MA 434 Thurs. 2/3 ① Read the syllabus!!

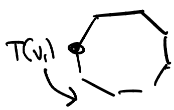
② Generators

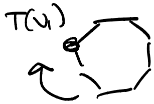
Ⓐ $D_n$ is generated by the smallest rotation $R$ and any reflection $\tau$

counter-clockwise

<u>proof</u> let $v_1, v_2, \dots, v_n$ be a numbering of the vertices of a regular $n$-gon

If $T, S$ are symmetries of the $n$-gon so that $T(v_i) = S(v_i)$ for all $i$ then $T = S$. Thus, given $T(v_1)$ and a choice of clockwise or counter clockwise

e.g. 

OR 


we determine a unique element of $D_n$.

If the vertex numbering is counterclockwise and $T(v_1) = v_j$ then $T = R^j$. If $T$ makes the vertex numbering clockwise, then $\tau T$ makes it counter clockwise. If $\tau \circ T(v_1) = v_k$ then $\tau \circ T = R^k$

$\Rightarrow$ $T = \tau^{-1} R^k = \tau R^k$ b/c $\tau$ is a reflection. Thus $R$ and $\tau$ generate $D_8$.

(b) If $H < G$ and $G$ is a cyclic group then $H$ is cyclic.

Proof By definition, since $G$ is cyclic there exists $g \in G$ s.t. $\forall g' \in G$ $\exists n \in \mathbb{Z}$ with $g' = g^n$.

* This is just "divide $|m|$ by $n$ to get $x$ with remainder $r$"

Note that if $g^n \in H$ then $g^{-n} \in H$ b/c $H$ is a subgroup, so contains all its inverses. Let $n = \min \{a > 0 \mid g^a \in H\}$

Claim If $h \in H$, then $\exists k \in \mathbb{Z}$ with $(g^n)^k = h$ (in which case, $g^n$ generates $H$)

Since $G$ is cyclic, $\exists m \in \mathbb{Z}$ with $g^m = h$
$\Rightarrow g^{|m|} \in H \Rightarrow |m| = 0$ or $|m| > a$
If $|m| = 0$, let $k = 0$. Else suppose $|m| = xn + r$ for some $x \in \mathbb{Z}$, $x \geq 0$ and $0 \leq r < n$. *

So
$$g^{|m|} = g^{xn+r} = g^{xn} g^r \in H$$
$$\Rightarrow (g^n)^{-x} g^{xn} g^r \in H \Rightarrow g^{-xn} g^{xn} g^r \in H$$

Inverses

$$\Rightarrow g^r \in H \Rightarrow r = 0$$
or $r \in \{a > 0 \mid g^a \in H\}$. Since $0 \leq r < n$ we must have $r = 0$ by choice of $n$. $\Rightarrow h = g^{\pm |m|}$
$$= g^{\pm xn} = (g^n)^{\pm x}.$$

k

$\square$

③ Lagrange theorem

Suppose $G$ is a group and $H < G$.

ⓐ There is a bijection $H \to gH$ for all $g \in G$.

<u>proof</u> Let $\phi : H \to gH$ be defined by $\phi(h) = gh$. If $\phi(h_1) = \phi(h_2)$ then $gh_1 = gh_2 \Rightarrow g^{-1}gh_1 = g^{-1}gh_2$

$\Rightarrow h_1 = h_2$

so $\phi$ is injective. If $gh \in gH$ then $\phi(h) = gh$ so $\phi$ is surjective. □

ⓑ If $G$ is finite then

$$|G| = |H|\,[G:H].$$

<u>proof</u> Cosets partition $G$. By ⓐ for every coset $gH$, $|gH| = |H|$.

So $|G| = |H| \underbrace{[G:H]}_{\#\text{ of cosets.}}$.

size of each coset

④ Orbit-Stabilizer Theorem

If $G$ is finite group of symmetries of $X$

then $\forall x \in X$ $\quad |G| = \underbrace{|\text{stab}(x)|}_{\substack{\text{\# of group} \\ \text{elements} \\ \text{that} \\ \text{don't move } x}} \underbrace{|\text{orb}(x)|}_{\substack{\text{number of} \\ \text{Points that} \\ x \text{ can} \\ \text{be moved} \\ \text{to.}}}$

Proof We show that there is a bijection $\text{orb}(x) \to \underbrace{G/\text{stab}(x)}_{\substack{\text{cosets for} \\ \text{stab}(x).}}$

Suppose $y \in \text{orb}(x)$. By def, $\exists\, g \in G$ s.t. $g(x) = y$. Define $\Phi(y) = gH$ where $H = \text{stab}(x)$.

If $\Phi(y_1) = \Phi(y_2)$ then $g_1 H = g_2 H$ where $g_i(x) = y_i$ for $i = 1, 2$. $\Rightarrow \exists\, h \in H$ s.t. $g_1 h = g_2 \Rightarrow g_1^{-1} g_2 \in H. \Rightarrow g_1^{-1} g_2(x) = x$ $\Rightarrow g_2(x) = g_1(x) \Rightarrow y_2 = y_1$. So $\Phi$ is injective.

Conversely if $gH \in G/\text{stab}(x)$ then

$\Phi(g(x)) = gH$ so $\Phi$ is surjective.

The result follows from Lagrange Theorem.

$\square$