Orbits, Cycles, and the Alternating Groups

Def. Let σ be a permutation of a set A. The equivalence classes in A determined by $a \sim b$ if and only if $b = \sigma^n(a)$, for some $n \in \mathbb{Z}$, are called the **orbits** of σ.

Ex. Find the orbits of the permutation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 6 & 1 & 2 & 8 & 4 & 3 \end{pmatrix}.$$

Let's start with 1 and follow where it goes under powers of σ:

$\sigma(1) = 7, \ \ \sigma^2(1) = \sigma(7) = 4, \ \ \ \sigma^3(1) = \sigma(4) = 1.$

1 goes to 7, which goes to 4, which goes back to 1. We denote this by $(1, 7, 4)$.

Now go to 2 and see where σ sends it:

$\sigma(2) = 5, \ \ \ \sigma^2(2) = \sigma(5) = 2.$

So 2 goes to 5, which goes back to 2. We denote this by $(2,5)$.

Now go to 3:

$\sigma(3) = 6, \qquad \sigma^2(3) = \sigma(6) = 8, \quad \sigma^3(3) = \sigma(8) = 3.$

So 3 goes to 6, which goes to 8, which goes back to 3. We denote this by $(3, 6, 8)$.

Notice that we already know what σ does to 4 (and $5 - 8$). For example,

σ sends 4 into 1, into 7, into 4. That's already captured in $(1, 7, 4)$.

So σ has 3 orbits:

$$(1, 7, 4), \ \ (2, 5), \ \ (3, 6, 8).$$

Def. A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The length of a cycle is the number of elements in its largest orbit.

Ex. The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$ is a cycle because its orbits are $(1,4,2,5)$ and (3).

Let's go back to the first example of the permutation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 6 & 1 & 2 & 8 & 4 & 3 \end{pmatrix}$$

with orbits: $(1,7,4)$, $(2,5)$, $(3,6,8)$.

We can associate to each orbit a permutation that is a cycle:

$$(1,7,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 3 & 1 & 5 & 6 & 4 & 8 \end{pmatrix}$$

$$(2,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 3 & 4 & 2 & 6 & 7 & 8 \end{pmatrix}$$

$$(3,6,8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 6 & 4 & 5 & 8 & 7 & 3 \end{pmatrix}$$

and:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 6 & 1 & 2 & 8 & 4 & 3 \end{pmatrix} = (1,7,4)(2,5)(3,6,8).$$

That is, we can write any $\sigma \in S_A$ as a product of disjoint cycles (i.e. any integer is moved by only one cycle).

Since the cycles are disjoint, it also doesn't matter which order we multiply them in. For example,

$$(1,7,4)(2,5)(3,6,8) = (2,5)(3,6,8)(1,7,4).$$

However, even though multiplication of disjoint cycles is commutative, multiplication of general permutations is not.

Ex. Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 3 & 2 \end{pmatrix}$ as a product of disjoint cycles.

Notice $1 \to 5 \to 3 \to 1$ so $(1,5,3)$ is one cycle.

$2 \to 6 \to 2$ so $(2,6)$ is another cycle.

Thus $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 3 & 2 \end{pmatrix} = (1,5,3)(2,6)$.

Note: we also could have written $(2,6)(1,5,3)$.

Also, since $(1,5,3) = (5,3,1)$ we could have written $(5,3,1)(2,6)$.

Ex. Find $(1,3,6,5)(2,1,4,6)$ in S_6 and write it as a product of disjoint cycles.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 6 & 5 & 2 \end{pmatrix}$$

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

$1 \to 4 \to 5 \to 1 \qquad (1,4,5)$

$2 \to 3 \to 6 \to 2 \qquad (2,3,6)$

So, $(1,3,6,5)(2,1,4,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix} = (1,4,5)(2,3,6)$.

Notice that $(1,3,6,5)(2,1,4,6) \neq (2,1,4,6)(1,3,6,5)$ since:

$$(2,1,4,6)(1,3,6,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 6 & 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix}.$$

Now write this as a product of disjoint cycles:

$1 \to 3 \to 2 \to 1$ $\quad\quad (1,3,2)$

$4 \to 6 \to 5 \to 4$ $\quad\quad (4,6,5)$

So $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix} = (2,1,4,6)(1,3,6,5) = (1,3,2)(4,6,5)$

Def. A cycle of length 2 is a **transposition**.

Thus, a transposition leaves all elements but two fixed and switches the two unfixed elements. It can be shown through a calculation that any cycle can be written as a product of transpositions. That is:

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

Ex. Write the cycle $(1,3,4,6)$ in S_6 as a product of transpositions.

$$(a_1, a_2, a_3, a_4) = (a_1, a_4)(a_1, a_3)(a_1, a_2)$$

So, $(1,3,4,6) = (1,6)(1,4)(1,3)$. Let's show that this works:

$$(1,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}$$

$$(1,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 1 & 5 & 6 \end{pmatrix}$$

$$(1,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$(1,4)(1,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 1 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}$$

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

$$(1,6)(1,4)(1,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 5 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 5 & 1 \end{pmatrix} = (1,3,4,6).$$

Notice that the identity permutation is the square of any transposition. In particular, $i = (1,2)(2,1)$.

The decomposition of a permutation into a product of transpositions may not be disjoint and is not unique (we could always insert $(1,2)(2,1)$ into any decomposition). However, any decomposition of a permutation into transpositions either always has an even number of transpositions or always has an odd number. For example, if a permutation can be written as a product of an even number of transpositions then any other representation of that permutation as a product of transpositions will also have an even number.

Def. A permutation of a finite set is called **even** or **odd** according to whether it can be expressed as a product of an even number of transpositions or the product of an odd number of transpositions.

Ex. The identity permutation in S_n is even since $i = (1,2)(2,1)$.

If $n = 1$, we define i to be even.

Ex. Write $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 3 & 2 \end{pmatrix}$ as a product of transpositions.

We saw in an earlier example that:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 3 & 2 \end{pmatrix} = (1,5,3)(2,6).$$

$(1,5,3)$ can be factored into transpositions as:

$$(1,5,3) = (1,3)(1,5).$$

$$(a_1, a_2, a_3) = (a_1, a_3)(a_1, a_2)$$

so $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 3 & 2 \end{pmatrix} = (1,3)(1,5)(2,6).$

This permutation is odd because it can be factored into three transpositions.

Let A_n be the set of even permutations and B_n be the set of odd permutations in S_n. A_n and B_n have the same number of elements $(\frac{n!}{2})$ because:

$$f: A_n \rightarrow B_n \text{ by } f(\sigma) = (1,2)\sigma \text{ is 1-1 and onto.}$$

Notice that the product of two even permutations is even (because they each factor into an even number of transpositions so the product does as well).

So A_n is closed under multiplication.

The identity permutation is also even and so is in A_n (assuming $n \geq 2$).

And if $\sigma \in A_n$, then σ^{-1}, which reverses the permutation σ, is also even.

Thus, A_n is a subgroup of S_n of order $\frac{n!}{2}$ if $n \geq 2$.

Def. The subgroup of S_n containing all of the even permutations, denoted A_n, is called the **alternating group**.