

Lagrange's theorem:-

PAGE NO. 44
DATE

State and prove Lagrange's theorem in group theory OR
[If G is a finite group and H is a subgroup of G , then $|H|$ is a divisor of $|G|$]

OR i.e. prove that $|H| \mid |G|$ where H is a subgroup of G .

Statement:- The order of each sub-group of finite group is a divisor of the order of the group.

Proof:- Let H be a sub-group of a finite group G . Then H is clearly finite. Let the order of H and G be m and n respectively.

We shall prove that n is divisible by m .

Since the order of H is m , H contains m distinct elements, say $h_1, h_2, h_3, \dots, h_m$. Let a be any arbitrary element of G , then the left co-set aH is given by

$$aH = \{ah_1, ah_2, ah_3, \dots, ah_m\}$$

Since, $ah_i = ah_j \Rightarrow h_i = h_j$ [By left cancellation law]

Which is not possible because $h_i \neq h_j$ that implies

$$ah_i \neq ah_j$$

Hence all the m elements of aH are distinct

Let the total number of ^{disjoint} left co-sets of H in G be k .

These co-sets are disjoint and each will contain " m " distinct elements.

Hence the total number of distinct elements contains in the union of all the left co-sets of H in G is mk .

Since the union of these left co-sets is equal to G .

So G must contain " mk " distinct elements. But order of G is " n ".

Hence $n = mk$ ~~to be integer~~

$$\Rightarrow \frac{n}{m} = k = \text{integer}$$

Thus n is divisible by m .

Hence the statement

Index: If H is a subgroup of a group G , the index of H in G is the no. of disjoint right or left co-sets of H in G .

$$\therefore \text{Index} = \frac{O(G)}{O(H)} \quad \text{or} \quad O(H)/O(G)$$

Remark - We shall denote the index of H in G by $I_G(H) = \frac{O(G)}{O(H)}$
or $I_G(H) = O(H)/O(G)$

Corollary - Let G be a finite group and a be any element of G . Then order of " a " divides order of G [i.e. $O(a)/O(G)$]

Let,

$$O(a) = m$$

Then $H = \{e, a, a^2, \dots, a^{m-1}\}$, $a^m = e$ is a cyclic subgroup of G . $\therefore O(H) = m$

By Lagrange's theorem $O(H)/O(G)$

$$\therefore O(a)/O(G)$$

Theorem If G is an infinite cyclic group then G exactly two generators. Prove that

Proof - Let $G = \langle a \rangle$ be an infinite cyclic group generated by a .

The elements of G will be integral power of a . We claim that no two distinct integral powers of a can be equal.

If possible, let

$$a^r = a^s, \quad r > s$$

then, $a^r a^{-s} = a^s a^{-s} = a^0 = e$

$$\therefore a^{r-s} = e$$

Since $r-s$ is positive integer

$$\therefore a^{r-s} = e \Rightarrow o(a) \text{ is finite}$$

We know that order of the generator of a cyclic group is equal to the order of the group. If $o(a)$ is finite then order of G is also finite. But $o(G)$ is infinite.

Hence $a^r \neq a^s$.

Therefore any integral powers of a are distinct elements of G . Since G is generated by a , we can write

$$G = \{ \dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots \}$$

Since a is generator of G then a^{-1} is also a generator of G as $a^r = (a^{-1})^{-r}$

Now we shall show that G has not more than two generators.

Let a^m ($m \neq 1, -1$) be a generator of G .

$\therefore a \in G$ and a^m is generator therefore a must be equal to some integral power of a^m .

$$\text{Let } a = (a^m)^k$$

$$\Rightarrow a = a^{mk} \Rightarrow 1 = mk$$

Since $m \neq 1, -1$ and k and m are integers, so $mk = 1$ gives a contradiction.

Hence a^m is not a generator of G .

Hence the problem.

Theorem Every group of prime order is cyclic.

Proof - Let G be a finite group of order p , p being a prime number so that only divisors of p are 1 and p .
To prove that G is cyclic.

Q: Prove that every group of prime order is abelian.

Ans: [Q0 @ Theorem] (page - 46)

[Theorem Q0 @ Theorem] (page - 26)

PAGE NO: 047
DATE: / /

Let $H = \{a\}$ be a cyclic subgroup of G .

Where $a \neq e$ then, $O(H)$ = order of generator of H
i.e. $O(H) = O(a)$. But $O(a) \neq 1$ Hence
 $O(H) \neq 1$

By Lagrange's theorem, $O(H)$ is a divisor of $O(G)$

Hence $O(H) = p$ or 1

$$\Rightarrow O(H) = p = O(G) \Rightarrow H = G$$

Since H is a cyclic subgroup of G and $H = G$

Hence G is cyclic.

Thm (3)
X

Every finite group of composite ^{order} possesses proper subgroups.
Proof - Let G be a finite group of order p which is not prime.
So that $m > 1, n > 1$

To prove that G possesses proper subgroups.

Case (I): When G is cyclic

Let 'a' be any generator of G

$$\text{Then } O(a) = O(G) = mn$$

Hence $O(a) = mn$, so that $O(a^m) = n$ and $O(a^n) = m$

$$\text{Take } H_1 = \{a^m\}, H_2 = \{a^n\}$$

$$\text{Then } O(H_1) = n < O(G), O(H_2) = m < O(G)$$

Thus H_1 and H_2 are proper subgroups of G . These subgroups are cyclic groups generated by a^m and a^n resp.

Hence G possesses proper subgroups.

Case (II): When G is not cyclic

$$\text{Then say } a \in G \Rightarrow O(a) < O(G) = mn$$

$$\Rightarrow O(a) < mn$$

$\Rightarrow G$ will contain at least one element a

Such that $o(a) = r$ ~~$o(a) = r$~~ for $o(e) = 1$

$\Rightarrow \{a, e\}$ is a proper sub-group of G

Hence the result.

Problems

① If G is a group then show that

$C = \{c \in G, cx = xc \forall x \in G\}$ is a subgroup of G

Ans:- Let G be a group and

$$C = \{c \in G, cx = xc \forall x \in G\}$$

To prove that C is a subgroup of G for this we shall show that

any (i) $a \in C \Rightarrow a^{-1} \in C$

(ii) any $a, b \in C \Rightarrow ab \in C$

(i) $a \in C \Rightarrow ax = xa \forall x \in G \Rightarrow x = a^{-1}xa$

$\Rightarrow xa^{-1} = a^{-1}x \forall x \in G \Rightarrow a^{-1} \in C$

(ii) $a, b \in C \Rightarrow ax = xa, bx = xb \forall x \in G$

Now,

$(ab)x = a(bx)$ (by Ass. law)

$= a(xb)$ ($bx = xb$)

$= (ax)b$ (by Ass. law)

$= (xa)b$ ($ax = xa$)

$= x(ab)$ (By ass. law)

$\Rightarrow ab \in C$ and so C is a subgroup of G .

② If G is a group and $a \in G$ then show that $N(a) = \{x \in G : ax = xa\}$ is a subgroup of G .

Ans. Let a be an arbitrary element of a group G .
We have to show that

$$(i) x \in N(a) \Rightarrow x^{-1} \in N(a)$$

$$(ii) x \in N(a) \Rightarrow x^{-1} \in N(a)$$

$$(iii) x \in N(a) \Rightarrow ax = xa \Rightarrow a = xax^{-1} \Rightarrow x^{-1}ax = a \Rightarrow x^{-1} \in N(a)$$

$$(iv) x \in N(a) \Rightarrow ax = xa \Rightarrow a = xax^{-1} \Rightarrow x^{-1}ax = a \Rightarrow x^{-1} \in N(a)$$

*3 If G be a group of prime order p then show that G has no proper subgroup.

Ans. Let G be a group of prime order p so that only divisors of p are 1 and p .

To prove that G has no proper subgroup.

Let H be a subgroup of G . By Lagrange's theorem

$$|H| \text{ is a divisor of } |G| = p$$

$$\text{This } \Rightarrow |H| = p \text{ or } 1$$

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

\Rightarrow In every case H is not a proper subgroup of G .

$\Rightarrow G$ has no proper subgroup.

*4 If $G = \langle a \rangle$ be a finite cyclic group of order n then for any divisor d of n there is a unique subgroup of G of order d .

Let $G = \langle a \rangle$ be a finite cyclic group of order n .