Math 122 Monday, November 14

Last time: G = group of permutations of cube $\hookrightarrow S_8 \times S_{12} \hookrightarrow S_{20}$
6 basic generators $h \longmapsto$ (4-cycle) $\times$ (4-cycle) $\in A_{20}$

Claim $G = A_{20} \cap (S_8 \times S_{12}) \supsetneq A_8 \times A_{12} \leftarrow$ Show this subgroup is contained in G by producing elements (3-cycle) $\times e$, $e \times$ (3-cycle) as commutators.
But can also get (2-cycle) $\times$ (2-cycle), not generated by the commutators as it's in the non-trivial coset of $A_8 \times A_{12}$. Ok though because so are the 6 basic generators.

Groups definition + examples $GL_n(\mathbb{R})$, $GL_n(F) = \mathrm{Aut}(V)$, S_n, $\mathrm{Aut}(S)$, C_n, $D_n \leftarrow$ dihedral of order $2n$
homomorphisms, kernel, image, $H \subset G$ subgroup, $H \triangleleft G \Rightarrow$ define G/H
$\# G = \# H \cdot \# G/H$, $\det: GL_n(F) \to F^*$, $\mathrm{sign}: S_n \to \langle \pm 1 \rangle$ (kernels $= SL_n(F)$, A_n respectively)

If C_n is cyclic of order n with generator g $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} C_n$ $a \mapsto g^a$
There are $\varphi(n)$ generators g^a for each a s.t. $\gcd(a,n) = 1$.

First Isomorphism Thm $G \xrightarrow{f} G'$ $G/\ker f \simeq \mathrm{Im} f \subset G'$

Theory of Vector Spaces over a field $F \leftarrow \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}$, $F - \{0\}$ have multiplicative inverses.
V finite dimensional $\longleftrightarrow$ finite spanning set, linear independence, $\#$ lin indep $\leq \#$ spanning set
Basis, $\dim V = \#$ elements in a basis

$T: V \to W$ a linear transformation of F-vector spaces. Choose bases of V and $W \leadsto$ matrix A for T.
Char poly $f(x)$ of a transformation $T: V \to V$ $f(x) = \det(xI - T|V) = x^n - \mathrm{Tr}(T)x^{n-1} + \cdots \pm \det(T)$
Roots of $f(x) \longleftrightarrow$ eigenvalues of T, $Tv = cv$ $v \neq 0$ in V.

Back to $F = \mathbb{R}$, put a dot product (inner product) on V, $T: V \to V$ with $\langle Tv, Tw \rangle = \langle v, w \rangle \Longrightarrow$ preserves length $\|v\| = \sqrt{\langle v, v \rangle}$ and angle. These are called orthogonal transformations.
$V \simeq \mathbb{R}^n$ using an orthonormal basis. A = matrix of T satisfies ${}^tA \cdot A = I$.

Group of motions $M(n)$ of $\mathbb{R}^n \xrightarrow{m} \mathbb{R}^n$ $\|mv - mw\| = \|v - w\|$, $m(v) = Av + b$, $O(n) \subset M(n)$ preserves the origin, $\mathbb{R}^n \subset M(n)$ the translations $m(v) = v + b$. Finite subgroups of $SO(2)$ ($\simeq C_n$) and $O(2)$ ($\simeq C_n$ and D_n) and discrete subgroups of $M(2)$. Lattices $L = G \cap \mathbb{R}^2 = \begin{cases} 0 & \\ \mathbb{Z}a & a \neq 0 \\ \mathbb{Z}a + \mathbb{Z}b & \{a,b\} \text{ a basis} \end{cases}$
$\bar{G}$ = image of G in $O(2)$ preserves L.

G acting on a set S, $g(s) = s'$ in S, $e(s) = s$, $gh(s) = g(h(s))$. Equivalent to $f: G \to \mathrm{Aut}(S)$
$g \mapsto$ permutation of S given by $s \mapsto g(s)$ a group homomorphism.

e.g. $G = GL_n(\mathbb{R})$ acts on $S = \mathbb{R}^n$ by linear maps. G acts on any S trivially $g(s) = s$ $\forall g\ \forall s$.
$M(2)$ acts on $\mathbb{R}^2$ and on triangle (A, B, C) in $\mathbb{R}^2$.

G can act on $S=G$ 1) by left multiplication $g(s)=gs$ 2) by conjugation $g(s)=gsg^{-1}$.
$O_s=$ orbit of $s=\{s'=g(s): g\in G\}\subset S$, $G_s=$ stabalizer of $s=\{g: g(s)=s\}\subset G$
$S=\cup O_s$ a disjoint union over orbits. If $s'=g(s)$, $O_s=O_{s'}\simeq G/G_s$ as a set $g(s)\leftrightarrow gG_s$
$G_{s'}=gG_sg^{-1}$ a conjugate subgroup of G. When G acts on itself by conjugation,
$O_s=$ Conjugacy class of s, $G_s=$ centralizer of s. When G acts on G by left mult, $O_e=G$, $G_e=\{e\}$.
transitive

ex $M(2)$ acts on triangles, $O_{ABC}=$ all triangles congruent to ABC, $G_{ABC}=\begin{cases} e & \text{mostly} \\ S_2 & \text{if isosceles} \\ S_3 & \text{if equilateral}\end{cases}$

Counting formula for $\#S=\sum_{\text{orbits}}\#G/\#G_s$. When applied to action of G on itself by conjugation,
$\#G=\sum_{\text{conj classes}}\#G/\#G_s=\sum_{s\in Z=\text{center of }G} 1+\sum_{\text{conj classes where }G_s\neq G}(\text{divisors of }G>1)$. Called the class equation:
$\#G=\#Z+\sum_{\text{non-central classes}}\#G/\#G_s$

p-group G $\#G=p^a$ (includes the groups of order p)
1) $Z(G)\neq e$ when G a p-group
2) G of order p^2 is abelian (either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}+\mathbb{Z}/p\mathbb{Z}$)
3) G non-abelian of order $p^3\Rightarrow Z(G)$ has order p.

Sylow-p subgroups of a finite group G $\#G=p^n m$ $\gcd(m,p)=1$. $\#H_p=p^n$ a Sylow-p subgroup.
1) Sylow p-subgroups always exist
2) All conjugate in G
3) # of conjugates divides m and is congruent to $1 \pmod p$. $\Rightarrow$ If $\#=1$ then $H_p\triangleleft G$.

Method A p-group G acting on a set S of order prime to p has a fixed point (an orbit $O_s=\{s\}$ of one element, $G_s=G$).

Applications to groups of order $=pq$ $p<q$. $H_q\triangleleft G$ always. If $H_p, H_q\triangleleft G$ then $G\simeq\mathbb{Z}/pq\mathbb{Z}$
H_p is normal unless $q=1 \pmod p$ when you can get q Sylow-p subgroups.
If H_p is not normal, can have non-abelian groups (e.g. D_q of order $2q$).

Analysis of $g\in S_n$, $g=(\ )\cdots(\ )$ disjoint cycle decomposition determines order, sign, and conjugacy class of g in S_n (not always in A_n). $g=(ab)$ transpositions, generate S_n,
$g=(abc)$ 3-cycles generate A_n, $[g,h]=\begin{cases} e & \mathrm{Supp}(g)\cap\mathrm{Supp}(h)=\phi \\ \text{3-cycle} & \text{if } \mathrm{Supp}(g)\cap\mathrm{Supp}(h)=\text{one point}\end{cases}$