Lecture 4

(4.0) Let G be a group and $H \leq G$ a subgroup.

Definition (set of left cosets modulo H).

For $x, y \in G$; we say $x \underset{L}{\sim} y$ if $x^{-1}y \in H$. (L for left)

Note. (1) $\forall\, x \in G$, $e = x^{-1}x \in H \Rightarrow x \underset{L}{\sim} x$

(2) if $x \underset{L}{\sim} y$, then $x^{-1}y \in H$. As H is a subgroup,

we get $(x^{-1}y)^{-1} = y^{-1}x \in H \Rightarrow y \underset{L}{\sim} x$.

(3) if $x \underset{L}{\sim} y$ and $y \underset{L}{\sim} z$, then $x^{-1}y \in H$ & $y^{-1}z \in H$

$\Rightarrow x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$

$\Rightarrow x \underset{L}{\sim} z$.

Thus the relation $\underset{L}{\sim}$ among elements of G is <u>symmetric</u> (2), <u>reflexive</u> (1) and <u>transitive</u> (3). [called <u>equivalence relation</u>]

G/H = set of equivalence classes in G modulo $\sim$.

More explicitly, an element of G/H is a <u>subset</u> $C \subset G$ s.t. $\forall\, x, y \in C$, $x \underset{L}{\sim} y$ (i.e. $x^{-1}y \in H$).

Such a subset of G is called an equivalence class modulo $\underset{L}{\sim}$. (also <u>left coset</u>)

Lemma. – Let $C \subset G$ be an equivalence class modulo $\underset{L}{\sim}$, as before. Pick $x \in C$. Then the set map

$$\begin{array}{ccc} H & \longrightarrow & C \\ \Psi & & \Psi \\ h & \longmapsto & xh \end{array}$$

is a bijection.

Proof. – One-one: $x h_1 = x h_2 \underset{\uparrow}{\Rightarrow} h_1 = h_2$.

multiply on the left by x^{-1}

Onto: given $y \in C$, $x \underset{L}{\sim} y \Rightarrow x^{-1} y = h \in H$

$\Rightarrow y = xh$ in the image of the set map. □

(4.1) In conclusion. Every equivalence class $C \subset G$ is of the form $x \cdot H = C \subset G$. Here $x \in C$ is <u>a choice that needs to be made</u>:

$$x \cdot H = y \cdot H \iff x^{-1} y \in H$$

(as subsets of G) ← 2 different choices are related

As G breaks into disjoint union of equivalence classes modulo $\underset{L}{\sim}$, we get: for any choice of representatives g_α of equivalence classes modulo $\underset{L}{\sim}$:

$(\alpha \in A)$

$$G = \bigsqcup_{\alpha \in A} g_\alpha H$$

↑ set with same ~~elements~~ cardinality as G/H.

Thus, if G and H are finite, we get

$$\boxed{|G| = |G/H| \cdot |H|} \quad \text{— (4.2)}$$

e.g. $G = S_n$ = permutations of $\{1, \ldots, n\}$

$$\begin{array}{l} G = S_n \\ \text{IV} \\ H = S_{n-1} = \{\sigma \in S_n \mid \sigma(n) = n\} \end{array}$$

Ex. We have a bijection $S_n/S_{n-1} \longrightarrow \{1, \ldots, n\}$

$$(\pi \in S_n \longmapsto \pi(n))$$

$$\Rightarrow \left| S_n/S_{n-1} \right| = n = n!/(n-1)! \quad \checkmark$$

e.g. $G = D_{2n} = \langle s, r \mid s^2 = e = r^n ;\ srs = r^{-1} \rangle$

$$\text{IV}$$

$H = \{e, ~~s~~, r, r^2, \ldots, r^{n-1}\}$

$G/H = \{H, \boxed{sH}\}$ 2 left cosets of G modulo H.

↑ also same as, for instance $(s \cdot r)H$.

(4.3) Some consequences of the identity (assume G is finite)

$$|G/H| \cdot |H| = |G|$$

(1) $H \leq G \Rightarrow |H|$ divides $|G|$

(2) Special case: H = subgroup generated by $a \in G$.

$\Rightarrow |H| = \mathrm{ord}(a)$. We get: $\mathrm{ord}(a)$ divides $|G|$ for any $a \in G$.

Example. If $|G| = p \geq 2$ is prime, then every $a \in G \setminus \{e\}$ is a generator of G. In particular, $G \cong \mathbb{Z}/p\mathbb{Z}$ (abelian).

Example. Let G be a group (finite). Assume $a, b \in G$ are such that $ab = ba$. Then

$$\mathrm{ord}(ab) \text{ divides l.c.m. } (\mathrm{ord}(a), \mathrm{ord}(b))$$

[Ex. $\mathrm{ord}(ab) = $ l.c.m. if $\langle a \rangle \cap \langle b \rangle = \{e\}$.]
(if ↓ in addition to $ab = ba$)

(4.4) Similarly, we can define $H\backslash G$ = the set of <u>right cosets modulo H</u>. Thus, a typical element of $H\backslash G$ is a subset of G, of the form $H.x$. Clearly, $Hx = Hy$ (as subsets of G)

$$\iff yx^{-1} \in H \leftarrow \text{defines equivalence}$$

$\underset{R}{\sim}$, relation analogous to $\underset{L}{\sim}$ of §4.0.

(4.5) $(G:H)$, called <u>index of H in G</u>, is defined to be $|G/H|$. Note that $(G:H)$ could be finite even though G is infinite. eg.

$$G = \mathbb{Z} \geq H = n.\mathbb{Z}$$

$$(G:H) = \left| \mathbb{Z}/_{n\mathbb{Z}} \right| = n.$$