Useful facts about S_n

1a) $S_n = \langle \{ (i\ j) : 1 \le i < j \le n \} \rangle$ (S_n is generated by transpositions)

Pf: Every element of S_n is a product of cycles (Cycle Decomposition Algorithm). Therefore it is enough to show that every cycle can be written as a product of transpositions.

- 1-cycles ✓ (identity element)
- 2-cycles ✓
- 3-cycles: ✓

$$(a_1\ a_2\ a_3) = (a_1\ a_3)(a_1\ a_2)$$

- 4-cycles: ✓

$$\begin{aligned}(a_1\ a_2\ a_3\ a_4) &= (a_1\ a_4)(a_1\ a_2\ a_3) \\ &= (a_1\ a_4)(a_1\ a_3)(a_1\ a_2)\end{aligned}$$

$\vdots$

- k-cycles: ✓ (inductive argument)

$$\begin{aligned}(a_1\ a_2 \cdots a_k) &= (a_1\ a_k)(a_1\ a_2 \cdots a_{k-1}) \\ &= (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_4)(a_1\ a_3)(a_1\ a_2). \ \blacksquare\end{aligned}$$

1b) $S_n = \langle \{ (i\ \ i+1) : 1 \le i < n \} \rangle$

Pf: Write $H = \langle \{ (i\ \ i+1) : 1 \le i < n \} \rangle$.

Then: (after playing around with products)

$$(2\ 3)(1\ 2)(2\ 3) = (1\ 3) \in H$$

$$(3\ 4)(1\ 3)(3\ 4) = (1\ 4) \in H$$

$$(4\ 5)(1\ 4)(4\ 5) = (1, 5) \in H$$

$$\vdots$$

$$(n-1\ \ n)(1\ \ n-1)(n-1\ \ n) = (1, n) \in H.$$

Similarly, $\forall\, 1 \le i < n-1$

$$(i+1\ \ i+2)(i\ \ i+1)(i+1\ \ i+2) = (i\ \ i+2) \in H$$

$$(i+2\ \ i+3)(i\ \ i+2)(i+2\ \ i+3) = (i\ \ i+3) \in H$$

$$\vdots$$

$$(n-1\ \ n)(i\ \ n-1)(n-1\ \ n) = (i\ \ n) \in H.$$

Therefore, $\forall\, 1 \le i < j \le n$, $(i\ j) \in H$, which implies

that $S_n = \langle \{ (i\ j) : 1 \le i < j \le n \} \rangle \le H$. Conclusion: $H = S_n$. ∎

(from 1a)

2) For $n \geq 2$, $S_n = \langle (1\ 2), (1\ 2 \cdots n) \rangle$.

Pf: Let $H = \langle (1\ 2), (1\ 2 \cdots n) \rangle$.

Then: $(1\ 2 \cdots n)^{-1} = (n\ n\text{-}1 \cdots 2\ 1) \in H$

$(1\ 2 \cdots n)(1\ 2)(n\ n\text{-}1 \cdots 3\ 2\ 1) = (2\ 3) \in H$

$(1\ 2 \cdots n)(2\ 3)(n\ n\text{-}1 \cdots 3\ 2\ 1) = (3\ 4) \in H$

$\vdots$

$(1\ 2 \cdots n)(n\text{-}2\ n\text{-}1)(n\ n\text{-}1 \cdots 3\ 2\ 1) = (n\text{-}1\ n) \in H$

So, $\{(i\ i{+}1) : 1 \leq i < n\} \subseteq H$

$\Rightarrow S_n = \langle \{(i\ i{+}1) : 1 \leq i < n\} \rangle \subseteq H \Rightarrow H = S_n$. $\blacksquare$

(from 1b)

Alternating groups

Def: A permutation $\sigma \in S_n$ is odd if it can be written as a product of an odd number of transpositions, and it is even if it can be written as a product of an even number of transpositions.

Exs:

$$e \quad \text{(even)}$$
$$(1\ 3) \quad \text{(odd)}$$
$$(1\ 2\ 3) = (1\ 3)(1\ 2) \quad \text{(even)}$$
$$(4\ 1\ 3)(3\ 2\ 1\ 4) = (4\ 3)(4\ 1)(3\ 4)(3\ 1)(3\ 2) \quad \text{(odd)}$$

Notes:

- By (1a) and (1b), every element $\sigma \in S_n$ is a product of transpositions. Therefore σ is even or odd.
- For $n \geq 2$, there are always multiple ways to write $\sigma \in S_n$ as a product of transpositions.

  Ex: $e = (1 2)(1 2)$, $\quad (3\ 4) = (1\ 2)(3\ 4)(1\ 2)$, ...

Question: Can an element $\sigma \in S_n$ be both even and odd?

Thm: Every element of S_n is either even or odd, but not both.

Pf: $\forall \sigma \in S_n$, let

(fixed point of σ)

$\kappa(\sigma) = \#\{\text{cycles in cycle decomp. of } \sigma\} + \#\{1 \le i \le n : \sigma(i) = i\}$.

Claim: $\forall \sigma \in S_n$ and $\forall (i\ j) \in S_n$, $\kappa((i\ j)\sigma) = \kappa(\sigma) \pm 1$.

Pf. of claim: There are 2 cases to consider.

Case 1: If i and j both appear in the same cycle in the cycle decomposition of σ, then that cycle has one of 4 forms:

$(i\ j)$, $(i\ a_1 \cdots a_k\ j)$, $(i\ j\ b_1 \cdots b_\ell)$, or $(i\ a_1 \cdots a_k\ j\ b_1 \cdots b_\ell)$.

Note:

- $(i\ j)(i\ j) = e$ (-1 cycle, +2 fixed points)
- $(i\ j)(i\ a_1 \cdots a_k\ j) = (i\ a_1 \cdots a_k)$ (+1 fixed point)
- $(i\ j)(i\ j\ b_1 \cdots b_\ell) = (j\ b_1 \cdots b_\ell)$ (+1 fixed point)
- $(i\ j)(i\ a_1 \cdots a_k\ j\ b_1 \cdots b_\ell) = (i\ a_1 \cdots a_k)(j\ b_1 \cdots b_\ell)$ (+1 cycle)
- All other cycles are disjoint.

Therefore $\kappa((ij)\sigma) = \kappa(\sigma) + 1$.

Case 2: i and j do not appear in the same cycle in the cycle decomposition of σ. Then write the cycles that they appear in as

$(i\ a_1 \cdots a_k)$ and $(j\ b_1 \cdots b_\ell)$. (again, there are 4 possibilities)

((i) if $\sigma(i)=i$) ((j) if $\sigma(j)=j$)

Then:

- $(ij)(i\ a_1 \cdots a_k)(j\ b_1 \cdots b_\ell) = (i\ a_1 \cdots a_k\ j\ b_1 \cdots b_\ell)$
- All other cycles are disjoint. (considering all 4 possibilities)

Therefore $\kappa((ij)\sigma) = \kappa(\sigma) - 1$. ∎

Now suppose that $\sigma \in S_n$ and that

$\sigma = (a_1\ b_1)(a_2\ b_2)\cdots(a_k\ b_k)$ and $\sigma = (c_1\ d_1)(c_2\ d_2)\cdots(c_\ell\ d_\ell)$.

Then $(a_1\ b_1)(a_2\ b_2)\cdots(a_k\ b_k) = (c_1\ d_1)(c_2\ d_2)\cdots(c_\ell\ d_\ell)$

$\Longrightarrow (a_2\ b_2)\cdots(a_k\ b_k) = (a_1\ b_1)(c_1\ d_1)(c_2\ d_2)\cdots(c_\ell\ d_\ell)$

$\Longrightarrow (a_3\ b_3)\cdots(a_k\ b_k) = (a_2\ b_2)(a_1\ b_1)(c_1\ d_1)(c_2\ d_2)\cdots(c_\ell\ d_\ell)$

$\vdots$

$\Longrightarrow e = (a_k\ b_k)\cdots(a_1\ b_1)(c_1\ d_1)\cdots(c_\ell\ d_\ell)$

$\Longrightarrow \kappa(e) = \kappa\big((a_k\ b_k)\cdots(a_1\ b_1)(c_1\ d_1)\cdots(c_{\ell-1}\ d_{\ell-1})(c_\ell\ d_\ell)e\big)$

$\Longrightarrow n = \underbrace{\pm 1 \pm 1 \cdots \pm 1}_{k}\ \underbrace{\pm 1 \pm 1 \pm \cdots \pm 1}_{\ell} + n \Longrightarrow 0 = \underbrace{\pm 1 \pm 1 \cdots \pm 1}_{k}\ \underbrace{\pm 1 \pm 1 \pm \cdots \pm 1}_{\ell}$

$\Rightarrow 0 = k + \ell \mod 2 \Longrightarrow k = \ell \mod 2$. ∎

($1 = -1 \mod 2$)

The subset $A_n \subseteq S_n$ consisting of all even permutations is non-empty and closed under multiplication. Therefore it is a group, called the <u>alternating group of degree n</u>.

Note: If $n \geq 2$ then $|A_n| = \frac{n!}{2}$.

Pf: Follows from the fact that the map $\sigma \mapsto (1\,2)\sigma$ is a bijection from the collection of even permutations to the collection of odd permutations. ∎

Exs:

1) $A_1 = \{e\}$ $\quad (S_1 = \{e\})$

2) $A_2 = \{e\}$ $\quad (|A_2| = \frac{2!}{2} = 1)$

3) $A_3 = \{e, (1\,2\,3), (1\,3\,2)\}$ $\quad (|A_3| = \frac{3!}{2} = 3)$

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

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

# of 3 cycles in $S_3 = \frac{3 \cdot 2 \cdot 1}{3}$

3 choices 2 choices 1 choice

$(a_1\ a_2\ a_3) = (a_2\ a_3\ a_1) = (a_3\ a_1\ a_2)$

3 ways of choosing each 3-cycle

4) $A_4 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3),$ $\left(|A_4| = \frac{4!}{2} = 12\right)$

$(2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

- # of 3 cycles in $S_4 = \frac{4 \cdot 3 \cdot 2}{3} = 8$

4 choices, 3 choices, 2 choices

$(a_1\ a_2\ a_3) = (a_2\ a_3\ a_1) = (a_3\ a_1\ a_2)$

3 ways of choosing each 3-cycle

- # of pairs of disjoint 2-cycles in S_4 $= \frac{\#\text{ of ways of choosing a 2-cycle}}{2} = \frac{\binom{4 \cdot 3}{2}}{2} = 3$

2-cycles

$\sigma_1 \sigma_2 = \sigma_2 \sigma_1$ $\quad (a_1\ a_2) = (a_2\ a_1)$

5) Suppose $n \geq 4$, $\sigma = (1\ 2\ 3)$, and $\tau = (1\ 4\ 2)$.

Then $\sigma, \tau \in A_n$, $\sigma\tau = (1\ 4\ 3)$, and $\tau\sigma = (2\ 3\ 4)$.

Therefore A_n is non-Abelian for $n \geq 4$.