Group Theory
Week #4, Lecture #15

I Center of a group

$$Z(G) = \{ g \in G : gx = xg, \ \forall x \in G \} \trianglelefteq G$$

Recall: $\mathrm{Aut}(G) = \{ \varphi : \varphi : G \to G \text{ automorphism} \}$

$\qquad \vee$

$\mathrm{Inn}(G) = \{ \tau_g : g \in G \}$ where $\tau_g(x) = gxg^{-1}$

note: $g \in Z(G) \iff \tau_g(x) = gxg^{-1} = gg^{-1}x = x$

$\iff \tau_g = id_G$ (The identity in $\mathrm{Inn}(G)$ and also in $\mathrm{Aut}(G)$)

Prop $G/Z(G) \cong \mathrm{Inn}(G)$

Proof Let
$$\tau : G \twoheadrightarrow \mathrm{Inn}(G), \quad g \longmapsto \tau_g$$

This is a surjective homomorphism, with $\boxed{\ker(\tau) = Z(G)}$ (by the note)

By FTH:
$$\begin{tikzcd} G \arrow[r, two heads, "\tau"] \arrow[d, "\pi"'] & \mathrm{Inn}(G) \\ G/Z(G) \arrow[ur, dashed, "\bar{\tau}"'] & \end{tikzcd}$$
with $\bar{\tau}$ an isomorphism

QED

II Simple groups

Def A group is <u>simple</u> if it is nontrivial and it contains no nontrivial proper <u>normal</u> subgroups

$$G \text{ simple} \overset{def}{\iff} \big(G \neq \{e\} \text{ and } (N \trianglelefteq G \Rightarrow N = \{e\} \text{ or } N = G) \big)$$

Equivalently:

$$G \text{ simple} \iff \big(\forall \varphi : G \to H \text{ hom} \Rightarrow \ker\varphi = \{e\} \text{ or } \ker\varphi = G \big)$$

$\iff$ G has no factor groups, except for G and $\{e\}$

Examples (1) $G = \mathbb{Z}_p$, p prime ($\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \dots$)
is simple

reason: If $H \triangleleft G \underset{G \text{ abel}}{\iff} H < G$, then $|H| \mid |\mathbb{Z}_p| = p$

$\underset{p \text{ prime}}{\Longrightarrow} |H| = 1$ or $|H| = p$

$\Updownarrow$ $H = \{e\}$ $\quad$ $\Updownarrow$ $H = G$

Note: The cyclic groups of prime order are the only finite abelian groups which are simple.
(Proof: later on)

(2) The smallest non-abelian simple group is
(i.e., non-cyclic)
A_5 (the alternating group of order $\frac{5!}{2} = 60$)
(this implies that one cannot solve the quintic equation by radicals — Galois)

III Symmetric & Alternating groups

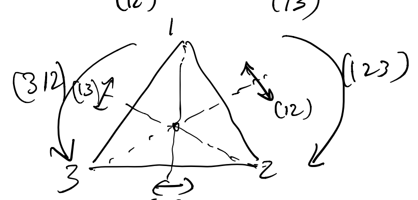
Let $S_n = \mathrm{Sym}([n])$, where $[n] = \{1, 2, \dots, n\}$ (ordered set)
— the group of all bijections of the set $[n]$ with group operation = composition

Simplest examples: $S_1 = \{id\}$ trivial group

$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} \cong \mathbb{Z}_2$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

cycle notation $\rightarrow$ $()$, (12), (13), (23), (123), (312).



note: $|S_n| = n!$

reason: $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \boxed{n} & \boxed{n-1} & \boxed{n-2} & & \boxed{1} \end{pmatrix}$

choices

Def (Sign of a permutation) Given a permutation $\sigma \in S_n$, we define its <u>sign</u> to be

$$\boxed{\mathrm{sgn}(\sigma) = (-1)^{N(\sigma)}} \in \{\pm 1\} \cong \mathbb{Z}_2 = \{0, 1\}$$

$$1 \longleftrightarrow 0 \qquad -1 \longleftrightarrow 1$$

where

$$\boxed{N(\sigma) = \#\{(x,y) \in [n]^2 : \ x < y \text{ and } \sigma(x) > \sigma(y)\}}$$

eg: (1) $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \to N(\sigma) = \#\{(1,2)\}$ $\left(\begin{matrix} 1 < 2 \text{ but} \\ \sigma(1) = 2 > 1 = \sigma(2) \end{matrix}\right)$

$\to \mathrm{sgn}(\sigma) = -1$ (more generally, any transposition has sign $= -1$)

(2) $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\quad \left.\begin{matrix} (1,2) \to (2,3) \checkmark \\ (1,3) \to (2,1) \\ (2,3) \to (3,1) \end{matrix}\right\} \to N(\sigma) = 2 \quad \to \mathrm{sgn}(\sigma) = 1$

$(123) = (13)(12)$

Def Permutations with sign 1 (i.e., 0 in $\mathbb{Z}_2$) are called <u>even</u>.

The ones with sign -1 (i.e., 1 in $\mathbb{Z}_2$) are called <u>odd</u>.

<u>Remark</u> It can be shown that

$$N(\sigma) = \#\{\text{transpositions in a decomposition of } \sigma \text{ into a product of transpositions}\}$$

exercise $\to$ [Such a decomposition is not unique, but the parity of this quantity depends only on σ (i.e. $N(\sigma) \bmod 2$ is well-defined)]

The above discussion yields a map

$$\mathrm{sgn} : S_n \longrightarrow \mathbb{Z}_2 \qquad \mathrm{sgn}(\sigma) = \begin{cases} 0 & \sigma \text{ even} \\ 1 & \sigma \text{ odd} \end{cases}$$

For $n \geq 2$, this function is surjective, since $\begin{cases} \mathrm{sgn}\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = 0 \\ \mathrm{sgn}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = 1 \end{cases}$

Furthermore, sgn is a homomorphism, since we are counting the parity of # of transpositions in a decomposition, so

$$N(\sigma \cdot \sigma') = N(\sigma) + N(\sigma') \pmod 2$$

$$\therefore \underbrace{(-1)^{N(\sigma\sigma')}}_{\operatorname{sgn}(\sigma\sigma')} = (-1)^{N(\sigma)+N(\sigma')} = \underbrace{(-1)^{N(\sigma)}}_{\operatorname{sgn}(\sigma)} \cdot \underbrace{(-1)^{N(\sigma')}}_{\operatorname{sgn}(\sigma')}$$

Problem (#5, §3.8) Show that #{even perms} = #{odd perms}

Definition Define the <u>alternating group</u> on n elements as the set of even permutations in S_n.

Notation: A_n

Lemma A_n is a normal subgroup of S_n, and has order $n!/2$.

Proof $A_n = \ker(\operatorname{sgn} : S_n \twoheadrightarrow \mathbb{Z}_2)$

$\therefore A_n \trianglelefteq S_n$

$$\therefore |A_n| = \frac{|S_n|}{|\mathbb{Z}_2|} = \frac{n!}{2}$$

$\blacksquare$

Corollary #{even permutations} = #{odd permutations}

Proof ($n \geq 2$)

$$\boxed{S_n = \underbrace{\{\text{even perms}\}}_{A_n} \sqcup \underbrace{\{\text{odd perms}\}}_{(12)A_n \text{ coset of } A_n}}$$

But $|A_n| = |(12)A_n|$ (The cosets of a subgroup always have the same size!)

i.e. $|\{\text{even perms}\}| = |\{\text{odd perms}\}|$

QED

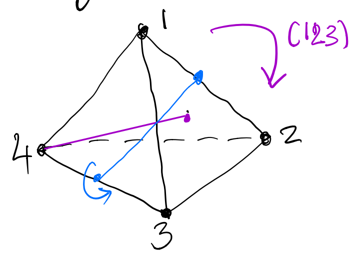
Eg: $A_1 = S_1 = \{1\}$

$A_2 = \{1\}$

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \cong \mathbb{Z}_3$$

A_4 is a group of order 12

It can be realized as the group of rotations of a regular tetrahedron



(4 vertices, 6 edges, 4 faces)

elements:

- identity — 1
- 120° rotations through axes joining a vertex to the barycenter of the opposite face: — 8

  (123), (134), (234), (124)
- (12)(34), (13)(24), (14)(23) — 3

  180° rotation through axis joining (12) to (34) edges.

note: all non-identity elements of A_4 are products of exactly two transpositions

Exercise Find all the subgroups of A_4

Exercise Show that $A_4 \cong PSL_2(\mathbb{Z}_3)$