Lecture III: Presentation of a group; Generators for S_n

Recall • A non-empty subset $H \subseteq G$ is a subgroup ($H \leq G$) if $a, b \in H \Rightarrow a * b^{-1} \in H$.

• G group, $A \subseteq G$ we write $\langle A \rangle$ = subgroup generated by A

= smallest subgroup of G containing A.

Definition: • We say A generates G (A is a set of generators of G) if $\langle A \rangle = G$

non-uniqueness!

• We say G is finitely generated if $\exists$ finite set $A \subseteq G$ which generates G.

• Cyclic groups = groups admitting one generator

$\rightsquigarrow$ Classification: $\mathbb{Z}$, $\mathbb{Z}/k\mathbb{Z}$ for $k = 1, 2, \ldots$ $\left(\mathbb{Z}/\mathbb{Z} = \{e\} = \langle e \rangle\right)$

§3.1 Order of an element.

Fix a group G

Definition: Fix $a \in G$. The order of a (abbreviated as $\operatorname{ord}(a) \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$) is the smallest positive integer l such that $a^l = e$

Example: $\operatorname{ord}(a) = 1$ means $a^1 = e$

$\operatorname{ord}(a) = \infty$ means $\langle \{a\} \rangle = \mathbb{Z}$

Remark: If $a, b \in G$ satisfy $a * b = b * a$, then

$$\operatorname{ord}(a * b) \leq \text{l.c.m.}(\operatorname{ord}(a), \operatorname{ord}(b))$$

⚠ In general, product of elements of finite order need not have finite order.

§3.2 S_n revisited:

Q: Can we find a nice set of generators for S_n?

Proposition 1: Any permutation can be written as a product of disjoint cycles.

eg $(123)(45) = (45)(123)$ represent the permutation
$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix}$$

Claim: Any cycle is a product of 2-cycles, also called transpositions.

Pf/ $(i_1 i_2 \cdots\cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots\cdots (i_{k-2}, i_{k-1})(i_{k-1}\ i_k)$

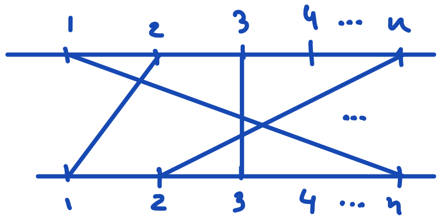
↳ a Typical k-cycle

Notation: $\sigma_{ij} = (i\,j)$ Transposition switching i & j.

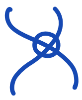
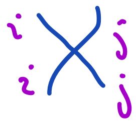
Proposition 2: S_n is generated by $\{\sigma_{ij} \quad 1 \le i < j \le n\}$ ($\binom{n}{2}$ elements)

Proposition 3: $S_n = \langle \sigma_{i,i+1} : 1 \le i \le n-1 \rangle$ ($n-1$ generators)

Pictorial proof:



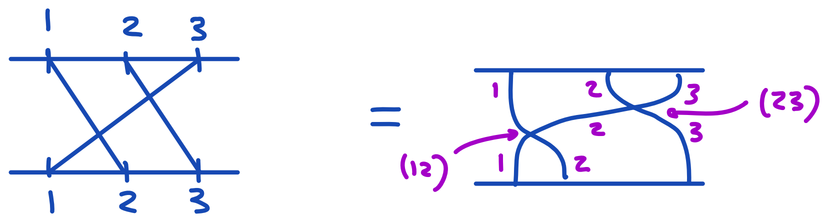
↓ read crossings from Top To bottom & write from right To left

- We rearrange the strings To see only one crossing per level
- We label  the crossings by index of a strings above & preserving them after the crossing 

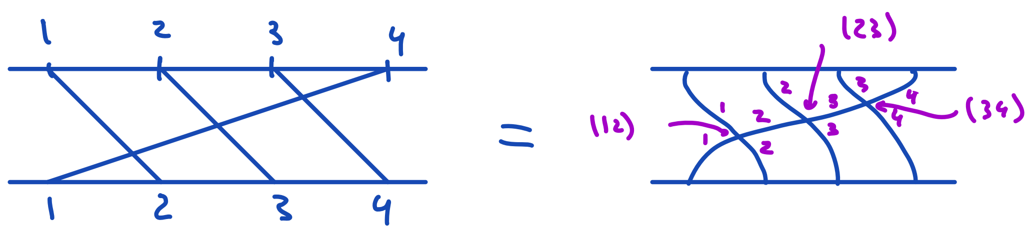
$\longleftrightarrow$ $(i\,j)$
- We write down the crossings from right To left, reading from top To bottom.

Example:

$(1\,2\,3) = (1\,2)(2\,3)$

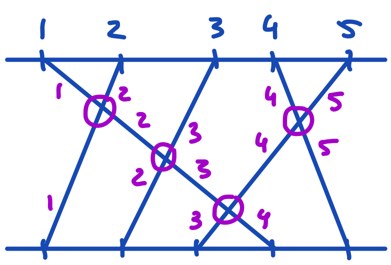


$(1\,2\,3\,4)$



$= (1\,2)(2\,3)(3\,4)$ ✓

$(1\,4\,5\,3\,2)$



↓ $= (3\,4)(2\,3)(4\,5)(1\,2)$

KEY: Show that in the construction, the only transpositions featuring are $\sigma_{i,i+1}$. (Exercise)

Conclude that $S_n = \langle \{ \sigma_{i,i+1} : 1 \leq i \leq n-1 \} \rangle$ (n-1 generators!)

§3.3 Presentation of a group:

Q: How do we write cyclic groups?

A: In terms of generators & relations, we write them as:

$$G = \langle \underset{\text{gens.}}{a} \mid \underset{\text{relations}}{a^k = e} \rangle \quad \begin{cases} k=0 : & \mathbb{Z} \\ k \geq 1 : & \mathbb{Z}/k\mathbb{Z} \end{cases} \quad \text{List of all cyclic groups}$$

To present a group is to write it as < generators | relations >

More precisely: $G = \langle \underbrace{a_1, a_2, \ldots}_{\text{symbols/alphabet}} \mid \underset{\text{relations}}{r_1, r_2, r_3, \ldots} \rangle$ means:

- G consists of words in the alphabet $\{a_1, a_2, \ldots\}$ eg, $a_3^{-1} a_1^4 a_2^3$

  A Typical word $w = x_1^{n_1} x_2^{n_2} \cdots x_\ell^{n_\ell}$ where $x_1, x_2, \ldots, x_\ell \in \{a_1, a_2, \ldots\}$, $n_1, n_2, \ldots, n_\ell \in \mathbb{Z}$
- $r_1, r_2, r_3, \ldots$ are words in the alphabet $\{a_1, a_2, \ldots\}$
- Neutral Element: $e = \phi$ "empty word"
- Operation: word concatenation subject to the trivial rules

$$x^k x^\ell = x^{k+\ell} \quad \& \quad x^0 = \phi \quad \text{for } x \in \{a_1, a_2, \ldots\} \;\&\; k, \ell \in \mathbb{Z}$$

(Which we ommit from "relations") plus extra Rules (relations): $r_1 = e, \quad r_2 = e, \quad \ldots$.

This means, if one of r_j appears in w, say $w = w_1 r_j w_2$, then $w = w_1 w_2$.

QUESTIONS: • How do we know the rules are consistent?

• How do we recognize a group from such a presentation?

This will be answered more precisely when we introduce normal subgroups & quotients.

Example: Let $G = \langle a, b \mid a^2, b^2 \rangle$ (Note: $\mathrm{ord}(a) \leq 2$ & $\mathrm{ord}(b) \leq 2$)

Then, $a^2 = e$ gives $a^{-1} = a$ & $b^2 = e$ gives $b^{-1} = b$

Conclusion: exponents are 0 or 1.

$\Rightarrow$ A typical element of G has the form $abab\ldots$ or $baba\ldots$ (these have infinite order if length ≥ 1)

§3.4 Issue with group presentations?

A trivial group can have a complicated presentation!

Example: (Bourbaki) $G = \langle x, y \mid xy^2 = y^3x,\ yx^2 = x^3y \rangle \simeq \langle e \rangle$

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

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

$\Rightarrow x^2y^8 = xy^{12}x = (xy^8)y^4x = y^{12}(xy^4)x = y^{12}(y^6x)x = y^{18}x^2$

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

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

(Indeed: $x^3y^8x^{-3} = x(x^2y^8x^{-2})x^{-1} = xy^{18}x^{-1} = (xy^8)y^{10}x^{-1}$

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

- Relation $yx^2 = x^3y$ gives $yx^2y^{-1} = x^3$, thus

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

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

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

$\Rightarrow \; xy^2 = y^3 x = x$ gives $y^2 = e$

But $y^2 = y^3 = e$ gives $y = e$.

To finish: relation $yx^2 = x^3 y$ gives $x = e$

[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)