

Last time:  $G$  a group. examples:  $S_n$ ,  $D_{2n}$ ,  $GL_2(\mathbb{R})$

Lemma: If  $a \in G$  and  $b, b' \in G$  are inverses of  $a$ , then  $b = b'$ .

pf:  $b = b1 = b(ab') = (ba)b' = 1b' = b'$ .  $\square$

Properties of inverse:  $(ab)^{-1} = b^{-1}a^{-1}$ .  $(a^{-1})^{-1} = a$ .

Cancellation prop.:  $ab = ac \Rightarrow b = c \Leftarrow ba = ca$

Defn: Subgroup. nonempty  $H \subseteq G$  closed under  $\cdot$  and  $^{-1}$ .  $H \leq G$  ( $H < G$  if proper)

Lemma:  $\emptyset \neq H \subseteq G$ ,  $H$  subgroup of  $G \Leftrightarrow xy^{-1} \in H \forall x, y \in H$ .

pf  $\Rightarrow$   $x, y \in H \Rightarrow x, y^{-1} \in H \Rightarrow xy^{-1} \in H$ .

$\Leftarrow$   $H \neq \emptyset \Rightarrow \exists a \in H \Rightarrow aa^{-1} = e \in H$

$x, e \in H \Rightarrow ex^{-1} = x^{-1} \in H$

$x, y \in H \Rightarrow xy^{-1} \in H \Rightarrow x(y^{-1})^{-1} = xy \in H$ .  $\square$

Subgroup generated by a subset.

$A \subseteq G \mapsto \langle A \rangle =$  smallest subgroup containing  $A$ .

Convention:  $\langle \emptyset \rangle = \{e\}$

$= \bigcap_{\substack{H \leq G \\ H \supseteq A}} H \longrightarrow$  ex: intersection of subgroups is a subgroup.

$\longrightarrow$  or  $A$  is a set of generators for  $A$

We say  $G$  is generated by  $A \subseteq G$  if  $G = \langle A \rangle$ .

Ex:  $G = S_4$ . Check:  $\overset{A_1}{\{(12), (1234)\}}$ ,  $\overset{A_2}{\{(13), (23), (34)\}}$  are both generating sets for  $S_4$ .

$G$  is finitely generated if  $G = \langle A \rangle$  w/  $|A| < \infty$ .

Ex:  $F_2 =$  free group on 2 letters. finitely generated infinite group.

Cyclic Group: a group generated by one element  $G = \langle \{a\} \rangle = \langle a \rangle$  for some  $a \in G$  notation.

$$G = \{ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots \}$$

option A: if  $G$  is infinite then  $G \cong \mathbb{Z}$  [isomorphism].  
 $\downarrow$   
 all cyclic groups  $\left\{ \begin{array}{l} a^n \leftrightarrow n \\ a^m = a^{n+m} \leftrightarrow nm = n+m \end{array} \right.$

option B: if  $G$  is finite then for some  $k$ ,  $a^k \in \{e, a, a^2, \dots, a^{k-1}\}$ .

let  $k$  be the smallest. claim:  $a^k = e$ .

$$\text{we know } a^k = a^l \Rightarrow a^{k-l} \in \{e, a, a^2, \dots, a^{k-1}\}$$

so if  $l \neq 0$ ,  $k$  isn't minimal. Thus  $G \cong \mathbb{Z}/k\mathbb{Z}$ .

Cyclic Groups:  $\langle a \mid \underbrace{a^k = e}_{\substack{\text{here or not}}} \rangle$  "free"

Example of  $S_n$ .

$(1\ 5\ 3\ 4)$  means



$(\ )(\ )$   
 $\leftarrow$   
 R to L

So one set of generators is all cycles  $(i_1, i_2, \dots, i_l)$

$$(12)(34) = (34)(12) \quad (\text{disjoint})$$

$$\text{but } (1534) = (15)(53)(34),$$

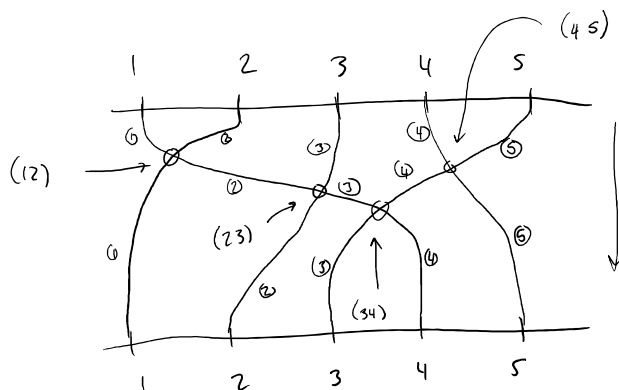
so we have a better set of generators:

transpositions.



Cycles of length 2.  $S_n = \{(i,j) \mid 1 \leq i < j \leq n\}$

Lemma:  $\{\sigma_{i,i+1} \mid 1 \leq i < n\}$  generate  $S_n$ .



$$\text{so } (14532) = (34)(23)(12)(45)$$

Puzzle: soul switching: 5 jumbled souls, how many<sup>extra people</sup> do you need to return them.