Abstract algebra

Lecture note 5. Orbits, cycles, and alternating groups

Lecturer : O-joung Kwon

Spring, 2019

Orbits Each permutation σ of a set A determines a natural partition of A into cells with the property that $a, b \in A$ are in the same cell if and only if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. This gives a natural equivalence relation:

- For $a, b \in A$, let $a \sim b$ if and only if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$.

One can easily check reflexive, symmetric, transtivie.

Definition 1. *Let σ be a permutation of a set A. The equivalence classes in A determined by the equivalence relation above are the* orbits *of σ.*

Find the orbits of the permutation $\sigma =$

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

Orbits are : $\{1, 3, 6\}$, $\{2, 8\}$, $\{4, 5, 7\}$.

Cycles Suppose $A = \{1, 2, \dots, n\}$, and we consider elements of the symmetric group S_n. Let

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

Definition 2. *A permutation $\sigma \in S_n$ is a cycle if it has at most one orbit containing more than one element. Then length of a cycle is the number of elements in its largest orbit.*

Each cycle can be represented by a permutation. For instance, $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}$

We introduce a single-row cyclic notation. We write it as $\mu = (1, 3, 6)$.

Using cyclic notation, we see that σ can be written as a product of cycles:

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

These cycles are *disjoint*, meaning that any integer is moved by at most one of these cycles.

Theorem 1. *Every permutation σ of a finite set is a product of disjoint cycles.*

Clearly, disjoint cycles are commutative. Howevery, generally, cycles are not commutative. For example $(1, 4, 5, 6)(2, 1, 5) \neq (2, 1, 5)(1, 4, 5, 6)$.

Even and odd permutations

Definition 3. *A cycle of length 2 is a transposition.*

A computation shows that

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

Therefore, any cycle is a product of tranpositions.

Corollary 1. *Any permutation of a finite set of at least two elements is a product of transpositions.*

This representation of products of transpositions is not unique; (we can put $(1, 2)(1, 2)$ arbitrarily for example) What is true is that the number of transpositions used must either always even or odd.

Definition 4. *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, respectively.*

Theorem 2. *No permutation in S_n can be expressed as a product of an even number of transpositions and as a product of an odd number of transpositions.*

PROOF

Alternating groups
We claim that for $n \geq 2$, the number of even permutations in S_n is the same as the number of odd permutations in S_n. For this, let A_n be the set of even permutations, and B_n be the set of odd permutations.

Theorem 3. $|A_n| = |B_n|$

PROOF

Definition 5. *The subgroup of S_n consisting of the even permutations of n letters is the alternating group A_n on n letters.*