LECTURE-32 COSET LAGRANGE'S THEOREM

LAGRANGE THEOREM IS ONE OF THE CENTRAL THEOREMS OF ABSTRACT ALGEBRA. IT STATES THAT IN GROUP THEORY, FOR ANY FINITE GROUP SAY G, THE ORDER OF SUBGROUP H OF GROUP G DIVIDES THE ORDER OF G. THE ORDER OF THE GROUP REPRESENTS THE NUMBER OF ELEMENTS. THIS THEOREM WAS GIVEN BY JOSEPH-LOUIS LAGRANGE.

- **LAGRANGE THEOREM STATEMENT**

AS PER THE STATEMENT, THE ORDER OF THE SUBGROUP H DIVIDES THE ORDER OF THE GROUP G. THIS CAN BE REPRESENTED AS; $|G| = |H|$

BEFORE PROVING THE LAGRANGE THEOREM, LET US DISCUSS THE IMPORTANT TERMINOLOGIES AND THREE LEMMAS THAT HELP TO PROVE THIS THEOREM.

WHAT IS COSET?

IN GROUP THEORY, IF G IS A FINITE GROUP, AND H IS A SUBGROUP OF G, AND IF G IS AN ELEMENT OF G, THEN;

gH = {gH: H AN ELEMENT OF H } IS THE LEFT COSET OF H IN G WITH RESPECT TO ELEMENT OF G

AND

Hg = { Hg: H AN ELEMENT OF H } IS THE RIGHT COSET OF H IN G WITH RESPECT TO THE ELEMENT OF G.

NOW, LET US HAVE A DISCUSSION ABOUT THE LEMMAS THAT HELPS TO PROVE THE LAGRANGE THEOREM.

- **LEMMA 1:** IF G IS A GROUP WITH SUBGROUP H, THEN THERE IS A ONE TO ONE CORRESPONDENCE BETWEEN H AND ANY COSET OF H.
- **LEMMA 2:** IF G IS A GROUP WITH SUBGROUP H, THEN THE LEFT COSET RELATION, $g1 \sim g2$ IF AND ONLY IF $g1 * H = g2 * H$ IS AN EQUIVALENCE RELATION.
- **LEMMA 3:** LET S BE A SET AND $\sim$ BE AN EQUIVALENCE RELATION ON S. IF A AND B ARE TWO EQUIVALENCE CLASSES WITH $A \cap B = \emptyset$, THEN $A = B$.

LAGRANGE THEOREM PROOF

WITH THE HELP OF THE ABOVE MENTIONED THREE LEMMAS, WE CAN EASILY PROVE THE LAGRANGE STATEMENT.

PROOF OF LAGRANGE STATEMENT:

LET H BE ANY SUBGROUP OF THE ORDER N OF A FINITE GROUP G OF ORDER M. LET US CONSIDER THE COST BREAKDOWN OF G RELATED TO H.

NOW LET US CONSIDER EACH COSET OF aH COMPRISES N DIFFERENT ELEMENTS.

LET $H = \{H_1, H_2, \ldots, H_N\}$, THEN $aH_1, aH_2, \ldots, aH_N$ ARE THE N DISTINCT MEMBERS OF aH.

SUPPOSE, $aH_I = aH_J \Rightarrow H_I = H_J$ BE THE CANCELLATION LAW OF G.

SINCE G IS A FINITE GROUP, THE NUMBER OF DISCRETE LEFT COSETS WILL ALSO BE FINITE, SAY P. SO, THE TOTAL NUMBER OF ELEMENTS OF ALL COSETS IS NP WHICH IS EQUAL TO THE TOTAL NUMBER OF ELEMENTS OF G. HENCE, M=NP

$p = m/n$

THIS SHOWS THAT N, THE ORDER OF H, IS A DIVISOR OF m, THE ORDER OF THE FINITE GROUP G. WE ALSO SEE THAT THE INDEX p IS ALSO A DIVISOR OF THE ORDER OF THE GROUP.

HENCE, PROVED, $|G| = |H|$

Lagrange Theorem Corollary

Corollary 1: If G is a group of finite order m, then the order of any $a \in G$ divides the order of G and in particular $a^m = e$.

Proof: Let p be the order of a, which is the least positive integer, so,

$a^p = e$

Then we can say,

$a, a^2, a^3, \ldots, a^{p-1}, a^p = e$, the elements of group G are all distinct and forms a subgroup.

Since, the subgroup is of order p, thus p the order of a, divides the group G.

So, we can write,

$m = np$, where n is a positive integer.

So,

$a^m = a^{np} = (a^p)^n = e$

Hence, proved.

Corollary 2: If the order of finite group G is a prime order, then it has no proper subgroups.

Proof: Let us consider, the prime order of the group G is m. Now, m has only two divisors 1 and m (prime numbers property). Therefore, the subgroups of G will be {e} and G itself. So, there are no proper subgroups. Hence, proved.

Corollary 3: A group of prime order (the order has only two divisors) is a cyclic group.

Proof: Suppose, G is the group of prime order of m and $a \neq e \in G$.

Since the order of a is a divisor of m, it is either 1 or m.

But the order of a, $o(a) \neq 1$, since $a \neq e$.

Therefore, the order of $o(a) = p$, and the cyclic subgroup of G generated by a are also of order m.

It proves that G is the same as the cyclic subgroup formed by a, i.e. G is cyclic.