LECTURE 22

(Friday NOV. 22, 2019)

$(G,*)$ group with subgroup $H \leqslant G$.

"Cosets" are subsets $a*H = \{a*h : h \in H\} = [a]$.

$\searrow$ partition G (i.e., every $a \in G$ lies in exactly <u>one</u> coset).

- Collection of all cosets:

$$a*H = b*H \iff a^{-1}*b \in H.$$

$$G/H = \{a*H : a \in G\}.$$

set. index $= [G:H] = |G/H|$.

(ex. $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z} =$ all <u>residue</u> classes $[a] = a + N\mathbb{Z}$).

(<u>LAGRANGE</u>: $|G| = [G:H] \cdot |H|$)

- Does G/H have a <u>group</u> structure?

(similar to $+$ on $\mathbb{Z}_N$ given by $[a]+[b]=[a+b]$).

<u>TRY</u>: Define a <u>composition</u> law $\bullet$ on G/H by

$$(a*H) \bullet (b*H) = (a*b)*H.$$

more briefly: $[a] \bullet [b] = [a*b]$.

<u>Problem</u>: Not always well-defined! May happen that $[a] = [a']$ and $[b] = [b']$ <u>but</u> $[a*b] \neq [a'*b']$.

rot. by $2\pi/N$ ref.

EX $D_N = \langle r, s \rangle$, $r^N = s^2 = e$ and $rs = sr^{-1}$.
(symmetries of an N-gon). Let $H = \langle s \rangle = \{e, s\}$. (idx. N)

Note: $rH = rsH$ (since $s \in H$) but

- $r^2 H \neq H$ since $r^2 \notin H$ (assuming $N \geq 3$)
- $(rs)^2 H = \underbrace{rs}rsH = \underbrace{sr^{-1}}rsH = s^2 H = H$

So $[r] = [rs]$ but $[r * r] \neq [rs * rs]$.

— shows **not** well-def. composition law on D_N/H.

Def. $H \leq G$ is a normal subgroup if

$$a * H = H * a \qquad \forall a \in G.$$

Remark: This does not mean $a*h = h*a$ for all $h \in H$. It means: For any two $a \in G$, $h \in H$ there's an $h' \in H$ with $a*h = h'*a$ — and vice versa. Possibly $h' \neq h$.

Notation: When $H \leq G$ is normal we write $\boxed{H \triangleleft G}$.

Obs: If G abelian every $H \leq G$ is normal.

Proposition When H is <u>normal</u> in G,

$\bullet$ is a <u>well</u>-<u>defined</u> composition law on G/H.

PROOF: Let's suppress $*$ in this proof (i.e. write $aH = a * H$ etc.). <u>Assume</u> $aH = a'H \wedge bH = b'H$.

must show $abH = a'b'H$. Now,

$$abH \underset{bH=b'H}{=} ab'H \underset{H \lhd G}{=} aHb' \underset{aH=a'H}{=} a'Hb' \underset{H \lhd G}{=} a'b'H$$

$\square$

- Thus $(G/H, \bullet)$ is a <u>group</u> when $H \lhd G$:
  (associative, neutral element $e * H = H$,
  inverse of $a * H$ is $a^{-1} * H$)

"<u>QUOTIENT</u> <u>GROUP</u> of G by H".

<u>EX</u> (cont) $H = \{e, s\}$ <u>not</u> normal in D_N:

$rH = \{r, rs\}$
distinct.
$Hr = \{r, sr\}$

and $rs = sr^{-1} \neq sr$ since $N > 2$.

compare w. $(\mathbb{Z}_N, +)$.

EXC Any $H \leqslant G$ of index $[G:H]=2$ is normal.

(Hint: For $a \notin H$, $G = H \cup aH = H \cup Ha$ so

$aH = Ha =$ complement of H in G.)

Ex.) $A_n \triangleleft S_n$ and $\langle r \rangle \triangleleft D_N$.

Lemma ("Normality Criterion"): Let $H \leqslant G$. T.F.A.E.:

(1) H is normal in G (i.e., $aH = Ha$ $\forall a \in G$)

compare subsets

(2) $aHa^{-1} = H$ $\forall a \in G$.

Compare subgroups.

[exc: Check aHa^{-1} is a subgroup.]

(3) $aHa^{-1} \subseteq H$ $\forall a \in G$.

PROOF. (1) $\Longleftrightarrow$ (2): $aH = Ha$ iff
$aHa^{-1} = Haa^{-1} = H$. ✓

(2) $\Rightarrow$ (3): Trivial.

(3) $\Rightarrow$ (2): Need the other inclusion $aHa^{-1} \supseteq H$.

i.e., $H \supseteq a^{-1}Ha$.

— follows from (3) applied to a^{-1} instead of a.

$\square$

Ex. A_4 with subgroup $V = \{e, (12)(34), (13)(24), (14)(23)\}$.

non-cyclic of size 4.

$V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

"Klein's 4-group".

$= \{\text{all } \alpha \in A_4 \text{ of order} \leq 2\}$.

$= \{\alpha \in A_4 : \alpha^2 = e\}$.

(to see this decompose α into cycles)

V is normal in A_4: $\quad \delta V \delta^{-1} \subseteq V \quad \forall \delta \in A_4$.

— indeed $\alpha^2 = e$ implies

$$(\delta \alpha \delta^{-1})^2 = \delta \alpha^2 \delta^{-1} = e.$$

A_4/V is a group of size $[A_4 : V] = \frac{12}{4} = 3$.

so $A_4/V \simeq \mathbb{Z}_3$.

~ An application of quotient groups:

Thm. Suppose G is finite and $H \trianglelefteq G$.
Then:
$$a^{[G:H]} \in H \quad \text{for all } a \in G.$$
(know this for $[G:H] = 2$).

PROOF. Apply (Corollary of) Lagrange to the group G/H: $\forall a \in G$,
$$\begin{array}{ccc} (aH)^{|G/H|} & = & eH \\ \| & & \\ a^{[G:H]}H & & \end{array}$$
I.e., $a^{[G:H]}$ belongs to H. $\square$