# §4 - Symmetric Groups

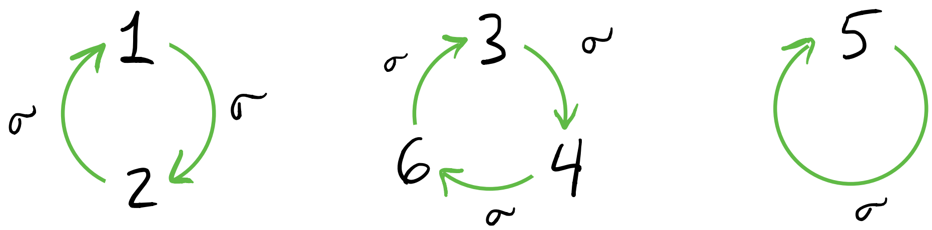
Now that we have a stronger understanding of groups in general, it's time to revisit and more closely analyze the group $S_n$.

## §4.1 Cycle Decomposition.

Recall that every element of $S_n$ can be expressed as an array:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix} \in S_6$$

If we apply $\sigma$ again and again, we may notice something interesting . . .




Thus, $\sigma$ consists of three disjoint cycles

Each cycle can be written compactly as

$$(1\ 2) \qquad (3\ 4\ 6) \qquad (5)$$

Thus, we may write

$$\boxed{\sigma = (1\ 2)(3\ 4\ 6)(5)}$$

to describe the permutation more compactly.

This is called cycle notation.

Ex:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$$

Ex: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} = (1\ 4\ 2\ 5)(3)$

Remarks

(1) We can write a cycle in many ways

e.g. $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 2\ 1)$

Convention: Begin with the smallest number in the cycle.

(2) In cycle notation, we often do not write the terms fixed by $\sigma$:

i.e. We write $\sigma = (1\ 2)(3\ 4\ 6)$

instead of $\sigma = (1\ 2)(3\ 4\ 6)(5)$

and understand that $\sigma$ fixes $5$.

**Definition:** A permutation $\sigma \in S_n$ of the form $\sigma = (a_1\ a_2\ \cdots\ a_m)$ is called a cycle of length $m$, or an $m$-cycle.

A 2-cycle is called a transposition.

Two cycles $(a_1\ a_2\ \cdots\ a_m)$ & $(b_1\ b_2\ \cdots\ b_k)$ are said to be disjoint if $\forall i,j$, $a_i \neq b_j$.

**Ex:** Using cycle notation, we can easily list all $3! = 6$ elements of $S_3$.

| identity | transpositions | 3-cycles |
|---|---|---|
| $e$ | $(1\ 2)$ | $(1\ 2\ 3)$ |
| | $(1\ 3)$ | $(1\ 3\ 2)$ |
| | $(2\ 3)$ | |

Just like with arrays, we can compose symmetries in cycle notation by reading right to left.

**Ex:** In $S_5$, if $\sigma = (1\ 2\ 4)(3\ 5)$

$\tau = (1\ 5)(2\ 3)$ then

$$\sigma\tau = \underline{(1\ 2\ 4)(3\ 5)}\,\underline{(1\ 5)(2\ 3)}$$

We can simplify this product by tracing the path of each number through the cycles from right to left.

$$1: \quad (1\ 2\ 4)(3\ 5)(1\ 5)(2\ 3)$$
$$3 \longleftarrow 3 \longleftarrow 5 \longleftarrow 1 \longleftarrow 1$$

$$3: \quad (1\ 2\ 4)(3\ 5)(1\ 5)(2\ 3)$$
$$4 \longleftarrow 2 \longleftarrow 2 \longleftarrow 2 \longleftarrow 3$$

4: $(1\ 2\ 4)(3\ 5)(1\ 5)(2\ 3)$

$1 \leftarrow 4 \leftarrow 4 \leftarrow 4 \leftarrow 4$

2: $(1\ 2\ 4)(3\ 5)(1\ 5)(2\ 3)$

$5 \leftarrow 5 \leftarrow 3 \leftarrow 3 \leftarrow 2$

5: $(1\ 2\ 4)(3\ 5)(1\ 5)(2\ 3)$

$2 \leftarrow 1 \leftarrow 1 \leftarrow 5 \leftarrow 5$

Thus, $\boxed{\sigma\tau = (1\ 3\ 4)(2\ 5).}$

**Note:** This simplified product consists of <u>disjoint cycles</u>!

**Theorem 4.1** Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles.

**Proof:** Start with any $a_1 \in \{1, 2, \ldots, n\}$.

Set $a_2 = \sigma(a_1)$, $a_3 = \sigma(a_2) = \sigma^2(a_1)$, etc...

until we reach $m$ such that $\sigma^m(a_1) = a_1$.

[<u>Exercise</u>: why must such an $m$ exist??]

$$\sigma = (a_1\ a_2\ \cdots\ a_m)\cdots$$

If we have not exhausted $\{1, 2, \dots, n\}$, choose

$b_1 \in \{1, 2, \dots, n\}$ with $b_1 \neq a_i$, $i = 1, \dots, m$.

Set $b_2 = \sigma(b_1)$, $b_3 = \sigma(b_2) = \sigma^2(b_1)$, etc...

until we reach $K$ such that $\sigma^K(b_1) = b_1$

[<u>Exercise</u>: Show that no $b_i$ appears in $(a_1\ a_2 \cdots a_m)$]

Thus, $$\sigma = \underbrace{(a_1\ a_2\ \cdots\ a_m)(b_1\ b_2\ \cdots\ b_K)}_{\text{disjoint}}\cdots$$

Eventually this process must stop. ∎

Using the disjoint cycle decomposition for $\sigma \in S_n$, one can quickly identify many key properties of $\sigma$.

For instance, if $\beta_1, \beta_2, \ldots, \beta_K$ are disjoint cycles in $S_n$, what is the order of $\sigma = \beta_1 \beta_2 \cdots \beta_K$?

Let's do an example with $K = 1$:

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

$\sigma^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$

$\sigma^3 = (1\ 3\ 2)(1\ 2\ 3) = (1)(2)(3) = e$

$\Rightarrow |\sigma| = 3$

In general:

**Proposition 4.2:** If $\sigma \in S_n$ is an $m$-cycle, then $|\sigma| = m$ (i.e., the order of a cycle is its length.)

**Proof:** Exercise. $\blacksquare$

To extend Proposition 4.2 to products of arbitrary length, we require the following lemma.

**Lemma 4.3:** Disjoint cycles commute.

**Proof:** Let
$$\alpha = (a_1\ a_2\ \cdots\ a_m)$$
$$\beta = (b_1\ b_2\ \cdots\ b_k)$$
be disjoint cycles in $S_n$. We show

that $(\alpha\beta)(x) = (\beta\alpha)(x) \quad \forall x \in \{1, 2, ..., n\}$

- If $x = a_i$ for some $i$, then

$$(\alpha\beta)(x) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$$

$$(\beta\alpha)(x) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$$

- If $x = b_i$ for some $i$, then

$$(\alpha\beta)(x) = \alpha(\beta(b_i)) = \alpha(b_{i+1}) = b_{i+1}$$

$$(\beta\alpha)(x) = \beta(\alpha(b_i)) = \beta(b_{i+1}) = b_{i+1}$$

- Finally, if $x \neq a_i$, $x \neq b_i$ $\forall i$, then

$$(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$$

$$(\beta\alpha)(x) = \beta(\alpha(x)) = \beta(x) = x$$

In all cases, $(\alpha\beta)(x) = (\beta\alpha)(x)$, so

$\alpha\beta = \beta\alpha$. $\blacksquare$

**Theorem 4.4:** If $\beta_1, \beta_2, \ldots, \beta_k$ are disjoint cycles in $S_n$ and $\sigma = \beta_1\beta_2\cdots\beta_k$, then

$$|\sigma| = \operatorname{lcm}(|\beta_1|, |\beta_2|, \ldots, |\beta_k|)$$

**Proof:** We'll prove for $k=2$ (general case is similar)

Suppose $\sigma = \beta_1\beta_2$. Set $m = |\sigma|$ and

$l = \operatorname{lcm}(|\beta_1|, |\beta_2|)$. We have that

$$e = \sigma^m = (\beta_1\beta_2)^m = \beta_1^m\beta_2^m$$

But $\beta_1$ and $\beta_2$ have distinct entries, so

$$\beta_1^m\beta_2^m = e \Rightarrow \beta_1^m = e \text{ and } \beta_2^m = e$$

$\Rightarrow |\beta_1|$ divides $m$ & $|\beta_2|$ divides $m$.

$\Rightarrow \ell$ divides $m$

But of course $\sigma^\ell = \beta_1^\ell \beta_2^\ell = e$, so $m \mid \ell$.

Consequently, $m = \ell$. i.e., $|\sigma| = lcm(|\beta_1|, |\beta_2|)$ ■

Ex: If $\sigma = (1\,4\,7)(2\,8)(5\,6\,9) \in S_9$,

then $|(1\,4\,7)| = |(5\,6\,9)| = 3$

and $|(2\,8)| = 2$.

Thus, $|\sigma| = lcm(3,3,2) = \underline{6}$.

Ex: What are the orders of the elements of $S_7$? Well ... it comes down to the possible cycle decompositions

| Cycle Decomposition | Order |
|---|---|
| (7) | 7 |
| (6)(1) | 6 |
| (5)(2) | 10 |
| (5)(1)(1) | 5 |
| (4)(3) | 12 |
| (4)(2)(1) | 4 |
| (4)(1)(1)(1) | 4 |
| (3)(3)(1) | 3 |
| (3)(2)(1) | 6 |
| (3)(1)(1)(1) | 3 |
| (2)(2)(2)(1) | 2 |
| (2)(2)(1)(1)(1) | 2 |
| (2)(1)(1)(1)(1)(1) | 2 |
| (1)(1)(1)(1)(1)(1)(1) | 1 |

How many permutations in $S_7$ have order 3? They are of the form

$(a\ b\ c)$ or $(a\ b\ c)(d\ e\ f)$

$(a\ b\ c)$

5 choices
6 choices
7 choices

$\left.\begin{matrix}5 \text{ choices}\\ 6 \text{ choices}\\ 7 \text{ choices}\end{matrix}\right\}$ Total $= 7\cdot 6\cdot 5 = 210$

But we've overcounted, as $(a\ b\ c) = (b\ c\ a) = (c\ a\ b)$

Thus, we must divide by 3. Total: $210/3 = 70$.

$(a\ b\ c)(d\ e\ f)$

$\left.\begin{matrix}2 \text{ choices}\\ 3 \text{ choices}\\ 4 \text{ choices}\\ 5 \text{ choices}\\ 6 \text{ choices}\\ 7 \text{ choices}\end{matrix}\right\}$ Total $= 7!$
$= 5040$

Again, we must divide by 3 for each 3 cycle.

Also, since $(a\ b\ c)(d\ e\ f) = (d\ e\ f)(a\ b\ c)$,

we must divide by 2. Total: $5040/(3\cdot 3\cdot 2) = 280$

Thus, there are $70 + 280 = \boxed{350}$ elements in $S_7$ of order 3.

## §4.2 - Even / Odd Permutations

Here's an interesting decomposition:

$$(1\ 2\ 3\ 4\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5)$$

$$(1\ 2\ 3\ 4)(5\ 6\ 7) = (1\ 2)(2\ 3)(3\ 4)(5\ 6)(6\ 7)$$

These permutations can be written as products of (non-disjoint) transpositions.

**Theorem 4.5**: Every permutation is a product of transpositions.

**Proof:** We will show that every cycle $(a_1\, a_2 \cdots a_m)$ is a product of transpositions. Since every permutation is a product of cycles, this will be sufficient.

Note that

$$(a_1\, a_2 \cdots a_m) = (a_1\, a_2)(a_2\, a_3) \cdots (a_{m-1}\, a_m) \quad \blacksquare$$

**Note:** The way in which a permutation decomposes into a product of transpositions is not unique, nor is the number of transpositions:

$$\begin{aligned}(1\,2\,3\,4\,5) &= (1\,2)(2\,3)(3\,4)(4\,5) \\ &= (4\,5)(2\,5)(1\,2)(2\,5)(2\,3)(1\,3)\end{aligned}$$

What is the same is the ~~parity~~ of the number of transpositions (even/odd)

Theorem 4.6: Let $\sigma \in S_n$. If

$$\sigma = \beta_1 \beta_2 \cdots \beta_K \quad \text{and} \quad \sigma = \gamma_1 \gamma_2 \cdots \gamma_m$$

where $\beta_i$ & $\gamma_i$ are transpositions, then either $K$ and $m$ are both even, or $K$ and $m$ are both odd.

To prove this result, we require the following Lemma:

Lemma 4.7: If $e = \beta_1 \beta_2 \cdots \beta_m$ where each $\beta_i$ is a transposition, then $m$ is even.

**Proof:** $m = 1$? No. $m = 2$? Done!

So assume $m > 2$ and proceed by induction.

Write $e = \beta_1 \beta_2 \cdots \beta_{m-1} \beta_m$ with $\beta_m = (a\ b)$

Look at $\beta_{m-1} \beta_m$.

Possibilities:

$$\beta_{m-1}\beta_m = \begin{cases} (a\,b)(a\ b) = e \\ (a\ c)(a\ b) = (a\ b)(b\ c) \\ (b\ c)(a\ b) = (a\ c)(b\ c) \\ (c\ d)(a\ b) = (a\ b)(c\ d) \end{cases}$$

Notice that either

(i) $\beta_{m-1} = (a\ b)$, in which case $\beta_{m-1}\beta_m$ can be removed and $e = \beta_1 \cdots\cdots \beta_{m-2}$. By induction $m-2$ (and hence $m$) is even

(ii) $\beta_{m-1} \neq (a\ b)$, in which case the last occurrence of $a$ "moves" to the left.

We can therefore repeat this process, eventually either deleting two transpositions (in which case $m$ is even) <u>or</u> we move $a$ all the way to the left with no other $a$ appearing to its right. But if the latter occurs, then $a$ is not fixed by $e$, a contradiction. Thus, $m$ is even. $\blacksquare$

<u>Proof of Theorem 4.6</u>:

If $\sigma = \beta_1 \beta_2 \cdots \beta_m = \gamma_1 \gamma_2 \cdots \gamma_k$, then $e = \beta_m^{-1} \beta_{m-1}^{-1} \cdots \beta_1^{-1} \gamma_1 \gamma_2 \cdots \gamma_k$. Since the inverse of a transposition is again a transposition, $e$ is a product of $m+k$ transpositions. Thus, by Lemma 4.7, $m+k$ is even. The result follows. ■

With the proof of Theorem 4.7 complete, we can now make the following definition responsibly:

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

Ex: $(1\,2\,3\,4\,5) = (1\,2)(2\,3)(3\,4)(4\,5)$

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

Exercise: An $m$-cycle is even if and only if $m$ is odd.

Exercise: If $\alpha, \beta$ are cycles, then $\alpha\beta$ is even if and only if $\alpha$ & $\beta$ are both even or both odd.

On Assignment 3, you will prove that the set

$$\boxed{A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}}$$

is a subgroup of $S_n$ of order $n!/2$.

We call $A_n$ the alternating group

With the machinery from this chapter, we are able to say a lot more about $S_n$. This is exciting, as many of our other examples of groups show up as subgroups of $S_n$.