Last time – Sylow theorems.

One more example, to show that things can get more complicated quickly.

Let's try to classify groups of order 12. If $|G|=12$ then Sylow gives

- a subgroup $H\subset G$, $|H|=4$; the number of these is $s_2\in\{1,3\}$ ($s_2|3$, $s_2\equiv 1 \bmod 2$)
- a subgroup $K\subset G$, $|K|=3$; the number is $s_3\in\{1,4\}$ ($s_3|4$, $s_3\equiv 1 \bmod 3$)

* At least one of these is normal: indeed, if $s_3=4$ then the nontrivial elements of $K_1,\dots,K_4$ all have order 3, and $K_i\cap K_j=\{e\}$ (order divide 3, <3), so we have 8 elements of order 3. So there are at most 4 elements of order $\in\{1,2,4\}$, hence $s_2=1$ and H is normal.

* If both H and K are normal then $G\simeq H\times K$ (using $|G|=|H|\cdot|K|$, $H\cap K=\{e\}$ see last time) and so G is abelian, one of $\mathbb{Z}/4\times\mathbb{Z}/3\simeq\mathbb{Z}/12$

$(\mathbb{Z}/2\times\mathbb{Z}/2)\times\mathbb{Z}/3\simeq\mathbb{Z}/2\times\mathbb{Z}/6$.

* If H is normal but K isn't, consider the action of G on $\{K_1,K_2,K_3,K_4\}$ by conjugation. Conjugation by a nontrivial element of K_1 maps K_1 to itself but doesn't fix any of the 3 others: indeed recall the stabilizer of K_i is $\{g\in G \,/\, gK_ig^{-1}=K_i\}=N(K_i)$, and by orbit-stabilizer, $|N(K_i)|=\frac{|G|}{s_3}=\frac{12}{4}=3$, so $N(K_i)=K_i$. So: a nontrivial element of K_1 acts on $\{K_1,K_2,K_3,K_4\}$ by a 3-cycle permuting $\{K_2,K_3,K_4\}$, and similarly for others.

Hence the action of G on $\{K_1\dots K_4\}$ gives a homom. $\varphi: G\longrightarrow S_4$, $y_i\longmapsto$ 3-cycles

This implies $\mathrm{Im}(\varphi)\supset A_4$, hence $=A_4$, and $G\simeq A_4$.

* If K is normal but H isn't, then there are 2 subcases – $H\simeq\mathbb{Z}/4$ or $\mathbb{Z}/2\times\mathbb{Z}/2$!

→ if $H\simeq\mathbb{Z}/4$, let $x\in H$ generator, let $K=\{e,y,y^2\}$, then $G\simeq K\rtimes H$ is determined by the conjugation action of H on K, ie. need to know $xyx^{-1}\in K$. Can't have $xyx^{-1}=e$ ($\Rightarrow y=e$) or $xyx^{-1}=y$ ($\Rightarrow x$ and y commute, $G\simeq H\times K$ abelian). So instead $xyx^{-1}=y^2\ (=y^{-1})$.

Then G is generated by x,y, with $x^4=y^3=e$ and $xy=y^2x$.

This group is unfamiliar to us – semidirect product $\mathbb{Z}/3\rtimes\mathbb{Z}/4$, where $\mathbb{Z}/4$ acts on the normal subgroup $\mathbb{Z}/3$ by $\mathbb{Z}/4\longrightarrow\mathrm{Aut}(\mathbb{Z}/3)=\{\pm id\}$, $k\longmapsto(-1)^k$

→ if $H \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$, then look at conjugation action $H \xrightarrow{\varphi} \mathrm{Aut}(K) \simeq \mathbb{Z}/2$, necess. $\ker(\varphi) \simeq \mathbb{Z}/2$, denote by z its generator, $x \in H$ st. x, z generate H, y generator of K, then G is gen. by x, y, z with

$$\begin{cases} x^2 = z^2 = y^3 = e \\ xz = zx & (\mathbb{Z}/2 \times \mathbb{Z}/2) \\ zy = yz & (z \in \ker\varphi) \\ xy = y^2 x & (xyx^{-1} = y^2) \end{cases}$$

Can check this is actually $G \simeq D_6$

(the subgroup gen^d by y and z is $\simeq \mathbb{Z}/6$ and normal in G, take y = rotation by $2\pi/3$
z = rotation by π
x = any reflection).

Thus there are 5 isom. classes of groups of order 12:

$$(\mathbb{Z}/12,\ \mathbb{Z}/2 \times \mathbb{Z}/6,\ A_4,\ \mathbb{Z}/3 \rtimes \mathbb{Z}/4,\ D_6).$$

Generators, presentations, and Cayley graph. Recall:

* The free group F_n on n generators $a_1, \dots, a_n$.

  Elements are all reduced words $a_{i_1}^{m_1} \dots a_{i_k}^{m_k}$ $\quad$ $k \geq 0$ (empty word is e)
  $i_1 \dots i_k \in \{1 \dots n\}$ $\quad i_j \neq i_{j+1}$
  $m_1, \dots m_k \in \mathbb{Z} - \{0\}$

  (non reduced words: reduce by:
  - if $i_j = i_{j+1}$, combine $a_i^m a_i^{m'} \rightsquigarrow a_i^{m+m'}$
  - if an exponent is zero, remove a_i^0).

  Repeat until word is reduced.

* This is the "largest" group with n generators, all others are $\simeq$ quotients of F_n.
  If G is generated by $g_1, \dots, g_n \in G$, define a homomorphism $\varphi : F_n \twoheadrightarrow G$ by setting $a_i \longmapsto g_i$ (and so, $\prod a_{i_j}^{m_j} \mapsto \prod g_{i_j}^{m_j}$)

* A finitely generated group is said to be finitely presented if the kernel of φ is the smallest normal subgroup of F_n containing some finite subset $\{r_1, \dots, r_k\} \subset F_n$ (↳ words in the generators), (ie. the subgroup generated by r_j's and their conjugates $x^{-1} r_j x$).

  Write $G \cong \langle \underbrace{a_1, \dots, a_n}_{\text{generators}} \mid \underbrace{r_1, \dots, r_k}_{\text{relations}} \rangle$, then $G \cong F_n / \langle \text{conj's of } r_1 \dots r_k \rangle$

  Ex: $\mathbb{Z}^n \cong \langle a_1, \dots, a_n \mid a_i a_j a_i^{-1} a_j^{-1} \ \forall i,j \rangle$.

  Ex: $S_3 \cong \langle s_1, s_2 \mid s_1^2, s_2^2, (s_1 s_2)^3 \rangle$

* Concretely, given generators $g_1, \dots, g_n \in G$, it is not hard to find relations $r_1, \dots, r_k$, ie. words in the free group F_n st. under $\varphi : \underset{a_i \mapsto g_i}{F_n \to G}$, $r_j \mapsto e$.

  If these relations hold in G, then φ induces a surjective homomorphism $\langle a_1 \dots a_n \mid r_1 \dots r_k \rangle = F_n / \langle \text{conjs. of } r_j \rangle \twoheadrightarrow G$.

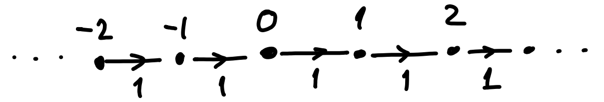
This is an isom. once we have found a complete set of relations among the g_i, ie. when $r_1 \dots r_k$ and their conjugates generate $\ker(\varphi)$.

- How to work w/ a group described by generators and relations?
  Sometimes we know what G is, but sometimes we don't.
  Two useful ideas (among many): 1 the Cayley graph
  2 normal forms.

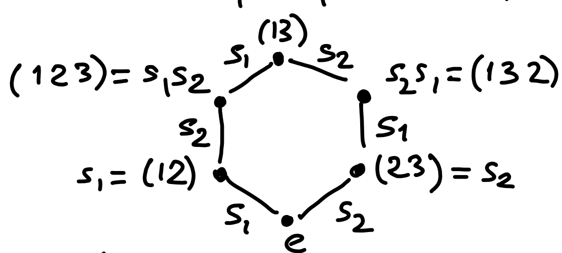
Cayley graph: Given generators $g_1, \dots, g_n \in G$, the Cayley graph of G has
- vertices = the elements of the group
- two vertices s, t are connected by an edge labelled g_i when $t = s g_i$

[here we're doing right multiplication; one could do left mult. instead]

Ex: $\mathbb{Z}$ with its usual generator 1:

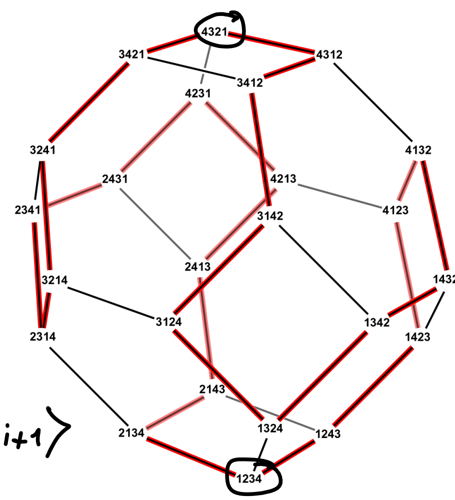


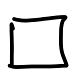
Ex. S_3 with generators $s_1 = (12)$
$s_2 = (23)$
$(s_i^{-1} = s_i$ so edges are undirected$)$

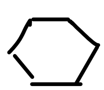


The fact that this closes up shows relation $s_1 s_2 s_1 = s_2 s_1 s_2$ $(\Leftrightarrow (s_1 s_2)^3 = e)$
Since any word in s_1, s_2 with relations $s_1^2 = s_2^2 = e$ can be reduced to $(\dots s_1 s_2 s_1 \dots)$, one can use this to check $S_3 \simeq \langle s_1, s_2 \mid s_1^2, s_2^2, (s_1 s_2)^3 \rangle$

Ex: S_4 with generators $s_i = (i\ i{+}1)$, $1 \le i \le 3$:
("permutohedron")



Faces are  relation $s_1 s_3 = s_3 s_1$

and  $s_1 s_2 s_1 = s_2 s_1 s_2$, $s_2 s_3 s_2 = s_3 s_2 s_3$

More generally, S_n has following presentation:

$$S_n \simeq \langle s_1, \dots, s_{n-1} \mid s_i^2 = 1\ \forall i,\ s_i s_j = s_j s_i\ \forall |i-j| \ge 2,\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \rangle$$

- Fact: G acts on its Cayley graph by "left multiplication":
  vertices $s \mapsto gs$, edges $(s \to s g_i) \mapsto (gs \mapsto gs g_i)$

  This action is transitive on vertices (& on edges w/ given label g_i): graph is very symmetric!

- Word length of an element of G (in given generators) := shortest distance from e to $g \in G$ in the Cayley graph.

- For *infinite* groups, we can ask about the *growth rate* of G:

  Given set of generators g_i, how does #elements represented by words of length $\leq N$ grow with N? esp: does it grow *polynomially* or *exponentially*?

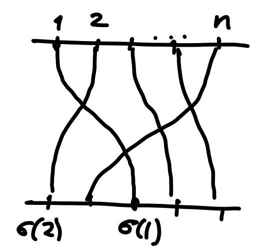
  Even if we change our set of generators to some other g_j', word length of a given element changes by a bounded factor only (bound = word lengths of new generators in terms of old ones & vice versa). So the exponential or polynomial nature of the growth is independent of the set of generators.

  Ex: f.g. abelian groups have polynomial growth / free groups have exp. growth.

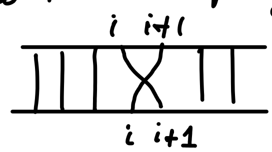
- For finite groups, the Cayley graph is finite and growth isn't relevant, but questions about word length remain interesting!

Ex: in S_n, $\{s_i = (i\ i{+}1)\}$: the longest element is $\begin{pmatrix} 1 & 2 & \cdots & n \\ \downarrow & & & \downarrow \\ n & n-1 & \cdots & 1 \end{pmatrix}$ of wordlength $\frac{n(n-1)}{2}$, and the word length of $\sigma \in S_n$ is #inversions ($i<j$ st. $\sigma(i)>\sigma(j)$).

This is best understood by representing permutations as diagrams

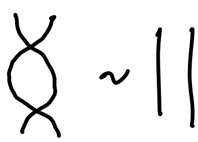


- Composition = stack diagrams
- Expression in terms of s_i comes from decomposing diagram into layers w/ single crossing

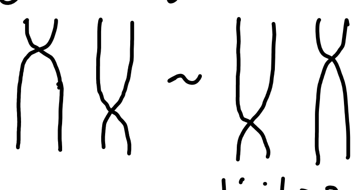


$= s_i$

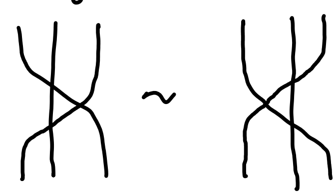
- Presentation of S_n $\longleftrightarrow$ any two diagrams for σ are related by

(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 $\Leftrightarrow$ $w(\sigma s_i) < w(\sigma)$

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

  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 prefered 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

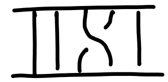
  This gives a *normal form* for elements of S_n (ie. a prefered word representing each element) and hence a solution to the *word problem* = when do two words represent the same element? ($\Leftrightarrow$ when does a word represent $e \in G$?).

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!

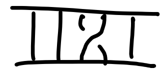
<u>Ex</u>: the <u>braid group</u> $B_n = \langle s_1 \dots s_{n-1} \mid s_i s_j = s_j s_i \ \forall |i-j| \geq 2, \ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \rangle$

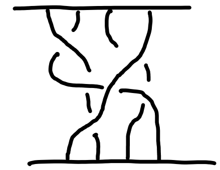
(but $s_i^2 \neq 1$)

(important in knot theory etc!)

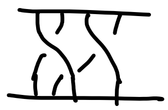
$s_i =$ 

$i \ \ i{+}1$

$s_i^{-1} =$ 



Algorithmics is similar to S_n, 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 + it conjugates $s_i \leftrightarrow s_{n-i}$.

  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).

<u>Further examples</u> (HW + next lecture):
- semidirect products
- Heisenberg group
- $SL_2(\mathbb{Z})$ and $PSL_2(\mathbb{Z})$.