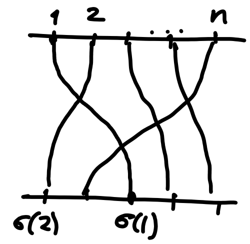
Last time, we discussed presentations of groups by generators & relations.

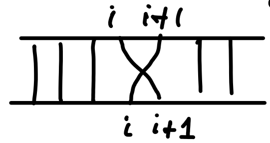
Ex: the symmetric group $S_n \simeq \langle s_1, \dots, s_{n-1} \mid s_i^2 = 1\ \forall i,\ s_i s_j = s_j s_i\ \forall |i-j| \geq 2,\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \rangle$

- the word length of $\sigma \in S_n$ is #inversions ($i<j$ st. $\sigma(i) > \sigma(j)$).
- the longest element is $\begin{pmatrix} 1 & 2 & \dots & n \\ \downarrow & & & \downarrow \\ n & n-1 & \dots & 1 \end{pmatrix}$ of wordlength $\frac{n(n-1)}{2}$

This is best understood by representing permutations as diagrams

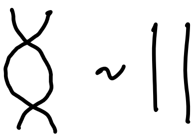


- Composition = stack diagrams
- Expression in terms of s_i comes from decomposing diagram into layers w/ single crossing

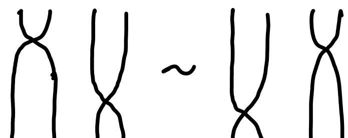


$= s_i$

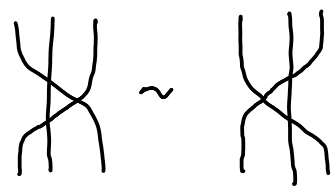
- Presentation of $S_n \iff$ any two diagrams for σ are related by

(1) 

$s_i^2 = e$

(2) 

$s_i s_j = s_j s_i \quad |i-j| \geq 2$

(3) 

$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$

- Word length $w(\sigma)$ = #inversions is now clear
- We can even list all the shortest words that can represent a given permutation!

  Namely: $\sigma \in S_n$ has a shortest word ending with $s_i \iff w(\sigma s_i) < w(\sigma)$

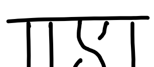
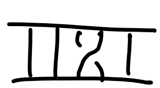
  Call the set of such i the "ending set" of σ. $\iff \sigma(i+1) < \sigma(i)$.

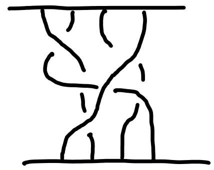
  Then for each $i \in$ ending set, repeat the process for $\sigma s_i^{-1} = \sigma s_i$.
- For each $\sigma \in S_n$ we can find a preferred expression of σ as a word in $s_1, \dots, s_{n-1}$ by choosing at each step the smallest i st. $\sigma(i+1) < \sigma(i)$ to end the word

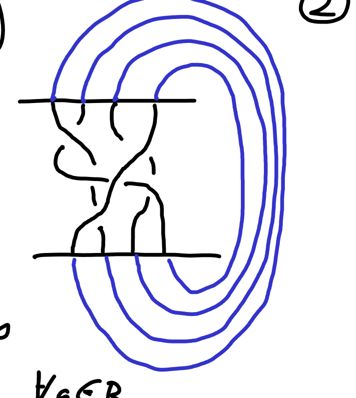
  This gives a normal form for elements of S_n (ie. a prefered word representing each element) and hence a solution to the word problem = when do two words represent the same element? ($\iff$ when does a word represent $e \in G$?).

★ For S_n, or other groups where it's well understood how to "calculate elements" (eg. groups of matrices, etc.), we don't need fancy algorithms or normal forms to solve the word problem. In many groups however this is all we have!

Ex: the braid group $B_n = \langle s_1 \dots s_{n-1} \mid s_i s_j = s_j s_i\ \forall |i-j| \geq 2,\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \rangle$

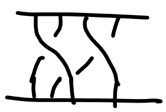
(but $s_i^2 \neq 1$) $\quad s_i =$  $\quad s_i^{-1} =$  

Thus a braid is something like:  (strands never $\circlearrowleft$) up to isotopy
(important in knot theory etc!)



> <u>Markov's theorem</u>: every knot or link in $\mathbb{R}^3$ can be represented as the closure of a braid, and two braids have isotopic closures iff they're related by sequence of moves of 2 types: $\begin{cases} \bullet \text{ conjugation in } B_n: \quad \sigma\in B_n \sim g\sigma g^{-1}\in B_n \ \forall g\in B_n \\ \bullet \text{ stabilization: } B_n \simeq \langle s_1\dots s_{n-1}\rangle \subset B_{n+1}. \quad \sigma\in B_n \sim \sigma s_n^{\pm 1}\in B_{n+1}. \end{cases}$

B_n is much bigger than S_n but its algorithmic aspects can be approached by the same method, using:

- permutation braids =  any 2 strands cross at most once, all crossings .
  These form a finite set, in bijection with S_n.
- let Δ = the longest permutation braid. Since its shortest word can start/end with any s_i, $s_i^{-1}\Delta$ is still a permutation braid. Also note $s_i^{\pm 1}\Delta = \Delta s_{n-i}^{\pm 1}$ $\Rightarrow$ move Δ's left.
  Thus any element of B_n can be written as $g = \Delta^{-k}P_1\dots P_r$, P_j = permut. braids
  "Moving to the left everything that can be" $\Rightarrow$ can find an expression st.
  $$\{\text{ending set of } P_j\} \supset \{\text{starting set of } P_{j+1}\} \quad \forall j$$
  ie. any way of adding initial letter of a shortest word of P_{j+1} to the end of P_j would cause it to be no longer a permutation braid.
- This gives rise to "<u>Garside normal form</u>" and solution to word problem in B_n.
  (Garside 1969 + Thurston & Elrifai-Morton early 1990s).

One more example: $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle/ \begin{matrix} a,b,c,d\in\mathbb{Z} \\ ad-bc=1 \end{matrix} \right\}$ and $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$

- <u>Prop</u>: $SL_2(\mathbb{Z})$ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

<u>Pf</u>: given $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, want to express it in terms of S and T:

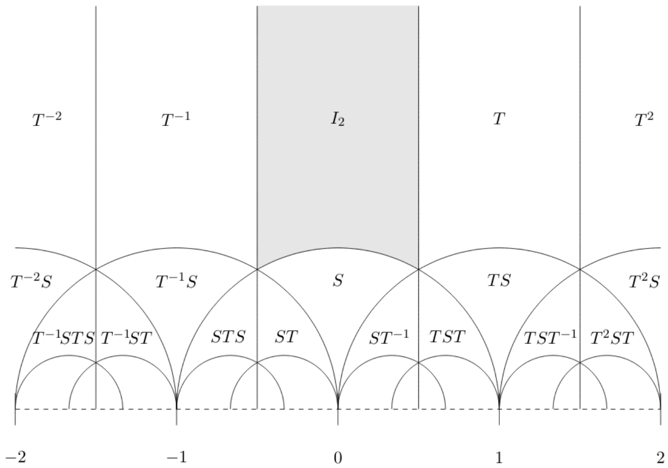
$\to$ if $c=0$ then $a,d=\pm 1$, M is either $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = T^n$ or $\begin{pmatrix} -1 & -n \\ 0 & -1 \end{pmatrix} = S^2T^n$.

$\to$ now assume $c\neq 0$, and repeatedly apply the following algorithm to modify M:

- if $|a|\geq|c|$, use Euclidean division to write $a = nc+r$, $|r|<|c|$.
  $T^{-n}M = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-nc & b-nd \\ c & d \end{pmatrix}$. This decreases $\max(|a|,|c|)$.
- if $|a|<|c|$, $S^{-1}M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}$ brings us back to $|a|>|c|$.

After finitely many steps we find that the product of M with some word in S and T has $c=0$ and $|a|=1$, hence is T^n or S^2T^n. □

- There is a different, geometric proof, based on the fact that $PSL_2(\mathbb{Z})$ acts on the upper half plane $\mathbb{H}=\{z\in\mathbb{C} / \operatorname{Im} z>0\}$ by $\begin{pmatrix} a & b \\ c & d\end{pmatrix} : z \mapsto \dfrac{az+b}{cz+d}$.
  Now S acts by $z\mapsto -\frac{1}{z}$ and T by $z\mapsto z+1$.



The region $\Delta=\{|z|\geq 1, |\operatorname{Re} z|\leq \frac{1}{2}\}$ is a <u>fundamental domain</u> of this action, in the sense that Δ and its images under $PSL_2(\mathbb{Z})$ exactly tile $\mathbb{H}$.
Since the regions immediately adjacent to Δ are $T^{\pm 1}(\Delta)$ and $S(\Delta)$, the regions immediately next to $g(\Delta)$ are $gT^{\pm 1}(\Delta)$, $gS(\Delta)$.
The structure of the tiling reproduces exactly the Cayley graph of $PSL_2(\mathbb{Z})$ with generators S, T, and the fact that all regions can be reached from Δ in finitely many steps is equivalent to: S,T generate $(P)SL_2(\mathbb{Z})$.

- <u>Other generators</u>: instead of S and T, could use
- $S=\begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix}$ and $R=ST=\begin{pmatrix} 0 & -1 \\ 1 & 1\end{pmatrix}$. These have finite order! $S^4=R^6=I$.
- $T=\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}$ and $T'=\begin{pmatrix} 1 & 0 \\ -1 & 1\end{pmatrix}=(TST)^{-1}$ These are conjugates! $T'=STS^{-1}$.
- The images of these matrices in $PSL_2(\mathbb{Z})=SL_2\mathbb{Z}/\{\pm I\}$ also generate $PSL_2(\mathbb{Z})$.

<u>Theorem</u>: $PSL_2(\mathbb{Z})\simeq \langle S,R \mid S^2, R^3\rangle$

<u>Proof</u>: $S^2=-I$ and $R^3=-I$ so S,R have orders 2 and 3 in $PSL_2(\mathbb{Z})$.
These relations $S^2=R^3=e$ reduce any word in $S^{\pm 1}, R^{\pm 1}$ to the form
$\dots SR^{\pm 1}SR^{\pm 1}SR^{\pm 1}\dots$ (the word can start & end with either S or $R^{\pm 1}$).
Mapping $F_2=\langle s,r\rangle$ to $PSL_2(\mathbb{Z})$ by $\begin{matrix} r\mapsto R \\ s\mapsto S\end{matrix}$ induces a surjective homom.
$\langle s,r \mid s^2,r^3\rangle = F_2/\langle \text{conj's of } s^2, r^3\rangle \twoheadrightarrow PSL_2(\mathbb{Z})$ and the kernel consists of all elements (words $\dots sr^{\pm 1}sr^{\pm 1}\dots$) such that the corresponding expansion in S and R equals e in $PSL_2(\mathbb{Z})$, ie. $\pm I$ in $SL_2(\mathbb{Z})$.
Observe: $S\neq e$, $R^{\pm 1}\neq e$. Assume some longer word w in S and $R^{\pm 1}$'s

(alternating between these) simplifies to $e \in PSL_2(\mathbb{Z})$.

- If starts and ends with S, get a shorter word w' by conjugating by S: since $S^2 = e$, $Sw'S = e \Leftrightarrow w' = e$.
- If starts with $R^{\pm 1}$, conjugate it to get another word that doesn't: $R^{\pm 1} w' = e \Leftrightarrow w' R^{\pm 1} = e$.

Iterating, we get eventually some word $SR^{\pm 1} \dots SR^{\pm 1} = \pm I$.

But: $SR = -T = -\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $SR^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. So some product of the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ equals $\pm I$.

Observe: when multiplying a matrix with entries ≥ 0 by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, its entries remain ≥ 0, and the sum of all entries $\nearrow$.

So we can't get $\pm I$. Hence no word in $SR^{\pm 1}$ simplifies to e in $PSL_2(\mathbb{Z})$
$PSL_2(\mathbb{Z}) \simeq \langle S, R \mid S^2, R^3 \rangle$. $\square$

* This presentation can be rewritten in terms of other generators:

$$PSL_2(\mathbb{Z}) \simeq \langle \underset{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}{S}, \underset{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}{T} \mid S^2, (ST)^3 \rangle \simeq \langle \underset{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}{T}, \underset{\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}}{T'} \mid (TT')^3 = e,\ TT'T = T'TT' \rangle$$

and $SL_2(\mathbb{Z}) \simeq \langle T, T' \mid (TT')^6 = 1,\ TT'T = T'TT' \rangle$

(and to connect the two strands of the discussion, the center of the braid group $B_3 = \langle s_1, s_2 \mid s_1 s_2 s_1 = s_2 s_1 s_2 \rangle$ is generated by $\Delta^2 = (s_1 s_2)^3$ and $\simeq \mathbb{Z}$, so mapping $\begin{matrix} s_1 \mapsto T \\ s_2 \mapsto T' \end{matrix}$ gives $1 \to \mathbb{Z} = \langle \Delta^2 \rangle \hookrightarrow B_3 \twoheadrightarrow PSL_2(\mathbb{Z}) \to 1$.)