SYMMETRIC GROUPS

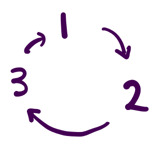
For each $n \geq 1$, let $S_n = \{\text{bijections } \{1,\dots,n\} \to \{1,\dots,n\}\}$, this is a group under composition. "the symmetric grp on n letters"

↑ other notation: Σ_n, $\mathfrak{S}_n$

An element $\sigma \in S_n$, $\sigma : \{1,\dots,n\} \to \{1,\dots,n\}$ can be represented
"permutation"

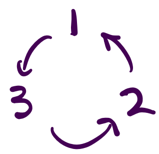
$$\begin{matrix} 1 \mapsto \sigma(1) \\ 2 \mapsto \sigma(2) \\ \vdots \\ n \mapsto \sigma(n) \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \begin{matrix} \leftarrow \text{input} \\ \leftarrow \text{output} \end{matrix}$$

Ex. $S_3 \ni \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (231)$ ← new notation



$(123) = (231) = (321)$

$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) \in S_3$



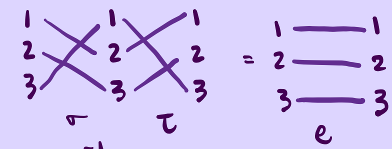
$(132) = (321) = (213)$

Note Can view $\sigma \in S_4$ as $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

$= (123)(4)$ ← sometimes omitted!

In this way, $S_n \underset{\leq}{\hookrightarrow} S_{n+k}$ $\forall k \geq 0$.

Multiplication + Inverses

$\sigma\tau$ 

$\Rightarrow \tau = \sigma^{-1}$

in the other notations:

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} \overset{\text{flip}}{=} \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$(231)^{-1} \underset{\text{reverse}}{=} (132)$

multiply: $(231)(132) = (1)(3)(2)$

Exs

$S_4 \ni \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)(3)(4) = (12)$ swap 1 & 2 ← "transpositions"

Note $(12) = (21)$ and $(12)(12) = e$ so $(12)^{-1} = (12)$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (23)$ (also $(23)^{-1} = (23)$)

Multiply: $(12)(23) = (123)$
$(23)(12) = (132)$ $\rightsquigarrow$ $(123) \neq (132)$ implies S_n not Abelian $(n \geq 3)$!

But if I chose (34) instead of (23), then $(12)(34) = (34)(12)$. This is b/c these cycles are disjoint ($(i_1 i_2 \cdots i_k), (j_1 j_2 \cdots j_m)$ disjoint if $\{i_1,\dots,i_k\} \cap \{j_1,\dots,j_m\} = \phi$)
"move different letters"

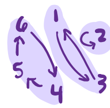
Thm If τ, σ disjoint, then $\tau\sigma = \sigma\tau$.

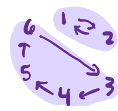
Pf/ For $k \in \{1,\dots,n\}$, will show $\tau\sigma(k) = \sigma\tau(k)$. If $\tau(k) = \sigma(k) = k$, then done. Otherwise, since σ and τ are disjoint, exactly one of them moves k. WLOG, $\tau(k) = k$ and $\sigma(k) \neq k$. Then $\sigma(\tau(k)) = \sigma(k)$ and $\tau(\sigma(k)) = \sigma(k)$ since (again by disjointness) τ can't move $\sigma(k)$. □

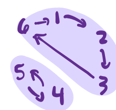
Prop (HW 7.1) If σ, τ disjoint and $\sigma\tau = e$, then $\sigma = e = \tau$.

Pf/ To show $\sigma = e$, will show $\sigma(k) = k$ $\forall k \in \{1, \dots, n\}$. Suppose $\sigma(k) \neq k$. By disjointness, must have $\tau(k) = k$. But then $\sigma\tau(k) = \sigma(k) \neq k$, contradicting $\sigma\tau = e$. Hence $\sigma(k) = k$ $\forall k$ so $\sigma = e$.
To show $\tau = e$, note that $\tau\sigma = \sigma\tau = e$ (by the Thm above) and apply the same argument. $\square$

Exs

$S_6 \ni \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 4 & 5 \end{pmatrix} = (13)(2)(465)$ 

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{pmatrix} = (12)(3456)$  "disjoint cycles"

$(13)(2)(465) \cdot (12)(3456) = (1236)(45)$ 

or $(12)(3456) \cdot (13)(2)(465) = (1432)(5)(6) = (1432)$ 

Thm Every elmt of S_n can be written as a product of disjoint cycles.
Every cycle can be written (non-uniquely) as a product of transpositions.

Ex $(13)(2)(456)$

$\hookrightarrow (456) = (45) \cdot (56)$ (imagine )

$(12)(3456)$

$\hookrightarrow (3456) = (43)(54)(65)$

Conjugation

Recall: • For any $g \in G$, the conjugate of $h \in G$ by g is the elmt $ghg^{-1} \in G$.

• Get automorphism $c_g : G \to G$, $h \mapsto ghg^{-1}$ conjugation by g.

• The assignment $c : G \to \mathrm{Aut}(G)$, $g \mapsto c_g$ is a group homomorphism. $c_{g_1 g_2} = c_{g_1} \circ c_{g_2}$

• The image and kernel get special names:

• $Z(G) = \ker(c) \trianglelefteq G$ "centralizer"

• $\mathrm{Inn}(G) = \mathrm{im}(c) \leq \mathrm{Aut}(G)$ "inner automorphisms"

Random Aside (feel free to ignore!!)

Q When is c an isomorphism?

A. Iff ① $Z(G) = e$, ② $\mathrm{Inn}(G) = \mathrm{Aut}(G)$.

① $Z(G) = e \iff G$ is Abelian

Pf/ ($\Leftarrow$) for all $g \in G$, $h \in G$, $ghg^{-1} = gg^{-1}h = h$ so $\sigma_g = id$ $\forall g \in G$.

($\Rightarrow$) we know for all $g, h \in G$, $\sigma_g = id$ so $\sigma_g(h) = h$. Thus

$$h = \sigma_g(h) = ghg^{-1} \iff hg = gh.$$

② But if G is Abelian, $Inn(G) = \{\sigma_g \mid g \in G\} = \{id\} \leq Aut(G)$. So $Inn(G) = Aut(G)$ for Abelian G implies the only automorphisms of G is the identity.

Claim This is true iff $G = e$ or $G = \mathbb{Z}/2$.

Lemma If G is Abelian, the "inversion" map $i : G \to G$, $g \mapsto g^{-1}$ is an automorphism

Pf/ Since G is a group, i is well-defnd (every $g \in G$ has a unique $g^{-1} \in G$). Moreover i is a homomorphism since for any $g, h \in G$,

$$i(gh) = (gh)^{-1} = h^{-1}g^{-1} \underset{\uparrow \text{Ab}}{=} g^{-1}h^{-1} = i(g)\,i(h). \qquad \square$$

Note that $i = id \iff g = g^{-1}$ $\forall g \in G$.

$\iff G = \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2 \times \cdots = (\mathbb{Z}/2)^n$ where $0 \leq n \leq \infty$ need to be careful

But if $n \geq 2$, then can swap the factors to get a non-trivial automorphism. Thus $n = 0$ or $n = 1$. Therefore:

A (for real) σ is an isomorphism iff $G = e$ or $G = \mathbb{Z}/2\mathbb{Z}$.

and not a very interesting one: $\sigma = id : e \to e$.

Back to Symmetric groups:

Let $\tau, \sigma \in S_n$ and $\delta = \tau\sigma\tau^{-1} = c_\tau(\sigma)$.

Claim If $\sigma(i) = j$ then $\delta(\tau(i)) = \tau(j)$

Pf/ $\delta(\tau(i)) = \tau\sigma\tau^{-1}\tau(i) = \tau\sigma(i) = \tau(j)$

Thus If σ has cycle representation

$$(a_1 \cdots a_k)(b_1 \cdots b_j) \cdots$$

then δ has cycle representation

$$(\tau(a_1) \cdots \tau(a_k))(\tau(b_1) \cdots \tau(b_j)) \cdots$$

Ex. $\sigma = (1438)(265)$
$\tau = (163)(752)$ $\Rightarrow$ $\delta = \tau\sigma\tau^{-1} = (6418)(732)$.

Minute sheet

- On a ☹-10 ☺ how prepared do you feel for the midterm?
- Which areas do you feel most confident v.s. worried about?
- What's your favorite candy / is there anything you're allergic to?

~ break ~ Practice Midterm

Index of a subgroup $H \leq G$

$$|G:H| = \frac{|G|}{|H|}$$

Exs • If $d \mid n$ then $\mathbb{Z}/d\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$ and $|\mathbb{Z}/n\mathbb{Z} : \mathbb{Z}/d\mathbb{Z}| = \frac{|\mathbb{Z}/n\mathbb{Z}|}{|\mathbb{Z}/d\mathbb{Z}|} = \frac{n}{d}$.

• If G is finite and $g \in G$ has order $o(g)$, then

$$|G:\langle g \rangle| = \frac{|G|}{o(g)}$$

Centralizers for $g \in G$: $C_G(g) := \{g' \in G \mid gg' = g'g \iff gg'g^{-1}g'^{-1} = e\} \leq G$

for $H \leq G$: $C_G(H) := \{g \in G \mid gh = hg \ \forall h \in H\} \leq G$

(these are related to something called normalizers)

The Center of G is $Z(G) = C_G(G) = \{g \in G \mid gg' = g'g \ \forall g' \in G\}$.

This is also the kernel of conjugation $\ker(c) = \{g \in G \mid c_g = id\}$

$c_g(g') = gg'g^{-1}$

Properties: • G is Abelian $\iff Z(G) = G$

• $H \leq G$ is Abelian $\iff H \leq C_G(H)$

• If $H \leq C_G(H)$ then $H' \leq C_G(H)$

Exc Show $H \leq C_G(C_G(H))$ always