Permutation Group / Alternating Group

denoted S_n denoted A_n

Recall

$S_n := (\{ \sigma \mid \sigma : \{1, \cdots, n\} \to \{1, \cdots, n\}$ that is bijective $\}$

$, \circ)$

composition

Goal: Define A_n, desrible A_n.

Normal Subgrp.

Recall we defined quotient ring for a ring R by an ideal $I \subseteq R$, R/I.

to be $(\{$ equivalence classes of "$\sim$" $\}, +, \times)$.

inherited from $+, \times$ in R

Here $a \sim b$ in R if $a - b \in I$.

Q: Can we do similar things for grp?

Last time, given $H \subseteq G$. we define "$\sim_H$" to be

$g_1 \sim g_2$ iff $g_1^{-1} \cdot g_2 \in H$

Can we define $\cdot$ grp operation on $\{$ equivalence classes $\}$

$g \cdot H := \{ g \cdot h \mid h \in H \}$

by picking repsesentatives?

$g_1 \cdot H \quad g_2 \cdot H \qquad g_1, g_2$ are the representatives for the two cosets.

$\tilde{g}_1 \in G \quad \tilde{g}_2 \in G \qquad \tilde{g}_1 \cdot \tilde{g}_2 \, H$??

$$(g_1 \cdot H) \cdot (g_2 H) \overset{??}{=} g_1 \cdot g_2 \, H$$

We need to check whether this multiplication is well-defined ?

$$\tilde{g}_1 \cdot \tilde{g}_2 \, H = g_1 \, g_2 \, H \iff \tilde{g}_1 \cdot \tilde{g}_2 \sim_H g_1 \cdot g_2$$

$$\iff \underbrace{(\tilde{g}_1 \cdot \tilde{g}_2)^{-1}}_{= \tilde{g}_2^{-1} \cdot \tilde{g}_1^{-1}} \cdot (g_1 \cdot g_2) \in H$$

Now since $\tilde{g}_1 \in g_1 \cdot H$ we have $\tilde{g}_1 = g_1 \cdot h_1$ for some $h_1 \in H$

similarly we have $\tilde{g}_2 = g_2 \cdot h_2$ for some $h_2 \in H$

$$\iff (g_2 \cdot h_2)^{-1} \cdot (g_1 \cdot h_1)^{-1} \cdot g_1 \cdot g_2 \in H$$

$$= h_2^{-1} \cdot g_2^{-1} \cdot h_1^{-1} \cdot \cancel{g_1^{-1}} \cdot \cancel{g_1} \cdot g_2 = \underbrace{h_2^{-1}}_{\in H} | g_2^{-1} \, h_1^{-1} \, g_2 \in H$$

$$\iff g_2^{-1} \cdot h_1^{-1} \cdot g_2 \in H$$

$$\iff h_1^{-1} \in \underbrace{g_2 H g_2^{-1}}_{= \{ g_2 h g_2^{-1} \mid h \in H \}}$$

$$\boxed{h \cdot g \in H \Rightarrow g \in H}$$

$$h \cdot g = h' \in H$$

$$h^{-1} \cdot$$

$$g = h^{-1} \cdot h' \in H$$

Notice that we can choose any $h_1 \in H$ and any $g_2 \in G$ since we can choose any representative for $g_1 H$ and $g_2 H$ and we can choose any two cosets to do grp operation.

In order to make the operation on cosets well-defined, we need $H \subseteq g_2 H g_2^{-1}$ for any $g_2 \in G$.

Def (normal subgrp). A subgrp $H \subseteq G$ is normal if $H \subseteq g^{-1}Hg$ for any $g \in G$. (Rmk: For finite grps G, $H \subseteq g^{-1}Hg \iff H = g^{-1}Hg$. since $|H| = |g^{-1}Hg|$)

We will write $H \triangleleft G$ to imply H is normal in G.

By the previous deductions, we show that:

Lemma: Given $N \triangleleft G$, we have

$(\{\text{cosets of } N\}, \cdot)$

forms a grp.

pf: Since $N \triangleleft G$, the operation $\cdot$ is well-defined.

The idendity law / associative law / inverse law

$(e \cdot H) \cdot (g \cdot H) = (g \cdot e)H = gH$ $\quad (g_1H)(g_2H)(g_3H) = (g_1H)[(g_2H)(g_3H)]$ $\quad (g_1H)^{-1} = g_1^{-1}H$

all follows from that of the original grp G.

Def (quotient grp) Given $N \triangleleft G$, then the grp

$(\{\text{cosets of } N\}, \cdot)$

is called the quotient grp of G by N. Denote it by G/N.

Fact: $\left| G/N \right| = \frac{|G|}{|N|} \overset{\text{Lagrange}}{=} [G:N]$

Example: S_3 contains 6 elements.

Flip

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Rotation

$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Identity.

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

Q: 1) $H_1 = \langle \sigma \rangle$ How large is H_1?

Is H_1 normal in $G = S_3$?

2) $H_2 = \langle \tau \rangle$ How large?

Normal?

Ans. 1) $\tau^{-1} \sigma \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H_1$

H_1 not normal

2) $[S_3 : H_2] = 2$. So H_2 must be normal in S_3.

H_2 $\sigma \cdot H_2$ $\sigma H_2 = H_2 \sigma$

Lemma. Given $H \subseteq G$, if $[G:H]=2$, then $H \trianglelefteq G$.

Pf: $H \trianglelefteq G \iff g^{-1}Hg = H \quad \forall g \in G$

$\iff Hg = gH \quad \forall g \in G$

right coset $\{hg \mid h \in H\}$ left coset. $= \{gh \mid h \in H\}$

But if $[G:H]=2$, the $\exists g_1 \in G$. $G = H \cup g_1 H$

$g_2 \in G$. $G = H \cup H \cdot g_2$

so $g_1 H = H \cdot g_2$

Actually $\forall g \notin H$ we have $gH = g_1 H$

$H \cdot g_2 = H \cdot g$

so. $\forall g \in G$. $gH = Hg$. D.

Another method for 2). is to check

$\sigma^{-1} \cdot \tau \cdot \sigma \overset{?}{\in} \langle \tau \rangle$

Lemma: $\forall g \quad gHg^{-1} = H \iff$

$\forall g_i \quad g_i H g_i^{-1} = H$ where g_i are within a set of representatives for left cosets of H.

(i.e. $G = \bigcup_{i=1}^{k} g_i H$, $k = [G:H]$).

Pf. Exercise.

This implies it is enough to check

$$\sigma^{-1}\tau\sigma \in \langle\tau\rangle .$$

After Class Rmk:

The definition on normal subgrps require

$$H \subseteq g^{-1}Hg \quad \forall g \in G$$

notice that by multiplying on both sides. by g and g^{-1}

$$gHg^{-1} \subseteq H,$$

So $\quad H \subseteq g^{-1}Hg \ \forall g \in G \iff H = g^{-1}Hg \ \forall g \in G$

This does not require a "size" argument in the lecture.