Lecture V: Cosets modulo a subgroup; Index of a subgroup

TODAY: First attempt to defining a quotient of a group by a subgroup

§5.1. Cosets modulo a subgroup:

Let G be a group and $H \leq G$ a subgroup

Definition: For $x, y \in G$, we say $x \sim_L y$ if $x^{-1}y \in H$ (L for left)

Proposition: $\sim_L$ is an equivalence relation on G

Proof: We check is reflexive, symmetric and transitive.

(1) $\forall x \in G$, $x \sim_L x$ since $x^{-1}x = e \in H$, so $\sim_L$ is reflexive

(2) If $x \sim_L y$, then $y \sim_L x$. Indeed $x^{-1}y \in H$ implies $(x^{-1}y)^{-1} \in H$, because H is a subgroup. But $(x^{-1}y)^{-1} = y^{-1}x \in H$ means $y \sim_L x$. So $\sim_L$ is symmetric.

(3) If $x \sim_L y$ and $y \sim_L z$, then $x^{-1}y \in H$ and $y^{-1}z \in H$. Multiplying both elements we get $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$ because H is a subgroup. So, $x \sim_L z$ by definition. Hence, $\sim_L$ is transitive.

Define: $G/H := G/\sim_L$ = set of equivalence classes in G modulo $\sim_L$.
We call it the set of left cosets of G modulo H.
More explicitly, an element of G/H is a subset $C \subseteq G$ st

$$x, y \in C \iff x \sim_L y \qquad (\text{ie } x^{-1}y \in H)$$

We typically write C as $[x]$ for any $x \in C$.

Q: How many elements does $[x]$ have?

Lemma: Let $C \subseteq G$ be an equivalence class modulo $\sim_L$. Pick $x \in C$. Then the set map

$$\begin{aligned} H &\xrightarrow{\Phi} C \\ h &\longmapsto xh \end{aligned}$$

is a bijection.

Proof: • $xh \sim_L x$ so $\operatorname{Im} \Phi \subseteq C$ (Φ is well defined)

- Φ is injective (one-to-one): $xh_1 = xh_2 \implies x^{-1}xh_1 = x^{-1}xh_2$. So, $h_1 = h_2$.
- Φ is onto (surjective): given $y \in C$, we know $x \sim_L y$, so $x^{-1}y \in H$

Write $h = x^{-1}y$. Then, $\Phi(h) = xh = xx^{-1}y = y$, ie $y \in \text{Image}(\Phi)$. $\square$

Corollary: Every equivalence class $C \subseteq G$ of $\sim_L$ is of the form xH for some $x \in C$.

Note: The choice of x is not unique, because any $x \in C$ gives $C = xH$. Thus, a choice needs to be made!

$$xH = yH \text{ as subsets of } G \iff x^{-1}y \in H.$$

As G breaks into disjoint union of equivalence classes modulo $\sim_L$, we get

Lemma: For any choice of representatives $(g_\alpha)_{\alpha \in A}$ of equivalence classes modulo $\sim_L$, we have:
$$G = \coprod_{\alpha \in A} g_\alpha H.$$

↳ stands for disjoint union

Here, A is a set with the same cardinality as G/H.

Corollary: If G and H are finite, we get $|G| = |G/H| \cdot |H|$

Example 1: $G = S_n$ = permutations on $\{1, 2, \ldots, n\}$ $\qquad |G| = n!$

$\quad$ IV

$H = S_{n-1} = \{\sigma \in S_n \mid \sigma(n) = n\}$ $\qquad |H| = (n-1)!$

We have a bijection
$$\begin{aligned} S_n/S_{n-1} &\longrightarrow \{1, \ldots, n\} \\ \sigma &\longmapsto \sigma(n) \end{aligned}$$

($(\sigma \circ \pi)(n) = \sigma(\pi(n)) = \sigma(n)$ $\quad \forall \sigma \in S_n$ so $\sigma(n)$ is the same for all σ in an equivalence class)

$$\implies |S_n/S_{n-1}| = n = n!/(n-1)!$$

Example 2: $G = D_{2n} = \langle s, r \mid s^2 = e = r^n \quad srs = r^{-1} \rangle$ $\qquad |G| = 2n$

$\quad$ IV

$H = \{e, r, r^2, \ldots, r^{n-1}\} = \langle r \rangle$ $\qquad |H| = n$ (last time)

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

Note: $sH = (sr^k)H$ $\forall k=0,\dots,n-1$ & $sH \neq H$ because $s \notin H$.
$H = r^k H$

§5.2 Index of a subgroup:

Definition: Given a group G & a subgroup $H \leq G$. The index of H in G is the size of the left cosets G/H. Write it as $(G:H)$

Recall: We have the identity $\boxed{|G| = |G/H| \cdot |H|}$ when G is finite. (*)

Remark: $(G:H)$ could be finite even though G is infinite.

Example: $G = \mathbb{Z}$ & $H = n\mathbb{Z} = \langle n \rangle$ Then, G is infinite and

$$G/H = \{ \underset{\overline{0}}{n\mathbb{Z}}, \underset{\overline{1}}{1+n\mathbb{Z}}, \dots, \underset{\overline{n-1}}{(n-1)+n\mathbb{Z}} \} = \mathbb{Z}/n\mathbb{Z}$$ & $(G:H) = n$ is finite.

Some consequences of the identity (*):

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

(2) Special case: $H = \langle a \rangle$ for some $a \in G$

$\implies |H| = \operatorname{ord}(a)$ & so $\operatorname{ord}(a)$ divides $|G|$ $\forall a \in G$.

Application: If $|G| = p \geq 2$ is prime, then every $a \in G \setminus \{e\}$ generates G. In particular, $G = \mathbb{Z}/p\mathbb{Z}$ (and so it is abelian)

Recall: Assume G is finite. If $a, b \in G$ & $a*b = b*a$, we know

$$\operatorname{ord}(a*b) \leq \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$$

Application 2: In these conditions, we have $\operatorname{ord}(a*b)$ divides $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$

Furthermore, $\operatorname{ord}(a*b) = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$ if, in addition, $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Proof: Define $H = \langle a, b \rangle \leq G$ Since $a*b = b*a$, we know H is an abelian group. Write $k = \operatorname{ord}(a*b)$. So $(a*b)^k \underset{a*b=b*a}{=} a^k * b^k = e$

- Claim: If $c \in G$ and $c^d = e$, then $\mathrm{ord}(c) \mid d$.

Pf/ Write $d = \mathrm{ord}(c) \cdot m + r$ for $0 \le r < \mathrm{ord}(c)$.

Then, $e = c^d = c^{\mathrm{ord}(c)\cdot m + r} = (c^{\mathrm{ord}(c)})^m c^r = e^m c^r = c^r$ forces $c^r = e$ so $r = 0$ since $0 \le r < \mathrm{ord}(c)$. $\square$

- Take $c = a * b$, $N = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$ Then:

$$(a*b)^N = a^N * b^N = e*e$$

because $\mathrm{ord}(a) \mid N$ & $\mathrm{ord}(b) \mid N$. So $\mathrm{ord}(a*b) \mid N$ by the claim.

- For the second part, write $k = \mathrm{ord}(a*b)$. So $(a*b)^k = a^k * b^k = e$

This means $a^k = b^{-k}$. Now $\langle a \rangle \cap \langle b \rangle = e$ implies $a^k = e = b^{-k}$.

By the claim, $\mathrm{ord}(a) \mid k$ & $\mathrm{ord}(b) \mid k$. Thus $N \mid k$.

Since $k \mid N$ & $N \mid k$, we get $k = N$. $\square$

Example: a & $b \in S_n$ two disjoint cycles. Then $a*b = b*a$

$\mathrm{ord}(a) =$ length of the cycle a, $\mathrm{ord}(b) =$ length of the cycle b.

$\langle a \rangle \cap \langle b \rangle = \{id\}$ because the cycles are disjoint.

$$\Rightarrow \mathrm{ord}(ab) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$$

Application: Compute order of all elements in S_5

Enough: determine the cycle type of each $\sigma \in S_5$ [length of disjoint cycles in the expression of σ]

Eg $\sigma = id = (1)(2)(3)(4)(5)$ cycle type $1+1+1+1+1$

$\sigma = (123)(45)$ cycle type $2+3$

Cycle Type	Order	# of Elements
$1+1+1+1+1$	1	1
$1+1+1+2$	2	$\binom{5}{2} = 10$
$1+1+3$	3	$\binom{5}{3} \frac{3!}{3} = 20$
$1+2+2$	2	$5 \binom{4}{2}\binom{2}{2}/2 = 15$
$1+4$	4	$\binom{5}{4} \frac{4!}{4} = 30$
$2+3$	6	$\binom{5}{2} \frac{3!}{3} = 20$
5	5	$5!/5 = 24$

TOTAL: $5! = 120$