NATIONAL ACADEMY

DHARMAPURI

TRB MATHEMATICS

ALGEBRA

TEST BATCH – SATURDAY & SUNDAY

‘Material Available with Question papers’

CONTACT

82486 17507 , 70108 65319

Class: 3

Permutation Groups:

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

The set S(E) is the set of all permutations of the set E is a group.

S(E) is contains n! elements,

S(E) is denoted by s_n is called same times as **symmetric group** of degree n.

Let S_3 be the symmetric grou on 3symbols.Then $O(S_3)$ is 3! = 6 **(TRB-2012)**

Let $x_1,x_2,x_3 \ldots x_n$ be distinct elements of the set E, the symbol ($x_1,x_2,x_3,\ldots \quad x_r$)) be denote the permutation that sent $x_1 \rightarrow x_2, x_2 \rightarrow x_3 \quad x_r \rightarrow x_1$ther element of E fixed.This permutation called a **cycle** of length r

$(x_1,x_2,x_3,\ldots. \quad x_n)$, $(x_2,x_3,x_4,\ldots \quad x_n,x_1)$, ….. $(x_r,x_1,x_2,x_3\ldots.. \quad x_{n-1})$ …… all are same permutations

Example:

E = {1,2,3,4,5}

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

Inverse of a cycle

Inverse of a cycle is obtained by writing its elements in the reverse order.

Example:

The inverse of (1,3,5) is (5,3,1)

In S_n there are $\frac{1}{r}\frac{n!}{(n-r)!}$ distinct r cycles **(TRB 2017)**

If p is prime number, than there are (p-1)!+1 element in s_p satisfies $x^p = e$ **(TRB-2004)**

Disjoint cycle

Two cycles are said to be disjoint if they have no element in common.

Example:

(1,2,5) and (3,4) are disjoint cycle.

(1,3,5) and (2,3,4) are not disjoint cycle.

- Every permutation can be expressed as product of disjoint cycles.

Transposition

A cycle of lengh 2 is called a transposition. **(TRB-2004,2006)**

Any permutation of a finite set can be expressed as a product of transpositions.

Example:

1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$ = (1,6,2,5)(3,4) = (1,6)(1,2)(1,5)(3,4)
2. If b = (1 2 3 4 5 6 7) , then c^3 *is*

   (a) (1 3) (2 4) (b) (1 3) (c) (2 4) (c) (2 3)(3 1)
3. order of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ is

   (a) 3 (b) 4 (c) 5 (d) 6
4. Given permutation a = (1 2 3 4 5 6 7), then a^3 is

   (a) (1 3 5 7 2 4) (b) (1 4 7 3 6 2 5) (c) (1 7 6 5 4 3 2) (d) (1 2 3 4 5 6 7)
5. The inverse of a cycle of cycle (4 6 2 7 3)

   (a) (4 2 7 3 6) (b) (3 7 2 6 4) (c) (2 6 4 3 7) (d) (6 7 3 2 4)
6. order of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}$ in S_7 **(TRB-2005)**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = e \text{ . Order} = 4$$

Express the permutation of disjoint cycles

(a) (1,2,3)(4,5)(1,6,7,8,9)(1,5) = (1,2)(1,3)(4,5)(1,6)(1,7)(1,8)(1,9)(1,5)

(b) .(1,2)(1,2,3)(1,2) = (1,2)(1,2)(1,3)(1,2) = (1,2)(1,3)

Odd and Even permutation

- A permutation of a finite set is even or odd If can be expressed as the product of an even or odd numbers of transposition.
- A cycle $(x_1,x_2,x_3,\ldots\ x_m)$ of length m can be expressed as the product of (m-1) transposition.
- cycle is even if m is odd.
- cycle is odd if m is even.

- The identity permutation is an even
- The product of two even permutations is an even.
- The product of two odd permutations is an even.
- The product of an even and odd permutations is odd.
- Inverse of even permutation is even.
- Inverse of odd permutation is odd.
- The set of all even permutations A_n is a subgroup of S_n

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

An is called the **alternating group**

Example:

product of (1,2)(2,4)(3,6) is $\begin{pmatrix}1&2&3&4&5&6\\4&1&6&2&5&3\end{pmatrix}$

Example:

Determine which of the following an even permutation

(a). $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&4&5&1&6&7&9&8\end{pmatrix}$ is odd

(b). (1,2,3,4,5)(1,2,3) is even

copute $a^{-1}ba$ of the following

(c).If a = (1,3,5)(1,2) , b = (1,5,7,9)

a = (1,3,5,2)

$a^{-1}ba$= (2,5,3,1)(1,5,7,9)(1,3,5,2) = (2,7,9,3)

(d).If a = (5,7,9) , b = (1,2,3) copute $a^{-1}ba$

$a^{-1}ba$ = (9,7,5)(1,2,3)(5,7,9) = (1,2,3)

(e). The solution of the equation ax = b in s_3 where a =$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$,b = $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, **(TRB-2005)**

x =$a^{-1}b$ =$\begin{pmatrix}3&2&1\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$,

Lagrange Theorem

If G is a finite group and H is subgroup of G, than O(H) is a divisor of O(G)

That is, O(H) \O(G)

Example:

A group of order 8 can not have subgroup of order 3,5,6 or 7

Group must be of order 2 or 4

Example:

G = {1,-1,i,-i}, H ={1,-1,i} or {i,-i,1} are not a subgroúp of G [O(H)\O(G)]

Converse of Lagrange theorem need not true. H ={i ,-i }is not a subgroup of G but O(H)\O(G)

Coset

If H is a subgroup of G,a∈ $A, than\ Ha = \{ha \backslash h \in H\}. Ha\ is\ called\ a\ right\ coset\ of\ H\ in\ G.$

$aH = \{ah \backslash h \in H\}. aH\ is\ called\ a\ left\ coset\ of\ H\ in\ G.$

Example:

Z ={ … -2,-1,0,1,2,… } is a group under addition

Let H be a multiples of 5. H ={ …-10,-5,0,5,10,… } is a sub set of Z

Than, 0+H ={ …-10,-5,0,5,10,… }

1+H ={ …-9,-4,1,6,11… }

2+H ={ …-8,-3,2,7,12… }

3+H ={ …-7,-2,3,8,13… }

4+H ={ …-6,-1,4,9,14… } are distinct left coset of H in Z and their union is Z

- H is a right and left coset of H

  eH =H =He
- If H is an abelian ,than aH =Ha
- Any two left cosets (right cosets) of H in G are either Identical or have no element in common.
- There is one-one correspondence between any two right cosets of H in G

Index of H in G

The number of distinct left coset of H in G is called the Index of H in G

It is denoted by [G:H] or $I_G(H)$

$[G:H] = I_G(H) = \frac{O(G)}{O(H)}$

If G is a finite group and a∈ $G, than\ O(a) divides\ O(G)$ **(TRB-2006)**

that is, O(a)\O(G)

If G is afinite group of order n and a∈ G,than $a^n = e$ { $a^{O(G)} = e$ }

Euler function

$\varphi(n)$ is called Eular function which is number of element and relatively prime to n lessthan n

If n is prime number,Than $\varphi(n)$ = n-1

If n is positive integer and a is relative prime to n, than $a^{\varphi(n)} \equiv 1(\text{mod } n)$

Fermat theorem

If p is a prime number and 'a' is any integer, than $a^p \equiv a(\text{mod } p)$ or $a^{p-1} \equiv 1(\text{mod } p)$

Wilson's theorem

If p is a prime number, than 1+(p-1)! is divisible by p

If G is group of order pq, where p and q are prime numbers,than there is atmost one cyclic subgroup of order p.

Example:

If O(G) = 30,Than it has atleast **8** number of subgroup.

Number of divisor of 30 is 8 which are 1,2,3,5,6,10,15,30

Divisor formula $N = p^a q^b r^c \Rightarrow d(N) = (a+1)(b+1)(c+1)$

Example:

A cyclic group have a generator of order 15 ,than the cyclic group may have **8** number of generators.

O(G) = 15. Number of relatively prime to 15 is 8 { 1,2,4,7,8,11,13,14 }

$\varphi(n) = n(1-\frac{1}{p})\left(1-\frac{1}{q}\right)(1-\frac{1}{r})$ { $15 = 3\times 5$, since $n = p^x q^y r^z$

$= 15(1-\frac{1}{3})\left(1-\frac{1}{5}\right) = 8$

Example:

1. Find the remainder when 2^{16} is divisible by 17

   $2^{17-1} \equiv 1(\text{mod } 17)$

   $2^{16} \equiv 1(\text{mod } 17)$

2. Find the remainder when 2^{50} is divisible by 17

   $2^{40} \equiv 5(\text{mod } 17)$

3. Find the remainder when 3^{100} is divisible by 13

   $a^{p-1} \equiv 1(\text{mod } p) \Rightarrow 3^{13-1} \equiv 1(\text{mod } 13)$

   $3^{12} \equiv 1(\text{mod } 13) \Rightarrow (3^{12})^8 \equiv 1(mod 13)$

   $3^{96} \equiv 1(mod 13) \Rightarrow 3^{96} \times 3^4 \equiv 3^4(mod 13)$

   $3^{100} \equiv 81(mod 13) \Rightarrow 3^{100} \equiv 3(mod 13)$

4. Find the remainder when 2^{103} is divisible by 5

   $2^{103} \equiv 3(\text{mod } 5)$

5. Find the remainder when 5^{50} is divisible by 12

   $a^{\varphi(n)} \equiv 1(\text{mod } n)$ { $\varphi(n) = n(1-\frac{1}{p})\left(1-\frac{1}{q}\right)(1-\frac{1}{r}) = 12(1-\frac{1}{2})\left(1-\frac{1}{3}\right) = 4$

   $5^4 \equiv 1(\text{mod } 12)$

   $(5^4)^{12} \equiv 1(\text{mod } 12) \Rightarrow 5^{48} \equiv 1(\text{mod } 12)$

   $5^{48} \times 5^2 \equiv 25(\text{mod } 12) \Rightarrow 5^{50} \equiv 1(\text{mod } 12)$

Example:

1. Find the remainder when 2^{16} is divisible by 17

   $2^{17-1} \equiv 1(\text{mod } 17)$

   $2^{16} \equiv 1(\text{mod } 17)$

2. Find the remainder when 2^{50} is divisible by 17

   $2^{40} \equiv 5(\text{mod } 17)$

3. Find the remainder when 3^{100} is divisible by 13

   $a^{p-1} \equiv 1(\text{mod } p) \Rightarrow 3^{13-1} \equiv 1(\text{mod } 13)$

   $3^{12} \equiv 1(\text{mod } 13) \Rightarrow (3^{12})^8 \equiv 1(mod 13)$

   $3^{96} \equiv 1(mod 13) \Rightarrow 3^{96} \times 3^4 \equiv 3^4(mod 13)$

   $3^{100} \equiv 81(mod 13) \Rightarrow 3^{100} \equiv 3(mod 13)$

4. Find the remainder when 2^{103} is divisible by 5

   $2^{103} \equiv 3(\text{mod } 5)$