Some background

May 11, 2020

1. Symmetric groups

Def. The symmetric group on n objects is the set

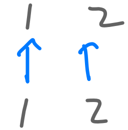
$$S_n = \{\text{bijective maps from } [n] := \{1, 2, \cdots, n\} \text{ to } [n] \text{ itself}\}.$$

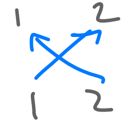
(bijective: injective (one-to-one) and surjective (onto))

with composition as its '<u>group operation</u>' or '<u>multiplication</u>'.

e.g. S_2 $\quad id = \begin{pmatrix} 1 & 2 \\ \uparrow & \uparrow \\ 1 & 2 \end{pmatrix}$ $\quad \sigma = \begin{matrix} 1 & & 2 \\ & \times & \\ 1 & & 2 \end{matrix}$ $\quad \cdots \quad \begin{matrix} 1 & 2 \\ \\ 1 & 2 \end{matrix}$

so $|S_2| = 2$. $\quad id \circ \sigma = \sigma = \sigma \circ id \qquad \sigma^2 = \sigma \circ \sigma = id$

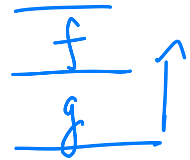
copied: $id =$ 

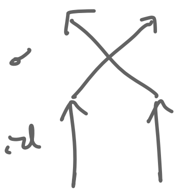
$\sigma =$ 

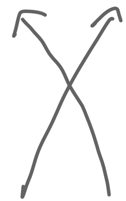
$\sigma \circ id = \sigma = id \circ \sigma$

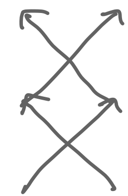
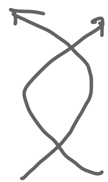
$\sigma^2 = id.$

$id^2 = id$

In pictures: $(f \circ g) =$ 

$\sigma \cdot id$ 

$=$  $= \sigma$

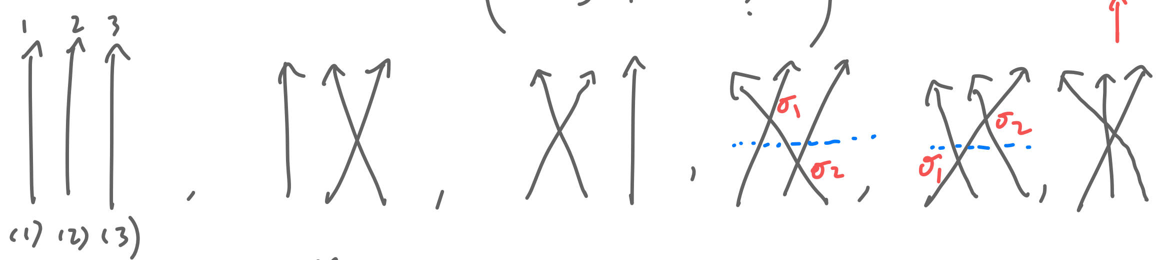
 $=$  $=$  $= id$

Theme: We'll often try to use diagrams to make algebraic computations easier/more intuitive

E.g. S_3. <u>Claim:</u> $|S_3| = 6$. $\begin{pmatrix} 1 \mapsto ? \\ 2 \mapsto ? \\ 3 \mapsto ? \end{pmatrix}$

$\sigma_1 \sigma_2 \sigma_1$

In pictures.



, the bijective map swapping i, i+1 but fixing all other numbers.

Thm: The "basic transpositions" $\sigma_i = (i, i+1)$ where $1 \le i \le n-1$ generate S_n in the sense that every elt $f \in S_n$ can be written as a product

$$f = f_1 f_2 \cdots f_k$$

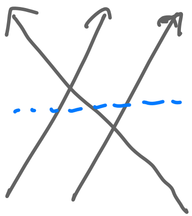
where each f_j is some basic transposition, i.e. $f_j = \sigma_i$ for some i.

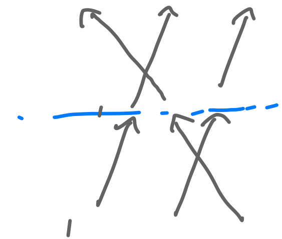
HW: Prove the theorem algebraically.

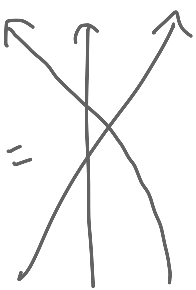
"Transposition": Swap only two entries $\longleftrightarrow$ notation $(i\ j)$, e.g. $(1\ 3)$.

"Basic": i, j are adjacent, i.e., $|i-j| = 1$.

A closer look at

$f =$  $= \sigma_1 \sigma_2$

check:  $= f$.

$g =$ 

(13)

We should be convinced now that

$$g = \sigma_1 \sigma_2 \sigma_1$$

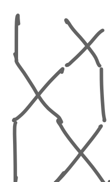
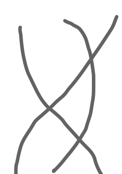
algebraically.

$\sigma_1 \sigma_2 (1) = 2 \overset{?}{=} f(1)$

$\sigma_1 \sigma_2 (2) = 3 \overset{?}{=} f(2)$

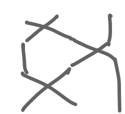
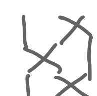
$\sigma_1 \sigma_2 (3) = 1 \overset{?}{=} f(3)$

Claim: $g = \sigma_2 \sigma_1 \sigma_2$

"pf" by pictures:  $=$  $= (13)$

More generally, in S_n, $\forall\, 1 \le i \le n-2$,

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$$

 $=$ 

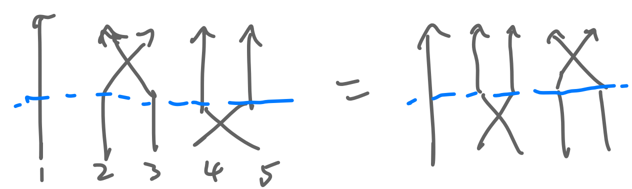
$i \quad i+1 \quad i+2 \qquad\qquad i \quad i+1 \quad i+2$

e.g. S_5. $\quad i=3 \quad \sigma_3=(3\,4) \quad \sigma_4=(4\,5)$.

We say $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ is a braid relation in S_n.

Another relation (that obviously holds) is $\sigma_i\sigma_j=\sigma_j\sigma_i$ whenever i,j are not adjacent, i.e., if $|i-j|>1$, eg

$\sigma_2\sigma_4=\sigma_4\sigma_2$ in S_n $(n\geq 5)$



Generators and relations

- We've seen that S_n is generated by the basic transpositions $\sigma_1, \ldots, \sigma_{n-1}$ and the generators satisfy the relations

$$\sigma_i^2 = 1 \ (\mathrm{id}), \qquad \sigma_i \sigma_j = \sigma_j \sigma_i \text{ if } |j-i|>1,$$

$$\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i \quad \forall\ 1 \le i \le n-1.$$

So... we can view elts as words on $\{\sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}$ and do multiplications in S_n using the relations.

If $f = \sigma_3\sigma_1\sigma_2$, $g = \sigma_2\sigma_1\sigma_2\sigma_3\sigma_2$,

$$fg = \sigma_3 \cancel{\sigma_1} \underline{\cancel{\sigma_2\sigma_2}} \cancel{\sigma_1} \sigma_2\sigma_3\sigma_2$$

$$= \sigma_3\sigma_2\sigma_3\sigma_2 = \sigma_2\sigma_3\cancel{\sigma_2\sigma_2}$$

$$= \sigma_2\sigma_3.$$

— In fact, not only can we understand S_n as a 'gp of words', given any set S, we can create gps whose elts are represented by words on S (and $S^{-1} := \{s^{-1} : s \in S\}$) and whose multiplication is given by concatenation plus possibly apply relations.

<u>e.g.</u> $S = \{a, b, c\}$. $\rightsquigarrow$ $w_1 = ab$, $w_2 = bc$ $\Rightarrow$ $w_1 w_2 = abbc$, $w_2 w_1 = bcab$

We can also impose relations on the words.

$S = \{a, b, c\}$. $G = \langle S \rangle / s^2 = 1 \ \forall s$ $\rightsquigarrow$ $w_1 = ab$, $w_2 = bc$ $\Rightarrow$ $w_1 w_2 = abbc = ac$

Point: It makes sense to define a gp

$$G_n = \left\langle s_1, \ldots, s_{n-1} \;\middle|\; \begin{array}{ll} s_i^2 = 1 & \forall s_i \\ s_i s_j = s_j s_i & \forall i,j \text{ w/ } |i-j| > 1 \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} & \forall 1 \le i \le n-1. \end{array} \right\rangle$$

presentation of G_n / S_n

Ex: $|G_3| \le 6$, $|G_4| \le 24$, $\ldots$, $|G_n| \le n!$

Thm: (In fact), we may identify S_n and G_n under the correspondence $\sigma_i \longleftrightarrow s_i$. e.g. $S_3 = \langle a, b \;/\; a^2 = b^2 = 1,\ aba = bab \rangle$

Point: The presentation allows us to think of S_n abstractly in terms of words. We'll generalize this idea to define Coxeter gps next time.