Section 9 – Orbits, Cycles, and the Alternating Groups

Instructor: Yifan Yang

Fall 2006
Outline

Orbits and cycles

Even and odd permutations

The alternating groups
**Lemma**
Let $\sigma$ be a permutation of a set $A$. Then the relation $\sim$ on $A$ defined by

$$a \sim b \iff b = \sigma^n(a)$$

for some integer $n$ is an equivalence relation.

**Definition**
The equivalence classes determined by the above equivalence relation are the orbits of $\sigma$. 
Orbits

Proof.
We check

1. Reflexive: \( a \sim a \) for all \( a \in A \) since \( a = \sigma^0(a) \).

2. Symmetric: If \( a \sim b \), i.e., if \( b = \sigma^n(a) \), then \( a = \sigma^{-n}(b) \) and thus \( b \sim a \).

3. Transitive: If \( a \sim b \) and \( b \sim c \), then \( b = \sigma^n(a) \) and \( c = \sigma^m(b) \) for some \( m, n \in \mathbb{Z} \). It follows that \( c = \sigma^m(b) = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a) \). Thus \( a \sim c \).
Example

Let

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

To find the orbit containing 1, we apply $\sigma$ repeatedly, obtaining

$$1 \rightarrow 3 \rightarrow 6 \rightarrow 1 \rightarrow 3 \rightarrow 6 \rightarrow \cdots.$$  

Thus, the orbit containing 1 is $\{1, 3, 6\}$. Likewise, we have

$$2 \rightarrow 8 \rightarrow 2 \rightarrow 8 \rightarrow 2 \rightarrow 8 \rightarrow \cdots,$$

$$4 \rightarrow 7 \rightarrow 5 \rightarrow 4 \rightarrow 7 \rightarrow 5 \rightarrow \cdots.$$  

We conclude that there are three orbits $\{1, 3, 6\}, \{2, 8\}, \{4, 5, 7\}$. 
In-class exercises

Find the orbits of the following permutations.

1. \[(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) \quad (3 \ 7 \ 1 \ 2 \ 8 \ 5 \ 9 \ 6 \ 4).\]

2. \[(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) \quad (8 \ 2 \ 7 \ 1 \ 5 \ 4 \ 3 \ 6 \ 9).\]

3. \[(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) \quad (2 \ 8 \ 7 \ 4 \ 9 \ 1 \ 3 \ 6 \ 5).\]
Observe that a permutation $\sigma$ can be decomposed into a product of several permutations, each of which acts non-trivially on at most one of the orbits. For example, we have

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

where the orbits are $\{1, 2, 3\}$ and $\{4, 5\}$, and we decompose it into a product of two permutations, one acting on $\{1, 2, 3\}$ and the other on $\{4, 5\}$. This motivates the following definition.
Cycles

Definition
A permutation \( \sigma \in S_n \) is a \textit{cycle} if it has at most one orbit containing more than one element. (That is, \( \sigma \) acts non-trivially on at most one orbit.) The \textbf{length} of a cycle is the number of elements in the largest cycle.

Notation
Since cycles have at most one orbit containing more than one element, we can represent cycles using only information of the largest orbit. Suppose that in the largest orbit of a cycle \( \sigma \) we have \( x_1 \to x_2 \to x_3 \to \cdots \to x_n \to x_1 \). Then we write

\[ \sigma = (x_1, x_2, \ldots, x_n). \]
Examples

1. \((1\ 2\ 3\ 4\ 5)\) is not a cycle since the orbits are \(\{1, 2, 3\}\) and \(\{4, 5\}\). Both of them have more than one element.

2. \((1\ 2\ 3\ 4\ 5)\) and \((1\ 2\ 3\ 5\ 4)\) are both cycles. The orbits of the former are \(\{1, 2, 3\}\), \(\{4\}\), and \(\{5\}\), and those of the latter are \(\{1\}\), \(\{2\}\), \(\{3\}\), and \(\{4, 5\}\). The lengths are 3 and 2, respectively. Moreover, in the cyclic notations, they are \((1, 2, 3)\) and \((4, 5)\).
Theorem (9.8)

Every permutation \( \sigma \) of a finite set is a product of disjoint cycles.

Proof.

Let \( B_1, \ldots, B_r \) be the orbits of \( \sigma \). Define cycles \( \tau_i \) by

\[
\tau_i(x) = \begin{cases} 
\sigma(x), & \text{if } x \in B_i, \\
x, & \text{if } x \notin B_i.
\end{cases}
\]

Then \( \sigma = \tau_1 \tau_2 \ldots \tau_r \). Clearly, these \( \tau_i \) are disjoint.
In \( \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \), we have

\[
1 \to 3 \to 2 \to 5 \to 1 \to 3 \cdots \\
4 \to 4 \to 4 \to 4 \to 4 \to 4 \cdots 
\]

Thus, we write \( \sigma = (1, 3, 2, 5) \), or

\( \sigma = (3, 2, 5, 1) = (2, 5, 1, 3) = (5, 1, 3, 2) \). (It is fine, though not necessary to write \( \sigma = (1, 3, 2, 5)(4) \).)
Example

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

We have $1 \to 3 \to 6 \to 1 \to 3 \to 6 \to \cdots$, $2 \to 8 \to 2 \to 8 \to 2 \to 8 \to \cdots$, $4 \to 7 \to 5 \to 4 \to 7 \to 5 \to \cdots$.

Thus, $\sigma = (1, 3, 6)(2, 8)(4, 7, 5)$. Also, $\sigma = (2, 8)(4, 7, 5)(1, 3, 6) = (4, 7, 5)(8, 2)(3, 6, 1) = \cdots$. But $\sigma \neq (1, 6, 3)(2, 8)(4, 7, 5)$. 
Remarks

1. The multiplication of disjoint cycles are commutative. For example, we have

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

2. Up to the order of the cycles, the representation of a permutation as a product of cycles is unique.

3. A product of several cycles can still be a cycle. For example, we have \((1, 2)(1, 3) = (1, 3, 2)\).
In-class exercise

Express the following permutations as products of disjoint cycles.

1. \[(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) \ (3 \ 7 \ 1 \ 2 \ 8 \ 5 \ 9 \ 6 \ 4)\].

2. \[(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) \ (8 \ 2 \ 7 \ 1 \ 5 \ 4 \ 3 \ 6 \ 9)\].

3. \[(1, 3, 2, 5)(4, 2, 8, 7)(3, 9, 1, 2)(6, 9)\].
Transposition

Definition
A cycle of length 2 is a transposition.

Theorem (9.12)
Any permutation of a finite set of at least two elements is a product of transposition.

Proof.
If \( \sigma \) is the identity element, we have \( \sigma = (1, 2)(1, 2) \). Otherwise, write \( \sigma \) as a product of cycles. Now for each cycle \((a_1, a_2, \ldots, a_n)\) we have

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

This proves the theorem.
Examples

1. We have \((1, 2, 3) = (1, 3)(1, 2)\).

2. We have \((2, 5, 1, 3) = (2, 3)(2, 1)(2, 5)\). Also, 
   \((2, 5, 1, 3) = (5, 1, 3, 2) = (5, 2)(5, 3)(5, 1)\), and 
   \((2, 5, 1, 3) = (1, 3, 2, 5) = (1, 5)(1, 2)(1, 3)\). Thus, there are 
   more than one way to write a cycle as a product of 
   transpositions.

3. We have \((1, 2, 3, 4) = (1, 4)(1, 3)(1, 2)\). Also 
   \((1, 2, 3, 4) = (1, 2)(3, 4)(1, 2)(1, 3)(1, 4)(3, 4)(1, 2)\).
Even and odd permutations

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.

Proof

It suffices to prove that if \( \tau = (i, j), \ i \neq j, \) is a transposition, and \( \sigma \in S_n, \) then the number of orbits of \( \sigma \) and that of \( \tau \sigma \) differ by 1. To see why this suffices, note that if \( \sigma = \tau_1 \tau_2 \ldots \tau_r, \) then \( \sigma = \tau_1 \ldots \tau_r \iota, \) where \( \iota \) is the identity permutation. Since the number of orbits of \( \iota \) is \( n, \) the number of orbits of \( \sigma \) will be congruent to \( n + r \) modulo 2. Thus, \( r \) must be congruent to \( n + (\text{the number of orbits of } \sigma) \) modulo 2.
Proof of Theorem 9.15, continued.

Write $\sigma \in S_n$ as a product of disjoint cycles.

Case 1. $i$ and $j$ are in two different cycles. Say,

$\sigma = (i, a_1, \ldots, a_r)(j, b_1, \ldots, b_s)\mu_1 \ldots \mu_m$, where the cycles are disjoint. ($r$ and $s$ could be 0.) Then

$$(i, j)\sigma = (i, j)(i, a_1, \ldots, a_r)(j, b_1, \ldots, b_s)\mu_1 \ldots \mu_m$$

$$= (i, a_1, \ldots, a_r, j, b_1, \ldots, b_s)\mu_1 \ldots \mu_m.$$ 

In this case, the number of orbits of $\tau \sigma$ is one less than that of $\sigma$.

Case 2. $i$ and $j$ are in the same cycle. Assume that

$\sigma = (i, a_1, \ldots, a_r, j, b_1, \ldots, b_s)\mu_1 \ldots \mu_m$. Then

$$(i, j)\sigma = (i, a_1, \ldots, a_r)(j, b_1, \ldots, b_s)\mu_1 \ldots \mu_m.$$ 

In this case, the number of orbits of $\tau \sigma$ is one more than that of $\sigma$. □
Even and odd permutations

Definition
A permutation of a finite set is \textit{even} or \textit{odd} according to whether it can be expressed as a product of an even number of transpositions or an odd number of transpositions.

Example

1. The identity permutation is equal to \((1, 2)(1, 2)\). Thus, the identity permutation is even.

2. Let \(\sigma = (a_1, \ldots, a_n)\) be a cycle. Then \(\sigma = (a_1, a_n) \ldots (a_1, a_2)\). Thus, if the length \(n\) is even, then the cycle is an odd permutation. If the length is odd, then the cycle is an even permutation.

3. Let \(\sigma = (1, 3, 6, 5)(2, 8, 4)\). Since \((1, 3, 6, 5)\) is odd and \((2, 8, 4)\) is even, \(\sigma\) is odd.
Alternating groups

Theorem (9.20)

If \( n \geq 2 \), then the set \( A_n \) of all even permutations of \( \{1, 2, \ldots, n\} \) forms a subgroup of order \( n!/2 \) of \( S_n \).

Proof.
The statement has two parts, one claiming that \( A_n \) is a subgroup, and the other asserting that \( |A_n| = n!/2 \). We first show that \( A_n \) is a subgroup. We need to check

1. Closed: If \( \sigma_1 \) and \( \sigma_2 \) are both products of an even number of transpositions, so is \( \sigma_1 \sigma_2 \).

2. Identity: \( \text{id} = (1, 2)(1, 2) \), which is even.

3. Inverse: If \( \sigma = \tau_1 \tau_2 \ldots \tau_{2n} \) is a product of an even number of transpositions \( \tau_j \), then \( \sigma^{-1} = \tau_{2n}^{-1} \tau_{2n-1}^{-1} \ldots \tau_1^{-1} \) is also even.
We now prove that $|A_n| = n!/2$. It suffices to prove that the number of even permutations in $S_n$ is equal to the number of odd permutations in $S_n$.

Let $B_n$ be the set of all odd permutations in $S_n$. (Note that $B_n$ is not a subgroup since it is not closed under multiplication.) Define $\lambda : A_n \rightarrow B_n$ by $\lambda(\sigma) = (1,2)\sigma$. We claim that $\lambda$ is one-to-one and onto. This shows that $|A_n| = |B_n| = |S_n|/2 = n!/2$.

**One-to-one**: If $(1,2)\sigma_1 = (1,2)\sigma_2$, then by the left cancellation law, we have $\sigma_1 = \sigma_2$. Thus $\lambda$ is one-to-one.

**Onto**: If $\sigma \in B_n$ is an odd permutation, then $(1,2)\sigma$ is even and we have $\lambda((1,2)\sigma) = (1,2)(1,2)\sigma = \sigma$. Thus, $\lambda$ is onto. \qed
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.

**Example**

1. $A_3$ has $3!/2 = 3$ elements. They are $\text{id}$, $(1, 2, 3)$, and $(1, 3, 2)$.

2. $A_4$ has $4!/2 = 12$ elements. They are $\text{id}$, 8 3-cycles $(1, 2, 3), (1, 3, 2), \ldots$, and $(1, 2)(3, 4), (1, 3)(2, 4)$, and $(1, 4)(2, 3)$. 
Homework

Do Problems 10, 12, 13, 18, 27, 29, 34, 39 of Section 9.