Math 741

9/4 Groups (finite & infinite) — #Assigned & due R.

↑ change! for quals. — Takehome final — emph. on finite gps ↓

Linear & Multi-Lin. alg. — Lang, Algebra, Isaacs

Intro. to Representation Theory — Dummit & Foote, Hungerford, Jacobson, Basic Algebra

General Ring Theory — Lary & careful

[742: Commutative Alg (Comm Rings)]

"Groups are sets w/ operations"

Ex: Matrix Groups

Given 2 $^{2\times2}$ matrices A, B, I can make a 3rd - the product AB.

$$\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\-1&1\end{bmatrix}=\begin{bmatrix}0&1\\-1&1\end{bmatrix}$$

There is also a product BA, which may not be the same.

→ $\begin{bmatrix}1&0\\0&1\end{bmatrix}=E$ = the identity matrix has the property $EA=AE=A \quad \forall A$.

→ Can also invert matrices: A^{-1} is a matrix s.t. $A^{-1}A=AA^{-1}=E$

If $A=\begin{bmatrix}1&1\\0&1\end{bmatrix}$, then $A^{-1}=\begin{bmatrix}1&-1\\0&1\end{bmatrix}$

Inversion is useful for solving eqns in matrices.

ex: $AB=C$ B, C known; solve for A.

$ABB^{-1}=CB^{-1}$ * Wait! LHS should be $(AB)B^{-1}$. But I wanted $A(BB^{-1})$.

$AE=CB^{-1}$

$A=CB^{-1}$

→ $(AB)B^{-1}=A(BB^{-1})$ bc matrix prod. is associative.

→ Other problem: How do I know B has an inv?

ex: $B=\begin{bmatrix}0&0\\0&0\end{bmatrix}$ has no inv. In this case $AB=\begin{bmatrix}1&2\\3&4\end{bmatrix}$ has no sol'n.

We call a matrix invertible if it has an inv.

Def: A group is a set G endowed w/ a binary operation, $G \times G \to G$, with the following properties:

(i) There is an identity $e \in G$ s.t. $eg = ge = g$ $\forall g \in G$.

(ii) Every elt $g \in G$ has an inverse, g^{-1}, which satisfies $gg^{-1} = g^{-1}g = e$

(iii) The operation is associative:

$(g_1 g_2) g_3 = g_1 (g_2 g_3)$ $\forall g_1, g_2, g_3 \in G$.

→ Can write $g_1 g_2 g_3$.

[A monoid or semigroup removes the condition that all elts have inverses].

Remark: The inverse of g is unique.

Pf: Suppose h & h' are inv. to g.

$gh = gh' = e$

$hgh = hgh' = he$

$eh = eh' = h$

$h = h' = h$

Ex: Let $GL_2(\mathbb{R})$ be the set of 2×2 matrices w/ real coefficients which are invertible, endowed w/ the oper. of matrix product. $GL_2(\mathbb{R})$ is a gp called the general linear gp (of deg. 2).

Pf: NTS $GL_2(\mathbb{R})$ has an op. given by matrix prod. ie, if A, B are invert, then AB is inv. We prove this by construction.

$ABB^{-1}A^{-1} = AA^{-1} = e$

This shows that in any gp $(gh)^{-1} = h^{-1}g^{-1}$.

Ex's: ① $GL_n(\mathbb{R})$

② $GL_n(\mathbb{Z})$ remark: $\begin{bmatrix} 1 & 1 \\ 1 & \end{bmatrix} \in GL_2(\mathbb{Z})$, but $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \notin GL_2(\mathbb{Z})$ b/c $\begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{bmatrix} \notin GL_2(\mathbb{Z})$ ↑ the inv.

③ $\mathbb{R}$, endowed w/ addition. $(e=0)$

④ $\mathbb{Z}$, op. = +

⑤ $\mathbb{R}^*$, op. = mult. set = $\mathbb{R}-0$ $(\mathbb{R}^\times)$

↑ $\mathbb{R}-0$ w/ mult

⑥ $\mathbb{Z}^*$, op = mult. set = invert. elts of $\mathbb{Z} = \{-1, 1\}$ $(\mathbb{Z}^\times)$

⑦ Let $m \in \mathbb{Z}-0$, then $\mathbb{Z}/m\mathbb{Z}$ is the gp of ints mod m, op = add.

ex: if $m=5$, $\{0,1,2,3,4\}$, $2+3=0$, $3+4=7=2$, ...

⑧ Let k a pos. int. Define the <u>free gp of rank k</u>, F_k.

Start w/ symbols $\gamma_1, \dots, \gamma_k$
$\gamma_1^{-1}, \dots, \gamma_k^{-1}$

Set of elts of F_k is the set of finite-length reduced words in these symbols. (eg. $\gamma_3\gamma_5^{-1}\gamma_1^{-1}\gamma_2$ = word.), where reduced = γ_i & γ_i^{-1} are never adjacent.

(Note: countably infinite gp) "the empty word" $\in F_k$.

Operation is concatenation (+ reduction)

id = empty word

inv = given by rule for matrices, iterated
$(\gamma_1\gamma_2^3\gamma_3)^{-1} = \gamma_3^{-1}\gamma_2^{-3}\gamma_1^{-1}$

assoc = true but we won't prove now.

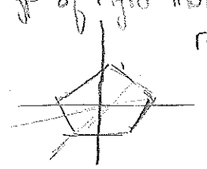
$\gamma_1\gamma_2 \neq \gamma_2\gamma_1$.

⑨ The gp of "rigid motions of $\mathbb{R}^2$" — transf. of $\mathbb{R}^2$ that preserve dist & $\measuredangle$s : transl, rotate, flip/reflect in line

⑩ The gp of rigid motions which preserve zero in $\mathbb{R}^2$. (rotate, reflect)

⑪ The gp of rigid motions preserving polygon P.

op = composition



ry-axis, $R_{2\pi/5}$
identity

5 rotations
5 reflections (thru each vertex)

Called the <u>dihedral gp</u> of order 10, D_5.

(12) Given a top sp. X, a homeomorphism $f: X \to X$ is a cont. fcn w/ a cont. inv. The homeomorphism from X to X form a gp w/ composition.

(13) Key example: X is a finite set S. The set of bijections $f: S \to S$ forms a gp. (A permutation gp)

9/6 The Symmetric Group HW due 9/20 on wiki

Let S be a finite set. $\mathrm{Sym}(S)$, (the symm. gp on S, consists of:

{bijections: $S \to S$} w/ op = composition.

↑ also called permutations.

$\mathrm{Sym}(\{1,\dots,n\})$ is usually called S_n, the symm. gp on n letters.

- S_n is finite b/c S finite.

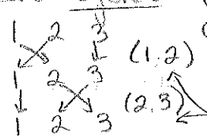
What is $|S_n|$, the order of S_n?

5 choices for $f(1)$
4 choices for $f(2)$
⋮
} 5! choices

$|S_n| = n!$

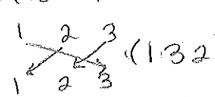
- Cycle notation: To write down a permutation, we usually record cycles: $(1\,3\,2\,5)$ or $(1\,3\,2\,5)(4)$ or $(2\,5\,1\,3)$ or etc.

Ex:



$(1\,2)$
$(2\,3)$
transposition - switch 2 letters, leave rest alone

composition.



$(1\,3\,2)$

in S_3: $(12), (13), (23)$

$(2\,3)(1\,2) = (1\,3\,2)$

- Cycle notation makes the product non-transparent, but it is good for revealing other props of perms.

Def: $g \in G$ a gp. The order of g is the smallest pos. int. n s.t. $g^n = e$.

Cf: if no such n exists, g has infinite order.

Remark: If G finite, then every $g \in G$ has finite order, at most $|G|$

Pf: $g, g^2, g^3, g^4, g^5, \ldots, g^{|G|+1}$

By Pigeonhole ($\exists$ $i \neq j$ $\in \{1, \ldots, |G|+1\}$ s.t.) (Pigeonhole Principle)

$g^i = g^j \Rightarrow g^{-i} g^i = g^{-i} g^j \Rightarrow e = g^{j-i}$ (wlog, $j > i$)

Q: Is this bound ever achieved? (ie, Is this Remark sharp?)

A: Yes; think of an example.

Ex: a) The order of $(1\,3\,2\,5)$ is 4. (b/c there are 4 elts)

b) The order of $(1\,3\,2)(4\,5)$ is 6.

$g^3 = (1)(2)(3)(4\,5)$

Thm: More generally, the order of an elt of S_n, is the lcm of the cycle lengths.

Try to prove this lcm must divide $n!$

Homomorphisms

Def: G_1, G_2 gps. A homomorphism $f: G_1 \to G_2$ is a map from the elts of G_1 to the elts of G_2 such that $f(g_1 g_1') = f(g_1) f(g_1')$ $\forall g_1, g_1' \in G_1$.

$$\begin{array}{ccccc} G_1 \times G_1 & \xrightarrow{\cdot_{G_1}} & G_1 & \xrightarrow{f} & G_2 \\ {\scriptstyle f \times f}\downarrow & & & \nearrow_{\cdot_{G_2}} & \\ G_2 \times G_2 & & & & \end{array}$$

- f is a homomorphism $\Leftrightarrow$ this diagram commutes. ie, given an input in $G_1 \times G_1$, the output in G_2 does not depend on the path chosen.

Examples

① $\det: GL_n(\mathbb{R}) \to \mathbb{R}^*$ b/c $\det(AB) = \det(A)\det(B)$

② similarly $GL_n(\mathbb{Z}) \to \mathbb{Z}^*$ "$\{\pm 1\}$"

③ $i: GL_n(\mathbb{Z}) \hookrightarrow GL_n(\mathbb{R})$ (inclusion matrix) • injective, not surjective.

$i\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ Not same as id fcn.

④ Reduction mod p

$\text{red}_p: \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ b/c $(a+b) \bmod p = a \bmod p + b \bmod p$

$n \longmapsto n \bmod p$ • Surjective, not injective

⑤ Let G a gp & let's think about homom's from
$F_k \to G$ (Free gp on k letters to G)

Prop: There is a bijection;

$$\{\mathrm{Hom}(F_k, G)\} \ni f$$
$$\Phi \downarrow \quad \updownarrow$$
$$G^k \ (\text{i.e. } \underbrace{G \times \cdots \times G}_{k})$$

given by $f \longmapsto (f(\gamma_1), \ldots, f(\gamma_k))$ $\quad (\gamma_i \in F_k)$

Pf: injective: Suppose f, g have $\Phi(f) = \Phi(g)$. Then
$f(\gamma_i) = g(\gamma_i)$ $\forall \gamma_i \Rightarrow f(\gamma_i^{-1}) = g(\gamma_i)^{-1} = g(\gamma_i^{-1})$.
If $x \in F_k$, $x = \gamma_{i_1}^{\pm} \gamma_{i_2}^{\pm} \gamma_{i_3}^{\pm} \cdots \gamma_{i_N}^{\pm}$, then
$f(x) = f(\gamma_{i_1})^{\pm} \cdots f(\gamma_{i_N})^{\pm}$
$g(x) = g(\gamma_{i_1})^{\pm} \cdots g(\gamma_{i_N})^{\pm}$ $\Big\} =$
So $f(x) = g(x)$ $\forall x \in F_k$

Surjective: NTS given k-tuple, $\exists f: F_k \to G$ s.t.
$f(\gamma_i) = g_i$ $\forall g_i$. What is this f? It sends
$\gamma_{i_1}^{\pm} \cdots \gamma_{i_N}^{\pm}$ to $(g_{i_1}^{\pm}, \ldots, g_{i_N}^{\pm})$
To check this is a homom, just need to check that
$f(\gamma_{i_1}^{\pm} \cdots \gamma_{i_N}^{\pm} \gamma_{j_1}^{\pm} \cdots \gamma_{j_N}^{\pm}) = f(\gamma_{i_1}^{\pm} \cdots \gamma_{i_N}^{\pm}) f(\gamma_{j_1}^{\pm} \cdots \gamma_{j_N}^{\pm})$
$= g_{i_1}^{\pm} \cdots g_{i_N}^{\pm} g_{j_1}^{\pm} \cdots g_{i_N}^{\pm}$

⑥ $f: \mathbb{Z}^* \to \mathbb{Z}/2\mathbb{Z}$ defined by $f(1) = 0$ $\quad [f(e) = e]$
$f(-1) = 1$

Check $f(-1 \cdot -1) = f(-1) + f(-1)$
$f(1) = 0$

- injective & surjective $\Rightarrow$ bijective gp hom. and as such is an isomorphism of gps.

Def: An isomorphism $f: G \to H$ gps is a homomorphism which admits an inverse homomorphism $f^{-1}: H \to G$,
i.e., $f^{-1} \circ f = id_G: G \to G$
$f \circ f^{-1} = id_H: H \to H$

Remark: A bijective hom. is an isomorphism. Namely, let $f^{-1}(h)$ be the unique $g \in G$ s.t. $f(g) = h$.

Why don't we define isom. as a bijection?
What if we defined an isom. of top. sps. to be a continuous map which is bijective?
Let $X = [0, 2\pi)$ $Y =$ unit $\odot$
$f: X \to Y$
$\theta \longmapsto (\cos\theta, \sin\theta)$ f is cont. & bijective.
But $X \not\cong Y$, topological
In top, a homeom. is a cont. map w/ a cont. inv.
We say an isom. is a hom. whose inv. is also a hom.
Analogy: Q: Is this f invertible?
A: If we think of f as a map of sets, yes.
But, if we think of f as a cont. map, no.
(Similar to is $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ invertible? B/c if it's over $\mathbb{R}$, yes. If it's over $\mathbb{Z}$, no.)

9/11 $\mathbb{Z}^\times \cong \mathbb{Z}/2\mathbb{Z}$. Any gp of 2 elts is isom. to $\mathbb{Z}/2\mathbb{Z}$
A hom. $f: G \to H$ is a fcn satisfying
$f(g_1 g_2) = f(g_1) f(g_2) \quad \forall g_1, g_2 \in G$
Remark: Suppose $g_1, \dots, g_k$ generate G. (ie, every elt of G can be written as a word in g_i, g_i^{-1})
Or equivalently, there is no proper subgp of G containing $g_1, \dots, g_k$. We say a gp is finitely generated if $\exists$ a finite generating set.
Non-ex: • $GL_n(\mathbb{R})$ ← uncountably inf. but list of words is countably inf.
* • $\mathbb{Q}/\mathbb{Z}$ (prove not finitely gen.)
If G is generated by $g_1, \dots, g_k$: $G = \langle g_1, \dots, g_k \rangle$, then to specify $f: G \to H$, we need only to specify what f does to generators. $[f(g_1), f(g_2), \dots, f(g_k)]$.
B/c $f(g_1 g_2) = f(g_1) f(g_2)$, etc.

But, there's no guarantee that ∃ hom. f w/ desired $f(g_1), \dots, f(g_k)$.

Silly ex: $\mathbb{Z}/2\mathbb{Z}$ is generated by 1.

$f: \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ s.t. $f(1) = 1$ (↑ $1 \bmod 2$)

But ∄!

B/c $f(1 \bmod 2 + 1 \bmod 2) = f(1 \bmod 2) + f(1 \bmod 2)$

$f(0) = 1 + 1$

$= 0 = 2$

↑

b/c hom. must take id to id.

elts of finite order must be taken to elts. of same finite order

Any hom.: $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ is the zero hom.

Ex: $SL_2(\mathbb{Z})$ (2×2 w/ det 1) is generated by

$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$

Can we map $f: SL_2(\mathbb{Z}) \to F_2 = F\langle r_1, r_2\rangle$

w/ $f\left(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\right) = r_1$

$f\left(\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\right) = r_2$? No.

$\left(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)^{-1}\right)^6 = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) = e$

So $\left(f\left(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\right) f\left(\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\right)^{-1}\right)^6 = e$

$\underbrace{r_1 r_2^{-1} \cdots r_1 r_2^{-1}}_{6} \neq e_{F_2}$

Relations btwn generators need to preserved under a hom.

Subgroups: A subset H of G is a subgp if it is closed under mult. & inversion. ⇒ H itself is a gp.

Examples:

1. $3\mathbb{Z} \subset \mathbb{Z}$ (Remark, $f: \mathbb{Z} \xrightarrow{\cong} 3\mathbb{Z}$, $1 \mapsto 3$, $n \mapsto 3n$ an iso. this hom. induces the isom, so $3\mathbb{Z} \simeq \mathbb{Z}$)
2. $\left\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right\} \subset SL_2(\mathbb{Z})$ $(\simeq \mathbb{Z}/2\mathbb{Z})$
3. $SL_2(\mathbb{Z}) \subset SL_2(\mathbb{R})$
4. rigid motions preserving ⬠ ⊂ rigid motions
5. permutations of $\{1, \dots, 5\}$ which fix 1 ⊂ S_5

↑ stabilizer of 1

↑ subgp of a gp that fixes smth.

Let $H \subset S_5$ be the stabilizer of 1
Note that H can be thought of as the perm. gp. on $\{2,3,4,5\}$:
$H \simeq S_4$.

Consider the following subsets $\subset S_5$:
- Permutations sending 1 to 1 (H)
- Permutations sending 1 to 2
- ⋮
- Perms sending 1 to 5

} decomp. of gp into 5 disjoint subsets.

:=Coset decomposition.

Aside: Could consider stabilizer of $\{1,2\} \subset S_5$ would contain things like (34) [fixes both $1 \& 2$] & $(12)(34)$ [flips $1 \& 2$]
stabilizer of $(1,2)$ would only contain things like (34)

Def: Let $H \subset G$ a subgp. A *left coset* of H in G is a subset of G of the form
$gH = \{gh \mid h \in H\}$ for some $g \in G$.
Similarly a *right coset* is $Hg = \{hg \mid h \in H\}$

- The subsets of S_5 above is a left coset:
$1 \to 2$: $(123)H$: $\forall h \in H$, $(123)h = 1 \to 1 \to 2$

* Show if $g \in 1 \to 2$, prove $g \in (123)H$
→ could have been $(12)H = (H123)H =$ etc.

Lemma: Suppose $g' \in gH$. Then $g'H = gH$.
Pf: B/c $g' \in gH$, so $g' = gh_0$, $h_0 \in H$. So any elt of gH is $gh = g'\underbrace{h_0^{-1}h}_{\in H}$. Similarly any elt of $g'H$ is $g'h = gh_0h \in gH$.

Prop: $H \subset G$. Then G is a disjoint union of the left (right) cosets of H.
Pf: Every $g \in G$ lies in gH, so union of cosets $= G$.
If $g \in g_1H \cap g_2H$, then, by lemma, $gH = g_1H$ so $g_1H = g_2H$.
$\|$
g_2H

Thm (Lagrange) Suppose G a finite gp &, $H \subset G$ a subgp.
Then $|H| \mid |G|$

Pf: G splits up into finitely many cosets $g_1H, \dots, g_dH$

[Aside: Lemma: The map $H \to gH$ which sends h to gh is a bijection.
Pf: The inverse sends $x \in gH$ to $g^{-1}x$, so a bijection.]

$|g_iH| = |H|$ so $|G| = \left|\coprod_{i=1}^{d} g_iH\right| = \sum_1 |g_iH| = d|H|$.

$\Rightarrow$ # of left cosets = # of right cosets.

$\Rightarrow$ # of left cosets $= |G|/|H|$ "

Q: What is the right coset $H(123)$?

A: Permutations sending 3 to 1. which is a left coset for a different subgp: the stabilizer of 3!

$\Rightarrow$ every right coset is a left coset, but of diff. subgp.

This is a general phenomenon:

$Hg = \{hg\}_{h \in H}$

$= \{gg^{-1}hg\}_{h \in H}$

$= g\{g^{-1}Hg\} = gH^g$.

Claim: $g^{-1}Hg$ is subgp! Call it H^g, or the conjugate of H by g.

Pf: $g^{-1}h_1g \cdot g^{-1}h_2g = g^{-1}h_1h_2g$.

[Ex: The stabilizer of 1 conjugated by (123) is Stab. of 3
$[\mathrm{Stab}(1)]^{(123)} = [\mathrm{Stab}(3)]$]

In fact $H \simeq H^g$

9/13 The set of left cosets gH is called G/H.

right cosets Hg $\quad H\backslash G$

which are in bijection $gH \rightsquigarrow Hg^{-1}$

$g^{-1}H \leftsquigarrow Hg$

More subgps:

How to make a subgp of G?

<u>One way</u>, take elts $g_1, \dots, g_k$ & consider subgp of G $\langle g_1, \dots, g_k \rangle$ they generate.

eg. Consider the gp $\langle g \rangle$ for $g \in G$; All elts of form, $\{\dots g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}$

Some of these might be the same:

<u>Ex</u> $g = (12) \in S_3$

$g^2 = id$

So $\langle g \rangle = \{e, g\}$ (ie the inf. seq. above is periodic)

If g has order m, $\langle g \rangle = \{e, g, g^2, \dots, g^{m-1}\}$.

A group C generated by one elt is called a <u>cyclic gp</u>.

If C is finite of order m, it is isomorphic to $\mathbb{Z}/m\mathbb{Z}$, by the isom. below:

The operation on this gp can be thought of as add. mod m on exponents. In fact a iso.

$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \to & C \\ \{0,1,\dots,m-1\} & & \\ k & \mapsto & g^k \end{array}$$

<u>Fact</u>: If $|G| < \infty$ & $g \in G$ has order m, then $m \mid |G|$

<u>Pf</u>: The gp generated by g has size m: $|\langle g \rangle| = m$.

By Lagrange, $|\langle g \rangle| \mid |G|$.

<u>Another way</u>:

Suppose given $f: G \to J$. Then $\ker f = \{g \in G \mid f(g) = e_J\}$

$\operatorname{im} f = \{j \in J \mid \exists g \in G \text{ w/ } f(g) = j\}$

* Check $\operatorname{im} f < J$ & $\ker f < G$ & $\operatorname{im} f < J$.

Pf: If $g_1, g_2 \in \ker f$, $f(g_1 g_2) = f(g_1) f(g_2) = e e = e$, so $g_1 g_2 \in \ker f$

& $f(g_1^{-1}) = f(g_1)^{-1} = e^{-1} = e$ so $g_1^{-1} \in \ker f$

"set of elts killed by hom. is a subgp"

Ex: The alternating gp $< S_n$.

We will define a hom.

$$\varepsilon : S_n \twoheadrightarrow \{\pm 1\}$$

$\twoheadrightarrow$: surjective hom. = epimorphism

Ch. 1 of Categories for Working Mathematician

First, we have a hom. $\rho : S_n \to GL_n\mathbb{Z}$

$\rho(\sigma)$ is the permutation matrix w/ $a_{\sigma(j),j}=1$, all other $a_{ij}=0$.

Ex: $\rho(123) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ $\in S_3$

(permutes the elts of a vector in same way as ρ)

* Check ρ a hom.

$$S_n \hookrightarrow GL_n(\mathbb{Z}) \xrightarrow{\det} \mathbb{Z}^* = \pm 1$$

(Int. matrices w/ an inv. have $\det = \pm 1$)

$\varepsilon = \det \circ \rho : S_n \twoheadrightarrow \pm 1$

Map is surjective b/c $\det \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \rho((12))$

$\ker \varepsilon \leq S_n$ called the alternating gp, or A_n.

Note: (12) is not in A_n b/c $\det(\rho(12)) = -1$

But $\varepsilon((12)(23)) = \varepsilon(12)\varepsilon(23) = -1 \cdot -1 = 1$, so

$(132) = 1$, so $(132) \in A_n$

Second def. of ε:

Suppose P a polynomial in n variables, $x_1, \ldots, x_n$

$\sigma \in S_n$. Then P^σ = polynomial obtained by relabelling variables x_i as instructed by σ.

eg: $x_1^2 + x_2 + 5x_3$ $\sigma = (123)$, then $P^{(123)} = x_2^2 + x_3 + 5x_1$

but $x_1 + x_2 + x_3$ is impervious to permutations.

We say P is symmetric if $P^\sigma = P$ $\forall \sigma \in S_n$.

Elementary symm. polys:

e_0: 1

e_1: $x_1 + \cdots + x_n$

e_2: $x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \sum_{(i)} x_i x_j$

$x_1^2 + \cdots + x_n^2 = e_1^2 - 2e_2$

* Any symm. poly. can be written from e_1, e_2.

Consider $\Delta = \prod_{i<j} (x_i - x_j)$

eg, when $n=2$, $\Delta = x_1 - x_2$

$\Delta^{(12)} = x_2 - x_1 = -\Delta$

Note that Δ^2 is symm.

$\Delta^2 = x_1^2 + x_2^2 - 2x_1x_2 = (x_1+x_2)^2 - 4x_1x_2 = e_1^2 - 4e_2$.

In fact, for any n, $(-1)^{\binom{n}{2}}\Delta^2 = \prod_{i\neq j} (x_i - x_j)$ is plainly symmetric.

For each $\sigma \in S_n$, $(\Delta^2)^\sigma = \Delta^2$

$(\Delta^\sigma)^2$

So $\Delta^\sigma = \pm\Delta$ (b/c their squares are equal)

Prop: $\varepsilon(\sigma) = \frac{\Delta^\sigma}{\Delta}$ is a hom.

Pf:

$$\varepsilon(\sigma\tau) = \frac{\Delta^{\sigma\tau}}{\Delta} = \frac{(\Delta^\tau)^\sigma}{\Delta} = \frac{(\varepsilon(\tau)\Delta)^\sigma}{\Delta} = \frac{\varepsilon(\tau)\Delta^\sigma}{\Delta} \quad (\text{b/c } \varepsilon(\tau) = \pm 1)$$

$$= \frac{\varepsilon(\tau)\varepsilon(\sigma)\Delta}{\Delta} = \varepsilon(\tau)\varepsilon(\sigma) = \varepsilon(\sigma)\varepsilon(\tau) \quad \checkmark$$

Note that $\Delta^{(12)} = \prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)}) = -\Delta$

$\varepsilon(12) = -1$

* Check: If σ is a perm. w/ cycle class decomposition ..... into cycles of length $c_1, c_2, \dots$)
then $\varepsilon(\sigma) = (-1)^{\#\text{ of even-length cycles}}$.

A_n = gp of perms. w/ evenly many even length cycles.

Recall:

① To specify hom. $f: G \to J$ I only need to tell you what $f(g_1), \dots, f(g_k)$ where $(g_1, \dots, g_k)$ generates G.

② detop $(12) = \varepsilon(12) = -1$.

But more is true.

Check that all transpos. are related by conjugacy *

Let $(ij) \in S_n$ be a transposition. Then $(ij) = g(12)g^{-1}$
where g is any perm sending 1 to i & 2 to j.

So for any hom. $f: S_n \to \pm 1$, $f(ij) = f(g)^{-1} f(12) f(g)$ } ±1 abel.

$= f(12) f(g)^{-1} f(g)$ }

$= f(12) = -1$

So in fact, $\varepsilon(ij) = -1$ & $\det\rho(ij) = -1$
It remains to show that $\langle (ij) \rangle = S_n$. True!
Thus, $\varepsilon = \det\rho$.
Moreover;
Let $f: S_n \to \pm 1$ a hom.
$f(12) = -1$, then $f \in \varepsilon$
$f(12) = 1$, then $(ij) \in \ker f < S_n$, but $\langle (ij) \rangle = S_n$,
so $\ker f = S_n$, so f sends everything to e.

9/18 Last time, homomorphisms $f: G \to J$

An <u>endomorphism</u> of a gp G is a hom. $f: G \to G$.
→ not a gp, b/c not every endo. has an inverse under composition
eg: $f: G \to G$
$g \mapsto e_G$

(Compare: endomorphisms of $(\mathbb{Z}^2, +)$
$f: \mathbb{R}^2 \to \mathbb{R}^2$
$f(\vec{v} + \vec{w}) = f(\vec{v}) + f(\vec{w})$ (linear map)
so f is a 2x2 matrix over $\mathbb{R}$, but not all matrices invertible)
In general $\mathrm{End}(G)$ is a <u>semigp</u> (<u>monoid</u>).

The invertible elements $\mathrm{End}(\mathbb{Z}^2) = M_2(\mathbb{Z})$ are a gp, $GL_2(\mathbb{R})$.

An <u>automorphism</u> of a gp G is a hom. $f: G \to G$. w/ an inverse, f^{-1}:
ie, $f^{-1}(f(g)) = g = f(f^{-1}(g))$
or, an isomorphism from G to itself.
These form a gp, called $\mathrm{Aut}(G)$.
eg: $\mathrm{Aut}(\mathbb{Z}^n) = GL_n(\mathbb{Z})$

Inner automorphisms:

Let $g \in G$. Then $\exists\ \alpha_g : G \to G$

$$\alpha_g(h) = g^{-1}hg \quad \text{"conjugate of } h \text{ by } g\text{"}$$

$\alpha_g(h_1 h_2) = g^{-1}h_1h_2g = g^{-1}h_1 g g^{-1}h_2 g = \alpha_g(h_1)\alpha_g(h_2) \Rightarrow$ hom.

α_g is called an <u>inner automorphism</u>.

$\alpha_g^{-1} = \alpha_{g^{-1}}$.

Check that $\alpha_g \circ \alpha_h = \alpha_{gh}$.

$\mathrm{Inn}(G)$ is the <u>inner auto gp</u> of G

eg. What is $\mathrm{Inn}(\mathbb{Z}^n)$?

Let $\vec{v} \in \mathbb{Z}^n$. Then $\alpha_{\vec{v}}(\vec{w}) = (-\vec{v}) + \vec{w} + \vec{v} = \vec{w}$

So all inner autos of $\mathbb{Z}^n$ are trivial (true for all abelian gps).

<u>Fact</u>: All autos of S_n are inner, except when $n=6$.

Last time, defined hom. $\varepsilon : S_n \to \pm 1$

$\ker \varepsilon = A_n$, the <u>alternating gp</u>.

Is every subgp of G the kernel of some hom? No.

Let $H = \ker f$, $f : G \to J$ hom.

If $h \in H$, ie, $f(h) = e$, then $f(g^{-1}hg) = f(g^{-1})f(h)f(g)$

$= f(g)^{-1}f(h)f(g) = f(g)^{-1}f(g) = e. \Rightarrow g^{-1}hg \in H.$

then any conjugate of h is in kernel.

In other words,

$H^g = \{g^{-1}hg \mid h \in H.\}$ is contained in H, $H^g \subset H$.

$\Rightarrow H^{g^{-1}} \subset H \Rightarrow H \subset H^g \Rightarrow H = H^g \ \forall g \in G.$ (*).

(conjugate by g.)

<u>Def</u>: A subgp H of G which satisfies (*) is called a <u>normal</u> subgp of G.

Prop: H is normal iff H is the kernel of a hom. $f: G \to J$ for some f, J.

Pf $\Leftarrow$: Shown

$\Rightarrow$: Consider $G/H = \{g_1 H, g_2 H, \dots\}$ (not nec. G countable)

Remark: $g_1 H = H^{g_1^{-1}} g_1 = H g_1$ b/c H normal.

ie. we can just say "the coset of g_1"

$J = G/H$ w/ operation $(g_1 H) \cdot_J (g_2 H) = g_1 g_2 H$

Worry: Is this well-def? eg. $g_1 H = g_1' H$ for any $g_1' \in g_1 H$.

So why should $g_1' g_2 H = g_1 g_2 H$.

General notation: If $A, B \subseteq G$, then $AB = \{ab \in G \mid a \in A, b \in B\}$

Suppose $g_1 H$, $g_2 H$ are cosets in G/H. Claim:

$(g_1 H)(g_2 H) = g_1 g_2 H$

Pf: $g_1 H g_2 H = \{g_1 h_1 g_2 h_2 \mid h_1, h_2 \in H\}$

$= \{g_1 g_2 g_2^{-1} h_1 g_2 h_2 \mid \downarrow \}$

$= \{g_1 g_2 h' h_2 \mid h_2 \in H,\ h' \in H^{g_2}\}$ ↑ b/c H normal.

$= \{g_1 g_2 h' h_2 \mid h', h_2 \in H\}$

$= g_1 g_2 HH = g_1 g_2 H$.

So, when H is normal, G/H carries a gp structure.

$f: G \to G/H$ a hom. b/c $f(g_1 g_2) = f(g_1) f(g_2)$

$g \longmapsto gH$ $\qquad g_1 g_2 H = g_1 H g_2 H$ ✓

$e_{G/H} = H$, so $g \in G$ is in $\ker f$ if $gH = H$, ie, if $g \in H$.

So $H = \ker f$.

When H is normal, $\exists$ a <u>quotient gp</u> G/H ?

$f: G \to G/H$ w/ $\ker f = H$.

ex: ① $A_n \trianglelefteq S_n$, In this case, $G/H \cong \pm 1$

② $G = SL_2(\mathbb{Z})$ $H = \pm I$

$h \in H$, $g^{-1} I g = I$ or $g^{-1}(-I)g = -I$. (scalar matrix commutes w/ other matrices)

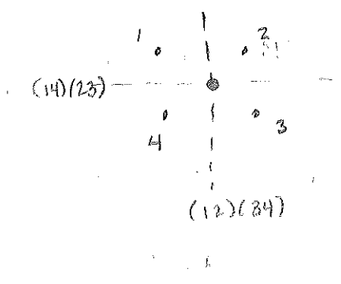
The coset $\begin{bmatrix} a & b \\ c & d \end{bmatrix} H$ is

$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}, -\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right\}$

$SL_2(\mathbb{Z})/H$ is called $PSL_2(\mathbb{Z})$, the "<u>projective special linear gp</u>" of "matrices up to sign" → 2 elts are = if they're negatives.

Remark: $B \subset GL_2(\mathbb{R})$ is not normal (B = upper Δ)
$(eB)(xB) = BxB$
If subgp normal, double cosets = single cosets are the same.

③ $G = S_4$ $H = V_4$, the Klein 4-gp $= \{e, (12)(34), (13)(24), (14)(23)\}$
(products of 2 disj. transpositions)



comp. of 2 refl's is refl. in pt of intersection
$= (13)(24)$
"perpendicularity is the avatar of commutativity"

Remember, if π, σ are permutations, π in cycle not., then π^σ is obtained by relabeling entries in the cycles of π.
$\pi = (1\,2\,3)(4\,5)\ldots$
$\pi^{\sigma^{-1}} = (\sigma(1)\,\sigma(2)\,\sigma(3))(\sigma(4)\,\sigma(5))$.
So the conjugate of a transposition is a transposition.
So every conj. of a double flip = a flip $\Rightarrow H$ is normal.
S_4/V_4 is a gp? $|V_4| = 4$, $|S_4| = 4! = 24$
$|S_4/V_4| = 24/4 = 6$ (there are 2 iso. classes of order 6)

Thm: (First Isomorphism Thm)
Let $f: G \to J$ hom, $H = \ker(f)$. Then $\mathrm{im}(f) \cong G/H$.
Pf: We need to construct hom $i: G/H \to \mathrm{im}(f)$ & $j: \mathrm{im}(f) \to G/H$ that are inv's.

$G/H \to \mathrm{im}\, f$ $\quad$ $gH \longmapsto f(g)$

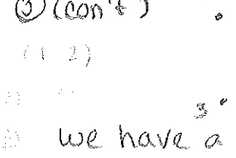
$\mathrm{im}\, f \to G/H$ $\quad$ $x \longmapsto f^{-1}(x)$
$f^{-1}(x)$: set, not elt. ← what is this subset?
if $f(g) = x$, then $f(gh) = f(g)f(h) = x$ ($f(h) = e$)
so $f^{-1}(x)$ a union of cosets of H

Let $g_1, g_2 \in f^{-1}(x)$. Then $f(g_1) = f(g_2) = x$, so
$f(g_1^{-1}g_2) = x^{-1}x = e$ so $g_1^{-1}g_2 \in H$. $\Rightarrow g_2 \in g_1 H$
$g_1 g_1^{-1} g_2 \in g_1 H$

So $f^{-1}(x)$ is a coset of H.

Check both well-def & they are inverses.

③ (con't)



$M = \{$matchings on 4 pts$\}$
$= 1\,1 \;\; X$

we have a hom.

$f: S_4 \to \mathrm{Sym}(M)$

(1 2): $= \to =$
$1\,1 \to X$
$X \to 1\,1$

(1 2 3): $= \to X$

$\mathrm{Sym}(M) \cong S_3$
$f: S_4 \to S_3$

$\ker f = V_4$
$\mathrm{im}\, f \cong S_4/V_4$
$\mathrm{im}\, f \leq S_3$, but $|\mathrm{im}\, f| = 6$ & $|S_3| = 6$
so $\mathrm{im}\, f = S_3$
$\Rightarrow S_4/V_4 \cong S_3$

9/20 Commutation: We say $x, y \in G$ commute if $xy = yx$.

If $x \in G$, define $Z_G(x) = \{y \in G \mid yx = xy\}$ to be the centralizer of x. (ie, $y \in G$ s.t. $y^{-1}xy = x$)

recall, $H \leq G$, $N_H(G) = \{y \mid y^{-1}Hy = H\}$ → doesn't fix $h \in H$, which centralizer does.

$Z_G(x) \leq G$ b/c if $y, z \in Z_G(x)$,
$yzx = yxz = xyz$ ✓, so $yz \in Z_G(x)$.

Z_G, the center of G: $Z_G = \bigcap_x Z_G(x)$
$= \{y \in g \mid \forall x \in G,\ xy = yx\}$

We say a gp is abelian if $Z_G = G$, ie, $xy = yx$ $\forall x, y \in G$.

Remark: G is abelian
$\Updownarrow$
$y^{-1}xy = x$ $\forall x, y \Leftrightarrow x^{-1}y^{-1}xy = e$ $\forall x, y$ ie, $[x,y] = e$
$\Updownarrow$ ↘ commutator: $[x,y]$
$Inn(G) = \{e\}$
$y^{-1}Hy = H$ $\forall y \in G$ $\forall H \leq G$
$\Updownarrow$
all subgps of G are normal

Warning: There are gps G s.t. $H \trianglelefteq G$ $\forall H \leq G$, but G not abel. (see HW)

Ex: What is the center of $SL_n(\mathbb{R})$?

Let $g \in Z_{SL_n(\mathbb{R})}$ $\begin{bmatrix} a_{11} & a_{12} & & \\ & \ddots & & \\ & & & a_{nn} \end{bmatrix}$

$$g \begin{bmatrix} 2 & & 0 \\ & 1 & \\ 0 & & \ddots \end{bmatrix} = \begin{bmatrix} 2a_{11} & a_{12} & \\ 2a_{21} & a_{22} & \\ & & \ddots \end{bmatrix}$$

$$= \begin{bmatrix} 2 & & \\ & 1 & \\ & & \ddots \end{bmatrix} g = \begin{bmatrix} 2a_{11} & 2a_{12} & \cdots & 2a_{1n} \\ a_{21} & & & \\ & & \ddots & \\ & & & a_{nn} \end{bmatrix}$$

So, $a_{1i} = a_{i1} = 0$ $\forall i \neq 1$ (In particular, $Z_{SL_2(\mathbb{R})} \begin{bmatrix} 2 & \\ & 1 \end{bmatrix} = \left[\begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array}\right]$)

$$\begin{bmatrix} * & \\ & * \end{bmatrix} \simeq \left((a_{11}, M) \;\; {}^{a_{11}\in\mathbb{R}^*}_{M\in GL_{n-1}(\mathbb{R})} : (\det M = 1/a_{11}) \right)$$

If $g \in Z_{SL_n(\mathbb{R})}$ then $a_{ij} = 0$ if $i \neq j$. ie, g is diagonal.
What else can we commute with?

Exercise: If $\pi \in SL_n$ is the perm. matrix attached to $\sigma \in S_n$, and $t \in SL_n(\mathbb{R})$ is a diagonal matrix. Then $\pi^{-1} t \pi$ is obtained from t by permuting the entries according to σ. (Implicit: if $T = \{\text{diag}\}$ then all perm. matrices $\subset N_{SL_n(\mathbb{R})}(T)$)
But for $t \in Z_{SL_n(\mathbb{R})}$, $\pi^{-1} t \pi = t \;\; \forall \pi$, so t is invariant under permutation of entries by A_n.

$t: \begin{bmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{bmatrix}$ if $a_{ii} \neq a_{jj}$, use π corresponding to σ which takes i to j., & t fails to commute w/ π.

eg: (ijk)

So t is a scalar matrix aI, w/ $a^n = 1$. ($b/c \in SL_n$)
$Z_{SL_n\mathbb{R}} = \mu_n^{(\mathbb{R})} \cdot I$, $\mu_n = n^{th}$ roots of unity.

$|Z_{SL_n\mathbb{R}}| = \begin{cases} 1 & \text{if } n \text{ odd} \quad (I \text{ or } \pm I) \\ 2 & \text{if } n \text{ even} \end{cases}$ $\quad |Z_{SL_n\mathbb{C}}| = n$

Groups w/ Presentations

Problem: Classify gps generated by 2 elts x, y s.t. $x^2 = y^2 = e$
2 examples: $\mathbb{Z}/2\mathbb{Z}$ generated by $1 \& 1$
$1 \& 0$

- S_3 gen. by $(12)(13)$ [any 2 distinct transp's]

Q: Can we classify all G of this form?
Q: Can we bound $|G|$ above?
Q: Is $|G| < \infty$

Not every G is of this form: eg: $\mathbb{Z}/3\mathbb{Z}$; any gp odd order; any abel. gp of order > 4 b/c $\langle x, y \rangle = \{1, x, y, xy = yx\}$; $\mathbb{Q}/\mathbb{Z}$,
↑ matrices $SL_n(\mathbb{R})$

What are the elts of G?

$e, x, y, xy, yx, yxy, xyx, \underbrace{xyxy}_{r^2}, \underbrace{yxyx}_{r^{-2}}, \ldots$

$r^0, xr^0, xr, r, r^{-1}, xr^2, xr^{-1}, \ldots$ commutator, $\ldots$

$r = xy$. Then every elt of G is of the form r^n or xr^n

More examples: • D_p = dihedral gp of order $2p$, p odd.
= gp of rigid motions preserving a p-gon

any reflection = involution, & any 2 refl. generates the gp.

• F_2 = free gp $F_2 = F\langle x,y\rangle$
Let $H \subset F_2$ be the subgp generated by x^2, y^2, & all conjugates of these.
For any $\gamma \in F_2$, $H^\gamma = \langle (x^2)^\gamma, (y^2)^\gamma$, & all conjugates of these $\rangle = H$
So $H \trianglelefteq F_2$.

* Denote by $\langle x,y \mid x^2=1, y^2=1\rangle = F\langle x,y\rangle / H$ (a gp)
This is called a gp with presentation
$\langle x_1,\ldots,x_k \mid r_1(x_1,\ldots,x_k)=1, r_2(x_1,\ldots,x_k)=1, \ldots\rangle$ is $F\langle x_1,\ldots,x_k\rangle$/gp normally generated by $r_1, r_2, \ldots$
↑ relation on generators

normally generated: generated by elts & all their conjugates.

$r_1(x_1,\ldots,x_k) \in F\langle x_1,\ldots,x_k\rangle$

Let $\Gamma = \langle x,y \mid x^2=y^2=1\rangle$ (the quotient gp)

Facts: 1. Γ is generated by 2 involutions, namely x & y
B/c $F\langle x,y\rangle \twoheadrightarrow \Gamma$ (b/c $G \twoheadrightarrow G/H$); & $x^2 \in H$, $y^2 \in H$,
↑ generated by x,y ⇒ ↑ gen by x,y.
so x^2 is trivial in Γ
$\Gamma = F\langle x,y\rangle / H$ (& y^2)
$H = \ker$ (hom.), so $x^2 \to e$
$y^2 \to e$
⇒ x & y are involutions

9/25 **Third Isomorphism Thm**: Let $N \trianglelefteq G$ a normal subgp.
[We say H is btwn N & G if $N \subset H \subset G$. Whence $N \trianglelefteq H \subset G$ (b/c $N^h = N$, since $N^g = N$ $\forall h \in G$)]
Given H btwn N & G, $\exists$ is a natural inclusion of $H/N \subset G/N$. The resulting map from subgps btwn N & G $(hN \longmapsto hN)$ to subgps of G/N is a bijection.
Moreover, if $H \trianglelefteq G$, then $H/N \trianglelefteq G/N$.
and the map

$$G/N \to G/H \qquad *\text{well-defined?}*$$
$$gN \mapsto gH$$

has kernel H/N. In other words,
$(G/N)/(H/N) = G/H$.

Ex: $G = S_4$, $N = V_4$. example subgp btwn N & G:
$N = \langle (12)(34), (13)(24) \rangle = \langle n_1, n_2 \rangle$ $\left[\langle (12), (23), (34) \rangle = S_4 \right.$
$H = \langle (12)(34), (13)(24), (12) \rangle$ $\left. \langle (12), (13), (14) \rangle = S_4 \right]$

What is $H/N \subset G/N$
12
S_3 (by considering way perms in S_4 permute set of matchings $= 3 \overset{1}{-} \overset{2}{-} 4$ $1\,2$ $\times$ $3\,4$ (elts of V_4 leave these alone))
S_3
12^3
$f: G \to G/N$. What is the image of H in G/N?

[**Aside**: If $N \trianglelefteq G$, $H \subset G$, then $HN = \{hn \mid h \in H, n \in N\}$ is a subgp of G.]

What does H/N look like?
An elt of H is a word $(12)n_1n_2(12)n_1(12)\ldots = h$
Note: $n_1(12) \in (12)N$ b/c N normal, so L cosets = R cosets
$(12)n_1n_2(12)n_1(12)N = (12)(12)(12)N = (12)N$

So $hN = \begin{cases} N & \text{if even \# of } (12)\text{'s} \\ (12)N & \text{if odd \#} \end{cases}$
H/N consists of 2 cosets: N & $(12)N$
$|H| = 8$ (4 elts in each coset)

$H/N \to G/N$

$N \longmapsto id$

$(12)N \longmapsto (23)$

Conclusion: H corresponds to the order 2 subgp generated by (23); $\langle(23)\rangle \subset S_3$.

Subgps of S_3:

$e, \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle, \langle(123)\rangle, S_3$

1. 2 2 2 3 6.

these correspond 1-1 to the 6 subgps of S_4 containing V_4.

Pf of 3rd Iso. Thm:

- Bijection btwn $N \lhd H \subset G$ & supgs of G/N.

As explained, given such an H, $H/N \subset G/N$ b/c hN is also a coset in G/N.
(If map is injectiven, then $H/N < G/N$)
Moreover, if $h_1N = h_2N$ in G/N, then $h_2h_1^{-1} \in N$, so $h_1N = h_2N$ is H/N. This proves injectivity of $H/N \to G/N$.
We have a map from {subgps $H \lhd N < G$} $\to$ {subgps of G/N}.
Given $\overline{H} \subset G/N$, associate to it $H = \bigcup_{gN \in \overline{H}} gN = \{g \mid gN \in \overline{H}\}$

Claim: $H < G$. Let $h_1, h_2 \in H$.
$h_1 \in g_1N$, $h_2 \in g_2N$ for $g_1N, g_2N \in \overline{H}$
ie, $h_1N, h_2N \in \overline{H}$, so $h_1Nh_2N \in \overline{H}$ (b/c $\overline{H} < G/N$)
$= h_1h_2NN = h_1h_2N \in \overline{H} \Rightarrow h_1h_2 \in H$ so $H < G$.
Note: $e_{G/N} \in \overline{H}$, but $e_{G/N} = N$, so $N \subset H$.

* Check the 2 associations are inverses.

• "Division" $N \trianglelefteq H \trianglelefteq G$

$f: G/N \to G/H$

$gN \mapsto gH$

For which cosets gN is it the case that $gH = H$?

So $g \in H$: This is the set of cosets

$\{hN \mid h \in H\} = H/N := \ker f$.

If $H \trianglelefteq G$, then $H/N \trianglelefteq G/N$.

Groups w/ Presentations:

$\Gamma = \langle x, y \mid x^2 = 1, y^2 = 1 \rangle = \langle x, y \mid x^2, y^2 \rangle$

Prop: Let G be a gp. Then $\exists$ natural bijection

$\mathrm{Hom}(\Gamma, G) \sim$ (pairs $(g_1, g_2) \in G^2$ w/ $g_1^2 = 1, g_2^2 = 1$)

$\cup$! $\cup$ ↑ ie, pairs of involutions in G

$\mathrm{Surj}(\Gamma, G) \sim$ (pairs $(g_1, g_2) \in G^2$ w/ $g_1^2 = g_2^2 = 1$, $\langle g_1, g_2 \rangle = G$)

"Classifies pairs of involutions"

Recall: $\mathrm{Hom}(F\langle x, y \rangle, G) \sim G^2$

e.g.: Γ is an infinite gp.

B/c consider gp of symmetries of regular p-gon. $= D_p$

D_p is generated by 2 reflections (& they square to 1),

so $\exists \Gamma \twoheadrightarrow D_p$.

If $|\Gamma| = N$, choose $p > N$, contradiction.

Given $f: \Gamma \to G$ a hom, associate to it the pair

$(f(x), f(y)) \in G^2$. $f(x)^2 = f(x^2) = e$; $f(y)^2 = f(y^2) = e$ ✓

Given $g_1, g_2 \in G$ with $g_1^2 = g_2^2 = 1$, Let

$\Phi: F\langle x, y \rangle \to G$ be the homomorphism

$\Phi(x) = g_1$, $\Phi(y) = g_2$.

Let $K = \ker \Phi$, $x^2 \in K$ b/c $\Phi(x^2) = \Phi(x)^2 = g_1^2 = 1$

& $y^2 \in K$

Since K is normal, it contains all conjugates of

x^2 & y^2. So recall: $\Gamma = F\langle x, y \rangle / R$, R normally gen.

by x^2 & y^2.

So $R \trianglelefteq F < G$ iff $R \trianglelefteq K \trianglelefteq F\langle x,y\rangle$.

As in pf above, we have a map

$$F\langle x,y\rangle/R \twoheadrightarrow F\langle x,y\rangle/K \qquad \text{(Kernel is } K/R\text{)}$$
$$\Gamma \longrightarrow \text{image } \Phi \subset G \quad \text{(by 1st Iso. Thm)}$$

So $(g_1,g_2) \in G$ w/ $g_1^2 = g_2^2 = 1$ yields a map from $\Gamma \to G$ which is surjective iff $\text{im}(\Phi) = G$

$$\| \\ \langle g_1, g_2\rangle \leq G.$$

ie, if $\langle g_1,g_2\rangle = G$, this is surjective.

Other examples:

① $\langle x,y \mid x^2, (xy)^3\rangle$ maps to $PSL_2(\mathbb{Z})$ via the map

$$x \longmapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad y \longmapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \uparrow SL_2(\mathbb{Z})/_{Z_{SL_2(\mathbb{Z})} = \pm 1}$$

The map is an isomorphism.

② Burnside gp: $\langle x_1, \dots, x_n \mid W^m = 1 \ \forall \text{ words } W \text{ in } x_1,\dots,x_n\rangle$
$B(n,m)$

This is an infinite gp b/c moding out by countably infinite elements: $x_2^m, (x_1x_2)^m, (x_1^{-1}x_2)^m, \dots$

$B(n,2)$ is finite.

$B(n,m)$ infinite for large m,n

$B(2,5)$???

9/27 Are there gps w/o presentations? Not really.

eg: Let $G = S_4$. $g_1, g_2, g_3 = (12), (23), (34)$

$\langle g_1, g_2, g_3 \rangle = G$

$\Phi : F\langle x_1, x_2, x_3 \rangle \twoheadrightarrow G$ hom.

$\Phi(x_1) = g_1$

$\Phi(x_2) = g_2$

$\Phi(x_3) = g_3$

So $G \cong F\langle x_1, x_2, x_3 \rangle / \ker \Phi$.

Ψ

x_1^2, x_2^2, x_3^3 $\quad x_1 x_3 x_1^{-1} x_3^{-1}$

w^{24} for any word

$(x_1 x_2 x_3)^4$

$x_1 x_2 x_1 = x_2 x_1 x_2$

$(x_1 x_2)^3$

Presentation: $S_4 = \langle x_1, x_2, x_3 \mid \text{every word in } \ker \Phi \rangle$.

↑ finite? in this case, yes.

Another eg: $[x,y] = xyx^{-1}y^{-1}$

$\langle x_1, \dots, x_k \mid [w_1, w_2] \rangle$ $\forall$ words $w_1, w_2 \in F\langle x_1, \dots, x_k \rangle$.

$\Gamma = \langle x_1, \dots, x_k \mid [x_i, x_j] \text{ for } i,j \in 1, \dots, k \rangle = \mathbb{Z}^k$

Why $[x_i, x_j]$ enough? B/c the fact that x_i & x_j commute means

$(x_1^2 x_3^2 x_4)(x_5 x_1^2 x_3) = (x_5 x_1^2 x_3)(x_1^2 x_3^2 x_4)$

since you can pull x_i's to end one at a time.

$Z_\Gamma(x_i)$ contains $x_1, \dots, x_k$, but these generate Γ,

so $Z_\Gamma(x_i) = \Gamma$ $\forall i$, so $x_i \in Z_\Gamma$ $\forall i$, so $\Gamma \subseteq Z_\Gamma$, so Γ is abelian.

Products

Recall, if $N \lhd G$, $H \leq G \Rightarrow HN \leq G$.

Suppose that $G = HN$ & $H \cap N = \{e\}$ "disjoint"

In this case, we say G is a semi-direct product of $N \rtimes H$.

[rtimes]

If elts of H commute w/ elts of N, G is a direct product

$N \oplus H$ ↑ oplus

2nd Iso Thm: If $N \trianglelefteq G$, $H \leq G$, then $HN \leq G$. & $N \trianglelefteq HN$ (already proven)
& $HN/N \cong H/H\cap N$

Pf: Define $f: H \longrightarrow HN/N$

$f(h) = hN$ ← $h_2N = Nh_2$ b/c N normal.

hom: $f(h_1h_2) = h_1h_2N = h_1Nh_2N$.

f surjective b/c elts HN/N are $hnN = hN$.

$\ker f = \{h \in H \mid hN = N\} = H \cap N$.

By 1st Iso Thm, $H/H\cap N \cong HN/N$.

Note: Useful for $G = N \rtimes H$.

Then $G/N = HN/N = H/H\cap N = H$ (b/c $H \cap N = \{e\}$)

(for finite gp, $|G| = |N| \cdot |H|$)

Let $G = N \rtimes H$. For every $h \in H$, we can define

$\alpha_h : N \to N$ s.t. $\alpha_h(n) = h^{-1}nh$

hom: $(h^{-1}n_1h)(h^{-1}n_2h) = h^{-1}n_1n_2h$.

inverse: $\alpha_{h^{-1}}$.

So $\alpha_h \in \mathrm{Aut}(N)$ [not an inner aut. b/c conjugating by elt in H, not N]

* One checks $\alpha_{h_1h_2} = \alpha_{h_1}\alpha_{h_2}$. So,

$\alpha : H \to \mathrm{Aut}(N)$

Ex: $G = S_n$, $N = A_n$. What is H?

[Def: index of $H \subset G$ is $|G/H|$, denoted $[G:H]$]

So $[S_n : A_n] = 2$, so $|H| = 2$

So $H = \langle \sigma \rangle$ where $\sigma^2 = 1$

For $H \cap N = \{e\}$, we need $\sigma \notin A_n$.

We also need $HN = G$

(In this case, this follows from $\sigma \notin A_n$, b/c

$|HN| = |HN/N| \cdot |N| = |H/H\cap N| \cdot |N| = \frac{|H||N|}{|H\cap N|} = \frac{2 \cdot 12}{1} = 24$ ✓)

eg. $S_4 = A_4 \rtimes \langle (12) \rangle$ (← any transp.)

$S_6 = A_6 \rtimes \langle (12) \rangle$

$= A_6 \rtimes \langle (12)(34)(56) \rangle$

Semi-direct product decomp. is not unique

Another decomp of S_4: $V_4 \triangleleft S_4$

$N = V_4$

$H \cong G/N \cong S_3$ $\quad |H| = 6$

H = {stabilizer of 1}, ie perms sending $1 \to 1$.

$H \cap V_4 = \{e\}$ b/c $V_4 = \{(12)(34), (13)(24), (14)(23), e\}$

So $S_4 = V_4 \rtimes H$

But not every normal subgp splits G into a semi-direct product.

Ex: $G = \mathbb{Z}/4\mathbb{Z}$

$N = 2\mathbb{Z}/4\mathbb{Z}$ [In abelian gps, semi-direct prods. are direct prods.]

If $G = N \rtimes H$

then $H \cong G/N \cong \mathbb{Z}/2\mathbb{Z}$

so $H = \langle h \rangle$ where $h^2 = e$ & $h \notin 2\mathbb{Z}/4\mathbb{Z}$

so $h = 1$ or $h = 3$, but then $|\langle h \rangle| = 1$. ↯

So G is not expressible as a semi-direct product.

Q: What do I mean by $(\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$? (Bottom-up explanation)

Given a gp M & a gp Q, and $\alpha : Q \to \mathrm{Aut}(M)$.

Can define a gp $M \rtimes Q$ as follows:

The elts are pairs (m, q) $m \in M$, $q \in Q$.

The gp law is

$(m, q)(m', q') \neq (mm', qq')$. This is for direct prod $M \oplus Q$.

$(m, q)(m', q') = (m\alpha_q(m'), qq')$ "twisted product".

Check associativity.

Does this have M as a normal subgp?

yes: $\{(m, e) \mid m \in M\} \cong M$.

subgp, b/c $(m, e)(m', e) = (m\alpha_e(m), e) = (mm', e)$.

normal b/c:

$M \times Q \to Q$ hom. b/c gp law on 2nd coord is gp law for Q.

$(m, q) \to q$

Kernel $= \{(m, e)\} = M$, surjects on Q, so

M is normal. (& $M \times Q / M \cong Q$!)

Q is a subgp of $M \times Q$: $Q = \{(e,q) \mid q \in Q\}$
e_H preserved by any auto., so this is a subgp. ✓

$M \cap Q = e$: $(m,q) = \begin{cases} (m,e) \\ (e,q) \end{cases} = (e,e)$. ✓

Generate gp ($QM = G$)
$(m,e)\cdot(e,q) = (m\alpha_e(e), q) = (m,q)$.
So conclude that $M \times Q$ as defined here is a semi-direct product of $\{(m,e)\} \cong M$ & $\{(e,Q)\} \cong Q$.
→ what gp this actually is depends on α: $M \times_\alpha Q$.

eg: $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$
$|\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})| = 2$: trivial aut; mult. by -1.
So $\alpha: \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ can be trivial or not.
α trivial: $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$
α non-trivial: $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong S_3$

S_3
$N = A_3 = \langle (123) \rangle \cong \mathbb{Z}/3\mathbb{Z}$
$H = \langle (12) \rangle$

$\alpha_{(12)}(123) = (213) = (132) = (123)^{-1}$
so is "mult by -1"

10/2 Group Actions

Def: Let X be a set & G a gp. An action of G on X is a hom $G \to \mathrm{Sym}(X)$.
Alternately, a map $\alpha: G \times X \to X$ (where we usually write gx as short-hand for $\alpha(g,x)$) which satisfies
$g(hx) = (gh)x$ & $ex = x$
↑ X

Ex: ① Should remind you of multiplying matrices by column vectors. $\underset{n\times n}{A}\ \underset{n\times 1}{\vec{v}} = \underset{n\times 1}{\vec{w}}$ ($n \times 1$ vectors not a gp)

ie, $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$, $\alpha(g,\vec{v}) = g\vec{v}$

① S_n acts on the set $X = \{1, \dots, n\}$

② Any gp G acts on itself by left multiplication
$\alpha(g_1, g_2) = g_1 g_2$

④ Any gp G acts on itself by conjugation
$\alpha(g_1, g_2) = g_1 g_2 g^{-1}$

⑤ S_n acts on the set of graphs on n vertices.
$\alpha(\sigma, \Gamma) = \Gamma$ with vertices relabeled by σ.

⑥ S_{2n} acts on the set of matchings (1-regular graphs) on $2n$ vertices.
eg. $n=2$, S_4 acts on $\{||, =, X\}$
So the action gives you a map from $S_4 \to S_3$
(ker = Klein 4-gp)

⑦ Gp of rigid motions preserving a polygon P acts on the set of vertices of P.

⑧ If G is a semi-direct product $N \rtimes H$, then H acts on N by conjugation $\alpha(h, n) = hnh^{-1}$
So the action is given by hom. $H \to \mathrm{Aut}(N) \to \mathrm{Sym}(N)$
("forgetful map")

↙ acts on
Def: We say an action $G \curvearrowright X$ is transitive if for every $x, x' \in X$, $\exists\, g \in G$ s.t. $gx = x'$. (can get from any where to any where else → connectedness)

Def: We say $G \curvearrowright X$ is faithful if $gx = x \ \forall x$ (ie image of g in $\mathrm{Sym}(X)$ is identity) $\Rightarrow g = e$.
Equivalently, the hom. $G \to \mathrm{Sym}(X)$ is injective (only ell of ker is $\{e\}$) $\Leftrightarrow$ $G \cong$ to its image, a subgp of $\mathrm{Sym}(X)$.
[↑ b/c $G/\ker \cong \mathrm{im}$]

Thm (Cayley's Thm): Every finite gp G is $\cong$ to a subgp of a symmetric gp S_n ($n < \infty$).

Pf: By above discussion, all we need is a faithful action of G on a finite set: Action of G on itself by left mult.

- faithful: $g \cdot h = h \ \forall h \Rightarrow g = e$

[- transitive: $h_1, h_2 \in G$, does $\exists\, g h_1 = h_2$? yes, $g = h_2 h_1^{-1}$.] (not nec. for pf)

Ex: $G = S_3$. $G \curvearrowright G$, so $G \to |\mathrm{Sym}(G)| \cong S_6$

(12): $e \to (12)$, $(12) \to e$ } flip
$(123) \to \tau$, $\tau \to (123)$ } 3-cycle
$(13) \to \tau'$, $\tau' \to (13)$ } flip

So $(12) \mapsto$ triple flip in S_6

(not most effective way to show $S_3 \leq S_6$)

Ex: - Action of $GL_n(\mathbb{R})$ on $\mathbb{R}^n$.
faithful? yes. (enough to fix elts of basis)
transitive? no, b/c 0 fixed: $g\vec{0} = \begin{bmatrix} \vdots \\ 0 \end{bmatrix}$ has no solution.
(would be transitive if it were non-zero vectors)

- Action $GL_n(\mathbb{R})$ on {lines in $\mathbb{R}^n$} (sub-vector sp of dim 1, contains 0.)
faithful? no. scalar matrices take lines to themselves.
transitive? yes.

Pf that $GL_n(\mathbb{R})$ acts transitively on non-0 vectors:
suffices to show $g\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \vec{v}$ is always solvable.
(WTS can get from any $\vec{v}$ to any $\vec{w}$)

$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \xrightarrow{g_1} \vec{v}$, $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \xrightarrow{g_2} \vec{w}$, $g_1 \to g_2$

$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix}$. If want $\vec{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = g\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \Rightarrow$

$g = \begin{bmatrix} v_1 & & & \\ \vdots & 1 & & \\ v_n & & \ddots & \\ & & & 1 \end{bmatrix}$ if $v_1 \neq 0$. If $v_1 = 0$, permute so non-0 $v_i \to v_1$.

Ex: $G \curvearrowright G$ by conjugation.
faithful? Suppose $ghg^{-1} = h \ \forall h \in G$. This means g commutes w/ every $h \in G$, ie, $g \in Z_G$.
yes iff $Z_G = \{e\}$.
transitive? no: $geg^{-1} = e$ (like $\vec{0}$ in $\mathbb{R}^n$).
e may not be the only problem: in general, $gh_1g^{-1} = h_2$ is often not solvable ($h_2 \neq h_1$ are conjugate to e/o)

Def: Let $G \curvearrowright X$. Let $x \in X$. The stabilizer of x, $\mathrm{Stab}(x)$ or G_x, is $\{g \in G \mid gx = x\}$, a subgp of G.
(not nec. a normal subgp of G.)

Def: The orbit of x, $\mathcal{O}(x)$ or Gx, is the subset of X consisting of those $y \in X$ s.t. $\exists g \in G$ w/ $gx = y$.
$= \{gx\}_{g \in G} \subseteq X$
Easy to check: $x \sim y$ means $\exists g \in G$ s.t. $gx = y$, is an equivalence relation & the orbits are the equivalence classes. (orbits are disjoint if not =). So X breaks up as a disjoint union of G-orbits.
(eg, if $H \leq G$ & H acts on G by left mult, the orbits of the action are the cosets $_H\backslash G$)
- transitivity $\Leftrightarrow$ one orbit $\mathcal{O}_x = X \ \forall x \in X$

Ex: Orbits of S_4 acting on itself by conjugacy.

orbit	$\{e\}$,	$\mathcal{O}_{(12)}$ = all transp's,	$\mathcal{O}_{(123)}$,	$\mathcal{O}_{(12)(34)}$,	$\mathcal{O}_{(1234)}$	
size	1 +	6 +	8 +	3 +	6	= 24

Orbits are called conjugacy classes

Thm (Orbit-Stabilizer Thm): $G \curvearrowright X$. Then, for each $x \in X$, $\exists$ bijection $G/G_x \xrightarrow{\sim} \mathcal{O}_x$. In particular, if G finite, $\frac{|G|}{|G_x|} = |\mathcal{O}_x| \Rightarrow |\mathcal{O}_x| \cdot |G_x| = G$.

Ex: ① $G = GL_2(\mathbb{R})$, $X = \{\text{lines in } \mathbb{R}^2\}$, $x = x\text{-axis} = \mathbb{R}\cdot\begin{bmatrix}1\\0\end{bmatrix}$

$\mathcal{O}_x = X$ (b/c action is transitive)

$G_x = \left\{\begin{bmatrix}a&b\\c&d\end{bmatrix} \text{ s.t. } \begin{bmatrix}a&b\\c&d\end{bmatrix}\begin{bmatrix}\alpha\\0\end{bmatrix} = \begin{bmatrix}*\\0\end{bmatrix}\right\} \Rightarrow c = 0$

$=$ upper Δ matrices

$=$ Borel subgp B.

So, $GL_2(\mathbb{R})/B \xrightarrow{1:1} \{\text{set of lines in } \mathbb{R}^2\}$

$\xrightarrow{\text{slope}} \mathbb{P}^1(\mathbb{R}) = \mathbb{R}\cup\{\infty\}$ = projective line over $\mathbb{R}$

② $G \curvearrowright G/H$ by left multiplication.

Stab. of H? $\{g \in G \mid gH = H\} = H$.

(every subgp is a stabilizer in some action)

10/4 $G \curvearrowright X$. O-S Thm: $\exists$ bijection from $G/G_x \xrightarrow{\sim} \mathcal{O}_x$.

Pf: The bijection sends a coset gG_x to gx.

1. Check well-def: Suppose $gG_x = g'G_x$ (WTS $gx = g'x$)

$gx = g'[(g')^{-1}g]x$, $(g')^{-1}gG_x = G_x$

$\in G_x$ (stab $\to$ sends x to x) $\Rightarrow (g')^{-1}g \in G_x$

$= g'x$

2. In opp. dir. $gx \mapsto gG_x$ (Check if $gx = g'x$, then $gG_x = g'G_x$)

Thm (Cauchy): If G a finite gp & $p \mid |G|$, then $\exists$ an elt $g \in G$ of order p. (p prime)

Pf: Let X be the set of ordered p-tuples $(g_1, \dots, g_p)$ drawn from G s.t. $g_1 g_2 \cdots g_p = e$.

$|X| = |G|^{p-1}$ (can freely choose $g_1, \dots, g_{p-1}$ ($|G|$ choices each) then g_p is completely determined)

$\mathbb{Z}/p\mathbb{Z}$ acts on X by cyclic permutation:

-ie, 1 sends $(g_1, \dots, g_p)$ to $(g_p, g_1, g_2, \dots, g_{p-1})$

(if do it p-times, get back to $(g_1, \dots, g_p)$)

(Check condition satis.): $g_p g_1 \cdots g_{p-1} = g_p(g_1 g_2 \cdots g_p)g_p^{-1}$

$= e^{g_p} = g_p e g_p^{-1}$

$= e$.

$\Rightarrow$ if cyclically permute order of mult, get a conjugate of orig. prod.

$\Rightarrow$ actually an action.

What are the orbits of $\mathbb{Z}/p\mathbb{Z}$ on X?

$|\mathcal{O}_x| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\text{Stab}(x)|}$ (no subgps of $\mathbb{Z}/p^2$ other than $\{e\} \neq \mathbb{Z}/p\mathbb{Z}$)

$\Rightarrow |\mathcal{O}_x| = 1$ or p.

N_1 = # of orbits of size 1

N_p = # ——"—— size p

$|X| = N_1 + pN_p$ now, reduce mod p:

$\|$

$|G|^{p-1}$ $\quad N_1 \equiv 0 \pmod p$, since $|X|$ & pN_p are mults of p.

Which x have $|\mathcal{O}_x| = 1$, ie $\text{stab}(x) = \mathbb{Z}/p\mathbb{Z}$

$(g_1, \dots, g_p) \Rightarrow (g_p, g_1, \dots, g_{p-1}) \Rightarrow g_1 = g_2 = g_3 = \dots$ etc

$= (g, g, \dots, g)$ with $g^p = 1$

(fixed pts are in bij. w/ elts of G s.t. $g^p = 1$)

So # of elts of G of exact order p is $N_1 - 1$.

$N_1 - 1 = -1 \bmod p \neq 0$, ↑ don't count $(e, \dots, e)$

thus $\exists\, g \in G$ s.t. $|g| = p$.

3 ways to prove smth exists:

1. Construct it
2. Show # smth > 0
3. Show # smth is not divisible by p. (as in prev. proof)

Thm: Let G be a finite p-group (ie, gp s.t. $|G| = p^n$)
Then Z_G is non-trivial.

Pf: Let G act on itself by conjugacy. For each
$x \in X$ $|\mathcal{O}_x| = p^m$ (b/c its a divisor of $|G|$) $m \leq n$.

$|X| = \sum_{\text{orbits}} |\mathcal{O}_x|$

$\|$

$|G|$

If $g \in X$ has $|\mathcal{O}_g| = 1$, then $hgh^{-1} = g$ $\forall h$ $\Rightarrow$ g central
ie $g \in Z_G$ $\Rightarrow$ # of orbits of size $1 = |Z_G|$

$|G| = |Z_G| + \sum_{\text{non-central orbits}} |\mathcal{O}|$ ← orbits of size > 1

Class Eqn: holds for any finite gp

$p \mid |G| \;\&\; p \mid \sum_{\substack{\text{n-c}\\ \text{orbits}}} |O| \Rightarrow p \mid |Z_G| \Rightarrow Z_G \neq \{e\}.$

(If $p \mid |G|$, $\exists\ H \leq G$ w/ $|H| = p$ otherwise $H = \langle g \rangle$ where $g^p = e$.)

In fact, Cauchy's thm can be greatly generalized to the Sylow Thm.

Thm (Sylow): Let G be a finite gp & let p^n be the largest power of p dividing $|G|$. Then $\exists$ a subgp $H \leq G$ w/ $|H| = p^n$, called a p-Sylow subgp

Pf: Let G be the smallest finite gp for which 1 thm is false.

If $H \leq G$ is a proper subgp, then $[G:H] = \frac{|G|}{|H|} = |G/H|$ is divisible by p. Otherwise, $p^n \mid H$ thus H satisfies thm & H has a subgp of order p^n, which would be a p-Sylow for G.

(G acts on self by conjugation)

Each $|O_x| = |G|/|G_x|$ for non-central, $G_x \neq G \Rightarrow G_x \subsetneq G$

$\Rightarrow |O_x|$ is a multiple of p.

$|G| = |Z_G| + \sum_{\substack{\text{n-c}\\ \text{orbits}}} |O_x| \Rightarrow p \mid |Z_G|$.

By Cauchy, $\exists\ z \in Z_G$, order of z is p. Let $K = \langle z \rangle$, $|K| = p$. K is normal in G b/c it's central.

Let $\bar{G} = G/K$. $|\bar{G}| < |G|$, so $\bar{G}$ has a Sylow p-subgp, $\bar{P}$ & $|\bar{P}| = p^{n-1}$ (b/c $|\bar{G}| = |G|/|K| = p^n/p = p^{n-1}$)

$f: G \to G/K$

Let $P = f^{-1}(\bar{P})$ By 3rd iso. thm, $K \leq P \leq G$ subgp & $P/K \cong \bar{P} \Rightarrow \frac{|P|}{|K|} = |\bar{P}| \Rightarrow |P| = p^n$. contradiction.

Ex: $|S_6| = 720 = 2^4 \cdot 3^2 \cdot 5$ & thus has subgp of order 16, 9, & 5.

$\langle (12345) \rangle$

$\langle (123), (456) \rangle$

Ex: S_3. $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$ are 2-Sylow subgps
$[|S_3| = 2^1 \cdot 3^1]$ ↑ all conjugate to e/o

Thm: All p-Sylow subgps of G are conjugate to e/o.
(⇒ "the" p-sylow subgp)

Burnside's Lemma: Let G be a finite gp acting on a finite set X. We say x is a fixed pt of g if $gx = x$
[Ex:  S^2: gp of rotations acts on S^2 (rotation by 20°) has 2 fixed pts: N & S pole]
Then, The average # of fixed pts of $g \in G$ = # of orbits of the action.
In particular, if $G \curvearrowright X$ is transitive, a random elt of G has 1 fixed pt on average.
Ex: A random permutation on n letters has 1 fixed pt on average.
For $S_3 = \{e, (12), (13), (23), (123), (132)\}$
# of fixed pts: 3 1 1 1 0 0 Ave = 1
(If randomly permute hats, on ave. one person gets their hat back)

Pf: Ave size of $Fix(g) = \frac{1}{|G|}\sum_{g\in G} |Fix(g)|$; $Fix(g) = \{x \in X \mid gx = x\}$

$= \frac{1}{|G|}\sum_{g\in G} |\{x \in X \mid gx = x\}| = \frac{1}{|G|}\sum_{g\in G}\sum_{x\in X} \varepsilon(g,x)$ $\quad \varepsilon(g,x) = \begin{cases} 1 & \text{if } gx = x \\ 0 & \text{otherwise} \end{cases}$

$= \frac{1}{|G|}\sum_{x\in X}\underbrace{\sum_{g\in G} \varepsilon(g,x)}_{\text{how many } g\text{'s fix } x} = \frac{1}{|G|}\sum_{x\in X} |G_x|$

$= \sum_{x\in X} \frac{|G_x|}{|G|} = \sum_{x\in X} \frac{1}{|\mathcal{O}_x|}$ = # of orbits.

Breaking X up into orbits, each orbit $\mathcal{O}$ contributes $|\mathcal{O}|$ copies of $\frac{1}{|\mathcal{O}|} \Rightarrow 1$

Ex: In transitive case, only one orbit, $\mathcal{O}_x = X$
$\sum_{x\in X} \frac{1}{|X|} = 1$

Burnside's Lemma is step 0 of
- Statistics of random permutations;
- Statistics of random matrices (eg in GL_n)
  (very active area in UW: Vallco; Yin; PH Wood)

Abelian Groups

- Finite abel. gps can be completely classified

Prop 1: Let A be a finite abel. gp (write gp law as $+$)
Then $A = \bigoplus_p A_p$ where A_p is a finite abel. p-gp.

Pf: It suffices to show (by induction on # of distinct primes dividing $|A|$) that for each p, we can write $A = A_p \oplus A_{p'}$ where $p \nmid |A_{p'}|$

A_p = gp of all $a \in A$ s.t. $p^N a = 0$ for some N ($\uparrow$ 1 prime, true by def b/c then A a p-gp.)
$A_{p'}$ = " " s.t. $ma = 0$ for m w/ $p \nmid m$. ($\uparrow$ or $(m,p)=1$)

Claim: A_p & $A_{p'}$ are subgps:
A_p is a gp: if $p^m a_1 = 0$ & $p^N a_2 = 0$, then $p^{m+N}(a_1 + a_2) = 0$
Similarly for $A_{p'}$.

To show: $A_p \cap A_{p'} = \{e\}$; $A_p + A_{p'} = A$; $A_p, A_{p'}$ normal ✓
↳ b/c if $a \in A_p \cap A_{p'}$, then $p^n a = 0$ & $ma = 0$, (all subgps of abel gps are normal)
but $(m, p^n) = 1 \Rightarrow rm + sp^n = 1 \Rightarrow (rm + sp^n)a = \{a$ $r(ma) + s(p^n a) = 0$
10/9 [Notation: $A[p] = \{a \in A \mid pa = 0\}$ (p-torsion subgp) $\longrightarrow \Rightarrow a = 0$.
use notation for abel gps only b/c then it will form a subgp. $A[p] \leq A[p^n]$
$A[p^n] = \{a \in A \mid p^n a = 0\}$. $A[p] = \bigcup_n A[p^n] = A[p^\infty]$ = "p-primary part of A" ↑ eventually killed by p^N]

Claim: $A = A_p \oplus A_{p'}$ suffices:
Note that $|A_{p'}| \mid |A|$
$p \nmid |A_{p'}|$ b/c then $\exists$ (would) $a \in A_{p'}$ s.t. $pa = 0$ &.
$A_{p'} = \bigoplus$ (simple) A_q.

To prove claim, need $A_p, A_{p'}$ normal ✓
need $A_p \cap A_{p'} = \{e\}$ ✓
need $A_p A_{p'} = A$

Pf that $A_p A_{p'} = A$.
$(|A_p|, |A_{p'}|) = 1 \Rightarrow$ so $\exists x, y$ s.t. $x|A_p| + y|A_{p'}| = 1$
So for any a,
$a = \underbrace{x|A_p|a}_{\in A_{p'}} + \underbrace{y|A_{p'}|a}_{\in A_p}$

Why is $|A_{p'}|a \in A_p$?
write $\text{ord}(a) = mp^k \quad (m,p) = 1$
$mp^k \mid |A|$
Since $p^k a$ is of order m, then $p^k a \in A_{p'}$, so $m \mid |A_{p'}|$
So $|A_p| = mb$ & $|A_{p'}|a = bma$ & $p^k(|A_{p'}|a) = bmp^k a = b \cdot 0 = 0$

$\Rightarrow |A_{p'}|a \in A[p^k] \subset A_p$.
($|A_{p'}|a$ is killed by p^k)

So $A_p \oplus A_{p'} = A$. ✓

eg. $(\mathbb{Z}/15\mathbb{Z}) = A_3 \oplus A_5$ (finite gps of prime order are cyclic)
$= (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z})$
$\Rightarrow$ equivalent to the Chinese remainder thm.

Remark: A_p is the p-Sylow subgp of A
$\prod_p |A_p| = |A|$ (gp "factors" into primes)

What can A_p be?

Thm: Let A be a finite abel. p-gp. Then $A \cong \bigoplus_{i=1}^{k} \mathbb{Z}/p^{r_i}\mathbb{Z}$
(breaks up into cyclic gps of prime order).
$\exists$ $(r_1, \dots, r_k)$ is unique up to permutation.
(won't prove in class)

What if we don't require finite?
- $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $\mathrm{Cont}(\mathbb{R}, \mathbb{R})$, $\mathbb{Q}/\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^{\aleph_0}$ Aaaah!

We will consider only finitely generated gps.

Thm: Let A be a finitely gen. abel. gp. Then
$A \simeq \mathbb{Z}^{\oplus r} \oplus T$, where T is finite. (so we can classify T further)
$\uparrow$
$(\bigoplus_{i=1}^{r} \mathbb{Z} = \mathbb{Z}^r)$

*every finitely gen abel gp is $\simeq$ to a $\oplus$ of cyclic gps (some ∞ & some finite).

Prop: Let A an abel. gp, & $f: A \to \mathbb{Z}^k$ a surjective hom.
Then $A \simeq (\ker f) \oplus \mathbb{Z}^k$
$\leq A$ $\quad$ quotient of A. (not subgp)

Pf: Let $b_1, \dots, b_k$ generate $\mathbb{Z}^k$.
$(1,0,\dots,0)$ $(0,\dots,0,1)$

Since f surj., Let $a_i \in A$ satisfy $f(a_i) = b_i$. Let
$A_0 = \langle a_1, \dots, a_k \rangle$.
$a \in A_0 \cap \ker f$, then $a = \sum n_i a_i$ & $f(a) = \sum n_i f(a_i) = \sum n_i b_i = 0$
$\Rightarrow n_i = 0 \ \forall i \Rightarrow a = 0$, so $A_0 \cap \ker f = \{e\}$

What is $A_0 + \ker f$? "diagram chasing argument"
Given $a \in A$, $f(a) = \sum n_i b_i \in \mathbb{Z}^k$
$f(\sum n_i a_i) = \sum n_i b_i$
So $f(a - \sum n_i a_i) = 0$ ($\in A_0$)
$\Rightarrow a = \underbrace{(a - \sum n_i a_i)}_{\in \ker f} + \underbrace{\sum n_i a_i}_{\in A_0} \Rightarrow A = \ker f \oplus A_0$.

Now $\frac{A_0 \oplus \ker f}{\ker f} \simeq A_0/A_0 \cap \ker f$ i.e. $\Rightarrow A/\ker f \simeq A_0$ ✓
$\uparrow$ and $\simeq \mathbb{Z}^k$

Usually this is described as an exact sequence of Abel. gp's.

$$0 \to \ker f \xrightarrow{i} A \xrightarrow{f} \mathbb{Z}^k \to 0$$

(i: inclusion; g: ← we constructed this hom.)

[exact : $\ker$(outward map) = im(inward map)]

What we just did is show that this exact sequence splits into $\ker f \oplus \mathrm{im}(g)$

ie, we constructed a hom: $\mathbb{Z}^k \to A$ w/ $g(b_i) = a_i$.

& $A_0 = \mathrm{im}(g)$

Def: A gp G is torsion-free if it has no non-trivial elts of finite order.

eg.: ① $\mathbb{Z}$ ✓ $n \neq 0$, $nz \neq 0$ $\forall z \in \mathbb{Z}$

Prop: Suppose A is finitely gen., abel, & torsion-free.
Then $A \cong \mathbb{Z}^k$ for some k.

Pf: Let k be minimal s.t. A can be generated by k elts.

Induct on k:

If $k=1$, A cyclic, so $A \cong \mathbb{Z}$ ✓

Now, let k arbitrary, & let A be gen by $a_1, a_2, \dots, a_k$.

If $\exists b \in A$ s.t. $mb = a_i$, $m > 1$, then replace a_i with b.

* [NTS this process terminates.]

Claim: $A = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_k$

To prove this, take

$B = A/\mathbb{Z}a_i$. B is still torsion-free:

(In general, a quotient of a t-free gp is not t-free: ex: $\mathbb{Z}/2\mathbb{Z}$)

If B not t-free, $\exists b \in B$, $b \neq 0$ s.t. $mb = 0$.

$A \twoheadrightarrow B$ so we can choose $\tilde{b} \in A$ which projects to b.

So $m\tilde{b}$ projects to $mb = 0$

So $m\tilde{b} \in \mathbb{Z}a_1$ (the ker of the surjection)

$m\tilde{b} = na_1$ (÷ by prime factor of m & n so that $(m,n) = 1$)

Suppose m & n have a common factor q. Then

$m = m'q$ & $n = n'q$ $\quad (m', n') = 1$ $\quad \Rightarrow q = \gcd(m,n)$

So, $m'q\tilde{b} = n'qa_1$

$q(m'\tilde{b} - n'a_1) = 0$ $\quad$ b/c A torsion-free;

$\Rightarrow m'\tilde{b} - n'a_1 = 0$

$\Rightarrow m'\tilde{b} = n'a_1$

So, $m\tilde{b} = na_1$ w/ $(m,n) = 1$

$rm + sn = 1$

Consider $s\tilde{b} + ra_1$

$m(s\tilde{b} + ra_1) = sm\tilde{b} + rma_1$

$= sna_1 + rma_1$

$= (sn + rm)a_1$

$= a_1$ $\quad \Rightarrow m = 1.$

So B is torsion-free.

And B is gen. by images of $a_2, \ldots, a_k$, so by induction $B \cong \mathbb{Z}^{k-1}$

Now, $A \twoheadrightarrow B$ gives $A \xrightarrow{f} \mathbb{Z}^{k-1}$ which, by prop. above, shows that $A = \ker f \oplus \mathbb{Z}^{k-1} = \mathbb{Z}a_1 \oplus \mathbb{Z}^{k-1} \cong \mathbb{Z}^k$.

10/11 Recall: If $f: A \to \mathbb{Z}^k$ is surjective (A abel.) then $A \cong \ker f \oplus \mathbb{Z}^k$

Finishing Classification of finitely gen. abel. gps:
Let A be an abel. gp.
Def: The torsion subgp of A $T(A) \subset A$ (or A^{tors})
is $\{a \in A \mid ma = 0 \text{ for } m \neq 0\}$ (finite order elts of A)
$ma_1 = 0$ & $na_2 = 0 \Rightarrow mn(a_1 + a_2) = 0 \Rightarrow$ subgp
Note: -torsion elts do not always form a subgp:
$\langle x, y \mid x^2 = y^2 = 1 \rangle$, but xy has ∞ order.
-only true for abel. gps.

Claim: $A/T(A)$ is torsion free.
Let $\bar{a} \in A/T(A)$. If $m\bar{a} = 0$, let $a \in A$ lie above $\bar{a}$.
I know that ma maps to 0 in $A/T(A)$, so
$ma \in T(A)$, so it is torsion, so $m'(ma) = 0$ for $m' \neq 0$
so $a \in T(A)$, so $\bar{a} = 0$.
$A/T(A)$ is a quotient of f.g. gp $\Rightarrow$ $A/T(A)$ is f.g.
So $A/T(A) \cong \mathbb{Z}^k$
$f: A \twoheadrightarrow A/T(A) \xrightarrow{\sim} \mathbb{Z}^k$
$f: A \to \mathbb{Z}^k$
$\ker f = T(A)$ (composing w/ an iso. doesn't change ker)
So $A \cong \mathbb{Z}^k \oplus T(A)$ * k is the rank A
modding out by $\mathbb{Z}^k$ gives a surjection $A \to T(A)$
so $T(A)$ is finitely gen.
(
Each generator of $T(A)$ has finite order $\Rightarrow$ $T(A)$ is finite. ✓

Remark: Every subgp of $\mathbb{Z}^k$ is finitely gen.
[Not true that every subgp of a f.g. gp is f.g.]
Every quotient of a f.g. gp is f.g.
↑ may be true if subgp has finite index

Composition Series

$1 \to N \to G \to G/N \to 1$ is <u>exact</u> means

the image of each arrow = kernel of subsequent arrow.

"breaks up G into N & G/N"
If G finite $|G| = |N| \cdot |G/N|$
Nicest case: $G = N \oplus N'$ (Is $G \simeq N \oplus G/N$?)
N' is G/N

(Yes, when G abel. & $G/N \simeq \mathbb{Z}^k$)

But not always true:

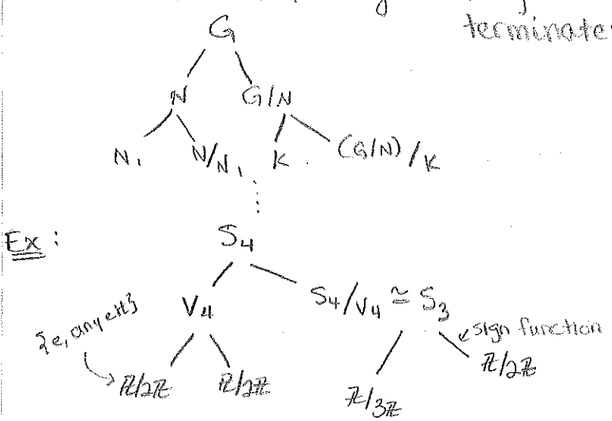
(a) $1 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$
$(a,0)$ $(a,b) \longmapsto b$
$\ker = (a,0)$

(b) $1 \to \frac{2\mathbb{Z}}{4\mathbb{Z}} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$
2 $1 \longmapsto 1$
$\mathbb{Z}/2\mathbb{Z}$

} same 2 pieces (ie 1st & 3rd), but diff G (ie middle) ↑ they're not $\simeq$

So N & G/N don't determine G. we have to know how they are "glued together."

Let G be finite, & imagine doing this iteratively, until it terminates.



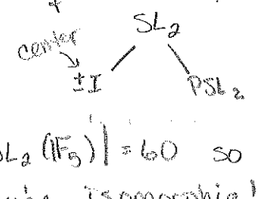
Ex:

This process terminates when each endpt is a gp having no normal subgps other than 1 & itself.
Such a gp is called <u>simple</u>.

<u>Exs</u>: i) Any gp of prime order is simple. In fact, if $|G|=p$, G is cyclic b/c if not for $g \in G$, nontrivial, $\langle g \rangle \subset G$ nontrivial & $|\langle g \rangle| \mid p \Rightarrow |\langle g \rangle| = p \Rightarrow \langle g \rangle = G. \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$

ii) A_n is simple if $n \geq 5$.
- A_5 = icosahedral gp; $|A_5| = 60$; smallest non-abel. simple gp

iii) $PSL_2(\mathbb{F}_q)$ is simple if $q \geq 4$.



- $|PSL_2(\mathbb{F}_5)| = 60$ so seems to tie w/ A_5, but they're isomorphic! (Klein, The icosahedron)

iv) $PSL_n(\mathbb{F}_q)$

v) Other algebraic families (ie, symplectic gp)
↑ matrices over finite fields

Also, 26 sporadic simple gps, & that's it.

<u>Def</u>: A <u>composition series</u> for a gp G is a sequence
$1 = G_0 \subset G_1 \subset \cdots \subset G_{k-1} \subset G_k \subset G = G_{k+1}$
where each G_i is a maximal normal subgp of G_{i+1}.
(recall: a normal subgp btwn G_i & G_{i+1} yields a normal subgp of G_{i+1}/G_i)
So G_i maximal normal in $G_{i+1} \Leftrightarrow G_i$ normal in G_{i+1} & G_{i+1}/G_i is simple.

This comp. series gives a list of simple gps (the quotient): G/G_k, G_k/G_{k-1}, ..., G_2/G_1, G_1. these are called <u>composition factors</u>.

<u>Thm (Jordan Hölder Decomposition)</u>: Let G a finite gp. Then every composition series for G has the same (multi) set of composition factors.

[Notation: The comp. series is a <u>filtration</u> of G & the comp. factors are called <u>graded pieces</u>]

<u>The Case of p-Gps</u>:
Let G be a finite gp of p-power order. Then Z_G is nontrivial. Let G_1 be an order p subgp of Z_G. $\mathbb{Z}/p\mathbb{Z}$
$1 \subset G_1 \subset \ldots$?

<u>Claim</u>: Every finite p-gp has a composition series in which every comp. factor is $\mathbb{Z}/p\mathbb{Z}$.

<u>Pf</u>: By induction on $|G|$, let G be the smallest counterex & G as above:

$0 \subset G_1 \subset Q_1 G_1 \subset Q_2 G_1 \subset \ldots \subset Q_k G_k \subset G$

$Q = G/G_1$ has a comp series $Q_1 \subset Q_2 \subset \ldots$

10/16 $1 \trianglelefteq G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$ a composition series.
- Successive quotients are simple gps.

Def: G is solvable if $\exists$ a series s.t. G_i/G_{i+1} is abelian.

Def: $G^{(0)} = G$, (all normal & quotients are all abel).
$G^{(1)} = [G,G]$
$G^{(2)} = [G^{(1)}, G^{(1)}]$ This is called the derived series.
⋮

Thm: If G is finite, then $G \trianglerighteq G^{(0)} \trianglerighteq G^{(1)} \cdots$ terminates iff G is solvable.
If $[H,H] = H$, then H is called perfect.

* G/H abelian $\Leftrightarrow$ H contains $[G,G]$.
The shortest solvable series is the derived series, but there may be other longer solvable series as well.

Pf: ($\Rightarrow$) If the derived series terminates, then you wrote a solvable series & the gp is solvable. ✓
($\Leftarrow$): Need a prop:
Prop: Let $N \trianglelefteq G$. G solvable iff N & G/N are solvable.

($\Leftarrow$): G solvable $\Rightarrow G^{(1)}$ solvable $\Rightarrow \cdots$
$\Leftarrow$ b/c $G^{(1)} \trianglelefteq G$.

Suppose the derived series stabilizes, ie
$G^{(k)} = [G^{(k)}, G^{(k)}]$. $G^{(k)}$ is solvable, so
$G^{(k)} \trianglerighteq G_1^{(k)} \trianglerighteq \cdots \trianglerighteq 1$, w/ abel. quotients
$\Rightarrow$ so $G_1^{(k)} \geq [G^{(k)}, G^{(k)}]$, so terminates at 1 step
$(G_1^{(k)} = G^{(k)})$, so $G^{(k)}$ not solvable $\Rightarrow$ contradiction

Pf of Prop. ($\Rightarrow$) Suppose G solvable.

$G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = 1$. Let $N \trianglelefteq G$.

$N \trianglerighteq G_0 \cap N \trianglerighteq G_1 \cap N \trianglerighteq \cdots \trianglerighteq G_n \cap N = 1$ (some terms could be trivial)

NTS: $G_i \cap N / G_{i+1} \cap N$ is abelian.

$G_i \cap N \hookrightarrow G_i \Rightarrow G_i \cap N \to G_i / G_{i+1}$

$\ker = G_{i+1} \cap N$ b/c $(G_i \cap N) \cap G_{i+1}$

$\Rightarrow G_i \cap N / G_{i+1} \cap N \hookrightarrow G_i / G_{i+1} \Rightarrow N$ solvable.

abel $\Uparrow$ $\uparrow$ injects $\uparrow$ abelian

$\phi: G \to G/N$

$\overline{G_i} = \phi(G_i)$

$\overline{G_{i+1}} \trianglelefteq \overline{G_i}$ & ϕ surjective, so $\overline{G_{i+1}} \trianglerighteq \overline{G_i}$

$\Rightarrow G/N \trianglerighteq \overline{G_0} \trianglerighteq \overline{G_1} \trianglerighteq \cdots \trianglerighteq \overline{G_n} = 1$

$\overline{G_i} / \overline{G_{i+1}} \cong \phi(G_i) / \phi(G_{i+1}) \overset{3\text{rd iso thm}}{\cong} \phi\left(G_i / G_{i+1}\right)$ (image of abel sp)

$\Rightarrow \overline{G_i} / \overline{G_{i+1}}$ abel & series is solvable, so G/N solvable.

($\Leftarrow$): N & G/N are solvable.

$N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_n = 1$ a solvable series

$G/N = \overline{G_0} \trianglerighteq \overline{G_1} \trianglerighteq \cdots \trianglerighteq \overline{G_m} = 1$ a solvable series

$\overline{G_i} \leftrightarrow G_i \leq G$ (correspondence)

if $\overline{G_i} \trianglelefteq G/N$ then $G_i \trianglelefteq G$

if $\overline{G_{i+1}} \trianglelefteq \overline{G_i}$ then $G_{i+1} \trianglelefteq G_i$

(Lattice thm for G/N)

$G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_n = 1$ is a normal series (by lattice thm), solvable?

$G_i / G_{i+1} \cong \frac{G_i/N}{G_{i+1}/N} \cong \overline{G_i} / \overline{G_{i+1}}$ abelian.

G_m / N_0 is trivial, so ok. $\Rightarrow$ solvable. ✓

Ex: 1. abelian gps are solvable.

2. S_n solvable $\Leftrightarrow n \leq 4$

(related to: A_n simple $n \geq 5$)

$[S_n, S_n] = A_n$:

S_n/A_n abel, so $A_n \geq [S_n, S_n]$

$(a\,b)(b\,c) = (a\,b\,c)$

$(a\,b)(c\,d) = (a\,b\,c)(b\,c\,d)$

so any pair is a prod. of 3-cycles, so 3-cycles generate A_n.

$A_n \trianglelefteq S_n$ & all k-cycles are conjugates of e/o.

If $H \trianglelefteq G$, $H \leq A_n$, & H contains a single 3-cycle, then $H = A_n$. So only need one 3-cycle in $[S_n, S_n]$, & $A_n = [S_n, S_n]$

& $((a\,b)(b\,c))^2 = (a\,b\,c)^2 = (a\,c\,b)$

$\in [S_n, S_n]$ ✓

If $n \geq 5$: $S_n \trianglerighteq A_n \trianglerighteq A_n \trianglerighteq \cdots$ & series stabilizes

↑simple, so only normal subgps are 1 & A_n,

but A_n not abelian, so $[A_n, A_n] \neq 1 \Rightarrow [A_n, A_n] = A_n$.

$\Rightarrow S_n$ not solvable.

Def: G a gp.

$Z_0(G) = 1 \trianglelefteq \underset{\substack{\| \\ Z(G)}}{Z_1(G)} \trianglelefteq \cdots \trianglelefteq Z_{i+1}(G)$

$Z_{i+1}(G) = \pi_i^{-1}\left(Z(G/Z_i(G))\right)$ where $\pi_i : G \to G/Z_i(G)$

$Z_i(G) \trianglelefteq G \Rightarrow Z_i(G) \trianglelefteq Z_{i+1}(G)$

called the upper central series.

→ If G has trivial center, then $Z_i(G) = 1 \ \forall i$, even for finite gps.

→ quotients will be abelian.