Math 122 Wednesday, November 9

Last time: Conjugacy classes in S_n $\longleftrightarrow$ lengths of cycles in decomposition of g
$\longleftrightarrow$ partition of $n = i_1 + \cdots + i_k$

e.g. $g = (123)(4567)(8)$ in S_8 $1+3+4=8$
$g^{-1} = (132)(4765)(8)$

Conclude: g is conjugate to g^{-1} in S_n!
(not true in most groups)

Moreover If g has order $n = \text{lcm}(i_k)$
and a is any integer prime to n (so prime to each i_k), then g^a is conjugate to g in S_n.
Hence any generator of $\langle g \rangle$ is conjugate to g in S_n.

Note: this is not true in A_n.

ex: $G = A_5$ has cycles of type: e, (abc), $(ab)(cd)$, $(abcde)$ but these are not conjugacy classes. Do have (abc) conjugate to (acb) (use $(de)(bc)$). But $g = (abcde)$ not conjugate to $g^2 = (acebd)$. Here h must be $(bced)g^q$, which are all odd.

Conjugacy classes in A_5:
1 element of order 1
20 elements of order 3 → $\exists$ 20 elements of order 3 $\Rightarrow$ $\exists$ 10 Sylow-3 subgroups all conjugate by Sylow thms. A_5 (abc) conjugate to $(abc)^2 = (acb)$ each element is conjugate to each other.
15 elements of order 2 → $\exists$ 5 sylow-2 subgroups (each of order 4), all conjugate. Remains to show that elements within a Sylow-2 subgroup are conjugate (exercise)
12+12=24 elements of order 4 (two conjugacy classes)
g, g^{11} not conjugate to g^2, g^3

Conclusion 5 conjugacy classes in A_5 of size $1, 15, 20, 12, 12$

Cor A_5 is a simple group (i.e. if $H \trianglelefteq A_5$ then either $H = \{e\}$ or $H = G$)
Pf: If $H \trianglelefteq A_5$ then $H = \bigcup$ (conj classes) where one of these must be $\{e\}$.
So $\#H = \sum_{\text{some conj. classes}} \#\text{classes (including } \{e\})$. But no non-trivial sum of 1 and some subset of $\{15, 20, 12, 12\}$ divides 60.

Similarly can show that A_6 is simple (exercise). $\exists$ 7 conjugacy classes:

order	1	3	3	2	4	5	5
size	1	40	40	45	90	72	72
cycle	e	(abc)	$(abc)(def)$	$(ab)(cd)$	$(abcd)(ef)$	$(abcde) = g$	g^2

Thm A_n is a simple group for all $n \geq 5$. (Idea: 1) $A_5 < A_6 < A_7 < \cdots < A_n$
2) A_n is generated by 3-cycles which are conjugate

Pf: Every $g \in A_n$ is a product of an even number of transpositions $(ab)(bc) = (abc)$, $(ab)(cd) = (cba)(acd)$. All of these 3-cycles are conjugate by the construction we used for A_5 (basically there is enough room to permute fixed points if needed). Will need two lemmas to finish this proof. provided $n \geq 5$

Lemma II $H \trianglelefteq A_n$ and $(abc) \in H \Rightarrow H = A_n$

Pf: $H \trianglelefteq A_n \Rightarrow H$ contains all conjugates of $(abc) \Rightarrow$ contains all generators of $A_n \Rightarrow$ contains A_n.

Lemma II $H \trianglelefteq A_n$ and $H \cap A_k \neq e$ for some $5 \leq k \leq n$ then $H = A_n$.

Pf: By induction on $n \geq 5$ (true for $n = 5, 6$ by simplicity). Claim: $H \cap A_k \trianglelefteq A_k$ so if $H \cap A_k \neq \{e\}$ then $H \cap A_k = A_k$ (as A_k simple for $k \leq n$ by inductive hypothesis) $\Rightarrow$ H contains A_k so contains a 3-cycle in $A_k \Rightarrow H = A_n$.

To finish take $H \trianglelefteq A_n$, $H \neq \{e\} \Rightarrow \exists\ h \neq e$ in $H \Rightarrow h(i) = j$. Take a 3-cycle g in A_n such that $g(i) = i$, $g(j) \neq j$. So $ghg^{-1}h^{-1} \neq e$ in A_n as $[g,h](j) = g(j) \neq j$. Hence $gh \neq hg$ in A_n (again $gh(i) = g(j) \neq hg(i) = j$). But $[g,h] = (ghg^{-1})h^{-1} \in H$ as H is normal. Also $[g,h]$ moves at most six letters as it is a product of two three-cycles g, and hgh^{-1}. So $[g,h] \neq e \in H \cap A_6 \Rightarrow H \supset A_6$ by simplicity of $A_6 \Rightarrow$ H contains a 3-cycle $\Rightarrow H = A_n$. QED

So we have found an infinite chain of simple groups $A_5 \subset A_6 \subset A_7 \subset \cdots$
One more infinite chain, p prime ≥ 3

Consider $GL_2(\mathbb{Z}/p\mathbb{Z}) \supset SL_2(\mathbb{Z}/p\mathbb{Z})$ the kernel of the determinant homomorphism.
The center of $SL_2(\mathbb{Z}/p\mathbb{Z})$ is $\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a^2 \equiv 1 \pmod p\right\} \Rightarrow a \equiv \pm 1 \pmod p$.

$\left(\#GL_2(\mathbb{Z}/p) = (p^2-1)(p^2-p) = (p^2-1)(p-1)p,\ [GL_2(\mathbb{Z}/p) : SL_2(\mathbb{Z}/p)] = (p-1) \Rightarrow \#SL_2(\mathbb{Z}/p) = (p^2-1)p\right)$

$PSL_2(p) = SL_2(\mathbb{Z}/p\mathbb{Z}) \Big/ \left\langle \begin{pmatrix} +1 & 0 \\ 0 & +1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$ So $\#PSL_2(\mathbb{Z}/p) = \frac{(p^2-1)p}{2}$

Can show $PSL_2(5) \simeq A_5$ and is simple for $p \geq 5$ (Note $\#PSL_2(5) = \frac{(5^2-1)5}{2} = 60$)

Rubik's cube Each move gives a permutation of 6 centers, 8 corners, 12 edges
$g \in S_6 \times S_8 \times S_{12}$. But really the centers are fixed so $g = (e, g_8, g_{12})$. $G \subset S_8 \times S_{12} \subset S_{20}$.

Also $G \subset A_{20}$ as each generator is the product of two 4-cycles = even. So $G = A_{20} \cap (S_8 \times S_{12})$.

Can solve the cube by producing 3-cycles of corners and 3-cycles of edges as they generate $A_{20} \cap (S_8 \times S_{12})$. How can you do this? Use a commutator $[g,h]$ where $\mathrm{Supp}(g) \cap \mathrm{Supp}(h)$ is a single edge or corner.