Define Alternating group of degree n. Also prove that A_n has order $\frac{n!}{2}$ if $n > 1$.

(OU) May/June-19, Q9(b)

OR

For $n > 1$, show that A_n has order $\frac{n!}{2}$.

(KU) PP-1, Q3

OR

For $n > 1$, show that the alternating group A_n has order $\frac{n!}{2}$.

Answer : (OU) June-18, Q2

Alternating Group

An alternating group on a set can be defined as a group of all even permutations of a finite set. For a set $\{1, 2, \ldots, n\}$, an alternating group on n letters is a group of order $\frac{n!}{2}$ and is designated by A_n.

Proof: Let, $S_n = \{e_1, e_2, \ldots e_m, o_1, o_2, \ldots o_n\}$ be the permutation group of order $n!$.

Here $e_1, e_2, \ldots e_m$ are even permutations

$o_1, o_2, \ldots o_n$ are odd permutations

$\therefore \quad |S_n| = n!$

Let t be a transposition in S_n since multiplication of permutations satisfies closure property,

$\{e_1, e_2, \ldots e_m), (o_1, o_2, \ldots o_n) \in S_n$

$\Rightarrow \quad (te_1, te_2, \ldots te_m, to_1, to_2, \ldots to_n) \in S_n$

Since t is an odd permutation,

$\Rightarrow \quad te_1, te_2, \ldots te_m$ are all odd

And, $to_1, to_2, \ldots to_n$ are all even,

Let $te_i = te_j$ for $i \leq m, j \leq m$

$e_i = e_j \qquad [\because$ Left cancellation law]

Since S_n is group, $e_i = e_j$ is absurd.

$\Rightarrow \quad te_i \neq te_j$

$\therefore$ The m permutations $te_1, te_2, \ldots te_m$ are all distinct in S_n.

and S_n has exactly n odd permutations.

$\therefore \quad m \leq n \qquad \ldots (1)$

Similarly, n permutations $to_1, to_2, \ldots to_n$ are all distinct in S_n and S_n has exactly m even permutations.

$\therefore \quad n \leq m \qquad \ldots (2)$

From equations (1) and (2),

$$m = n = \frac{n!}{2} \qquad [\because m + n = n!]$$

$\Rightarrow$ Number of even permutations = Number of odd permutations

$$= \frac{1}{2} n!$$

$\therefore$ There are equal number of even and odd permutations.

Let A_n be the alternating group of permutations having n degree.

Then, $|A_n| = \frac{n!}{2}$ $\quad [\because |S_n| = n!]$

$\therefore$ A_n has order $\frac{n!}{2}$

Q36. **Let $\alpha, \beta \in S_6$ and $\alpha = (1\ 2\ 4\ 5\ 3\ 6)$, $\beta = (1\ 4\ 3\ 2\ 5\ 6)$ then evaluate α, β, $\alpha\beta^{-1}$, α^2.**

Answer : **(OU) June-18, Q9(b)(ii)**

Given,

$$\alpha, \beta \in S_6$$

$$\alpha = (1\ 2\ 4\ 5\ 3\ 6)$$

$$\beta = (1\ 4\ 3\ 2\ 5\ 6)$$

i.e., $$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}$$

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

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

$$\therefore \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 6 & 1 & 2 \end{pmatrix}$$

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

$$\alpha\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$$\therefore \quad \alpha\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 2 & 4 & 3 \end{pmatrix}$$

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

$$\therefore \quad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix}$$

Q34. Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$ and

$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}$ then compute

(a) α^{-1} (b) $\beta\alpha$ (c) $\alpha\beta$

(MGU) July/Aug.-22, Q2

OR

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

$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{pmatrix}$ then compute α^{-1} and $\beta\alpha$.

(MGU) May/June-19, Q1

Answer :

Given permutations are,

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

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

(a) The value of α^{-1} can be obtained as,

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

(b) The value of $\beta\alpha$ can be obtained as,

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

$$\therefore \quad \beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 4 & 5 \end{bmatrix}$$

(c) The value of $\alpha\beta$ can be obtained as,

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

$$\therefore \quad \alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{bmatrix}$$

Q35. **If $\sigma \in S_6$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$ then find σ^{2014}.**

March/April-15, Q9(b)

Answer :

Given permutation is,

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

The value of σ^{2014} can be obtained as,

$\sigma^2 = \sigma.\sigma$

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

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

$$\therefore \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 2 & 1 \end{pmatrix}$$

$\sigma^3 = \sigma^2.\sigma$

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

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

$\sigma^4 = \sigma^3.\sigma$

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

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

$$\therefore \quad \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

$\sigma^5 = \sigma^4.\sigma$

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

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

$$\therefore \quad \sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 4 & 5 \end{pmatrix}$$

$\sigma^6 = \sigma^5.\sigma$

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

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

$\therefore \quad \sigma^6 = I$

Thus, σ^{2014} can be written as,

$\sigma^{2014} = \sigma^{2010}\ \sigma^4$

$= (\sigma^6)^{335}\ \sigma^4 = (I)^{335}\ \sigma^4 = I.\ \sigma^4 = \sigma^4$

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

$$\therefore \quad \sigma^{2014} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

1. **Permutation**

A permutation of a set 'A' is defined as a function $f: A \to A$ which is both one-to-one and onto.

2. **Transposition**

A cycle of length 2 known as transposition.

3. **Properties of Permutation**

(i) Every permutation of a finite set can be expressed as a cycle or a product of disjoint cycles.

(ii) Every permutation can be expressed as a product of transpositions.

(iii) Identity permutation is always even.

(iv) A permutation can be either even or odd but not both.

4. **Even permutation**

If a permutation is expressed as a product even number of transpositions, then it is called an even permutation.

5. **Odd Permutation**

If a permutation is expressed as a product of odd number of transpositions, then it is called an odd permutation.

6. **Group of Permutation**

A permutation group of a set A is defined as a set of permutations of A which form a group under composition function.

7. **Coset**

If H is a subgroup of $(G, *)$ and $a \in G$, then $aH = \{a * h : h \in H\}$ and $Ha = \{h * a : h \in H\}$ are called the cosets of H in G.

aH is the left coset and Ha is the right coset of H.

8. **Properties of Cosets**

Let a, b be the elements and H be the subgroup of G.

(i) $a \in aH$

(ii) $aH = H$ if and only if $a \in H$

(iii) $aH = bH$ if and only if $a \in bH$

(iv) $aH = bH$ or $aH \cap bH = \phi$

(v) $aH = bH$ if and only if $a - b \phi H$

(vi) $|aH| = |bH|$

(vii) aH is a subgroup of G if and only if $a \in H$.

(viii) $\bigcup_{a \in G} aH = G$

9. **Lagrange's Theorem**

It states that "if G is a finite group and H is a subgroup of G, then (H) divides $|G|$".

10. **Index of a Subgroup**

The number of distinct left or right cosets of subgroup H in G is called as index of a subgroup. It is denoted by $|G : H|$.

11. **Orbit-stabilizer Theorem**

If G is a finite group of permutations of a set s, then for any from s.

$$|G| = |\text{Orb}_G(i)| \, |\text{Stab}_G(i)|$$

Where,

$\text{Orb}_G(i)$ = Orbit of ; Under G

$\text{Stab}_G(i)$ = Stabilizer of i in G.

12. **Isomorphism**

The homomorphism $\phi : G \to \overline{G}$ is said to be isomorphism if it satisfies the condition.

$\ker \phi = \{e\}$ i.e., f is both one-one and onto.

13. **Properties of Isomorphism**

(i) $\phi^{-1} \overline{G} \to G$ is an isomorphism.

(ii) $G = < a >$ if and only if $\overline{G} = < \phi(a) >$

(iii) $|a| = |\phi(a)|$ for all $a \in G$

(iv) $G \approx G^*, G^* \approx G^{**} \Rightarrow G \approx G^{**}$

14. **Cayley's Theorem On Isomorphism**

It states that "Every group is isomorphic to some permutation group".

15. **Automorphism**

If G is a group, then the isomorphism of G onto itself is known as automorphism.