The symmetric groups S_n

Given $\sigma \in S_n$ and $a \in \{1, \dots, n\}$ we can consider $a, \sigma(a), \sigma^2(a), \dots$. Since σ has finite order $\exists\, m > 0$ such that $\sigma^m(a) = a$. This gives us a cycle $(a \ \sigma(a) \ \sigma^2(a) \dots \sigma^{m-1}(a))$

In this way every $\sigma \in S_n$ can be written as a "product" of disjoint cycles: $\sigma = (a \ \sigma(a) \dots \sigma^{m_1}(a))(b \ \sigma(b) \dots \sigma^{m_2}(b)) \dots (e \ \sigma(e) \dots \sigma^{m_r}(e))$

choose b not in

This representation is unique to re ordering of cycles and shifting internally in a cycle.

Ex. $\sigma = (123)(456) \in S_6$ is the map

$$\sigma: \begin{array}{l} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \\ 4 \to 5 \\ 5 \to 6 \\ 6 \to 4 \end{array}$$

- $\sigma = (12)(53)(4)(6) \in S_6$ is the map

$$\sigma: \begin{array}{l} 1 \to 2 \\ 2 \to 1 \\ 3 \to 5 \\ 4 \to 4 \\ 5 \to 3 \\ 6 \to 6 \end{array}$$

- Try some by yourself!

Note ① We usually supress fixed points of σ i.e. $(12)(53)(4)(6)$ is usually written $(12)(53)$ and it's understood that the rest is fixed.

② Now composition of cycles is much clearer than composition of functions:

Ex • $\sigma = (1\,2\,3)$, $\tau = (1\,3)(2) \in S_3$.

$$\sigma\tau = (1\,2\,3)(1\,3)(2)$$

$$= (2\,3)(1)$$

Work right to left

$2 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3$
$3 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 2$ $\rightsquigarrow (2\,3)$

$1 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 1$ $\rightsquigarrow (1)$

$$\tau\sigma = (1\,3)(1\,2\,3)$$

$$= (1\,2)(3)$$

It even works when you ignore fixed points

Since $\sigma\tau \neq \tau\sigma \Rightarrow S_3$ is not abelian!

Cor S_n is not abelian for $n \geq 3$.

Pf $\sigma = (1\,2\,3)(4)\cdots(n) \in S_n$

$\tau = (1\,3)(2)(4)\cdots(n) \in S_n$

$\sigma\tau = (2\,3)(1)$ and $\tau\sigma = (1\,2)(3)$ are distinct ∎

(This is the power of cycle notation).

• S_1 is trivial and $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

(3) A cycle $(a_1 \cdots a_m)$ is said to have length m

(4) Given $\sigma \in S_n$, the lengths of each disjoint cycle gives a partition of n. This is called the cycle structure

So $(1\,2)(5\,3)(4)(6)$ has cycle structure $1, 1, 2, 2$.

Prop Let $\sigma \in S_n$ decompose as a disjoint product of cycles of lengths $n_1, \dots, n_m$ (so $\sum n_i = n$). Then $\operatorname{ord}(\sigma) = \operatorname{lcm}(n_1, \dots, n_m)$.

Pf ~~Homework~~/ Exercise (check that $\sigma^n = (\sigma_1 \cdots \sigma_m)^n = \sigma_1^n \cdots \sigma_m^n$).

Theorem Two permutations are conjugate in S_n $\iff$ they have the same cycle structure

Pf If $\sigma = (a_1 \cdots a_r) \cdots (a_t \cdots a_n)$ and $\tau = (b_1 \cdots b_r) \cdots (b_t \cdots b_n)$
Define $\alpha \in S_n$ by $\alpha(a_i) = b_i \ \forall i$. Notice that $\alpha^{-1} \tau \alpha = \sigma$

Defn A transposition is a cycle of length 2.

- Every cycle is a product of transpositions, $(a_1 \cdots a_r) = (a_1 a_r) \cdots (a_1 a_4)(a_1 a_3)(a_1 a_2)$.
- ↑ representation is not unique: Take $n = 4$ and
$(12)(34)(42)(23) = (124) = (14)(12)$

Thm Let $\sigma \in S_n$ be expressed as a product of transpositions in two potentially different ways. If the first has m transpositions and the second has n transpositions, then $2 \mid (m-n)$ i.e. m, n are both even or both odd.

Proof omitted.

Since $(a_1 \cdots a_m) = (a_1 a_m) \cdots (a_1 a_3)(a_1 a_2)$,

- even length cycles are always a product of an odd number of transpositions
- odd lengths cycles are always a product of an even number of transpositions.