Lecture 16

Tuesday, 6/9/2022

Note Title 9/5/2022

Let G be a group, and let $H \leq G$.

For $a, b \in G$, we can consider $a^{-1}b$, $b^{-1}a$, ab^{-1}, ba^{-1}

<u>Case I:</u> We define a relation $\sim_L$ in G as follows:

$$a \sim_L b \text{ if } a^{-1}b \in H \quad \left(\text{equivalently, } b^{-1}a \in H \atop H \leq G, \text{ so } a^{-1}b \in H \Leftrightarrow b^{-1}a \in H\right).$$

Clearly, $\sim_L$ is an equivalence relation.

For $a \in G$, the equivalence class containing 'a'

$$= \{b \in G \mid a \sim_L b\} = \{b \in G \mid a^{-1}b \in H\} = \{b \in G \mid b \in aH\},$$

Here, $aH = \{a \cdot h \mid h \in H\}$ $\qquad = aH.$

- aH is called the left coset of H containing 'a'.

<u>Case II</u>: For $a, b \in G$, we define $a \sim_R b$ if $ab^{-1} \in H$.
(equivalently, $ba^{-1} \in H$)

In this case, the equivalence class containing 'a'

$$= \{b \in G \mid a \sim_R b\} = \{b \in G \mid b \sim_R a\} = \{b \in G \mid ba^{-1} \in H\}$$

$$= \{b \in G \mid b \in Ha\} = Ha, \quad \text{where } Ha = \{h \cdot a \mid h \in H\}$$

- Ha is called the right coset of H containing 'a'.

- Since left cosets / right cosets are equivalence classes, so we have: For any $a, b \in G$, either $aH = bH$ or $aH \cap bH = \phi$

Also, $Ha = Hb$ or $Ha \cap Hb = \phi$.

__Theorem 1:__ Let H be a subgroup of G. Then,

$$\#\{aH \mid a \in G\} = \#\{Ha \mid a \in G\}.$$

__Proof:__ Define $\phi : \{aH \mid a \in G\} \longrightarrow \{Ha \mid a \in G\}$.

$$\phi(aH) = Ha^{-1}.$$

(i) __ϕ is well-defined:__ Let $aH = bH$. Then, $b^{-1}a \in H$

$\Rightarrow a^{-1}b \in H \Rightarrow (a^{-1})(b^{-1})^{-1} \in H \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow \phi(aH) = \phi(bH)$.

$\therefore$ ϕ is well-defined.

(ii) __ϕ is 1-1:__ $\phi(aH) = \phi(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow (a^{-1})(b^{-1})^{-1} \in H$

$\Rightarrow a^{-1}b \in H \Rightarrow aH = bH$ $\therefore$ ϕ is 1-1.

(iii) It is clear that ϕ is onto. Hence, ϕ is a bijection. #

__Definition:__ (Index of a subgroup): For $H \leq G$, the index of H in G is defined as the cardinality of $\{aH \mid a \in G\}$ or as the cardinality of $\{Ha \mid a \in G\}$, and we denote it by $[G:H]$.

$\therefore \; [G:H] = \#\{Ha \mid a \in G\} = \#\{aH \mid a \in G\}$.

__Ex:__ Let $n \geq 1$. Then, $\{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$.

Thus, $n\mathbb{Z}$ has n distinct right (left) cosets in $\mathbb{Z}$ and hence $[\mathbb{Z} : n\mathbb{Z}] = n$.

__Ex:__ In case of $G = (\mathbb{R}, +)$ and $H = \mathbb{Z}$, the set of distinct right (left) cosets is $\{r + \mathbb{Z} \mid r \in [0,1)\}$.

__Theorem 2:__ Let G be a group, and $H \leq G$. Then, for $a, b \in G$, $\# Ha = \# Hb$, that is, $|Ha| = |Hb|$. Same is true for left cosets.

__Proof:__ $\psi : Ha \to Hb$ given by $\psi(ha) = hb$ is a bijection. #

__Theorem 3 (Lagrange Theorem):__

Let G be a finite group, and $H \leq G$. Then, $|H|$ divides $|G|$.

__Proof:__ Let $a_1 H, a_2 H, \ldots, a_m H$ be the distinct left cosets of H in G.

Then, $G = a_1 H \cup a_2 H \cup \cdots \cup a_m H$ and $a_i H \cap a_j H = \phi$ if $i \neq j$

$\Rightarrow |G| = |a_1 H| + |a_2 H| + \cdots + |a_m H| = |H| + \cdots + |H| = m \cdot |H|$

$\Rightarrow |H|$ divides $|G|$. Also, $m = [G : H] = \frac{|G|}{|H|}$. #

§ Application of Lagrange theorem:

(I) Let G be a finite group. Then, $o(a) \mid |G|$ for every $a \in G$

Proof: We have, $o(a) = |\langle a \rangle|$. But, $|\langle a \rangle|$ divides $|G|$, and hence $o(a) \mid |G|$.

(II) If $|G| = n$, then $a^n = e$ $\forall\, a \in G$.

Proof: Let $o(a) = k$. Then, by (i), $k \mid n$. Let $n = km$.
Then, $a^n = a^{km} = (a^k)^m = e$.

(III) **Fermat's little theorem:** Let $a \in \mathbb{Z}$ and p is a prime.
If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: Let p be a prime. Then, $U(p) = \{1, 2, \dots, p-1\}$ is a group under multiplication modulo p. If $a \in \mathbb{Z}$ and $p \nmid a$, then $a \pmod p \in U(p)$. We have $|U(p)| = p-1$.

By Lagrange theorem, $a^{p-1} \equiv 1 \pmod p$.

#

(iv) Euler's generalization: Let $n \geq 2$. Let $a \in \mathbb{Z}$ be such that $\gcd(a, n) = 1$. Then, $a^{\phi(n)} \equiv 1 \pmod n$.

<u>Proof</u>: $U(n) = \{x \mid 1 \leq x \leq n, \gcd(n, x) = 1\}$ is a group under multiplication modulo n, and $|U(n)| = \phi(n)$.

If $a \in \mathbb{Z}$ and $\gcd(a, n) = 1$, then $a \pmod n \in U(n)$.

Hence, by Lagrange theorem, $a^{\phi(n)} \equiv 1 \pmod n$.

#

(v) Every group of prime order is cyclic.

<u>Proof:</u> Let $|G| = p$, where p is a prime number.

Let $a \in G$ and $a \neq e$. Then, $o(a) \mid |G|$, that is, $o(a) \mid p$.

$\Rightarrow o(a) = 1$ or p. Since $a \neq e$, so $o(a) > 1$.

$\therefore o(a) = p \Rightarrow a$ is a generator of G.

Hence, G is cyclic.

We have proved that, every $a \neq e$ is a generator of G if $|G|$ is a prime.

#