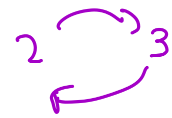
Every permutation is a product of transpositions

DEFINITION:

A *transposition* is a cycle of length 2. (23)

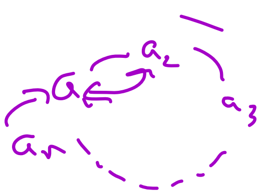


Proposition: Every permutation can be written (in many ways) as a product of transpositions. (The identity is a product of zero transpositions).

Proof: It suffices to show that a cycle is a product of transpositions. For that:

Every $\sigma \in S_n$ is a product of disjoint cycles
$\sigma = r_1 r_2 \cdots r_K$ where each r_i is a cycle.

$$(a_1 a_2 \cdots a_n) = (a_1 a_n)(a_1 a_{n-1})(a_1 a_{n-2}) \cdots (a_1 a_4)(a_1 a_3)(a_1 a_2)$$



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

$(1\,3\,2\,5) = (1\,5)(1\,2)(1\,3)$

$\checkmark = (1\,3\,2\,5)$

$(1325) = (15)\underbrace{(15)(15)}(12)(13)$

Remark: Any list can be sorted by repeatedly exchanging two elements.

13524	
13254	(34)
12354	(23)(34)
12345	(45)(23)(34)

Even and odd permutations

Theorem: Suppose the identity is written as a product of r transpositions:

$$e = \tau_1 \tau_2 \cdots \tau_r.$$

Then r is an even number.

Proof: $e = \underbrace{(15)(15)}$

By induction: $r = 1$ can't occur since $e = \tau_1$

$\tau_1 = (ab) \neq e$ so $e \neq$ any transpositions

For induction we assume that if e is a product of r,

where r is

of fewer than n transpositions $(r < n)$ then r is even.

$e = \tau_1 \cdots \underbrace{\tau_n}$

τ_{n-1} = 4 possibilities

$\tau_n = (ab)$

① $\tau_{n-1} = (cd)$ $c, d \neq a, b$. ② $\tau_{n-1} = (ac)$ ③ $\tau_{n-1} = (bc)$

④ $\tau_{n-1} = (ab)$.

Case ④. $\tau_{n-1} = (ab)$ $\tau_n = (ab)$ $(ab)(ab) = e$

$e = \tau_1 \cdots \tau_{n-2}\underbrace{(ab)(ab)} \Rightarrow \tau_1 \cdots \tau_{n-2} = e$

By induction $n-2$ is even so n is even.

Case ①. $\overset{\tau_{n-1}}{(cd)}\overset{\tau_n}{(ab)}$ since disjoint cycles commute.

$= (ab)(cd)$

a occurs in τ_{n-1}, not τ_n

Case ②. $(a\,c)(a\,b) = (a\,b\,c) = (b\,c\,a) = (b\,a)(b\,c)$

$\tau_{n-1} \quad \tau_n$ a occurs in τ_{n-1}, not τ_n

Case 3: $(b\,c)(a\,b) = (a\,c\,b) = (c\,b\,a) = (c\,a)(c\,b)$

a in τ_{n-1}, not τ_n.

$e = \tau_1 \cdots \tau_{n-1}\tau_n$

Look at $\tau_{n-2}\tau_{n-1}$

repeat – either cancel ($n-2$ even, so n even)

OR move a to the left one step.

a in τ_{n-2}, but not τ_{n-1}, τ_n.

Repeat: either there's a cancellation so by induction n is even.

OR a appears in τ_1 but not $\tau_2, \ldots, \tau_n$.

if that happens our e moves a!

$$e = \underset{(a\,x)}{\tau_1} \cdots\cdots \underset{\text{no } a\text{'s}}{\tau_n}$$

That can't happen! e doesn't move anything!

Conclude that cancellation happens somewhere,

$e =$ ~~n-2~~ product of $n-2$ transpositions,

$n-2$ even by induction

$\Rightarrow$ n even.

Theorem: Let $\sigma \in S_n$ be a permutation. Then either every expression of σ as a product of transpositions has an even number of transpositions, or every such expression has an odd number of transpositions. In the first case σ is called an *even* permutation, in the second it is called *odd*.

(ab) odd (1 transposition)

$(abc) = (ac)(ab)$ (2 trans so even)

Proof:

$\sigma \in S_n$

$\sigma = \tau_1 \cdots\cdots \tau_m$ $\quad$ τ_i are transpositions

$\sigma = \alpha_1 \cdots\cdots \alpha_k$ $\quad$ α_i are transpositions

$\sigma^{-1}\sigma = (\alpha_1 \cdots \alpha_k)^{-1}(\tau_1 \cdots \tau_m).$

$(\alpha_1 \cdots \alpha_k)^{-1} = \alpha_k^{-1} \cdots \cdots \alpha_1^{-1} = \alpha_k \cdots\cdots \alpha_1$

$\alpha = (xy)$ $\quad$ $\alpha^2 = (xy)(xy) = e$

$\sigma^{-1}\sigma = e = \alpha_k \alpha_{k-1} \cdots \alpha_1 \tau_1 \cdots\cdots \tau_m$

$k+m$ is even.

k, m both odd or both even.

$(1\,3\,2) = (12)(13)$ even

$(1\,2\,3\,4) = (14)(13)(12)$ odd

<u>Lemma</u>: A cycle is even $\Leftrightarrow$ it's length is odd.

$$\underbrace{\overbrace{(1\,2\,3)}}_{\text{even}}\underbrace{\overbrace{(5\,6)}}_{\text{odd}}\underbrace{\overbrace{(7\,8\,9\,10)}}_{\text{odd}} \Leftrightarrow \text{even}$$

<u>Prop</u>: Product of even permutations is even

even · odd → odd

odd · odd → even.

The Alternating Group

Definition: The subset of S_n consisting of even permutations is a subgroup called the alternating group A_n. It has $n!/2$ elements.

Proof: $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$.

A_n is a subgroup.

Let $\sigma, \tau \in A_n$.

Check $\sigma\tau^{-1} \in A_n$.

$\sigma = \alpha_1 \cdots \alpha_m$ m even.

$\tau = \beta_1 \cdots \beta_r$ r even

$$\sigma\tau^{-1} = \alpha_1 \cdots \alpha_m (\beta_1 \cdots \beta_r)^{-1}$$

$$= \underbrace{\alpha_1 \cdots \alpha_m}_{m} \underbrace{\beta_r \cdots \beta_1}_{r}$$

$m+r$ even

so $\sigma\tau^{-1}$ is even

$\sigma\tau^{-1} \in A_n$.

$|A_n| = n!/2$.

Pick a transposition.

(12) $\sigma \in A_n$

$\sigma(12)$ is odd

$B = \{\sigma \in S_n \mid \sigma \text{ is odd}\}$

$A_n \cup B = S_n$ $A_n \cap B = \emptyset$

$\lambda : A_n \to B$

$\lambda(\sigma) = \sigma(12)$

$\lambda^{-1}(\tau) = \tau(12)$

$\lambda^{-1}\lambda(\sigma) = \sigma(12)(12) = \sigma$

$\lambda\lambda^{-1}(\tau) = \tau(12)(12) = \tau$

Since λ is bijective (it has an inverse),

$|A_n| = |B|$.

$|A_n| + |B| = n!$

$|A_n| = n!/2$ elements.

The group A_4

12 $\quad 4! = 24 \quad 4!/2 = 12$.

e

(123) (132) $(12)(34)$

(124) (142) $(13)(24)$

(134) (143) $(14)(23)$

(234) (243)

e identity

8 3 cycles

3 products of 2 transpositions.