Proposition

Let σ, τ be disjoint cycles in S_X. Then $\sigma\tau = \tau\sigma$.

Proof:

Let $\sigma = (a_1, \ldots, a_k)$, $\tau = (b_1, \ldots, b_\ell)$

Show $\sigma\tau(x) = \tau\sigma(x) \quad \forall x \in X$

If $x \notin \{a_1, \ldots, a_k\}$ and $x \notin \{b_1, \ldots, b_\ell\}$

$\Rightarrow \sigma(x) = x$, $\tau(x) = x$

$\tau\sigma(x) = \sigma\tau(x) = x$

Suppose $x \in \{a_1, \ldots, a_k\}$ (WLOG)

So $x = a_j$ for some j

$$\sigma(a_j) = a_{(j \bmod k)+1}$$

$x = a_j \notin \{b_1, \ldots, b_\ell\}$

$$\tau(a_j) = a_j$$

$$\therefore \sigma\tau(a_j) = \sigma(\tau(a_j)) = \sigma(a_j) = a_{(j \bmod k)+1}$$
$$= \tau(a_{(j \bmod k)+1})$$
$$= \tau(\sigma(a_j))$$
$$= \tau\sigma(a_j)$$

$$\therefore \sigma\tau = \tau\sigma \qquad \blacksquare$$

Theorem Every permutation in S_n can be written as a product of disjoint cycles.

Proof: Assume $X = \{1, \dots, n\}$. If $\sigma \in S_n$ set

$$X_1 = \{\sigma(1), \sigma^2(1), \sigma^3(1), \dots\}$$

$\uparrow$ X_i is finite since X is finite

smallest

Let i be the first integer in X where $i \notin X_1$

$$X_2 = \{\sigma(i), \sigma^2(i), \dots\}$$

Similarly define $X_3, X_4, \dots, X_r$

Since X is finite, all $i \in X$ must appera in some finite number of steps

Define cycles

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i \end{cases}$$

Note that $X_1, \dots, X_r$ are disjoint by construction

Then $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$ is a product of disjoint cycles and all elements $x \in X$ appear #.

Ex)

$$\tau = \begin{array}{c} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix} \begin{array}{l} - x \\ - \tau(x) \end{array} \end{array}$$

$$\tau = (1\,3)(\cancel{2})(4\,5\,6) = (1\,3)(4\,5\,6)$$

Def: Transpositions = Cycles of length two

$(a_1, \dots, a_n) = (a_1\, a_n)(a_1\, a_{n-1}) \cdots (a_1\, a_4)(a_1\, a_3)(a_1\, a_2)$

Ex look at a_2

Then / all the rest

First $a_2 \mapsto a_1 \mapsto a_3 \mapsto a_3$

$\therefore \quad a_2 \mapsto a_3$

Prop) Any permutation of a finite set (i.e. of S_n) for $n \geq 2$ can be written as a product of transpositions.

Note: writing as a product of transpositions is not unique.

$(16)(253) = (16)(23)(25)$
$= (16)(45)(23)(45)(25)$

No permutation can be written as a product of both an odd and an even number of transpositions.

Lemma) If the identity is written as

$id = \tau_1 \tau_2 \cdots \tau_r$

for $\tau_1, \dots, \tau_r$ transposition, then r is even.

Proof: (sketch) Idea is induction on r

id cannot be a single transposition $\therefore r \geq 2$

if $r=2$ we can write the identity, and r is even
$\therefore$ this is the base case for induction

$\therefore$ By induction we may assume that if

$id = \tau_1 \cdots \tau_{r-2}$ then $r-2$ is even.

Since adding only one transposition cannot give id we must add 2

$\therefore$ $id = \tau_1 \cdots \tau_r \Rightarrow r$ is even. ∎

Thm If σ can be written as a product of an even (resp. odd) number of transpositions then any other product of transposition equal to σ contains an even (resp. odd) number of transpositions.

Proof: (Even case)

Transpositions

Suppose $\sigma = \sigma_1 \cdots \sigma_m = \tau_1 \cdots \tau_n$ where m is even

$\sigma_j^{-1} = \sigma_j$ since $\sigma_j^2 = id$.

$$\sigma^{-1} = (\sigma_1 \cdots \sigma_m)^{-1} = \sigma_m^{-1} \cdots \sigma_1^{-1} = \sigma_m \cdots \sigma_1$$

$$id = \sigma\sigma^{-1} = \sigma\,\sigma_m \cdots \sigma_1 = \tau_1 \cdots \tau_n \sigma_m \cdots \sigma_1$$

$\therefore$ id = product of $n+m$ transposition, this must be even

but m is even $\Rightarrow$ n is even ∎

Def: A permutation is <u>even</u> if it can be written as an even number of transpositions

The Alternating Group (on n letters)

$\downarrow$

A_n = Set of all even permutations in S_n

Thm.) A_n is a subgroup of S_n

Proof:

- Closed since product of two even permutations is even
- id is even
- By argument in previous Thm. if σ is even $\Rightarrow \sigma^{-1}$ is even

$\blacksquare$.

Prop | For $n \geq 2$ the number of even permutations is equal to the number of odd permutations

$$\Rightarrow \quad |A_n| = \frac{n!}{2}.$$

Proof:

A_n - even perm.

B_n - odd perm.

Show $\exists$ a bijection between A_n and B_n.

Fix an arbitray transposition $\sigma \in S_n$

Define a map $\lambda_\sigma : A_n \longrightarrow B_n$

$$\tau \longmapsto \sigma \cdot \tau$$

1-1: Suppose $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$ for $\mu, \tau \in A_n$

$\Rightarrow \quad \sigma\tau = \sigma\mu \Rightarrow \tau = \mu \quad \therefore \lambda_\sigma$ is 1-1.

onto: Show that for $\alpha \in B_n$ arbitrary $\exists\, \tau \in A_n$ s.t

$$\lambda_\sigma(\tau) = \alpha$$

consider $\tau = \sigma^{-1}\alpha$

$$\lambda_\sigma(\tau) = \sigma\sigma^{-1}\alpha = \alpha \quad \blacksquare$$

Dihedral groups - subgroups of S_n

= reflections and rotations

n^{th} dihedral group = group of rigid motions of a regular n-gon