Notation: Throughout, let $\mathbb{N}_n := \{1, ..., n\}$.

Definition 0.1. *Let $n \in \mathbb{N}$. A* ***permutation*** *of $\mathbb{N}_n$ is a bijection $\mathbb{N}_n \to \mathbb{N}_n$. We write S_n for the set of permutations of $\mathbb{N}_n$. The set S_n together the function*

$$S_n \times S_n \to S_n$$

that maps (α, β) to the composition of functions $\alpha \circ \beta$ is a group. We call this group the ***symmetric group*** *on n elements.*

Why is S_n a group?

(i) If $\alpha, \beta \in \mathrm{S}_n$ then $\alpha \circ \beta$ is bijective and thus $\alpha \circ \beta \in \mathrm{S}_n$.
(ii) The identity map $\epsilon : \mathbb{N}_n \to \mathbb{N}_n$, defined by $\epsilon(i) := i$ for all $i \in \mathbb{N}_n$, is the identity element for S_n.
(iii) Bijective maps have inverses. If $\alpha \in \mathrm{S}_n$ then there exists $\beta \in S_n$ such that $\alpha \circ \beta = \epsilon$.
(iv) Multiplication is associative since function composition is always associative.

Notation: From now on, for $\alpha, \beta \in \mathrm{S}_n$ we will write $\alpha\beta$ to mean $\alpha \circ \beta$. For a permutation σ of $\mathbb{N}_n$, we write:

$$\begin{pmatrix} 1 & 2 & \dots & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \dots & \sigma(n) \end{pmatrix}.$$

Example: The permutation $\sigma \in \mathrm{S}_5$ with $\sigma(1) = 3, \sigma(2) = 5, \sigma(3) = 4, \sigma(4) = 1, \sigma(5) = 2$ is written

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Definition 0.2. *If $\sigma \in S_n$ has the property that there exist $a_1, ..., a_m \in \mathbb{N}_n$ such that*

$$\begin{aligned} &\sigma(a_i) = a_{i+1}, \quad &&\text{for } 1 \leq i \leq m-1; \\ &\sigma(a_m) = a_1, && \\ &\text{and } \sigma(x) = x, &&\text{for } x \notin \{a_1, ..., a_m\}. \end{aligned}$$

*we say σ is an m-**cycle** and write σ in **cycle notation** as $(a_1 a_2 .... a_m)$. A **transposition** is a 2-cycle.*

Example: The permutation

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

is a 3-cycle. We write σ in cycle notation as (142).

Definition 0.3. *We say $\alpha, \beta \in S_n$ are **disjoint** if,*

$$\{x \mid \alpha(x) \neq x\} \cap \{x \mid \beta(x) \neq x\} = \emptyset.$$

Example: Let

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

and

$$\gamma := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

The permutations σ and τ are disjoint but σ and γ are not disjoint.

Lemma 0.4. *Let $\alpha_1, ..., \alpha_m \in S_n$ be pairwise disjoint permutations and let $\tau \in S_n$. The permutations $\alpha_1\alpha_2...\alpha_m$ and τ are disjoint if and only if α_i and τ are disjoint for all $0 < i \leq m$.*

Proof. See exercise sheet. □

Proposition 0.5. *Every $\sigma \in S_n$ can be written as a product of disjoint cycles.*

Proof. Fix $n \in \mathbb{N}$. We shall prove the statement by induction on

$$\Gamma(\sigma) := |\{a \in \mathbb{N}_n \mid \sigma(a) \neq a\}|.$$

If $\Gamma(\sigma) = 0$ then σ is the identity map on $\mathbb{N}_n$ so $\sigma = (1)(2)...(n)$.

Let $\sigma \in \mathrm{S}_n$. Suppose $k = \Gamma(\sigma) > 0$ and suppose the assertion is true for all permutations τ with $\Gamma(\tau) < k$.
Let $i_0 \in \mathbb{N}_n$ be such that $\sigma(i_0) \neq i_0$. Let $i_s := \sigma^s(i_0)$. Since $\mathbb{N}_n$ is finite, there exists $p, q \in \mathbb{N}$ with $p < q$ such that $\sigma^p(i_0) = \sigma^q(i_0)$. Since σ is bijective, $\sigma^{p-q}(i_0) = i_0$. Take $r \in \mathbb{N}$ least such that $\sigma^{r+1}(i_0) = i_0$. Let τ be the $r+1$-cycle, $(i_0 i_1 ... i_r)$.
Now

$$\{a \in \mathbb{N}_n \mid (\tau^{-1}\sigma)(a) = a\} = \{a \in \mathbb{N}_n \mid \sigma(a) = a\} \cup \{i_0, ..., i_r\}.$$

So $\Gamma(\tau^{-1}\sigma) < k = \Gamma(\sigma)$.
So, by the induction hypothesis, $\tau^{-1}\sigma$ can be written as a product of pairwise disjoint cycles, say $\tau^{-1}\sigma = \alpha_1\alpha_2...\alpha_m$. So $\sigma = \tau\alpha_1\alpha_2...\alpha_m$.
Since $\alpha_1\alpha_2...\alpha_m(i_j) = \tau^{-1}\sigma(i_j) = i_j$ for $0 \leq j \leq m$, the permutations $\alpha_1\alpha_2...\alpha_m$ and τ are disjoint. By the lemma, this means τ and α_i are disjoint for $0 < i \leq m$. So σ is a product of disjoint cycles.

□

Example: The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

written as a product of disjoint cycles is

$$(134)(25).$$

Notation:

Proposition 0.6. *Every permutation on $\mathbb{N}_n$ can be written as a product of transpositions.*

Proof. The identity is (12)(21).
Since every permutation can be written as a product of cycles, it is enough to show that every cycle can be written as a product of transpositions. Let $(i_1...i_r) \in \mathrm{S}_n$ be an r-cycle. Then

$$(i_1 i_2 ... i_r) = (i_1 i_r)(i_1 i_{r-1})...(i_1 i_3)(i_1 i_2).$$

For i_1,

$$(i_1 i_r)(i_1 i_{r-1})...(i_1 i_3)(i_1 i_2) i_1 = (i_1 i_r)(i_1 i_{r-1})...(i_1 i_3) i_2 = i_2.$$

For $s > 1$,

$$\begin{aligned}(i_1 i_r)(i_1 i_{r-1})...(i_1 i_3)(i_1 i_2) i_s &= (i_1 i_r)(i_1 i_{r-1})...(i_1 i_{s+1})(i_1 i_s) i_s \\ &= (i_1 i_r)(i_1 i_{r-1})...(i_1 i_{s+2})(i_1 i_{s+1}) i_1 \\ &= (i_1 i_r)(i_1 i_{r-1})...(i_1 i_{s+2}) i_{s+1} \\ &= i_{s+1}\end{aligned}$$

□

Example: The permutation $(123) \in \mathrm{S}_4$ can be written as both

$$(13)(12)$$

and

$$(13)(42)(12)(14).$$

So factorisation into transpositions is not unique, even more, the number of transpositions used in a factorisation is not unique. So, what is unique?
In order to answer this question we first need to define the action of a permutation $\sigma \in \mathrm{S}_n$ on a function from $\mathbb{Z}^n$ to $\mathbb{Z}$. (Reminder $\mathbb{Z}^n := \underbrace{\mathbb{Z} \times ... \times \mathbb{Z}}_{n-times}$).
Let $\sigma \in \mathrm{S}_n$ and $f : \mathbb{Z}^n \to \mathbb{Z}$ be a function. We define σf to be the function from $\mathbb{Z}^n \to \mathbb{Z}$ defined by

$$(\sigma f)(x_1, ..., x_n) := f(x_{\sigma(1)}, ..., x_{\sigma(n)}).$$

Example: Let $f : \mathbb{Z}^3 \to \mathbb{Z}$ be the function defined by $f(x_1, x_2, x_3) := x_1 x_2 + x_3$ and $\sigma := (123) \in \mathrm{S}_3$. The function

$$(\sigma f)(x_1, x_2, x_3) = f(x_2, x_3, x_1) = x_2 x_3 + x_1.$$

Lemma 0.7. *Let $\sigma, \tau \in S_n$ and $f, g : \mathbb{Z}^n \to \mathbb{Z}$. Then*
(i) $\sigma(\tau f) = (\sigma\tau)f$
(ii) $\sigma(fg) = (\sigma f)(\sigma g)$

Proof. See exercise sheet. $\square$

Theorem 0.8. *There is a map $sign : S_n \to \{1, -1\}$ such that:*
(a) For every transposition $\tau \in S_n$, $sign(\tau) = -1$.
(b) For permutations σ, σ'

$$sign(\sigma\sigma') = sign(\sigma)sign(\sigma').$$

This function is unique with these properties. For $\sigma \in S_n$, we call $sign(\sigma)$ the ***signature*** *of σ.*

Proof. Fix $n \in \mathbb{N}$. Let $\Delta : \mathbb{Z}^n \to \mathbb{Z}$ be the function defined by

$$\Delta(x_1, ..., x_n) := \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Claim: For a transposition $\tau \in \mathrm{S}_n$, $\tau\Delta = -\Delta$.
Let $\tau = (rs)$ with $r < s$.
By lemma 0.7(i)

$$\tau\Delta(x_1, ..., x_n) = \prod_{1 \leq i < j \leq n} \tau(x_j - x_i).$$

Clearly, if $i, j \notin \{r, s\}$ then $\tau(x_j - x_i) = (x_j - x_i)$.
For the factor $(x_s - x_r)$, we have that $\tau(x_s - x_r) = -(x_r - x_s)$.
The remaining factors can be put into pairs as follows:

$$\begin{array}{ll} (x_k - x_s)(x_k - x_r), & \text{if } k > s; \\ (x_s - x_k)(x_k - x_r), & \text{if } r < k < s; \\ (x_s - x_k)(x_r - x_k), & \text{if } k < r. \end{array}$$

Each pair is unaffected by τ.
Therefore $\tau\Delta = -\Delta$. So we have proved the claim.

Now suppose $\sigma \in S_n$. We can write $\sigma = \tau_1 ... \tau_m$ where $\tau_1, ..., \tau_m$ are transpositions. By lemma 0.7(ii),

$$\sigma\Delta = \tau_1(\tau_2(...(\tau_m\Delta)...))$$

and by the claim

$$\tau_1(\tau_2(...(\tau_m\Delta)...)) = (-1)^m\Delta.$$

So $\sigma\Delta = \Delta$ or $\sigma\Delta = -\Delta$.

For $\sigma \in \mathrm{S}_n$, let $\mathrm{sign}(\sigma) = +1$ if $\sigma\Delta = \Delta$ and let $\mathrm{sign}(\sigma) = -1$ if $\sigma\Delta = -\Delta$. This map is well-defined since $\Delta(1, 2, ..., n) \neq 0$.

Let $\sigma, \tau \in \mathrm{S}_n$. By lemma 0.7(i),

$$(\sigma\tau)\Delta = \sigma(\tau\Delta).$$

So

$$\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau).$$

The function $\mathrm{sign} : \mathrm{S}_n \to \{1, -1\}$ is unique with properties (a) and (b) since every permutation is a product of transpositions.

$\square$

Remark: Let $\sigma \in \mathrm{S}_n$ and let $\tau_1, ..., \tau_m \in \mathrm{S}_n$ be transpositions such that $\sigma = \tau_1 ... \tau_m$. Then

$$\mathrm{sign}(\sigma) = (-1)^m.$$

Definition 0.9. *We call a permutation even if it can be written as a product of an even number of transpositions.*
We call a permutation odd if it can be written as a product of an odd number of transpositions.

Corollary 0.10. *A permutation σ is even if and only if sign(σ) $= 1$ and is odd if and only if sign(σ) $= -1$. Thus, a permutation can not be written as both a product of an even number transpositions and an odd number of transpositions.*