LECTURE 21

(Wednesday NOV. 20, 2019)

EX $D_N = \langle r, s \rangle$ $\quad r^N = e \quad s^2 = e \quad rs = sr^{-1}$.

(= symetries of N-gon).

r = rotation by $\frac{2\pi}{N}$

s = reflection.

~ recall, $|D_N| = 2N$.

- $H = \langle r \rangle = \{\text{rotations in } D_N\}$.
  has index $[D_N : H] = 2$.

$$D_N = \{e, \dots, r^{N-1}\} \cup \{s, \dots, sr^{N-1}\}$$

H two cosets. sH.

- $K = \langle s \rangle = \{e, s\}$,
  has index $[D_N : K] = N$.

$$D_N = \{e, s\} \cup \{r, rs\} \cup \{r^2, r^2 s\} \cup \dots \cup \{r^{N-1}, r^{N-1} s\}$$

$$= K \cup rK \cup r^2 K \cup \dots \cup r^{N-1} K.$$

EX S_n with subgroup A_n. $\quad [S_n : A_n] = \dfrac{n!}{\frac{n!}{2}} = 2$.

$$S_n = \{\text{even perm}\} \cup \{\text{odd perm}\}$$

A_n $\quad (12) \circ A_n$.

EX

$$\mathbb{Z} = \{\text{even int.}\} \cup \{\text{odd int.}\} \qquad [\mathbb{Z} : 2\mathbb{Z}] = 2$$

$2\mathbb{Z}$ $\quad 1 + 2\mathbb{Z}$

Ex. $(\mathbb{Z}_{15}, +)$ with subgroup $H = \langle [3] \rangle$.

$= \{[0], [3], [6], [9], [12]\}$.

- index?

$[\mathbb{Z}_{15} : H] = \frac{15}{5} = 3$.

- cosets?

$[0] + H = H$.

$[1] + H = \{[1], [4], [7], [10], [13]\}$

$[2] + H = \{[2], [5], [8], [11], [14]\}$.

Ex. $(\mathbb{Z}_{13}^{\times}, \bullet)$ with $K = \langle [3] \rangle$

$= \{[1], [3], [9]\}$.

index:

$[\mathbb{Z}_{13}^{\times} : K] = \frac{12}{3} = 4$.

cosets?

$[1] \bullet K = K$.

$[2] \bullet K = \{[2], [6], [5]\}$

$[4] \bullet K = \{[4], [12], [10]\}$

$[7] \bullet K = \{[7], [8], [11]\}$

Ex $(A_4, \circ)$ with subgroup $H = \langle (124) \rangle$
$= \{e, (124), (142)\}$.

index
$[A_4 : H] = \frac{12}{3} = 4.$

cosets: $e \circ H = H.$

$(123) \circ H = \{(123), (13)(24), (143)\}$ — see below: *

$(132) \circ H = \{(132), (243), (14)(23)\}$

$(234) \circ H = \{(234), (134), (12)(34)\}$.

*)

$$(123) \circ (124) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

$$(123) \circ (142) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (143)$$

Application of LAGRANGE:

Corollary $|G| < \infty$. Let $a \in G$. Then:

(1) $\operatorname{ord}(a)$ divides $|G|$.

(clear: Recall $\operatorname{ord}(a) = |\langle a \rangle|$. Take $H = \langle a \rangle$ in LAGRANGE.)

(2) $a^{|G|} = e$.

By (1) write $|G| = q \cdot \operatorname{ord}(a)$. Then

$$a^{|G|} = \left(a^{\operatorname{ord}(a)}\right)^q = e^q = e \checkmark.$$

(3) $|G| = p$ then $G \simeq \mathbb{Z}_p$ (cyclic). (any $a \neq e$ generates G.)

EX $G = (\mathbb{Z}/N\mathbb{Z})^\times = \mathbb{Z}_N^\times$ with $\bullet$.
(inv. residue classes mod N)

Recall: $|\mathbb{Z}_N^\times| = \varphi(N)$ Euler function.

By (2): $\forall a \in \mathbb{Z}$ coprime to N, $[a]^{\varphi(N)} = [1]$.

I.e.,

$$\boxed{a^{\varphi(N)} \equiv 1 \pmod N}$$

"Euler's Theorem"

$\Rightarrow$ special case $N = p$: prime number. Here $\varphi(p) = p - 1$, so

$$\boxed{a^{p-1} \equiv 1 \pmod p}$$

"FERMAT'S LITTLE THEOREM".

for all $a \in \mathbb{Z}$ s.t. $p \nmid a$.

Exc. Equivalently $a^p \equiv a \pmod{p}$
for all $a \in \mathbb{Z}$.

Ex. Find the $r \in \mathbb{Z}$ in the range $0 \leq r < 11$ s.t.

$r \equiv 3^{2019} \pmod{11}$. $\quad 2019 = 201 \cdot 10 + 9$.

(use $3^{10} \equiv 1 \pmod{11}$; Fermat) $\quad 3^{2019} \equiv 3^9 = 19683$

$\equiv 4 \pmod{11}$

$\Rightarrow \boxed{r = 4}$.

NOTE:

Index Two Subgroups: $H \leq G$ with $[G:H] = 2$.

I.e., $G = H \cup xH$ (disjoint) for any $x \in G$ not in H.

Similarly:

$G = H \cup Hx$.

- Consequently: $\boxed{xH = Hx}$ ($=$ complement of H in G)

(left/right cosets are the same — we say
H is "normal" in G)

Observation: $x^2 \in H$ for all $x \in G$.
($[G:H] = 2$)

Why?

— Obvious if $x \in H$. Otherwise (if x not in H):

$G = H \cup xH$.

Suppose x^2 is not in H. Then

$x^2 \in xH$. I.e., $x^2 = xh$ some $h \in H$.

Cancellation: $x = h \in H$ contradiction. ✓

Application: "Converse to LAGRANGE" fails for A_4:

A_4 has no $H \leq A_4$ with $|H| = 6$. ← i.e. index $= 2$.

— for the sake of contradiction suppose $\exists H$.

$(abc) = (acb)^2 \in H$. — by observation.

↑ any 3-cycle

They generate A_4, cf. HW7.

Infer $H = \langle (abc) \rangle = A_4$.

all

contradiction. ✓