

Discrete Structures and Theory of Logic

Lecture-36

Dr. Dharmendra Kumar

(Associate Professor)

United College of Engineering and Research, Prayagraj

October 2, 2023

Lagrange's theorem

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

Proof: Let H be any subgroup of order m of a finite group G of order n .

Consider all the left cosets of H in G .

Let $H = \{h_1, h_2, h_3, \dots, h_m\}$. Then the left cosets of H i.e. aH also consists of m elements i.e. $aH = \{ah_i \mid 1 \leq i \leq m\}$.

Clearly, each cosets of H in G consists of m distinct elements. Since G is a finite group, therefore the number of distinct left cosets is also finite. Let this be k . Therefore,

$$km = n \Rightarrow m \text{ is a divisor of } n.$$

It is proved.

Exercise

1. Consider the group $G = \{1, 2, 3, 4, 5, 6\}$ under multiplication modulo 7.
 - 1.1 Find the multiplication table of G .
 - 1.2 Find $2^{-1}, 3^{-1}, 6^{-1}$.
 - 1.3 Find the orders and subgroups generated by 2 and 3.
 - 1.4 Is G cyclic?
- 2.
3. Let Z be the group of integers with binary operation $*$ defined by $a * b = a + b - 2$, for all $a, b \in Z$. Find the identity element of the group $(Z, *)$.

Exercise

1. What do you mean by cosets of a subgroup? Consider the group \mathbb{Z} of integers under addition and the subgroup $H = \{\dots, -12, -6, 0, 6, 12, \dots\}$ consisting of multiples of 6.
 - 1.1 Find the cosets of H in \mathbb{Z} .
 - 1.2 What is the index of H in \mathbb{Z} .
2. Prove or disprove that intersection of two normal subgroups of a group G is again a normal subgroup of G .

Exercise

1. Let $(A, *)$ be a monoid such that for every x in A , $x * x = e$, where e is the identity element. Show that $(A, *)$ is an abelian group.
2. Let H be a subgroup of a finite group G . Prove that order of H is a divisor of order of G .
3. Prove that every group of prime order is cyclic.

Permutation group

Permutation

Let A be a finite set. Then a function $f: A \rightarrow A$ is said to be a permutation of A if f is bijective.

Degree of permutation

The number of distinct elements in the finite set A is called the degree of the permutation.

Suppose $A = \{a_1, a_2, a_3, \dots, a_n\}$. Then the notation of permutation will be of the following type:-

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

Equality of two permutations

Let f and g be two permutations defined on the set A .

$$f = g \text{ iff } f(a) = g(a), \forall a \in A.$$

Example: $f = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, g = \begin{pmatrix} b & a & c \\ a & c & b \end{pmatrix}$

Clearly $f = g$ because image of each element is same.

Identity permutation

If each element of a permutation is replaced by itself, then it is called an identity permutation.

Example: Identity permutation defined on set $A = \{a,b,c\}$ is

$$I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$

Product of permutations or Composition of permutations

The product of two permutations f and g of same degree is denoted by fg or gf , meaning first perform f and then perform g .

Example: If $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$,

and $g = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$

Then $fg = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$

Note 1: $fg \neq gf$.

Therefore, the product of two permutations is not commutative.

Note 2: The product of permutations is associative.

Inverse permutation

Consider a permutation $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$

Then the inverse of this permutation will be

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

5cm

Total number of permutations

If n is the degree of the permutation, then the number of permutations of degree n is $n!$.

If S_n be the set of all permutations of degree n , then S_n is said to be symmetric set of permutations of degree n .

Permutation group

An algebraic structure $(S_n, *)$ is said to be permutation group, where the operation $*$ is the composition or product of permutations and set S_n is symmetric set of permutations of degree n . This group is also called symmetric group.

Cyclic permutation

A permutation which replaces n objects or elements cyclically is called a cyclic permutation of degree n .

Example: Permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

It is written as $(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3)$

The number of elements in a cycle is said to be its length.

Permutation group

Disjoint cycle;

Two cycles are said to be disjoint if there is no common element in both the cycles.

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

Example: Permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$

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

Permutation group

Transposition

A cyclic permutation with length 2 is said to be transposition.

Ex.: $(1\ 2)$, $(4\ 5)$ are transpositions.

Even or odd permutation

A permutation is said to be even or odd according as it can be expressed as a product of even or odd number of transpositions.

Example: Find out following permutations are even or odd.

$$(1) f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}, \quad (2) f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

Permutation group

Solution:

$$\begin{aligned} \text{(1)} \quad f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} \\ &= (1 \ 5) (2 \ 6 \ 3) (4) \\ &= (1 \ 5) (2 \ 6) (2 \ 3) \end{aligned}$$

Clearly, this permutation is expressed as 3 number of transpositions, therefore this permutation is odd permutation.

$$\begin{aligned} \text{(2)} \quad f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix} \\ &= (1 \ 6) (2 \ 3 \ 4 \ 5) \\ &= (1 \ 6) (2 \ 3) (2 \ 4) (2 \ 5) \end{aligned}$$

Clearly, this permutation is expressed as 4 number of transpositions, therefore this permutation is even permutation.