

LECTURE 21
(Wednesday Nov. 20, 2019)

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

(= symmetries of N -gon).

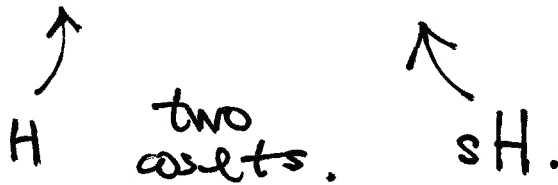
r = rotation by $\frac{2\pi}{N}$

s = reflection.

$\circ H = \langle r \rangle = \{ \text{rotations in } D_N \}$.

has index $[D_N : H] = 2$.

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



$\circ K = \langle s \rangle = \{ e, s \}$,

has index $[D_N : K] = N$.

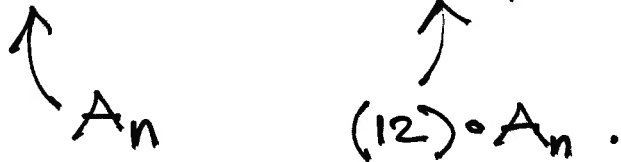
$D_N = \{ e, s \} \cup \{ r, rs \} \cup \{ r^2, r^2s \} \cup \dots \cup \{ r^{N-1}, r^{N-1}s \}$

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

EX S_n with subgroup A_n .

$[S_n : A_n] = \frac{n!}{\frac{n!}{2}} = 2$.

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



EX $\mathbb{Z} = \{ \text{even int.} \} \cup \{ \text{odd int.} \}$

$[\mathbb{Z} : 2\mathbb{Z}] = 2$



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

- index?

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

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

- cosets?

$$[0] + H = H.$$

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

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

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

index:

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

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

cosets?

$$[1] \cdot K = K.$$

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

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

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

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

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

cosets: $e \cdot H = H.$ — see below.*

$$(123) \circ H = \{ (123), \overbrace{(13)(24)}, \overbrace{(143)} \}$$

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

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

*)

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

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

Application of LAGRANGE:

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

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

(clear: Recall $\text{ord}(a) = |\langle a \rangle|$. Take

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

$H = \langle a \rangle$
in LAGRANGE.)

(3) $|G| = p$ then

$G \cong \mathbb{Z}_p$ (cyclic).

(any $a \neq e$ generates G)

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

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

EX $G = (\mathbb{Z}/N\mathbb{Z})^\times = \mathbb{Z}_N^\times$ with \cdot .

(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.,

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

"Euler's
Theorem"

special case

$N = p$:

prime
number.

Here $\varphi(p) = p - 1$, so

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

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

"FERMAT'S
LITTLE
THEOREM".

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.

$$r \equiv 3^{2019} \pmod{11}.$$

$$2019 = 201 \cdot 10 + 9.$$

(use $3^{10} \equiv 1 \pmod{11}$; Fermat)

$$3^{2019} \equiv 3^9 = 19683$$

$$\equiv 4 \pmod{11}$$

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

NOTE:

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

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

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:

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

Why?

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

$$G = H \cup xH.$$

Suppose x^2 is not in H . Then

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

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

Application: "Converse to LAGRANGE" fails for A_4 :

A_4 has no $H \leq A_4$ with $|H| = 6$.

— for the sake of contradiction

i.e. index = 2.

suppose $\exists H$.

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

↑ any 3-cycle

They generate A_4 , of. HW7.

$$\text{Infer } H = \langle \underset{\text{all}}{(abc)} \rangle = A_4, \quad \text{contradiction.} \quad \checkmark$$