Reminder: Midterm 2 next Monday!

Previously in Math 103a

Lagrange's Thm: G group (finite), $H \leq G$, then $\boxed{|H| \text{ divides } |G|.}$

+ many interesting corollaries,

e.g. $a \in G \Rightarrow |a| \mid |G|$

Proof will use cosets: $a \in G$, $H \leq G$

Left coset of $a = \{ah : h \in H\} \subset G$

Right coset of $a = \{ha : h \in H\} \subset G$

Note: $aH = H \iff a \in H$

Thm ① $\boxed{|aH| = |H|}$ $\forall\, a \in G$

② If $a, b \in G$, then either

$\boxed{aH = bH}$ or $\boxed{aH \cap bH = \emptyset}$.

Pf: ① Let $T: H \longrightarrow aH$ given by

$T(h) = ah$

T is onto ✓

T 1-1? If $T(h_1) = T(h_2)$ then

$ah_1 = ah_2 \Rightarrow h_1 = h_2$. (cancellation)

$\therefore T$ is bijective!

(2) Either $a^{-1}b \in H$ or $a^{-1}b \notin H$

If $a^{-1}b \in H$ then $a^{-1}bH = H$

so $bH = aH$

If $a^{-1}b \notin H$, assume, by contradiction,

$\exists\ c \in (aH) \cap (bH)$ i.e. $c = ah_1 = bh_2$

Then $h_1 = a^{-1}bh_2 \Rightarrow h_1h_2^{-1} = a^{-1}b \Rightarrow a^{-1}b \in H$.

$\Rightarrow\Leftarrow$

$\therefore (aH) \cap (bH) = \emptyset$ //Thm.

Lagrange's theorem follows immediately from:

Thm G finite group, $H \leq G$. Then

$\exists\ a_1, a_2 \ldots, a_d \in G$ s.t.

$$G = \bigcup_{i=1}^{d} (a_iH) \quad \text{with } a_iH \cap a_jH = \emptyset \text{ for } i \neq j$$

and $|G| = d|H|$ *

Pf: If $a \in G$, then $a \in aH$. By (2) of previous Thm, choose $a_1, a_2 \ldots, a_d$ so that $a_iH \cap a_jH = \emptyset$, $i \neq j$ and

$a \in G \Rightarrow \exists i$ s.t. $a \in a_iH$.

(check that this can be done!)

Since $|a_iH| = |H|\ \forall i$ by (1) of previous thm, (*) holds. //

Notation: $G:H$ denotes $|G|/|H|$ and H is said to be of **index** $|G|/|H|$ in G.

Ex: A_n is of **index 2** in S_n, since $|S_n| = n!$, $|A_n| = n!/2$.

Some "fun" with cosets: Let $p > 2$ be prime & let G be a group of order $2p$. Show that either $G \approx \mathbb{Z}_{2p}$ or $G \approx D_p$, i.e., up to isomorphism, there are only 2 groups of order $2p$.

Here we go: if $a \in G$, $a \neq e$, then $|a| = 2p$ (1) or $|a| = p$ (2) or $|a| = 2$ (3)

since $|a| \mid |G|$. If $\exists\ a \in G$ satisfying (1), then G is cyclic and $G \approx \mathbb{Z}_{2p}$. (Why?). Then done. Claim $\exists\ a \in G$ with $|a| = p$. If not $|a| = 2\ \forall\ a \neq e$,

If $a_1, a_2 \in G$, $a_1 \neq e$, $a_2 \neq a_1$, $|a_1| = |a_2| = 2$ & $|a_1 a_2| = 2$

then $(a_1 a_2)^2 = e = a_1^2 a_2^2$

$a_1 a_2 a_1 a_2 = a_1^2 a_2^2$

$\Rightarrow a_2 a_1 = a_1 a_2$

$\therefore \{e, a_1, a_2, a_1 a_2\}$ is a subgroup of order 4

$\Rightarrow\Leftarrow$ since $4 \nmid 2p$.

Since not all $a \neq e$ one of order 2, $\exists\, a \in G$ with $|a| = p$. By above thms,

$$G = \langle a \rangle \cup b\langle a \rangle$$

for any $b \notin \langle a \rangle$. In particular, $b^2 \in \langle a \rangle$ or $b^2 \in b\langle a \rangle$

If $b^2 \in b\langle a \rangle$, then $b^2 = ba^j \Rightarrow b \in \langle a \rangle$ impossible.

$\therefore b^2 = a^j$ for some j, $0 \leq j < p$. Must have $j = 0$

(otherwise $\langle b \rangle \supset \langle a^j \rangle = \langle a \rangle \Rightarrow \langle b \rangle = G$, impossible

why?) $\therefore$ $b \notin \langle a \rangle \Rightarrow |b| = 2$.

In particular, $|ba| = 2$

$$ba = (ba)^{-1} = a^{-1}b^{-1} = a^{-1}b = a^{p-1}b$$

$ba = a^{p-1}b$ determines Cayley Table for G!

$\therefore$ if $G \not\cong \mathbb{Z}_{2p}$, must have $G \cong D_p$.

Stabilizers & orbits

Def S a set & G a group of permutations of S. (we say G acts on S)

For $i \in S$, let $\text{stab}_G(i) = \{\varphi \in G : \varphi(i) = i\} \subset G$

stabilizer of i in G.

Ex: $S = \{1, 2, 3\}$ $\text{stab}_{S_3}(2) = \{(1)\ (13)\}$.

The G-orbit of $i \in S$ is defined by

$$\text{orb}_G(i) = \{\varphi(i) : \varphi \in G\} \subseteq S$$

Ex: If $S = \{1,2,3\}$, $G = S_3$, then

$\text{orb}_G(2) = \{1,2,3\}$, since

$1 = \varphi_1(2)$, $\varphi_1 = (1,2)$

$2 = \varphi_2(2)$ $\varphi_2 = (1)$

$3 = \varphi_3(2)$ $\varphi_3 = (2,3)$

Important: $\text{stab}_G(i)$ is a group! (check it!)

Observation: $|\text{stab}_{S_3}(2)| \times |\text{Orb}_{S_3}(2)|$

$= 2 \times 3 = 6 = |S_3|$ Coincidence?

No! Theorem!

Orbit-Stabilizer Thm. Let G be a group of permutations of a finite set S. Then

$\forall i \in S$, $\boxed{|G| = |\text{stab}_G(i)| \cdot |\text{orb}_G(i)|}$

Pf Let $H = \text{stab}_G(i)$. Then

$|G|/|H| = \#$ of left cosets of $\text{stab}(i)$

Claim $\exists$ 1-1 correspondence

$\boxed{\text{left cosets of } \text{stab}_G(i)} \longleftrightarrow \boxed{\text{orb}_G(i)}$

Put $T(\varphi H) = \varphi(i)$

Well defined? If $\varphi_1 H = \varphi_2 H$ then $\varphi_1^{-1}\varphi \in H$

$\Rightarrow \varphi_1^{-1}\varphi_2(i) = i$ $\therefore \varphi_2(i) = \varphi_1(i)$

1-1? $\varphi_1(i) = \varphi_2(i) \Leftrightarrow \varphi_2^{-1}\varphi_1(i) = e$

$\Leftrightarrow \varphi_2^{-1}\varphi_1 \in H \Leftrightarrow \varphi_1 H = \varphi_2 H.$

onto? $\varphi(i) = T(\varphi H)$ //

Ex 1. Another way to check $|S_n| = n!$.

By induction. OK for $n=1$, assume for $n-1$.

Let $H_n = \{\sigma \in S_n : \sigma(n) = n\}$. Then $|H_n| = |S_{n-1}|$

$H_n = \text{stab}_{S_n}(n)$, $\text{orb}_{S_n}(n) = \{1, 2, \ldots, n\}$

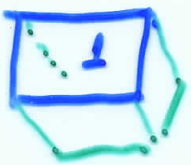
By Orbit-Stabilizer theorem,

$$|S_n| = |H_n|\,|\text{orb}_{S_n}(n)| = (n-1)!\, n = n!$$

↑ by induction

Ex 2. Rotations of a cube. How many are there?

Think of a rotation as a permutation of faces. Then $G \subset S_6$ permuting $\{1,2,3,4,5,6\}$



6 faces

Let $H = \{g \in G : g(1) = 1\} = \text{stab}_G(1)$

$|H|$ = number of rotations of face 1

$\therefore |H| = 4$

$\text{orb}_G(1) = \{1, 2, 3, 4, 5, 6\}$ $\therefore |\text{orb}_{S_6}(1)| = 6$

(Can rotate 1 to any other face)

By orbit-stabilizer thm,

$$|G| = |H| \times |\text{orb}_G(1)| = 4 \times 6 = 24. \;//$$