Permutation Groups

Definition: Let A be a set. A permutation of A is a bijection $f: A \to A$.

Special case $A = \{1, 2, \dots, n\}$

$$\left.\begin{aligned} f(1) &= 3 \\ f(2) &= 4 \\ f(3) &= 1 \\ &\vdots \end{aligned}\right\} \quad \begin{pmatrix} 1 & 2 & 3 & \dots \\ 3 & 4 & 1 & \end{pmatrix}$$

Notation: We write $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$ to denote the function $f: \{1, \dots, n\} \to \{1, \dots, n\}$

$$f(1) = a_1$$
$$f(2) = a_2 \quad \text{and so on...}$$

Proposition: The set S_A of permutations of A forms a group with

- product $\sigma * \tau = \sigma \circ \tau$
- identity $e = id_A$
- inversion σ^{-1} = inverse as a function! $\sigma^{-1}: y \mapsto x$ for $\sigma(x) = y$.

Def: The group S_A is called the symmetric group on A. A subgroup $H \leq S_A$ is called a group of permutations.

Special case: we write S_n instead of S_A when $A = \{1, \dots, n\}$.

Ex: $\sigma, \tau \in S_3$ $\quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau$$

$$\sigma : \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{array} \qquad \sigma(1) = 3 \qquad \sigma^{-1} : \begin{array}{l} 3 \mapsto 1 \\ 2 \mapsto 2 \\ 1 \mapsto 3 \end{array}$$

$$\underline{\sigma\tau} = \sigma \circ \tau : \left.\begin{array}{l} 1 \overset{\tau}{\mapsto} 2 \overset{\sigma}{\mapsto} 2 \\ 2 \mapsto 1 \mapsto 3 \\ 3 \mapsto 3 \mapsto 1 \end{array}\right\} \underline{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}$$

$$\tau\tau^{-1} = \tau \circ \tau^{-1} : \left.\begin{array}{l} 1 \overset{\tau^{-1}}{\mapsto} 2 \overset{\tau}{\mapsto} 1 \\ 2 \mapsto 1 \mapsto 2 \\ 3 \mapsto 3 \mapsto 3 \end{array}\right\} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id$$

Def: Let $\sigma \in S_A$ for some set A. The orbit of an element $a \in A$ under σ is

$$orb_\sigma(a) = \{a, \sigma^{\pm 1}(a), \sigma^{\pm 1}(\sigma^{\pm 1}(a)), \ldots\} = \{\sigma^k(a) \mid k \in \mathbb{Z}\}$$

Ex:

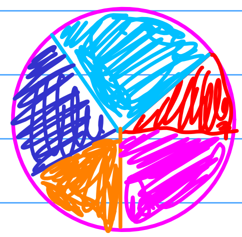
$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{aligned} orb_\sigma(1) &= \{1, \sigma(1), \sigma(\sigma(1)), \ldots\} \\ &= \{1, 3, 1, 3, 1, 3, \ldots\} \\ &= \{1, 3\} \end{aligned}$$

$$\begin{aligned} orb_\sigma(2) &= \{2, \sigma(2), \sigma(\sigma(2)), \ldots\} \\ &= \{2, 2, \sigma(2), \ldots\} \\ &= \{2, 2, 2, \ldots\} = \{2\} \end{aligned}$$

$$\begin{aligned} orb_\sigma(3) &= \{3, \sigma(3), \sigma(\sigma(3)), \ldots\} \\ &= \{3, 1, \sigma(1), \ldots\} \\ &= \{3, 1, 3, 1, 3, 1, \ldots\} \\ &= \{3, 1\} \ \checkmark \end{aligned}$$

Remember: a partition of A is a collection of disjoint subsets whose union is A.



$A = \{1,2,3\}$

$orb_\sigma(1)$, $orb_\sigma(2)$

Theorem: Given $\sigma \in S_A$, the set $\{ orb_\sigma(a) \mid a \in A \}$ is a partition of A.

Ex: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$

$orb_\sigma(1) = \{1,3,4\} = orb_\sigma(3) = \{3,4,1\}$
$= orb_\sigma(4) = \{4,1,3\}$

$orb_\sigma(2) = \{2,5\} = orb_\sigma(5) = \{5,2\}$

$\{1,3,4\}, \{2,5\}$ is a partition of $\{1,2,3,4,5\}$

Def: A permutation σ which sends $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $a_3 \mapsto a_4, \ldots, a_r \mapsto a_1$ and fixes every other element of A is called a <u>cycle</u> and denoted $(a_1 a_2 a_3 \ldots a_r)$

Ex: $(1\,2\,3) \in S_5$ is the same permutation as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$

Ex: $(2\,1\,4\,3) \in S_5$ is the same as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$

Ex: If $\tau = (3\,9\,2\,7\,4) \in S_{10}$

Q: $\tau(2) = 7$ $\tau(7) = 4$, $\tau(4) = 3$

$\tau(1) = 1$.

Def: Two cycles $(a_1 \dots a_r)$, $(b_1 \dots b_s)$ are disjoint if $\{a_1, \dots, a_r\} \cap \{b_1 \dots b_s\} = \emptyset$.

Prop: If τ, σ are disjoint cycles, $\tau\sigma = \sigma\tau$.

Ex: $\tau, \sigma \in S_5$ $\tau = (325)$. $\sigma = (14)$

$$\tau\sigma : 2 \xmapsto{\sigma} 2 \xmapsto{\tau} 5$$
$$\sigma\tau : 2 \xmapsto{\tau} 5 \xmapsto{\sigma} 5$$

Ex: $\tau, \sigma \in S_5$ $\tau = (325)$, $\sigma = (12)$

$$\tau\sigma : 2 \xmapsto{\sigma} 1 \xmapsto{\tau} 1$$
$$\sigma\tau : 2 \xmapsto{\tau} 5 \xmapsto{\sigma} 5$$

Theorem: $|A| < \infty$

If $\tau \in S_A$, then τ is a product of disjoint cycles
$$\tau = \sigma_1 \sigma_2 \cdots \sigma_k$$

Moreover, the cycles are unique up to reordering!

Ex: $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} \in S_5$

$\mathrm{orb}_\tau(1) = \{4, 3, 1\}$ $\boxed{\tau = (431)(52)}$

$\mathrm{orb}_\tau(2) = \{5, 2\}$

Double-check:

$$(431)(52):\quad \begin{array}{l} 1 \xmapsto{(52)} 1 \xmapsto{(431)} 4 \\ 2 \mapsto 5 \mapsto 5 \\ 3 \mapsto 3 \mapsto 1 \\ 4 \mapsto 4 \mapsto 3 \\ 5 \mapsto 2 \mapsto 2 \end{array} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$$

<u>Ex</u>: $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 7 & 2 & 1 & 5 & 6 \end{pmatrix} = (1423765)$

$\mathrm{orb}_\tau(1) = \{1,4,2,3,7,6,5\}$

<u>Def</u>: An m-cycle is a cycle w/ m entries.
A 2-cycle is called a <u>transposition</u>.

<u>Theorem</u>: Every m-cycle can be expressed as a product of transpositions. Hence every permutation can be also.

The decomposition into transpositions is <u>not</u> unique!

<u>Theorem</u>: If τ can be written as a product of an even number of transpositions, it can't also be a product of an odd number!

<u>Definition</u>: A permutation is <u>even</u> if it can be written as an even # of transpositions. Otherwise it's <u>odd</u>. The even or odd property is called the <u>parity</u>. The <u>sign</u> of a cycle is

$$\mathrm{sgn}(\tau) = \begin{cases} 1, & \tau \text{ even} \\ -1, & \tau \text{ odd.} \end{cases}$$

τ, σ odd $\Rightarrow \tau\sigma$ even

τ odd, σ even $\Rightarrow \tau\sigma$ odd $\qquad \sigma\tau$ odd

τ, σ even $\Rightarrow \tau\sigma$ even

$A_A = \{\sigma \in S_A \mid \sigma \text{ even}\} \leq S_A$ $\boxed{\text{alternating group}}$