Herstein TIA ch 2.10
Herstein AA ch 3

10/9/2022

The Symmetric Group (Better name: Permutation Group)

NO one really sure why it is called "Symmetry" – maybe because of Symm polys. The subgrp which is Dihedral group is about actually reflection and rotation symms of regular polygons.

Consider a finite set $\mathcal{S}$. It has n elts

Consider the set of all one-to-one and onto maps $\theta : \mathcal{S} \leftrightarrow \mathcal{S}$

This set $B_{ij}(\mathcal{S} \to \mathcal{S}) =: \boxed{A(\mathcal{S}) =: S_n}$ is the 'Symm Group (on n letters)'.

If we give every elt an index number, we can write any perm θ as

$$\theta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$$

This means (item name ↦ position) $1 \mapsto i_1$, $2 \mapsto i_2$ etc..., $3 \mapsto i_3$

$\overrightarrow{x\theta\psi}$

Let's work an example (Herstein TIA p.76 but NOT in algebraists notation, in std notation) compose perms like any other fcns.

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$\mathcal{S} \xrightarrow{\theta} \mathcal{S} \xrightarrow{\psi} \mathcal{S} \quad \text{This is } \psi \circ \theta(\cdot)$$

Then $\psi \circ \theta(\cdot) = \overset{\psi}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}} \overset{\theta}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ because

$1 \to 3 \to 2$
$2 \to 1 \to 1$
$3 \to 2 \to 3$
$4 \to 4 \to 4$

[Since only 1 & 2 are interchanged in the end, this whole thing could be written as the cycle $(1\ 2)$]

Now lets write this in terms of matrices (even though multiplying matrices is more work).

BE CAREFUL – THIS IS VERY TRICKY TO GET RIGHT!

$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ means (item → position) $1 \to 3$, $2 \to 1$, $3 \to 2$, $4 \to 4$

so
$$\underbrace{\begin{bmatrix} \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix}}_{P} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 1 \\ 4 \end{bmatrix}$$

it is NOT
$$\underbrace{\begin{bmatrix} \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix}}_{\text{This is actually } P^{-1} = P^T} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 2 \\ 4 \end{bmatrix}$$

(perms are O.N. matrices).

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \rightsquigarrow \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix}$$

and matrices

$$[\psi]\cdot[\theta] = \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} \begin{bmatrix} \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} = \begin{bmatrix} \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} \checkmark$$

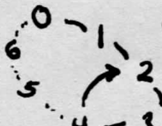
▷ Going back to the general discussion,
since $\theta : \mathcal{S} \to \mathcal{S}$ is a bijection, for an elt $a \in S$ we can iterate θ on it $\theta^i(a)$ and generate a bunch of elts of $\mathcal{S}$ called the Orbit of a under θ

Technically the Orbit is $\theta^i(a)$ for ~~any~~ all $i \in \mathbb{Z}$, whereas the Cycle $\langle a \rangle = \{a, \theta(a), \ldots \theta^k(a)\}$ ordered set where $\theta^{k+1}(a) = a$ cycle has closed.

Being in an orbit is an equivalence relation.

$\boxed{\text{Thm since } \mathcal{S} \text{ is finite, } \exists \text{ smallest } k > 0 \ni \theta^k(a) = a \text{ (cycle closes on itself)}}$

pf. (1.) No cycle can close back on itself except at the initial pt: If $\theta^k(a) = a$ then no way $\theta^{k-p}(a) = \theta^r(a)$ $0 < r < p < k$
Say $\theta^4(a) = \theta^2(a)$. apply θ^{-2} since bij $\Rightarrow \theta^2(a) = a$ ⇏



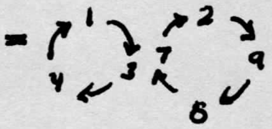
Can't happen since θ has an inverse. (is one-to-one and onto)

(2) In worst case scenario $k = \#\mathcal{S} = n$ and one cycle covers all of $\mathcal{S}$ but still $\theta^{n+1}(a) = a$ by step 1.

Every perm can be written as the product of <u>disjoint</u> cycles.

Disjoint cycles commute, since they don't touch each other's elts.

AA p. 132

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 4 & 1 & 5 & 6 & 2 & 7 & 8 \end{pmatrix} =$  $5 \to 5$, $6 \to 6$ $= (1\,3\,4)(2\,9\,8\,7)(5)(6)$

This is in S_9

we typically omit writing the 1-cycles, with the understanding that elts not listed are fixed.

<u>Lemma 3.2.3</u> Let $\sigma \in S_n$ be a k-cycle $\Rightarrow$ order of σ is k [i.e. $\sigma^k = e$, $\sigma^j \neq e$ for any $j \in \{0, \dots, k-1\}$]

No pf given, but it is obvious. After k steps around the circle, you are back where you started.

Let $\tau = (1\,2)(3\,4\,5\,6)(7\,8\,9)$ perm in S_9

What is its order? call it m. Then $\tau^m = e$ so

$(1\,2)^m \overset{!}{=} e \Rightarrow 2 \mid m$ → contains 2

$(3\,4\,5\,6)^m \overset{!}{=} e \Rightarrow 4 \mid m$ $\mathrm{lcm}(4,3) = 12$

$(7\,8\,9) \overset{!}{=} e \Rightarrow 3 \mid m$ $m = 12$

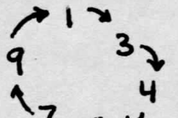
<u>Thm</u> $\sigma \in S_n$

σ is composed of <u>disjoint</u> cycles of lengths $m_1, \dots, m_k$ $\Rightarrow$ Order of $\sigma = \mathrm{lcm}(m_1, m_2 \dots m_k)$

Basic idea of pf apparent from example above

▷ How to write a cycle as a product of transpositions?

$(1\,3\,4\,6\,7\,9)(\cdot) = (1\,9)(1\,7)(1\,6)(1\,4)(1\,3)(\cdot)$



step 0 [1→3] 1 2 3 4 5 6 7 8 9

step 1 3 _ 1 _ _ _ _ _ _ ← apply (13) This transp puts elt ① in its final position in slot 3 and ③ goes in staging area slot 1

step 2 [3→4] 4 _ 1 3 _ _ _ _ _ ← (1 4) and ③ in final pos

step 3 [4→6] 6 _ 1 3 _ 4 _ _ _ ← (1 6) and ④ in " "

4,6 7 _ 1 3 _ 4 6 _ _ ← (1 7) ⑥

9 2 1 3 5 4 6 8 7 ← (1 9) ⑦ 8 ⑨ in final pos.

Systematic way(s) to do any perm by transpositions: Transpose elt ① to its final position, say 3, put that elt ③ in pos 1. Now transpose ③ to its final pos, say 4. Put elt ④ in pos 1. Keep going, we never touch any elt already put in final position.

<u>Here is another example</u>: show $(1\,2\,4\,3)(2\,4\,3) = (2\,3)(3\,4)(1\,4)$

apply to an array: $(1\,2\,4\,3)(2\,4\,3)[a\,b\,c\,d] \Rightarrow abcd \xrightarrow{(243)} \underline{a}\,\underline{c}\,\underline{d}\,\underline{b} \xrightarrow{(1\,243)} \underline{d}\,\underline{a}\,\underline{b}\,\underline{c}$

whereas $abcd \xrightarrow{(14)} \underline{d}\,\underline{b}\,\underline{c}\,\underline{a} \xrightarrow{(34)} \underline{d}\,\underline{b}\,\underline{a}\,\underline{c} \xrightarrow{(23)} \underline{d}\,\underline{a}\,\underline{b}\,\underline{c}$

Any transposition of 2 elts which are separated by k slots can be effected by $k + (k-1)$ nearest neighbor exchanges.

_ _ ⓘ _ _ _ _ _ (i+k) _ _

we can move ⓘ to pos $i+k$ by k nearest nbhr swaps. Then we get (i+k) back to pos i by $(k-1)$ nn swaps.

10/15/2022

<u>Thm</u> Every perm σ can be achieved by either an <u>even</u> or <u>odd</u> number⊛ of transpositions, but not both. That is, if an even number achieves the result, no odd number can — and vice versa.

⊛ actually many even numbers or many odd numbers – not unique there, only the parity.

<u>tricky pf</u>: $\sigma \in S_n$ so we have $1, 2, 3, \dots, n$ This is the natural order and we construct a <u>symbolic poly</u> of all pairs of indices, always with the lowest first (low – higher):

Say for $n=3$ $P(1,2,3) = \underbrace{P(x_1, x_2, x_3) = P(x,y,z)}_{\text{renaming for convenience}} = \overbrace{(x-y)(x-z)}^{B_1}\overbrace{(y-z)}^{B_2}$

For $n=5$ (and pretending the alphabet is ordered x, y, z, u, v)

$$P(1,2,3,4,5) = P(x,y,z,u,v) = \underbrace{(x-y)(x-z)(x-u)(x-v)}_{B_1} \cdot \overbrace{(y-z)(y-u)(y-v)}^{B_2}\overbrace{(z-u)(z-v)}^{B_3}\underbrace{(u-v)}_{B_4}$$

The whole reason for this is to construct something that changes sign if any 2 elts (indices!) are transposed.

(1) Consider nearest neighbor pairs – they occur only at the start of each block B_i and occur only once and only in their block. For example $x-y$ occurs only in B_1 and $P(y, x, z)$ makes $B_1 \to -B_1$ and $P(y,x,z) = -P(x,y,z)$

Likewise for any other nearest neighbor pair.

(2) Any transpose of elts separated a dist k can be achieved by $k+(k-1)$ nearest nbhr exchanges, so P would change sign $2k-1$ times (odd number) So for any transpose $P \to -P$

$(-1)^{2k-1} = -1$.

(3) Any perm σ can be attained by N transpositions. So $P \mapsto (-1)^N P$

If N is even $P \to +P$ and N odd $P \to -P$.

(4) Since $P(\sigma(x))$ will definitely equal either P or $-P$. If $\text{sign}(P(\sigma)) = +1$ σ is even and no odd number of transposition can make it. Same idea if $P(\sigma)$ has sign -1 and σ is odd.

□

Given S_n, Let $A_n \subset S_n$ consist of all even perms

A_n is a subgroup (in fact Normal subg $A_n \triangleleft S_n$) and it is called the Alternating Group.

(I couldn't find an explanation of why it has this name and it <u>doesn't</u> seem related to anything like alternating forms $\omega \in \Omega^k(M)$ $dx \wedge dy = -dy \wedge dx$)