Lecture V: Order & exponent, Group presentations by Generators & Relations

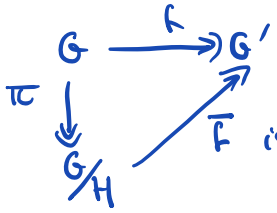
Last time: 3 Isomorphism thms. Key: $\frac{G}{\ker\varphi} \xrightarrow{\sim} \mathrm{Im}\,\varphi$ $\forall \varphi: G \to G'$ gp hom.

§ 1 Iso Theorems:

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

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

($\Leftarrow$) Consider



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

$\ker(\bar{F}) = e_{G/H} = eH$

$\| $

$\ker(f)/H$ □

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

Take $\varphi: G \longrightarrow \mathbb{Z}^2$

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

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

ψ

$a^m b^n \longmapsto (m, n)$

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 Order & exponent of a group:

- Any $g \in G$ generates a subgroup $\langle g \rangle$. So we define:

Def The order of an element g of G is the order of $H = \langle g \rangle$.

Obs.: If $|\langle g \rangle| = n < \infty$, then $g^n = e$ ($H = \{1, g, \dots, g^{n-1}\} \simeq \mathbb{Z}/n\mathbb{Z}$). $g^l \longleftrightarrow \bar{l}$

Corollary: $\text{Order}(g) \mid |G|$ whenever G is finite.

Def: $S := \{k \in \mathbb{Z} : g^k = e \ \forall g \in G\} \cap \mathbb{Z}_{>0}$

$$\text{Exponent of } G \ (\exp(G)) := \begin{cases} 0 & \text{if } S = \emptyset \\ \min(S) & \text{if } S \neq \emptyset \end{cases}$$

Obs: • If $|G| < \infty$, then $\exp(G) > 0$ ($g^{|G|} = e \ \forall g \in G$)

Converse is false: $G = \prod_i (\mathbb{Z}/2\mathbb{Z}) = \{(a_1, a_2, \dots) \ a_i = 0, 1 \ \forall i\}$ with term-by-term multiplication has $\exp(G) = 2$

Prop: • $\exp(G) = 1 \Rightarrow G = \{e\}$

• ——— $= 2 \Rightarrow$ G is abelian (Exercise)

• ——— $= 3$ need not be abelian

[**Ex:** Heisenberg gp / $\mathbb{F}_3$: $H_3 = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/3\mathbb{Z} \right\} < GL_3(\mathbb{F}_3)$]

Burnside Problem (1902): Find all $(m, n) \in \mathbb{Z}_{>0}^2$ such that if G is a group with m generators (minimal #) & $\exp(G) = n$, then $|G| < \infty$.

Status: Known cases: $(1, n)$, $(m, 2)$, n, m any. Still **OPEN!** [(2, 5)???]
$G \simeq \mathbb{Z}/n\mathbb{Z}$; $G \simeq (\mathbb{Z}/2\mathbb{Z})^m$. (see Wikipedia)

$(m, 3)$, $(m, 4)$, $(m, 6)$ m any

§ 3. 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)

→ 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 5)

§ 4. Free Groups

Definition: Given a set A let $\underline{\text{Free}(A)} = \{\text{words in } A\}$

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

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

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?

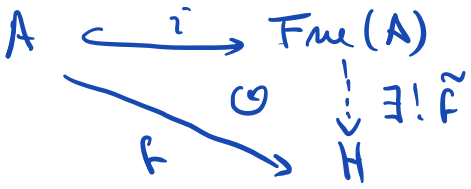
A: ① Specify $f(a) \in H \;\; \forall a \in A$ (free will, nothing to check!)

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

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

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

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



§3 Relations

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

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

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

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

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

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

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

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

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

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

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

$$\left.\begin{array}{l} \Rightarrow e = x^{-1}y^9x = (x^{-1}y^3x)^3 = (x^{-1}xy^2)^3 = y^6 \end{array}\right\} \Rightarrow \boxed{y^3 = e} \quad (1)$$

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

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

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

[NP-hard]

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)

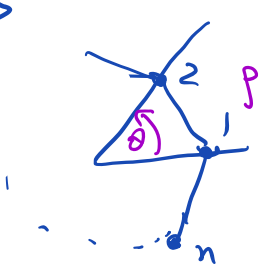
Example 2: $D_n = \{1, \rho, \rho^2, \dots, \rho^{n-1}, s, s\rho, \dots, s\rho^{n-1}\}$ **Dihedral Gp**

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

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

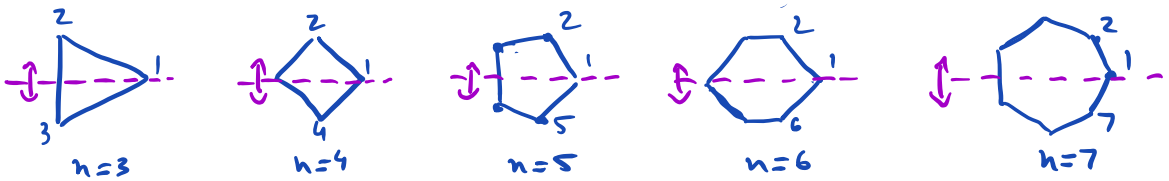
Claim: $D_n = \langle s, \rho \mid s^2, \rho^n, s\rho \rangle$

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.

Lemma: There exists a group homomorphism

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

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

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

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

To define the map $\overline{f}$ 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. $\square$

- $\ker f = \{$ words in s, ρ with even # of $s\}$
  $= \{e, \rho, \rho^2, \dots, \rho^{n-1}\} =: K \simeq \mathbb{Z}/n\mathbb{Z}$
- $\operatorname{Im} f = \{\pm 1\}$, so f is surjective.

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

Example 3: 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: $\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix} = (123)(45) = (45)(123)$

FACT 2: Any cycle is a product of transpositions

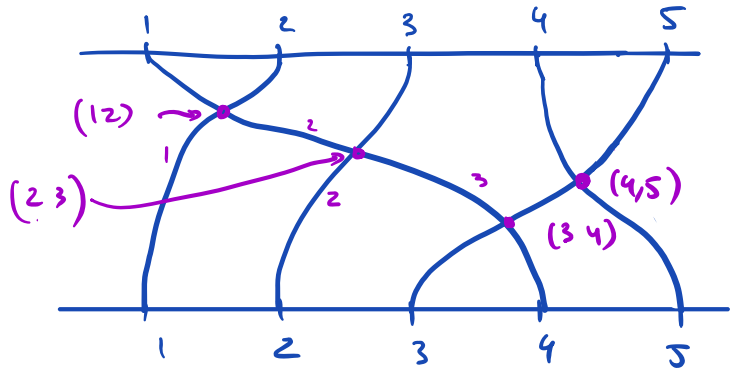
Pf/ $(i_1\ i_2, \dots i_k) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k)$

- More is true!

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

simple transpositions ($n-1$) many!

- Pictorial Proof in one example: $(14532) = (34)(45)(23)(12)$



read transpositions in this order.

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

Formal Proof: By Facts 1 & 2, can reduce to transpositions σ_{ij}

- $j = i+1$, nothing to show.
- If $j > i+1$, use:

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

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

§3 Aside: Free Gps & paths in $\mathbb{Z}^n$

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

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

- $H = \ker\varphi \lhd G$, $aba^{-1}b^{-1} \in H$

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

Claim: $\langle a,b \mid aba^{-1}b^{-1}\rangle = \langle a,b \mid ab=ba\rangle \overset{\overline{\varphi}}{\simeq} \mathbb{Z}^2$

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

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

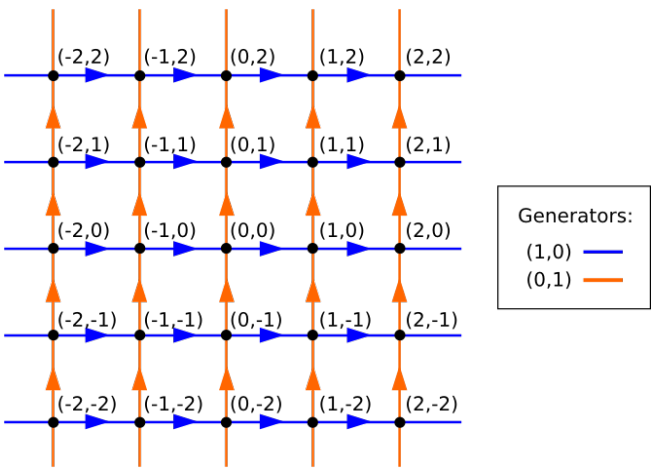
Obs: • Smallest subgroup containing $x = aba^{-1}b^{-1}$ is $\langle x\rangle \simeq \mathbb{Z}$.

• Smallest normal 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

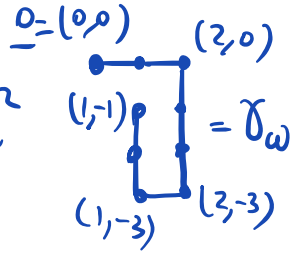
$a \longleftrightarrow (1,0)$

$b \longleftrightarrow (0,1)$



- Define a function $d: \mathrm{Free}\{a,b\} \longrightarrow \mathbb{R}_{>0}$ as follows: given $w \in \mathrm{Free}\{a,b\}$, trace a path in $\mathbb{R}^2$ by reading w from left to right:

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



Ex: $\omega = a^2 b^{-3} a^{-1} b^2 \rightsquigarrow \gamma_\omega$ follow path in $\mathbb{R}^2$

Set $d(\omega) = \max_{p \in \gamma_\omega} \{ \text{distance}(0, p) \}$

Remarks (1) $\forall\, \omega \in H$ Endpoint of $\omega = 0$.

(2) If $\omega_1, \omega_2 \in H \Rightarrow d(\omega_1 \omega_2) \leq \max\{d(\omega_1), d(\omega_2)\}$

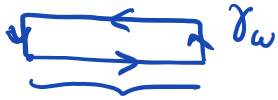
To finish, we argue by contradiction:

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

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

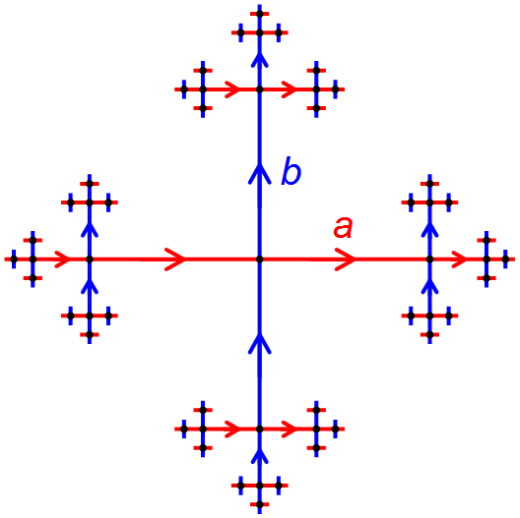
Then $d(h) \leq R \quad \forall\, h \in H$

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 $n >> 0$



Contr!

Obs: ∃ Alternative Proof via Algebraic Topology.



• Cayley graph of $\text{Free}(a,b)$

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

• $\text{Free}(\{a,b\})$ = 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: $\pi_1\left(\tilde{X}/F_2'\right) \simeq \langle V, RUT \rangle$

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

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

T = a spanning trees 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:

Thm: Fix G an infinite group & $\phi : F_{rk(n)} \twoheadrightarrow G$ s.t. homomorph.

Then: $\ker(\phi)$ is trivial or it is not finitely generated.