Symmetric Groups

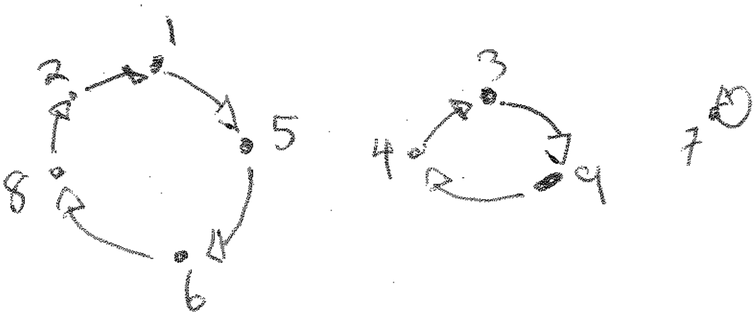
Let $n \in \mathbb{N}$.

$$\mathrm{Sym}(n) = \{ \sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\} \mid \sigma \text{ is a bijection} \}$$

Elements of $\mathrm{Sym}(n)$ are called permutations.

Motivation for new way to represent elements of $\mathrm{Sym}(n)$:

$n = \cancel{8}\,9$ $\quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 9 & 3 & 6 & 8 & 7 & 2 & 4 \end{pmatrix}$



Think of σ as 3 cycles of lengths 5, 3 and 1

Def: Let $a_1, \ldots, a_k$ be k distinct elements of $\{1, \ldots, n\}$. We define

$$(a_1 a_2 \ldots a_k) \in \mathrm{Sym}(n)$$

as the permutation that maps a_1 to a_2, a_2 to a_3, $\ldots$ a_{k-1} to a_k, and a_k to a_1. Every element in $\{1, \ldots, n\} \setminus \{a_1, \ldots, a_k\}$ is mapped to itself. A element as above is called a k-cycle and k is called its length.

Note that every 1-cycle (a) is equal to the identity.

2-cycles are called transpositions. Two cycles $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_\ell)$ are called disjoint if $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_\ell\} = \phi$.

<u>Example:</u> $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 9 & 3 & 6 & 8 & 7 & 2 & 4 \end{pmatrix}$

$$\sigma = (15682)(394)(7) = (15682)(394)$$

<u>Note:</u> $(15682) = (56821) = (68215) = (82156) = (21568)$

$(394) = (943) = (439)$

<u>Note:</u> Also have the relation

$\sigma = (394)(15682) = (15682)(394)$

The different cycles of σ don't talk to each other.

$$\mathrm{Sym}(3) = \{ id, (12), (13), (23), (123), (132) \}$$

$$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right.$$

$$\mathrm{Sym}(3) = \{ id, (12), (13), (23), (123), (132) \}$$

$$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Symmetric Groups cont.

Thm: Let $n \in \mathbb{N}$. Every element $\sigma \in Sym(n)$ can be written as a product $\gamma_1 \cdots \gamma_r$ of pairwise disjoint cycles $\gamma_1, \dots, \gamma_r$ of lengths ≥ 2.

Proof: See proof of Thm 6.6 in notes.

proof idea: Let $\sigma \in Sym(n)$. If $\sigma = id$, then $\sigma = (1)(2)\cdots(n)$ and we are done. If $\sigma \neq id$, then $\exists\ a \in \{1, 2, \dots, n\}$ s.t. $\sigma(a) \neq a$. Let $a_1 = a$, $a_2 = \sigma(a)$, $a_3 = \sigma(a_2)$, etc. Eventually we get ~~[illegible]~~ a repetition, $\sigma(a_j) =$ ~~[illegible]~~ a_i for some $i < j$ because the set ~~[illegible]~~ $\{1, 2, \dots, n\}$ is finite. If $i \neq 1$, then $\sigma(a_j) = \sigma(a_i)$ and $\sigma(a_{i-1}) = \sigma(a_j)$ contradicting that σ is 1-1. Therefore $\sigma(a_j) = a_1$.

The first cycle to write for σ is

$$(a_1\, a_2 \cdots a_j)$$

If $\{a_1, \dots, a_j\} = \{1, 2, \dots, n\}$ we are done. If $\forall b \in \{1, 2, \dots, n\} - \{a_1, \dots, a_j\}$ $\sigma(b) = b$, then ~~[illegible]~~ we are done. Say $\exists b \notin \{a_1, \dots, a_j\}$ s.t. $\sigma(b) \neq b$. Then repeat the process just described to get a cycle

$$(b_1\, b_2 \cdots b_\ell)$$

It must be the case that $\{a_1, \dots, a_j\} \cap \{b_1, \dots, b_\ell\} = \emptyset$, for if $a_i = b_k \in \{a_1, \dots, a_j\} \cap \{b_1, \dots, b_\ell\}$, then $\sigma(a_{i-1}) = a_i = b_k = \sigma(b_{k-1})$ contradicting that σ is injective.

Therefore the cycles $(a_1 \cdots a_j)$ and $(b_1 \cdots b_\ell)$ are disjoint.
Repeating the process, we write σ as a product of disjoint cycles:

$$\sigma = (a_1 \cdots a_j)(b_1 \cdots b_\ell) \cdots (f_1 \cdots f_k) \quad \square$$

<u>Prop</u>: Let $n \in \mathbb{N}$ and let γ and δ be two disjoint cycles in $Sym(n)$. Then γ and δ commute.

<u>proof</u>: ~~Let~~ Let $\gamma = (a_1 a_2 \cdots a_k)$, $\delta = (b_1, \dots, b_\ell)$ and let $c \in \{1, \dots, n\}$.
we need to show that

$$\gamma\delta(c) = \delta\gamma(c)$$

If $c \notin \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_\ell\}$, then $\gamma(c) = c$ and $\delta(c) = c$, so

$$\gamma\delta(c) = \gamma(c) = c \quad \text{and} \quad \delta\gamma(c) = \delta(c) = c$$

~~Let~~ Say $c \in \{a_1, \dots, a_k\}$, $c = a_i$. Then $\gamma(a_i) = a_{i+1}$ (or a_1 if $i = k$)
and $\delta(a_i) = a_i$ and $\delta(a_{i+1}) = a_{i+1}$

so
$$\gamma\delta(a_i) = \gamma(a_i) = a_{i+1}$$
$$\delta\gamma(a_i) = \delta(a_{i+1}) = a_{i+1}$$

Similarly if $c \in \{b_1, \dots, b_\ell\}$. $\square$

Def: Let $\sigma \in Sym(n)$. Writing σ as a product of disjoint cycles is called a cycle decomposition of σ

Note: Let $\sigma = (a_1 \cdots a_\ell)(b_1 \cdots b_k) \cdots (f_1 \cdots f_m)$ be a cycle decomposition of σ. The cycle decomposition is unique up to two different factors/conditions

(1) Ordering of the cycles, since disjoint cycles commute;

i.e.

$$(a_1 \cdots a_\ell)(b_1 \cdots b_k) \cdots (f_1 \cdots f_m) = (f_1 \cdots f_m)(b_1 \cdots b_k) \cdots (a_1 \cdots a_\ell)$$

(2) An individual cycle stays the same under a cyclic permutation of the numbers: i.e.

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

Example

$G = Sym(5)$, $\sigma = (123)(45) = (45)(123) = (54)(123) = (54)(231) = (54)(312)$

σ: $1 \mapsto 2$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$
$2 \mapsto 3$
$3 \mapsto 1$
$4 \mapsto 5$
$5 \mapsto 4$

Practice composing: $\sigma = (123)(45)$, $\tau = (14325)$

$\sigma\tau = (1524)(3) = (1524)$

start with 2: (2415)

Prop: Every element of Sym(n) can be written as a product of transpositions.

proof: Let $\sigma \in \text{Sym}(n)$. By previous Thm, σ may be written as a product of cycles of length ≥ 2. Therefore if we show that an arbitrary cycle of length $k \geq 2$ can be written as the product of transpositions, then we are done. Let

$$\sigma = (a_1\, a_2 \cdots a_k)$$

be a cycle of length k. Then we have that

$$(a_1\, a_2 \cdots a_{k-1}\, a_k) = (a_1\, a_k)(a_1\, a_{k-1})(a_1\, a_{k-2}) \cdots (a_1\, a_3)(a_1\, a_2) \quad \square$$

~~Prop: Let σ∈Sym(n) and decompose σ into~~

Prop: Let $\sigma \in \text{Sym}(n)$, and assume that σ may be written as the product of disjoint cycles of length $n_1, \ldots, n_m$. Then

$$o(\sigma) = \text{lcm}(n_1, \ldots, n_m)$$

That is, the order of σ is the least common multiple of $n_1, n_2, \ldots, n_m$.

proof: First observe that a cycle $\gamma = (a_1\, a_2 \cdots a_d)$ of length d has order d:

$$\gamma^d : a_1 \xrightarrow{\gamma} a_2 \xrightarrow{\gamma} a_3 \to \cdots \to a_d \to a_1$$

$$a_2 \to a_3 \to a_4 \to \cdots \to a_1 \to a_2$$

$$\vdots$$

$$a_d \to a_1 \to a_2 \to \cdots \to a_{d-1} \to a_d$$

The a_i are all distinct (since γ is injective), so $\gamma^i(a_j) \neq a_j$ if $i < d$.

Therefore the order of γ is d.

Recall: If $x \in G$, then $x^e = 1$ iff $o(x) \mid e$.

Now let

$$\sigma = (a_1 \cdots a_{n_1})(b_1 \cdots b_{n_2}) \cdots (f_1 \cdots f_{n_m})$$

be a cycle decomposition of σ. Since disjoint cycles commute,

$$\sigma^d = (a_1 \cdots a_{n_1})^d (b_1 \cdots b_{n_2})^d \cdots (f_1 \cdots f_{n_m})^d$$

Since the cycles are disjoint

$$\sigma^d = id \quad \text{iff} \quad \begin{array}{l} (a_1 \cdots a_{n_1})^d = id \\ (b_1 \cdots b_{n_2})^d = id \\ \vdots \\ (f_1 \cdots f_{n_m})^d = id. \end{array}$$

$$\text{iff} \quad \begin{array}{l} n_1 \text{ divides } d \\ n_2 \text{ divides } d. \\ \vdots \\ n_m \text{ divides } d \end{array}$$

The smallest positive integer d such that $n_1 | d$, $n_2 | d$, $\ldots$, $n_m | d$ is the least common multiple of $n_1, n_2, \ldots, n_m$.

Hence $o(\sigma) = lcm(n_1, \ldots, n_m)$. $\square$

Def: Let $\sigma \in Sym(n)$. We say that σ is even if there are an even number of even length cycles in a cycle decomposition of σ. We say σ is odd if there are an odd number of even length cycles in a cycle decomposition of σ. We say that σ has sign 1 if σ is even and sign -1 if σ is odd, denoted by $sgn(\sigma)$.

Thm: Let $\sigma \in \mathrm{Sym}(n)$ be expressed as the product of transpositions in two potentially different ways. If the first has m transpositions and the second has n transpositions, then $2 \mid (m-n)$.

proof: First we see what happens to the sign of an arbitrary element $\tau \in \mathrm{Sym}(n)$ if we multiply τ by a transposition. Let $(i\,j)$ be a transposition. There are two cases: Either i and j both show up in the same cycle in a cycle decomposition of τ or i and j show up in different cycles.

1. Say i and j show up in the same cycle. We can then write the cycle as

$$(i\, a_2\, a_3 \cdots a_{k-1}\, j\, a_{k+1} \cdots a_\ell)$$

Then

$$(i\,j)(i\,a_2\,a_3\cdots a_{k-1}\,j\,a_{k+1}\cdots a_\ell) = \overbrace{(i\,a_2\,a_3\cdots a_{k-1})(j\,a_{k+1}\,a_{k+2}\cdots a_\ell)}^{\text{Note: these are disjoint cycles}}$$

If ℓ is even then we get two odd length cycles or two even length cycles. Therefore $\mathrm{sgn}((i\,j)\tau) = -\mathrm{sgn}(\tau)$.

2. Say i and j show up in different cycles. We can then write the cycles as

$$(i\,a_1\,a_2 \cdots a_{k-1})(j\,b_2 \cdots b_{\ell-1}\,b_\ell)$$

Then

$$\cancel{(ij)(a_1 a_2 \cdots a_{k-1}\, i)(j b_2 \cdots b_{\ell-1} b_\ell) = (a_1 \cdots a_{k-1}\, i\, j b_2 \cdots b_{\ell-1} b_\ell)}$$

$$(ij)(i a_2 a_3 \cdots a_k)(j b_2 \cdots b_{\ell-1} b_\ell) = \underbrace{(i a_2 \cdots a_k j b_2 \cdots b_{\ell-1} b_\ell)}_{k+\ell\text{ - cycle}}$$

k - even (odd), ℓ - odd (even), then $k+\ell$ is odd.
k, ℓ both even or both odd, then $k+\ell$ is even.

In any case $sgn((ij)\tau) = -sgn(\tau)$, because the number of even cycles either goes up 1 or down 1.

~~We deduce the for any~~

Now note that the sign of a transposition is -1. We therefore deduce that if τ may be written as a product of r transpositions, then

$$sgn(\tau) = (-1)^r$$

Let $\sigma \in Sym(n)$ be written as the product of m and n transpositions. Then

$$sgn(\sigma) = (-1)^n \quad \text{and} \quad sgn(\sigma) = (-1)^m.$$

Therefore $(-1)^n = (-1)^m$ so 2 divides $m-n$. $\square$

<u>Cor</u>: The map $sgn: Sym(n) \longrightarrow \{1,-1\}$, $\sigma \longmapsto sgn(\sigma)$ is a gp homomorphism from $(Sym(n), \circ)$ to $(\{1,-1\}, \cdot)$.

Proof: Let $\tau, \sigma \in Sym(n)$ and say that σ may be written as the product of r transpositions and τ the product of s transpositions. Then $\tau\sigma$ may be written as the product of $r+s$ transpositions. Therefore

$$\begin{aligned} sgn(\sigma\tau) &= (-1)^{r+s} \\ &= (-1)^r (-1)^s \\ &= sgn(\sigma) sgn(\tau). \end{aligned}$$

Hence sgn is a gp homomorphism. $\square$

Def: We define the alternating group, denoted ~~A~~ Alt(n) or Alt_n, to be the kernel of the sgn homomorphism. That is the alternating gp, $Alt(n) \subseteq Sym(n)$, is the set of even permutations.

Prop: $|Alt(n)| = \frac{n!}{2}$.

Proof: We have that $\sigma Alt(n) = \tau Alt(n)$ iff $\sigma^{-1}\tau \in Alt(n)$ iff $sgn(\sigma^{-1}\tau) = 1$. Now $sgn(\sigma^{-1}\tau) = sgn(\sigma^{-1}) sgn(\tau)$ and $sgn(\sigma^{-1}) = sgn(\sigma)^{-1}$. Furthermore $(-1)^{-1} = -1$ and $1^{-1} = 1$, so $sgn(\sigma)^{-1} = sgn(\sigma)$. Therefore $sgn(\sigma^{-1}\tau) = 1$ iff $sgn(\sigma) sgn(\tau) = 1$ iff $sgn(\sigma) = sgn(\tau)$.

We've shown that $\sigma \mathrm{Alt}(n) = \tau \mathrm{Alt}(n)$ iff $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau)$. $\mathrm{sgn}(\sigma)$ is either 1 or -1. Therefore there are 2 cosets of $\mathrm{Alt}(n)$ in $\mathrm{Sym}(n)$. Hence $|\mathrm{Alt}(n)| = \frac{|\mathrm{Sym}(n)|}{2} = \frac{n!}{2}$. $\square$

/9