Last Class:

Every permutation can be written as a product of 2-cycles

e.g. $(a_1 a_2 \dots a_r) = (a_1 a_2)(a_2 a_3) \dots (a_{r-1} a_r)$

$(1234) = (12)(23)(34)$

Lots of different ways how to write a permutation as a product of 2-cycles

e.g. $(123) = (12)(23)$

$= (23)(13)$

Lemma: Assume $\underset{\text{id}}{\overset{\shortparallel}{\varepsilon}} = \beta_1\beta_2\cdots\beta_k$ β_i's 2-cycles

$\Longrightarrow$ k is even

proof by ind. on k

$\underline{k=1}$ $\beta \neq \text{id}$ for any 2-cycle $\beta = (ab)$

$\beta(a) = b \neq a$

$\underline{k=2}$ $\beta_1\beta_2 = \text{id} \Rightarrow \underbrace{\beta_1^2}_{=\text{id}}\beta_2 = \beta_1 \Longrightarrow \beta_1 = \beta_2$

Assume $\text{id} = \beta_1\beta_2\cdots\beta_k$

claim 1: If $\beta_{k-1} \neq \beta_k$ $\quad \beta_k = (ab)$

$\Rightarrow$ can find 2-cycle γ_k s.t. $\gamma_k(a) = a$

$$\beta_{k-1}\beta_k = \beta_k \gamma_k$$

proof: have the following cases (a, b, c, d mutually distinct)

$$(ac)(ab) = (ab)(bc)$$

$$(bc)(ab) = (ac)(bc)$$

$$\underbrace{(cd)}_{\beta_{k-1}}\underbrace{(ab)}_{\beta_k} = \underbrace{(cd)}_{\beta_k}\underbrace{(ab)}_{\gamma_k}$$

straightforward calculation!

claim 2 If $id = \beta_1\beta_2\cdots\beta_k$
then there is an $i<k$ s.t. $\beta_i = \beta_k$

proof if not can use claim 1 repeatedly to transform

$$id = \beta_1\cdots\beta_{k-1}\beta_k = \beta_1\cdots\underbrace{\beta_{k-2}\beta_k}\gamma_k \qquad \gamma_k(a)=a$$

$$= \beta_1\cdots\underbrace{\beta_{k-3}\beta_k}\gamma_{k-1}\gamma_k \qquad \gamma_{k-1}(a)=a$$

$$\cdots$$

$$= \beta_k\gamma_2\gamma_3\cdots\gamma_k \qquad \gamma_i(a)=a, \quad 2\le i\le k$$

BUT:

$$\beta_k\gamma_2\cdots\gamma_k(a) = \beta_k(a) = b \neq a$$

↯ $\quad \|$

$\varepsilon(a)$

$\Rightarrow \exists i$ s.t. $\beta_i = \beta_k$

$\Rightarrow \mathrm{id} = \beta_1 \cdots \beta_k = \beta_1 \cdots \underbrace{\beta_i \underset{\beta_i}{\underset{\shortparallel}{\beta_k}}}_{= \mathrm{id}} \gamma_{i+2} \cdots \gamma_k = \underbrace{\beta_1 \cdots \beta_{i-1} \gamma_{i+2} \cdots \gamma_k}_{k-2 \text{ factors}}$

by ind. ass. $k-2$ even

$\Rightarrow$ k even ✓

<u>Theorem</u> Assume $\pi = \beta_1 \cdots \beta_s$ and $\pi = \gamma_1 \cdots \gamma_r$

all β_i's and γ_j' 2-cycles

$\Rightarrow$ either both r and s are even
or both r and s are odd.

Proof. $\pi^{-1} = \gamma_r \gamma_{r-1} \cdots \gamma_1 \Rightarrow \mathrm{id} = \pi \pi^{-1} = \underbrace{\beta_1 \beta_2 \cdots \beta_s \gamma_r \gamma_{r-1} \cdots \gamma_2 \gamma_1}_{r+s \text{ factors}}$

By lemma $r+s$ is even $\Rightarrow$ claim.

Def A permutation π is called odd/even if π is a product of an odd/even number of 2-cycles

Examples:

(12) odd

$(123) = (12)(23)$ even

$(1234) = (12)(23)(34)$ odd

$(12)(34)$ even

Remark: Our theorem makes sure that the definition makes sense, i.e. whether a permutation is odd or even does not depend on the choice of product of 2-cycles.

Theorem: let $A_n = \{\pi \in S_n, \pi \text{ even}\}$

$\Rightarrow$ A_n is a subgroup of S_n with $\frac{n!}{2}$ elements

proof. apply subgroup test

e.g. if $\pi = \beta_1 \beta_2 \cdots \beta_r$ $\quad r$ even

$$\Rightarrow \quad \pi^{-1} = \underbrace{\beta_r \beta_{r-1} \cdots \beta_1}_{\text{even \# of factors}}$$

$\Rightarrow \pi^{-1} \in A_n$

check for yourself. $\pi, \sigma \in A_n \Rightarrow \pi\sigma \in A_n$

Observe: π even $\Rightarrow$ $(12)\pi$ is odd permutation

by cancellation property, map $\pi \to (12)\pi$ is injective

$\Rightarrow$ $\#\{\text{odd permutations}\} \geq \#\{\text{even permutations}\}$

similarly: σ odd $\Rightarrow$ $(12)\sigma$ even

$\Rightarrow$ $\#\{\text{even perm.}\} \geq \#\{\text{odd perm}\}$

$\Rightarrow$ $\#\{\text{even perm.}\} = \#\{\text{odd perms.}\} = \dfrac{n!}{2}$

$\quad\quad \| $

$\quad |A_n|$

Examples:

A_3: (123), (132), id even permutation ✓

$$|A_3| = \frac{3!}{2} = \frac{6}{2} = 3$$

A_4: we have 8 3-cycles!

(123) (132)

(124) (142)

(134) (143)

(234) (243)

$\left.\begin{matrix}(12)(34) \\ (13)(24) \\ (14)(23)\end{matrix}\right\} 3$

id

$\Rightarrow$ get $12 = \frac{24}{2} = \frac{4!}{2}$ elements midterm max points 25 + 1 bonus point

median 15

mean 15.55

min 9

max 22

Problem 4

$H = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix},$ $a,b,c,d \in \mathbb{Z}$

$a \bmod 2 = 1 = d \bmod 2$

$c \bmod 2 = 0 = b \bmod 2$

(a) show $\det(A) \neq 0$ for $A \in H$

$\quad\ \ \shortparallel$

$ad - bc$

Calculate $\det A \bmod 2$

$ad - bc \bmod 2 = 1 \cdot 1 - 0 \cdot 0 = 1$

$\Rightarrow ad - bc \neq 0$

(b) try subgroup test

$A, A' \in H$ $\qquad A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$

$$A \cdot A' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

$$= \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \mod 2$$

$$= \begin{pmatrix} 1 \cdot 1 + 0 \cdot 0 & 1 \cdot 0 + 0 \cdot 1 \\ 0 \cdot 1 + 1 \cdot 0 & 0 \cdot 0 + 1 \cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\Rightarrow$ diag. entries a AA' are 1 mod 2
off diag " " AA' are 0 mod 2 $\Big\}$ $AA' \in H$.

⚠ inverse in general NOT in H

$$A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

get fractions if $ad-bc \neq \pm 1$

$\Rightarrow$ A^{-1} does not have integer entries in general!

$\Rightarrow$ NOT a subgroup!

Full credit for part(b)
if you could show
If A, A' in H, then also AA' in H

what I had intended was
H with additional condition

$$\det(A) = ad - bc = 1$$

Extra credit if you noticed that
the inverse of A may not be in H

with this condition H IS a subgroup?