Section II.9. Orbits, Cycles, and the Alternating Groups

Note. In this section, we explore permutations more deeply and introduce an important subgroup of S_n.

Lemma. Let σ be a permutation of set A. For $a, b \in A$, define $a \sim b$ if and only if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. Then $\sim$ is an equivalence relation on A.

Definition 9.1. Let σ be a permutation of a set A. The equivalence classes described in Lemma are the *orbits* of σ.

Exercise 9.2. Let

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

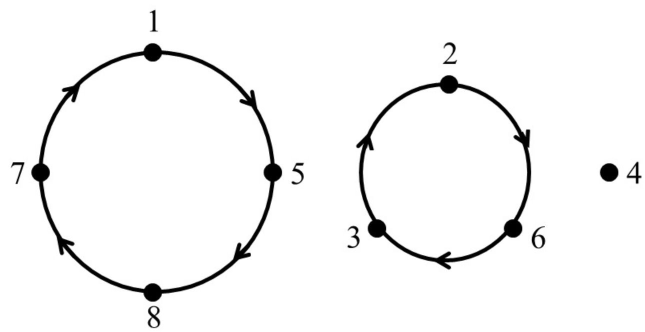
Find the orbits of σ.

Solution. We consider the powers of σ as applied to various elements of set A:

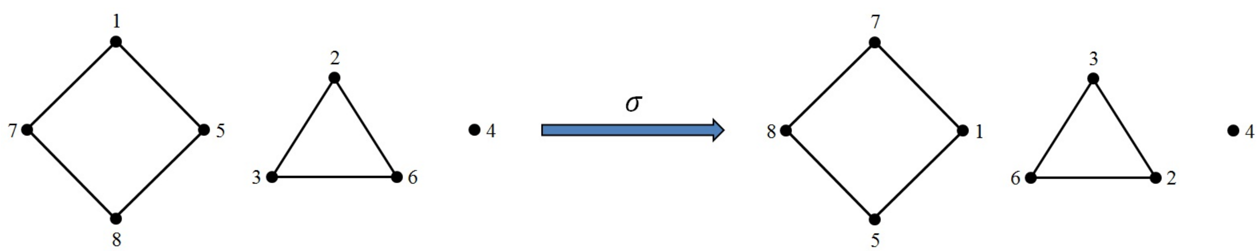
$$1 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 1, 2 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 2, \text{ and } 4 \xrightarrow{\sigma} 4.$$

So the orbits are $\{1, 5, 8, 7\}$, $\{2, 6, 3\}$, and $\{4\}$.

Note. In the previous example, we see that σ can be thought of as a permutation which cycles around the elements of A as follows:



We can connect the elements of A and think of the permutation as a combination of rotations that we encountered in the previous section:



Definition 9.6. A permutation $\sigma \in S_n$ is a *cycle* if it has at most one orbit containing more than one element. The *length* of the cycle is the number of elements in its largest orbit.

Example. $\sigma \in S_8$ given above is *not* a cycle since it contains two orbits which contain more than one point.

Note. So a *cycle in* S_n is either (1) a permutation which fixes all n points—this is a cycle of length 1, or (2) a permutation which fixes $k < n$ points and a single orbit of length $n - k$—this is a cycle of length $n - k$. It seems rather strange to think of these "cycles" which literally cycle around $n - k$ points as also including all the fixed points. This is necessary because such cycles are described as elements of S_n and so they are permutations of $\{1, 2, 3, \ldots, n\}$—hence it is necessary that they act on all n elements of this set. It is very common to express a cycle in terms of the non-fixed elements. Then, for example, if

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

then we represent this permutation ($\sigma \in S_5$) in *cyclic notation* by reflecting how the elements in the orbit of length greater than one are mapped around: $(1, 3, 5)$. That is, $\sigma(1) = 3$, $\sigma(3) = 5$, and $\sigma(5) = 1$.

Definition. Let $\sigma \in S_n$ be a cycle of length m where $1 < m \leq n$. Then the *cyclic notation* for σ is

$$(a, \sigma(a), \sigma^2(a), \ldots \sigma^{m-1}(a))$$

where a is any element in the orbit of length m which results when $\{1, 2, \ldots, n\}$ is partitioned into orbits by σ.

Notice. For a cycle of length m, there are m ways to represent it in cyclic notation:

$$(a, \sigma(a), \sigma^2(a), \ldots \sigma^{m-1}(a)),$$

$$(\sigma(a), \sigma^2(a), \ldots \sigma^{m-1}(a), a),$$

$$\vdots$$

$$(\sigma^{m-1}(a), a, \sigma(a), \ldots \sigma^{m-2}(a)).$$

Example. The cyclic notation for the permutation of Exercise 9.2 is

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

So we, have written this permutation from S_8 in terms of these *disjoint* cycles. At least, Fraleigh now calls these disjoint cycles, but technically (using Fraleigh's own definition) the cycles, which are elements of S_8 and hence have to act on all of the set $\{1,2,\ldots,8\}$, must each have 8 elements in their decomposition. So we should have the cycles:

$$\begin{aligned} \sigma_1 &= (1,5,8,7)(2)(3)(4)(6) \\ \sigma_2 &= (2,6,3)(1)(4)(5)(7)(8) \\ \sigma_3 &= (1)(2)(3)(4)(5)(6)(7)(8), \end{aligned}$$

and these cycles certainly are not disjoint! BUT, their *cyclic notation* is disjoint, and whenever we say "disjoint cycles," we technically mean cycles whose cyclic notations are disjoint! This could be streamlined by changing Fraleigh's definitions of "cycle" and "length" in a way which omits the fixed points when the length is greater than 1.

Theorem 9.8. Every permutation σ of a finite set is a product of disjoint cycles.

Note. Theorem 9.8 is the inspiration for some of my research in discrete math. If we have a finite set of n elements and construct a combinatorial structure called a *design* on the set, then the design is called *cyclic* if it admits as a permutation (as an automorphism, to be precise) a cycle of length n. If the design admits a permutation consisting of two disjoint cycles, one of length k and the other of length $n-k$, the design is called *bicyclic*. Similarly, we can define *tricyclic* designs, and so forth.

Note. Just as we can take products of permutations, we can take products of cycles. If the cycles are disjoint, this is not very interesting! But if the cycles are not disjoint, then we can produce a cycle product in terms of disjoint cycles.

Exercise 9.7. Calculate in S_8 the product $(1,4,5)(7,8)(2,5,7)$. Remember to read from right to left!

Exercise 9.10. Write as a disjoint product of cycles:

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

Definition 9.11. A cycle of length 2 is a *transposition*.

Note. Any cycle is a product of a sequence of transpositions:

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

This fact, combined with Theorem 9.8 implies the following.

Corollary 9.12. Any permutation of a finite set of at least two elements is a product of transpositions.

Note. Of course, there is no claim of uniqueness in terms of the representation of a permutation as a product of transpositions. For example, in S_6 (in terms of the cyclic notation)

$$(1, 4, 5, 6) = (1, 6)(1, 5)(1, 4) = (1, 6)(1, 2)(2, 1)(1, 5)(1, 4)$$

since $(1, 2)(2, 1) = (1)(2)$ (the identity). However, there is a type of uniqueness in the product of transpositions, as given next.

Theorem 9.15. No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Note. Fraleigh presents two proofs of this result. A cleaner (but more complicated) proof can be found in Hungerford's *Algebra* (Theorem I.6.7, page 48).

Definition 9.18. A permutation of a finite set is *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.

Note. We'll now show that the set of all even permutations of a given finite set form a group—these are alternating groups.

Lemma. For $n \geq 2$, the number of even permutations in S_n is $n!/2$.

Theorem 9.20. If $n \geq 2$, then the collection of all even permutations of $\{1, 2, 3, \ldots, n\}$ forms a subgroup of order $n!/2$ of the symmetry group S_n.

Definition 9.21. The subgroup of S_n consisting of the even permutations of n letters is the *alternating group* A_n *on* n *letters.*

Note. The fact that there is not an algebraic solution to 5th degree and higher polynomial equations is due to the structure of A_n. This is the result due to Abel, mentioned above (known as the "unsolvability of the quintic").

Note. At this stage, we have "met" the following finite groups:

Name	**Symbol**	**Order**
Cyclic Group	$\mathbb{Z}_n$	n
Dihedral Group	D_n	$2n$
Symmetry Group	S_n	$n!$
Alternating Group	A_n	$n!/2$

Revised: 7/6/2023