SEM-4 (MATHEMATICS GENERAL)

ANUP RAY

MIKADO
Page No.
Date

Proof (Th. 2): Let HK is a group of G. We are to show that $HK = KH$

Let $x \in HK$. Then $x^{-1} \in HK$ ($\because$ HK is a subgroup)

$\Rightarrow x^{-1} = hk$ for some $h \in H$ and $k \in K$

$\Rightarrow x = (hk)^{-1} = k^{-1}h^{-1} \in KH$

Then $HK \subseteq KH$ ... (1)

Again, let $y \in KH$ Then $y = kh$ for some $k \in K$ and $h \in H$

$\Rightarrow y^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$

$\Rightarrow y \in HK$ (as HK is a subgroup)

$\Rightarrow KH \subseteq HK$ --- (2)

Hence from (1) & (2) we get $HK = KH$

Conversely, let $HK = KH$

Let $a, b \in HK$. We are to show that $ab^{-1} \in HK$.

Since $a, b \in HK \Rightarrow a = h_1k_1$ ~~for some~~ and $b = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$

Then $ab^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1})$

$= h_1(k_1k_2^{-1})h_2^{-1}$

Now $(k_1k_2^{-1})h_2^{-1} \in KH = HK$, thus $(k_1k_2^{-1})h_2^{-1} = hk$ for some $h \in H$, $k \in K$.

Then $ab^{-1} = h_1(hk) = (h_1h)k \in HK$

Thus HK is a subgroup.

Lagrange's Theorem

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

Proof: Let G be a finite group of order n and H be any sub-group of G whose order is m. Let us consider the left decomposition of G relative to H.

Let $H = \{h_1, h_2, \cdots, h_m\}$

Then the m-members of aH ($a \in G$) are

$$ah_1, ah_2, \cdots, ah_m$$

These members are all distinct, since $ah_i = ah_j \Rightarrow h_i = h_j$ by cancellation law in G.

Now G being a finite group, the number of distinct left cosets is also finite. Let this number be k so that the total number of elements of the m cosets is km and this is the total number elements of G.

Therefore $n = mk$.

This proves that the order of H, that is m, is a divisor of n which is the order of the group G.

<u>Note</u>: The converse of Lagrange's Theorem is not true.

For instance, a group of order 12 which has no sub-group of order 6.

<u>Th</u>: Let G be a group of finite order n and $a \in G$. Then $o(a)$ divides n and $a^n = e$.

<u>Proof</u>: Let $H = \langle a \rangle$. Then H is a cyclic subgroup of G and $|H| = o(a)$. By Lagrange's Theorem, $|H|$ divides $|G|$. Hence $o(a)$ divides n. Let $o(a) = m$. Then $n = mk$ for some integer k. Now $a^m = e$ and hence $a^n = a^{mk} = (a^m)^k = e$.