Lecture 4: Group presentations by Generators & Relations

Last Time:
- order & exponent of a group
- 3 Isomorphism thms, $\boxed{G/\ker\varphi \xrightarrow{\sim} \operatorname{Im}\varphi \quad \forall\, \varphi: G \to G' \text{ gp hom.}}$

§1 Isomorphism Thm (continued)

Second interpretation Fix $f: G \twoheadrightarrow G'$ surjective gp hom. & $H \trianglelefteq G$ with $H \subseteq \ker f$. Then $H = \ker f \iff G/H \overset{\bar{f}}{\simeq} G'$

Pf/ $(\Rightarrow)$ 1st Isomorphism Thm

$(\Leftarrow)$ Consider
$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/H \arrow[ur, "\bar{f}\ \text{iso}"'] & \end{tikzcd}$$

$\bar{f}$ iso $\iff \bar{f}$ inj.

$$\underset{\ker(f)/H}{\overset{\|}{\ker(\bar{f})}} = e_{G/H} = eH$$

$\square$

Example $G = \text{Free}(2) = \langle a, b \mid \text{no relations} \rangle$ with concatenation + cancellation

Take $\varphi: G \longrightarrow \mathbb{Z}^2$
$\qquad w \longmapsto (\#a\text{'s}, \#b\text{'s})$

Ex: $\varphi(a^2b^2a^{-7}) = (2-7, 2) = (-5, 2) = \varphi(a^{-5}b^2) = \varphi(b^2a^{-5})$.

- φ is a surjection
- φ is group homomorphism

Consider $H = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle = [G:G] \subseteq \ker\varphi$

- $H \trianglelefteq G$ (Commutator subgroup (HW1)) (*)
- $G/H = \langle a, b \mid ab = ba \rangle \overset{\bar{\varphi}}{\simeq} \mathbb{Z}^2$

$$\underset{a^m b^n}{\overset{\Psi}{}} \longmapsto (m, n)$$

So $H = \ker\varphi$ by Thm above.

(*) **Lemma:** $H < G$ is normal $\iff g_j h_i g_j^{-1}$ $\forall\, h_i$ generators of H, g_j —— G
$H = \langle h_i : i \in I \rangle$
$G = \langle g_j : j \in J \rangle$

§2 Group Presentations

Q: How to describe a group?

A Many options: (1) Symmetries of a set (bijections $X \longrightarrow X$)

(2) Multiplication Table (eg Q_8)

$\longrightarrow$ (3) Generators & relations.

Advantages: (1) & (3) Associativity is automatic.

Disadvantage: (3) Presentation is not unique & can get trivial gp from a complicated presentation (Example 1 on page 4)

§3 Free Groups

Definition: Given a set A let Free (A) = {words on A} with operation = concatenation & cancellation.

Obs: If $w \in \text{Free}(A)$, then w has a unique expression of the form

$w = x_1^{n_1} x_2^{n_2} \cdots x_\ell^{n_\ell}$ $[\ell = \text{length}(w)]$ where

$$\begin{cases} \cdot\, x_1, x_2, \ldots, x_\ell \in A, & x_1 \neq x_2,\ x_2 \neq x_3, \ldots, x_i \neq x_{i+1}, \ldots, x_{\ell-1} \neq x_\ell \\ \cdot\, n_1, \ldots, n_\ell \in \mathbb{Z} \smallsetminus \{0\}. \end{cases}$$

Convention: $\ell = 0 \iff w = e \in \text{Free}(A)$ (empty word)

Note $w^{-1} = x_\ell^{-n_\ell} \cdots x_1^{-n_1}$.

Q: What would it take to define a group homomorphism $f: \text{Free}(A) \longrightarrow H$ for an arbitrary group H?

A: (1) Specify $f(a) \in H$ $\forall a \in A$ (free will, nothing to check!)

(2) $w \in \text{Free}(A) \rightsquigarrow w = x_1^{n_1} x_2^{n_2} \cdots x_\ell^{n_\ell}$ uniquely!

$\Longrightarrow f(w) = f(x_1)^{n_1} f(x_2)^{n_2} \cdots f(x_\ell)^{n_\ell}$ is the only possible defn! (unambiguous)

Corollary $\left\{ \begin{array}{c} \text{Group homomorphisms} \\ \mathrm{Free}(A) \longrightarrow H \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Set Maps} \\ A \longrightarrow H \end{array} \right\}$

Universal Property: Given any set map $f: A \longrightarrow H$, there exists a unique group homomorphism $\tilde{f}: \mathrm{Free}(A) \longrightarrow H$ satisfying

$$\begin{tikzcd} A \arrow[r, hook, "i"] \arrow[dr, "f"'] & \mathrm{Free}(A) \arrow[d, dashed, "\exists ! \tilde{f}"] \\ & H \end{tikzcd}$$

§3 Relations

Recall: $X \subseteq G$ gp. $\rightsquigarrow$ $N(X)$ = smallest normal subgp of G containing X
(Lecture 2)

$$= \bigcap_{\substack{N \trianglelefteq G \\ X \subseteq N}} N$$

Def: Given a set $\underline{\underline{A}}$ (generators) & $R \subseteq \mathrm{Free}(A)$ (relations), we define

$$\boxed{\langle A \mid R \rangle := \mathrm{Free}(A) / N(R)}$$

(want a group!)

Q: What would it take to define a group homomorphism $f: \langle A \mid R \rangle \longrightarrow H$ for an arbitrary group H?

A ① Specify $f(a) \in H \quad \forall a \in A$

$\rightsquigarrow \tilde{f}: \mathrm{Free}(A) \longrightarrow H$ gp homomorphism

② Make sure $\tilde{f}(r) = 0 \quad \forall r \in R \subset \mathrm{Free}(A)$

§4 Examples

Our first example, shows that a group presentation can be deceiving, namely, we might be giving the trivial group without knowing it.

Ex 1: $G = \langle x, y \mid xy^2 = y^3x,\ yx^2 = x^3y \rangle \simeq \{e\}$

Why? $xy^2 = y^3x \Rightarrow xy^4 = xy^2y^2 = y^3xy^2 = y^6x$

$\rightsquigarrow xy^8 = xy^4y^4 = y^6xy^4 = y^{12}x$

$\rightsquigarrow x^2y^8 = xy^{12}x = xy^8y^4x = y^{12}xy^4x = y^{12}y^6x^2$

So $\boxed{x^2y^8x^{-2} = y^{18}}$

- Similarly, $\boxed{x^3y^8x^{-3} = y^{27}}$

(Indeed $x^3y^8x^{-3} = x\,x^2y^8x^{-2}x^{-1} = xy^{18}x^{-1} = xy^8y^{10}x^{-1} =$
$= y^{12}xy^8y^2x^{-1} = y^{12}y^{12}xy^2x^{-1} = y^{24}y^3xx^{-1} = y^{27}$ $\square$)

- But 2^{nd} relation gives $yx^2y^{-1} = x^3$, thus:

$y^{27} = x^3y^8x^{-3} = yx^2y^{-1}y^8yx^{-2}y^{-1} = y\underbrace{x^2y^8x^{-2}}_{y^{18}}y^{-1} = y^{18}$

$\Rightarrow \boxed{y^9 = e}$

$\Rightarrow e = x^{-1}y^9x = (x^{-1}y^3x)^3 = (x^{-1}xy^2)^3 = y^6$

$\Rightarrow \boxed{y^3 = e}$ (1)

$\Rightarrow$ By 1^{st} relation: $xy^2 = y^3x = x$ so $\boxed{y^2 = e}$ (2)

Combining (1) & (2) we get $\boxed{y = e}$

Finally, 2^{nd} relation gives $x^2 = x^3 \Rightarrow \boxed{x = e}$

Obs: This example illustrates the difficulties underlying the WORD PROBLEM in groups (Algorithmic question proposed by Dehn 1911: How to decide if two words on a fin. gen. group represent the same element)

Ex 2

$G = \mathrm{Free}(\{a,b\})$, $\varphi : \mathrm{Free}(\{a,b\}) \twoheadrightarrow \mathbb{Z}^2$

$w \longmapsto (\#a\text{'s}, \#b\text{'s})$

- $H = \operatorname{Ker} \varphi \trianglelefteq G$, $aba^{-1}b^{-1} \in H$

Set $\mathcal{R} = \{aba^{-1}b^{-1}\} \in \mathrm{Free}(A) \rightsquigarrow N(\mathcal{R}) \subseteq H$

<u>Claim</u>: $\langle a, b \mid aba^{-1}b^{-1} \rangle = \langle a, b \mid ab = ba \rangle \overset{\varphi}{\cong} \mathbb{Z}^2$

$a^k b^m \longmapsto (k, m)$.

Conclude: $N(\mathcal{R}) = H = \ker \varphi$.

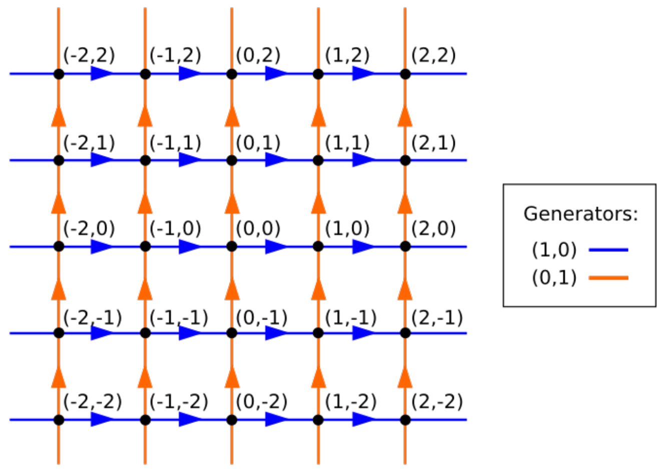
<u>Obs</u>: • Smallest subgroup containing $x = aba^{-1}b^{-1}$ is $\langle x \rangle \simeq \mathbb{Z}$.

• Smallest <u>normal</u> subgp containing x is $\ker \varphi$. This is not even finitely generated!

Pf/ View gens of $\mathrm{Free}(\{a,b\})$ inside $\mathbb{Z}^2$ via φ, ie

$a \longleftrightarrow (1,0)$

$b \longleftrightarrow (0,1)$

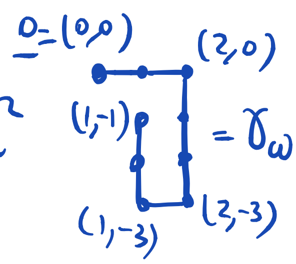


- Define a function $d : \mathrm{Free}\{a,b\} \longrightarrow \mathbb{R}_{\geq 0}$ as follows:

given $w \in \mathrm{Free}\{a,b\}$, trace a path in $\mathbb{R}^2$ by reading w from left to right:

$$\begin{cases} a^k : \text{ move } k \text{ steps along } x\text{-axis} \\ \quad k \geq 0 \rightsquigarrow \text{right } \underline{\text{move}} \\ \quad k < 0 \rightsquigarrow \text{left} \\ b^k : \text{ move } k \text{ steps along } y\text{-axis} \\ \quad k \geq 0 \rightsquigarrow \text{upwards} \\ \quad k \leq 0 \rightsquigarrow \text{downwards} \end{cases}$$

<u>Ex</u>: $w = a^2 b^{-3} a^{-1} b^2 \rightsquigarrow \gamma_w$ follow path in $\mathbb{R}^2$



$= \gamma_w$

Set $d(w) = \max_{p \in \gamma_w} \{ \text{distance}(\underline{0}, p) \}$

Remarks (1) $\forall\, w \in H$ Endpoint of $w = \underline{0}$.

(2) If $w_1, w_2 \in H \Rightarrow d(w_1 w_2) \leq \max\{d(w_1), d(w_2)\}$

To finish, we argue by contradiction:

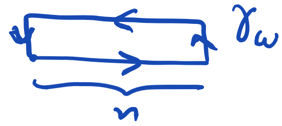
Assume H is f.g. say $H = \langle w_1, \dots, w_N \rangle$. Write:

$$R = \max\{d(w_1), \dots, d(w_N)\}$$

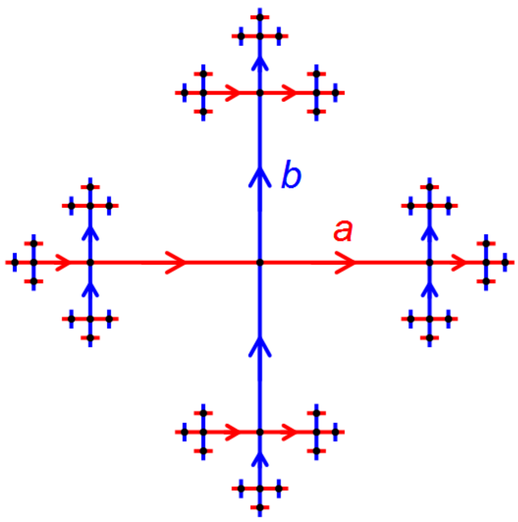
Then $d(h) \leq R \quad \forall\, h \in H$

But $d(\underbrace{a^n b a^{-n} b^{-1}}_{w = [a^n : b]}) = \text{distance}\{(0,0), (n,1)\}$

$= \sqrt{n^2+1} > R$ for $n \gg 0$ Contr!



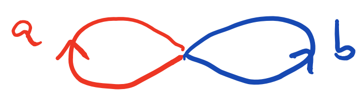
Obs: $\exists$ Alternative Proof via Algebraic Topology.



- Cayley graph of Free (a,b)

$\mathcal{G} = \tilde{X}/F_2'$ = Cayley graph of $\mathbb{Z}^2$ (grid on previous page)

- Free$(\{a,b\})$ = fundamental group of bouquet of 2 S^1's:



- $\tilde{X}$ = universal cover
- $F_2' = [\text{Free}(\{a,b\}), \text{Free}(\{a,b\})]$

Reidemeister-Schreier Thm:

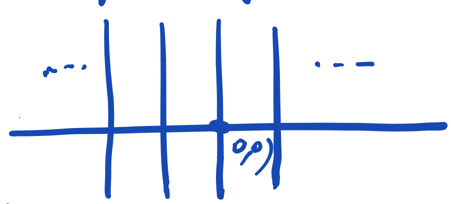
$$\pi_1(\tilde{X}/F_2') \simeq \langle V, R \cup T \rangle$$

with V = edges of graph $\mathcal{G}$

R = 2-cells of graph $\mathcal{G} = \emptyset$

T = a spanning tree of graph

Eg: $T = \bigcup_{y \in \mathbb{Z}} \{(x,y) : x \in \mathbb{Z}\} \cup \{(0,x) : x \in \mathbb{Z}\}$



Claim: After removing T, we still have infinitely many edges

Thus, F_2' cannot be finitely generated.

• This Topological proof leads to a general Theorem:

<u>Thm</u>: Fix G an infinite group & $\Phi: \mathrm{Free}(n) \twoheadrightarrow G$ gp homomorph.

Then: $\ker(\Phi)$ is trivial or it is <u>not</u> finitely generated.

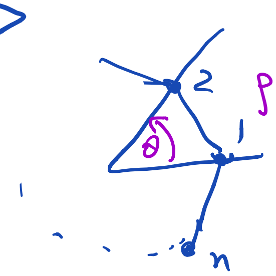
<u>Example 3</u>: $D_n = \{1, \rho, \rho^2, \dots, \rho^{n-1}, s, s\rho, \dots, s\rho^{n-1}\}$ <u>Dihedral Gp</u>

generators $= \{s, \rho\}$

Relations: $s^2 = \rho^n = e$, $s\rho s = \rho^{-1}$ $(\Leftrightarrow (s\rho)^2 = e)$

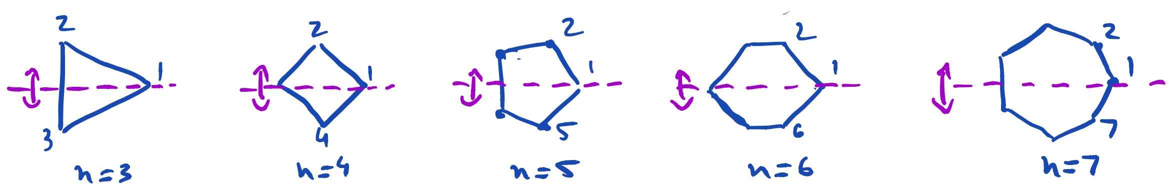
<u>Claim</u>: $D_n = \langle s, \rho \mid s^2, \rho^n, s\rho \rangle$

View • ρ = rotation of angle $\frac{2\pi}{n} = \theta$



• s = reflection along x-axis

Ex



viewed in S_n: $(2\ 3)$ $(2\ 4)$ $(2\ 5)(3\ 4)$ $(2\ 6)(3\ 4)$ $(2\ 7)(3,6)(4,5)$

In general: $s \longleftrightarrow$ $(2\ n)(3\ n-1) \cdots (\frac{n}{2}-1, \frac{n}{2}+1)$ n even

$(2\ n)(3\ n-1) \cdots (\frac{n+1}{2}, \frac{n+1}{2}+1)$ n odd

• $|D_n| = 2n$ & relations hold in D_n.

<u>Lemma</u>: There exists a group homomorphism

$$f: D_n \longrightarrow \{\pm 1\} \quad \text{with} \quad f(s) = f(\rho) = -1$$

Pf/ $D_n = \langle s, \rho \mid s^2 = \rho^n = (s\rho)^2 = e \rangle$

Write $\varphi: \mathrm{Free}(s, \rho) \twoheadrightarrow \{\pm 1\}$ with $f(s) = -1$, $f(\rho) = 1$

Want to factor this map through D_n i.e. $\bar{f} = \bar{\varphi} : D_n \longrightarrow \{\pm 1\}$

To define the map $\bar{f}$ we need to check: $f(s) = -1$, $f(\rho) = 1$ preserves the relations $f(s^2) = f(\rho^n) = f((s\rho)^2) = 1$

but this is clear. $\square$

- $\operatorname{Ker} f = \{$ words in s, ρ of even length$\}$

$$= \{e, \rho, \rho^2, \ldots, \rho^{n-1}\} =: K \simeq \mathbb{Z}/_{n\mathbb{Z}}$$

- $\operatorname{Im} f = \{\pm 1\}$, so f is surjective.

Conclusion: $D_n/K \simeq \{\pm 1\}$ by 1^{st} Iso Thm.

Example 4: D_n can be generated by 2 reflections (or involutions)

$$D_n = \langle \sigma_1, \sigma_2 \mid \sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^n = e \rangle$$

How? $\sigma_1 \leftrightarrow s$ $\quad$ ($\sigma_1\sigma_2 = ss\rho = \rho$ so relation holds!)

$\sigma_2 \leftrightarrow s\rho$ $\quad$ $\sigma_2^2 = s\rho s\rho = \rho^{-1}\rho = e$

This is an example of a Coxeter Group. (1934)

Def: A Coxeter group has presentation $\langle r_1, \ldots, r_n \mid (r_i r_j)^{m_{ij}} \rangle$,

where $m_{ij} = \begin{cases} 1 & i = j \\ \geq 2 & i \neq j \end{cases}$ $\quad$ ($m_{ij} = \infty$ means no relation between r_i & r_j is imposed)

$\mathbb{N} \cup \{\infty\}$

- $(xy)^2 = e$ means $xy = yx$
- Avoid redundancies by writing $m_{ij} = m_{ji}$

Pf/ $y^2 = e$ & $(xy)^m = e$ then $(yx)^m = (yx)^m yy = y(xy)^m y = y^2 = e$. $\square$

Classification of finite Coxeter groups (1935)

① Correspond to Coxeter-Dynkin Diagrams

② They can be realized as reflections of finite-dimensional Euclidean spaces

Obs: Word problem for Coxeter groups has polynomial time algorithm.

Example 5: S_n is generated by transpositions $\sigma_{ij} = (i, j)$ $1 \le i < j \le n$
$\binom{n}{2}$ many!

FACT 1: Any permutation is a product of disjoint cycles (in any order)

Eg:
$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix} = (1\,2\,3)(4\,5) = (4\,5)(1\,2\,3)$$

FACT 2: Any cycle is a product of transpositions

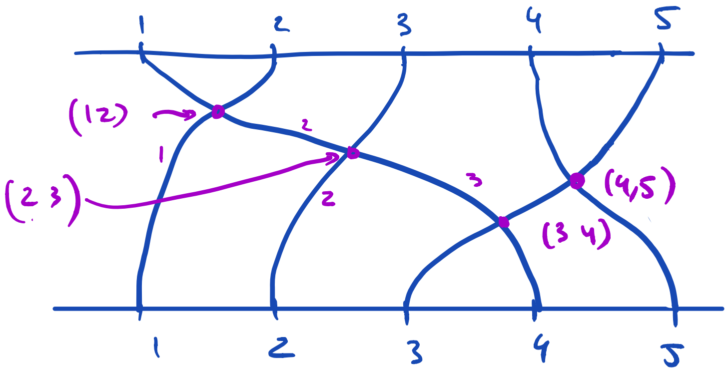
Pf/ $(i_1\ i_2, \ldots i_k) = (i_1\ i_2)(i_2\ i_3) \cdots\cdots (i_{k-1}\ i_k)$

- More is true!

$$\boxed{S_n = \langle \sigma_{i,i+1} \quad 1 \le i \le n-1 \rangle}$$

simple transpositions
$(n-1)$ many!

- Pictorial Proof in one example: $(1\,4\,5\,3\,2) = (3\,4)(4\,5)(2\,3)(1\,2)$



read transpositions in this order.

In general, "slide" strings so that we only transpose consecutive strings
Dots in between consecutive columns $\Longleftrightarrow (i, i+1)$.

- **Formal Proof:** By Facts 1 & 2, can reduce to transpositions σ_{ij}
  - $j = i+1$, nothing to show.
  - If $j > i+1$, use:

$$(i\ j) = (j-1\ j)\,\boxed{(i\ j-1)}\,(j-1, j)$$

$\uparrow$ induct.

Q: Relations among $s_i = (i\ i+1)$?

$s_i^2 = e$ ✓ ; $s_i s_j = s_j s_i$ if $|j-i| > 1$

$(s_i\, s_{i+1}) = (i\ i+1)(i+1, i+2) = (i\ i+1\ i+2)$ 3-cycle

So $(s_i s_{i+1})^3 = e$, so $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$.

Define $\mathcal{P}_n = \left\langle a_1, \ldots, a_{n-1} \;\middle|\; \begin{array}{l} a_i^2 = e \quad \forall i \\ a_i a_j = a_j a_i \quad \text{if } |i-j|>1 \\ a_i a_{i+1} a_i = a_{i+1} a_i a_{i+1} \end{array} \right\rangle$

<u>Prop</u> $\mathcal{P}_n \cong S_n$

Pf/ Above calculation yields $\mathcal{P}_n \xrightarrow{\varphi} S_n$ $\quad a_i \longmapsto s_i \;\forall i$

To finish, we must show $\ker \varphi = N\langle \text{relations} \rangle$. We'll do this using group actions.