Permutation Group

<u>Def</u>: Let A be a set. The set
$$S_A = \{ f : A \to A \mid f \text{ is a bijection} \}$$
is a group with binary operation $*$ given by $f * g = f \circ g$ called the <u>permutation group of A</u>.

Special case: $S_n = S_{\{1,2,\dots,n\}}$

<u>Ex</u>: S_3? What are the elements?

$$S_3 = \{ f : \{1,2,3\} \to \{1,2,3\} \mid f \text{ is bijective} \}$$

$$\begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 1 \\ 3 &\mapsto 3 \end{aligned} \qquad\qquad \begin{aligned} 1 &\mapsto 2 \\ 2 &\mapsto 3 \\ 3 &\mapsto 1 \end{aligned}$$

NOTATION: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

All elements of S_3:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Challenge: How many elements does S_n have?

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ \binom{n}{\text{poss.}} & \binom{n-1}{\text{poss}} & \binom{n-2}{\text{poss}} & \binom{n-3}{\text{poss}} & & \binom{1}{\text{poss}} \end{pmatrix}$$

$$n \cdot (n-1)(n-2)(n-3)\dots(1) = n!$$

A very cool alternative notation: **cycle notation**

Ex: $(1\,3\,2) \equiv \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ in S_3

Ex: $(1\,2)(3) \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ in S_3

$= (1\,2)$

Ex: $\underbrace{\overbrace{(1\,3\,5)}^{\text{cycles}}(2\,4)}_{\text{disjoint prod. of cycles}} \equiv \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$ in S_6

Remark: $(1\,3\,5) = (5\,1\,3) = (3\,5\,1)$

Quest: Take an arbitrary permutation and write it as a disjoint product of cycles.

Ex: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 2 & 1 & 4 \end{pmatrix} \equiv (1\,3\,6\,4\,2\,5)$

Ex: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 5 & 6 & 7 & 8 & 4 \end{pmatrix} \equiv (1\,3)(2)(4\,5\,6\,7\,8)$

$\equiv (1\,3)(4\,5\,6\,7\,8)$

Let's multiply!

$(1\,2), (2\,3) \in S_4$.

$(1\,2) * (2\,3) = (1\,2)(2\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ * & * & * & * \end{pmatrix}$??

$$\left.\begin{array}{l} 1 \mapsto 1 \mapsto 2 \\ 2 \mapsto 3 \mapsto 3 \\ 3 \mapsto 2 \mapsto 1 \\ 4 \mapsto 4 \mapsto 4 \end{array}\right\} \quad \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \\ 4 \mapsto 4 \end{array}$$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

$(1\,2\,3)$

Conclusion: $(12)(23) = (123)$

$(23)(12) = ?$

$$\left.\begin{array}{l} 1 \mapsto 2 \mapsto 3 \\ 2 \mapsto 1 \mapsto 1 \\ 3 \mapsto 3 \mapsto 2 \\ 4 \mapsto 4 \mapsto 4 \end{array}\right\} \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \\ 4 \mapsto 4 \end{array} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

(132)

Conclusion: $(23)(12) = (132)$

This is a non-abelian group!

Theorem: If $\tau = (a_1 a_2 \dots a_j)$, $\sigma = (b_1 b_2 \dots b_k) \in S_n$ are disjoint cycles, then $\tau\sigma = \sigma\tau$.

Def: The order of $g \in G$ is the smallest positive value of n such that $g^n = e$.

Ie. $\underbrace{g * g * g * \dots * g}_{n \text{ times}} = e$

Ex: What's the order of $(123) \in S_7$?

$1 \mapsto 2 \mapsto 3 \mapsto 1$

$2 \mapsto 3 \mapsto 1 \mapsto 2$

$3 \mapsto 1 \mapsto 2 \mapsto 3$

$(123) \quad (123) \quad (123)$

$$(123)(123)(123) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

The order of (123) is 3

Prop: The order of $(a_1 a_2 \dots a_r) \in S_n$ is r.

Prob: What is the order of $(12)(345)$?

$$(12)(345)(12)(345) = (12)(12)(345)(345)$$
$$= (345)(345)$$

$$(12)(345)\underbrace{(12)(345)(12)(345)}_{(345)(345)} = (12)(345)(345)(345)$$
$$= (12)$$

$$[(12)(345)]^6 = (12)^6(345)^6$$
$$= [(12)^2]^3[(345)^3]^2$$
$$= e^3 e^2 = e^5 = e.$$

The order is the lcm of 2 and 3 !!

<u>Subgroups</u>: G is a group.

<u>Def</u>: A subset $H \subseteq G$ is called a <u>subgroup</u> of G the binary operation $*$ of G restricts to a binary operation on H, making H a group.

<u>Theorem</u>: $H \subseteq G$ is a subgroup if and only if
(1) $a * b \in H$ for all $a, b \in H$
(2) $e \in H$
(3) $a^{-1} \in H$ of all $a \in H$.

<u>Ex</u>: $G = \mathbb{C}$, $* = +$
$H = \mathbb{R}$ is a subgroup

<u>Ex</u>: $G = GL_n(\mathbb{R}) = \{ n \times n \text{ invertible matrices} \}$
$H = SL_n(\mathbb{R}) = \{ n \times n \text{ matrices with } \det = 1 \}$
H is a subgroup!

<u>Def</u>: A cyclic subgroup of G is a set
$\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$ for some $a \in G$

where $a^n = \underbrace{a * a * \dots * a}_{n\text{-times}}$, $a^{-n} = a^{-1} * a^{-1} * \dots * a^{-1}$
$a^0 = e$.

A group is called <u>cyclic</u> if its generated by a single element, i.e. $G = \langle a \rangle$ for some $a \in G$.

<u>Ex</u>: $G = \mathbb{Z}$, $\langle 2 \rangle = \{0, \pm 2, \pm 4, \pm 6, \dots\}$ = even integers

$$G = \langle 1 \rangle = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

<u>Ex</u>: $G = S_3$, $\langle (123) \rangle = \{e, (123), (132)\}$.

<u>Theorem</u>: the size of $\langle a \rangle$ = order of a.

$G, \tilde{G}$ groups

<u>Def</u>: An isomorphism is a bijection $f: G \to \tilde{G}$ satisfying $f(a * b) = f(a) * f(b)$ $\forall a, b \in G$.

$\mathbb{Z}_n$ iso. to $U_n = \{e^{ik\pi/n} \mid 0 \le k \le n-1\}$

$\mathbb{Z}_n = \{0, \dots, n-1\}$