Symmetric groups

Let A be a nonempty set. The symmetric group on A is $S_A = \{\text{bijections } \sigma: A \to A\}$, with the binary operation of composition of maps.

Check that this is a group:

- associativity: ✓

  $\forall \sigma_1, \sigma_2, \sigma_3 \in S_A, \quad \forall a \in A,$

  $$((\sigma_1 \circ \sigma_2) \circ \sigma_3)(a) = (\sigma_1 \circ \sigma_2)(\sigma_3(a)) = \sigma_1(\sigma_2(\sigma_3(a)))$$
  $$= \sigma_1(\sigma_2 \circ \sigma_3(a)) = (\sigma_1 \circ (\sigma_2 \circ \sigma_3))(a).$$

  Therefore $(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3)$.

- identity: ✓

  Define $e: A \to A$ by $e(a) = a, \ \forall a \in A$.

  Then $e \in S_A$, and $\forall \sigma \in S_A, \quad e \circ \sigma = \sigma \circ e = \sigma$.

- inverses: ✓

  Every bijection $\sigma: A \to A$ has a well-defined inverse function $\sigma^{-1}: A \to A$, which satisfies $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e$. Therefore the inverse function is also an inverse element in S_A.

Notation:

- Elements $\sigma \in S_A$ are also called <u>permutations</u> of A.
- Special case: If $A = \{1, 2, \dots, n\}$ for some $n \in \mathbb{N}$ then S_A is called the <u>symmetric group of degree n</u>, and we write $S_n = S_A$.
- As usual, when working with elements of S_A, we often suppress the group operation (e.g. $\sigma_1 \sigma_2 = \sigma_1 \circ \sigma_2$).

Note: To understand what a product of permutations in S_A does to elements of A, we work from right to left.

(If $\sigma_1, \sigma_2 \in S_A$ and $a \in A$, then $(\sigma_1 \sigma_2)(a) = \sigma_1(\sigma_2(a))$.)

<u>Symmetric group of degree n</u>

Cauchy's notation: Denote $\sigma \in S_n$ by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

Ex: $n = 12$, $\sigma \in S_{12}$

$$\sigma: \begin{array}{llll} 1 \mapsto 3 & 4 \mapsto 11 & 7 \mapsto 4 & 10 \mapsto 10 \\ 2 \mapsto 9 & 5 \mapsto 2 & 8 \mapsto 12 & 11 \mapsto 1 \\ 3 \mapsto 7 & 6 \mapsto 6 & 9 \mapsto 5 & 12 \mapsto 8 \end{array}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 9 & 7 & 11 & 2 & 6 & 4 & 12 & 5 & 10 & 1 & 8 \end{pmatrix}$$

Basic facts:

- $|S_n| = n(n-1)(n-2)\cdots 2\cdot 1 = n!$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \underset{(n \text{ choices})}{\sigma(1)} & \underset{(n-1 \text{ choices})}{\sigma(2)} & \underset{(n-2 \text{ choices})}{\sigma(3)} & & \underset{(2 \text{ choices})}{\sigma(n-1)} & \underset{(1 \text{ choice})}{\sigma(n)} \end{pmatrix}$$

- $|S_1| = 1! = 1 \implies S_1 \cong C_1$

- $|S_2| = 2! = 2 \implies S_2 \cong C_2$

  Let $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in S_2$. Then $S_2 = \langle \sigma \rangle$.

  $$\left(\sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e \right)$$

- For $n \geq 3$, S_n is non-Abelian:

  Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & & n \end{pmatrix}$ $\left(\begin{array}{l} \sigma(1)=2,\ \sigma(2)=1, \\ \sigma(i)=i \text{ for } i \neq 1 \text{ or } 2 \end{array} \right)$

  and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & & n \end{pmatrix}$. $\left(\begin{array}{l} \tau(1)=3,\ \tau(3)=1, \\ \tau(i)=i \text{ for } i \neq 1 \text{ or } 3 \end{array} \right)$

  Then $(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 3$, but

  $(\tau\sigma)(1) = \tau(\sigma(1)) = \tau(2) = 2$,

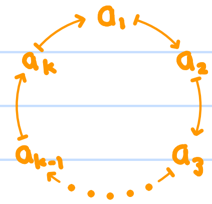
  so $\sigma\tau \neq \tau\sigma$. $\blacksquare$

Cycle notation:

Def: Suppose $k, n \in \mathbb{N}$, $1 \le k \le n$, and that $a_1, \dots, a_k \in \{1, 2, \dots, n\}$ satisfy $a_i \neq a_j$ for $i \neq j$. The <u>k-cycle</u> $(a_1\ a_2 \cdots a_k)$ is the permutation $\sigma \in S_n$ defined by

$\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\dots$, $\sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$,

and $\sigma(i) = i$ for $i \notin \{a_1, \dots, a_k\}$.



Notes:

- 1-cycles represent the identity element.
- 2-cycles are also called <u>transpositions</u>.
- For $k \ge 2$, there are k different ways of representing the same k-cycle

$$(a_1\ a_2 \dots a_k) = (a_2\ a_3 \dots a_k\ a_1) = (a_3\ a_4 \cdots a_k\ a_1\ a_2) = \cdots = (a_k\ a_1\ a_2 \cdots a_{k-1})$$

Exs: $n = 5$

Cauchy notation		Cycle notation
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$	$\longrightarrow$	$(1\ 2\ 5\ 3)$
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$	$\longrightarrow$	$(2\ 4)$
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$	$\longrightarrow$	e
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$	$\longleftarrow$	$(2\ 5\ 3)$
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$	$\longleftarrow$	$(1\ 2)(2\ 5)$

Scratch work: $\sigma = (1\ 2)$, $\tau = (2\ 5)$

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(1) = 2$$

$$(\sigma\tau)(2) = \sigma(\tau(2)) = \sigma(5) = 5$$

$$(\sigma\tau)(3) = \sigma(\tau(3)) = \sigma(3) = 3$$

$$(\sigma\tau)(4) = \sigma(\tau(4)) = \sigma(4) = 4$$

$$(\sigma\tau)(5) = \sigma(\tau(5)) = \sigma(2) = 1$$

Note: $(1\ 2)(2\ 5) = (1\ 2\ 5)$

Cauchy notation   Cycle notation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \longrightarrow (1\ 3\ 4)(2\ 5)$$

(disjoint cycles)

Def: Two cycles $(a_1 \cdots a_k)$ and $(b_1 \cdots b_\ell)$ are <u>disjoint</u> if $a_i \neq b_j$, $\forall\ 1 \le i \le k,\ 1 \le j \le \ell$.

Exs:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix} = (1\ 2)(2\ 5)$$

(non-disjoint cycles)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1\ 3\ 4)(2\ 5)$$

(disjoint cycles)

Note: If $\sigma, \tau \in S_n$ are disjoint cycles then $\sigma\tau = \tau\sigma$.

(disjoint cycles commute)

(Not true in general if σ and τ are not disjoint)

Cycle decomposition:

(i.e. every pair of cycles in the product is disjoint)

Every element $\sigma \in S_n$ can be written as a product of disjoint cycles. This product is called the cycle decomposition of σ, and it is unique up to the order in which the cycles appear.

Convention: We omit 1-cycles in the cycle decomposition, and we write the identity in S_n as e.

Algorithm to find the cycle decomposition of $\sigma \in S_n$:

Running example: $n=12$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 9 & 7 & 11 & 2 & 6 & 4 & 12 & 5 & 10 & 1 & 8 \end{pmatrix}$$

1) Let k be the smallest positive integer with $\sigma^k(1)=1$.

The first cycle in the cycle decomposition of σ is

$$(1 \ \ \sigma(1) \ \ \sigma^2(1) \ \ \cdots \ \ \sigma^{k-1}(1)).$$

First cycle: $(1\ 3\ 7\ 4\ 11)$

2) If there are any elements of $\{1, 2, \ldots, n\}$ which have not appeared yet, choose one, say i, and let ℓ be the smallest positive integer with $\sigma^\ell(i) = i$. The second cycle in the cycle decomposition of σ is

$$(i \;\; \sigma(i) \;\; \sigma^2(i) \;\; \cdots \;\; \sigma^{\ell-1}(i)).$$

Second cycle: $(2 \;\; 9 \;\; 5)$

3) Continue selecting cycles in this way until all elements of $\{1, 2, \ldots, n\}$ have been used.

Third cycle: (6)

Fourth cycle: $(8 \;\; 12)$

Fifth cycle: (10)

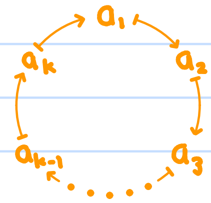
4) The cycle decomposition of σ is the product of all cycles constructed (omit 1-cycles).

$$\sigma = (1 \;\; 3 \;\; 7 \;\; 4 \;\; 11)(2 \;\; 9 \;\; 5)(8 \;\; 12)$$

Orders of elements:

- If $\sigma \in S_n$ is a k-cycle then $|\sigma| = k$.

Pf: Write $\sigma = (a_1 \cdots a_k)$.



Then $\forall\, 1 \le i \le k$, $\sigma^k(a_i) = a_i$.

It follows that $\sigma^k = e$, so $|\sigma| \le k$.

On the other hand, $\forall\, 1 \le j < k$, $\sigma^j(a_1) = a_{1+j} \neq a_1$,

so $\sigma^j \neq e$.

Therefore $|\sigma| = k$. $\blacksquare$

- If $\sigma_1, \dots, \sigma_\ell \in S_n$ are disjoint cycles then

$$|\sigma_1 \sigma_2 \cdots \sigma_\ell| = \operatorname{lcm}(|\sigma_1|, |\sigma_2|, \dots, |\sigma_\ell|).$$

Pf: ... use the fact that disjoint cycles commute ... $\blacksquare$

Ex:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 9 & 7 & 11 & 2 & 6 & 4 & 12 & 5 & 10 & 1 & 8 \end{pmatrix}$$

$$= \underbrace{(1\ 3\ 7\ 4\ 11)}_{\text{order } 5}\underbrace{(2\ 9\ 5)}_{\text{order } 3}\underbrace{(8\ 12)}_{\text{order } 2}.$$

So $|\sigma| = \operatorname{lcm}(5, 3, 2) = 30$.