Lecture 9: Permutation Groups

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Definition

A **permutation** of a nonempty set A is a function $\sigma : A \longrightarrow A$ that is one-to-one and onto. In other words, a pemutation of a set is a rearrangement of the elements of the set.

Theorem

Let A be a nonempty set and let S_A be the collection of all permutations of A. Then $(S_A, \circ)$ is a group, where $\circ$ is the function composition operation.

- The identity element of $(S_A, \circ)$ is the identity permutation $\iota : A \longrightarrow A, \iota(a) = a$.
- The inverse element of σ is the permutation σ^{-1} such that $(\sigma\sigma^{-1})(a) = \sigma(\sigma^{-1}(a)) = \iota(a)$.

Permutation Groups

Definition

The group $(S_A, \circ)$ is called a **permutation group** on A.

We will focus on permutation groups on finite sets.

Definition

Let $I_n = \{1, 2, \ldots, n\}$, $n \geq 1$ and let S_n be the set of all permutations on I_n.The group $(S_n, \circ)$ is called the **symmetric group** on I_n.

Let σ be a permutation on I_n. It is convenient to use the following two-row notation:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Example: Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Then

$$\begin{aligned} f \circ g &= \begin{pmatrix} 1 & 2 & 3 & \mathbf{4} \\ 1 & 3 & 4 & \mathbf{2} \end{pmatrix} \circ \begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ \mathbf{4} & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ \mathbf{2} & 4 & 3 & 1 \end{pmatrix} \\ g \circ f &= \begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ \mathbf{4} & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ \mathbf{1} & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ \mathbf{4} & 2 & 1 & 3 \end{pmatrix} \end{aligned}$$

which shows that $f \circ g \neq g \circ f$.

Note that we apply permutation multiplication $f \circ g$ from right to left.

Properties of Symmetric Groups

- $|S_n| = n!$
- $(S_n, \circ)$ is non commutative for $n \geq 3$.
- $\mathbb{Z}_6 \ncong S_3$ since $\mathbb{Z}_6$ is commutative but S_3 is not.
- $S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$
- $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$
- $$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Definition

Let σ be an element of S_n. Then σ is called a **k-cycle,** written $(i_1\, i_2 \ldots i_k)$, if

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_{k-1} & i_k \\ i_2 & i_3 & \cdots & i_k & i_1 \end{pmatrix}.$$

- If $\sigma = (i_1\, i_2 \ldots i_k)$, then
  $\sigma = (i_1\, i_2 \ldots i_k) = (i_2\, i_3 \ldots i_k\, i_1) = \cdots = (i_j\, i_{j+1} \ldots i_k\, i_1 \ldots i_{j-1})$.
- If $k = 2$, then a k-cycle is called a **transposition**.
- The identity of S_n is denoted (1) or e.
- The **order** of a cycle is the length of cycle.

Examples:

- $S_1 = \{(1)\}$
- $S_2 = \{(1), (12)\}$
- $S_3 = \left\{ (1), \underbrace{(123)}_{order\ 3}, \underbrace{(132)}_{order\ 3}, \underbrace{(23)}_{order\ 2}, \underbrace{(13)}_{order\ 2}, \underbrace{(12)}_{order\ 2} \right\}$
- $\sigma = \begin{pmatrix} 1 & 2 & \mathbf{3} & 4 & \mathbf{5} \\ 2 & 4 & \mathbf{3} & 1 & \mathbf{5} \end{pmatrix} = (124)(\mathbf{3})(\mathbf{5}) = (124) = (241) = (412)$
- $\sigma = \begin{pmatrix} \mathbf{1} & 2 & \mathbf{3} & \mathbf{4} & 5 \\ \mathbf{3} & 5 & \mathbf{4} & \mathbf{1} & 2 \end{pmatrix} = (\mathbf{134})(25) = (25)(134)$

Remark: If two cycle have no common element, then they can commute. But when we multiply two distinct permutations, the cycles may contain common elements so we can not rearrange them.

Example: Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$. Then

$$\begin{aligned} fg &= (1\mathbf{3}2)(1\mathbf{3}) = (12) \\ gf &= (1\mathbf{3})(1\mathbf{3}2) = (23). \end{aligned}$$

Also note that

$$\begin{array}{ccccc} & (132)\,(13) & & & = (\mathbf{12})\,(3) = (12) \\ 2 & \longleftarrow & 3 & \longleftarrow & \mathbf{1} \\ \mathbf{1} & \longleftarrow & 2 & \longleftarrow & 2 \\ 3 & \longleftarrow & 1 & \longleftarrow & 3 \end{array}$$

Definition

Let $\sigma_1, \sigma_2, \ldots, \sigma_k \in S_n$. Then $\sigma_1, \sigma_2, \ldots, \sigma_k$ are called **disjoint** if σ_i moves a, then all other permutations σ_j must fix a for all $a \in I_n$, that is, $\sigma_j(a) = a$ for all $j \neq i, 1 \leq j \leq k$.

- The multiplication of disjoint cycles is commutative.
- Each permutation σ of a set A determines a natural partition on A into the cells with the property

$$"a \sim b \Leftrightarrow b = \sigma^n(a), \exists n \in \mathbb{Z}"$$

for $a, b \in A$. The relation $\sim$ is equivalence relation and the equivalence classes in A are called the **orbits** of σ.

Example: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (134)(25)$. Thus orbits of σ are $\overline{1} = \{1, 3, 4\}$ and $\overline{2} = \{2, 5\}$. Note that

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

- Any permutation $e \neq \sigma \in S_n$ can be **uniquely** (up to the order of factors) expressed as a product of disjoint cycles.
- The inverse of a permutation can also be written as a product of disjoint cycles.

$$\begin{aligned} \sigma &= \sigma_1 \sigma_2 \dots \sigma_k \Rightarrow \sigma^{-1} = \sigma_k^{-1} \sigma_{k-1}^{-1} \dots \sigma_1^{-1} \\ \sigma_j &= (i_1 \, i_2 \dots i_r) \Rightarrow \sigma_j^{-1} = (i_1 \, \mathbf{i_r} \, \mathbf{i_{r-1}} \dots \mathbf{i_2}) \end{aligned}$$

So

$$(i_1 \, i_2)^{-1} = (i_1 \, i_2) \text{ and } (i_1 \, i_2)^2 = (1)$$

- Let $\sigma \in S_n$ and $\sigma = \sigma_1 \sigma_2 \dots \sigma_k$ be a product of disjoint cycles. If $\circ(\sigma_i) = n_i$ for $i = 1, \dots, k$, then

$$\circ(\sigma) = \operatorname{lcm}(n_1, n_2, \dots, n_k).$$

- Any permutation $\sigma \in S_{n\geq 2}$ can be expressed as a product of transpositions.

$$\begin{aligned} (1) &= (12)\,(12) \\ (i_1 i_2 \ldots i_k) &= (i_1 i_k)\,(i_1 i_{k-1}) \ldots (i_1 i_2) = (i_1 i_2)\,(i_2 i_3) \ldots (i_{k-1} i_k)\,. \end{aligned}$$

- No permutation can be written both as a product of an even number of transpositions and as a product of odd number of transpositions.
- The representation of σ as a product of transpositions need not be unique, but the number of transpositions in any representations is either even or odd.
- If $\sigma \in S_n$ is a product of even number of transpositions, then σ is called an **even permutation**; otherwise σ is called an **odd permutation**.
- Let $\sigma \in S_n$ is a k-cycle. σ is an even permutation $\Leftrightarrow$ k is odd.
- The identity permutation is even, since $(1) = (12)\,(12)$.
- Any transposition (ab) can be written as $(ab) = (1a)\,(1b)\,(1a)$.

Example: Let $f = (1243)$, $g = (1526)$. Then fg can be written uniquely as a product of disjoint cycles as

$$fg = \begin{array}{ccccc} & & (1243)\,(1526) & & \\ \mathbf{5} & \longleftarrow & 5 & \longleftarrow & \mathbf{1} \\ \mathbf{4} & \longleftarrow & 2 & \longleftarrow & 5 \\ \mathbf{3} & \longleftarrow & 4 & \longleftarrow & 4 \\ \mathbf{1} & \longleftarrow & 3 & \longleftarrow & 3 \\ \mathbf{6} & \longleftarrow & 6 & \longleftarrow & \mathbf{2} \\ \mathbf{2} & \longleftarrow & 1 & \longleftarrow & 6 \end{array} = (\mathbf{1543})\,(\mathbf{26})$$

Thus fg can be written as a product of transpositions

$$fg = (1543)\,(26) = (13)\,(14)\,(15)\,(26)\,.$$

On the other hand, fg can be written as a product of transpositions

$$fg = (1543)\,(26) = (13)\,(14)\,(15)\,(12)\,(16)\,(12)\,.$$

Observe that the number of transpositions are different but they are both even.

Alternating Groups

Definition

The subset of S_n consisting of all even permutations is denoted by A_n. For $n \geq 2$, $(A_n, \circ)$ is a group, called the **alternating group** on I_n.

- $A_n \leq S_n$
- $|A_n| = \frac{n!}{2}$
- Every $\sigma \in A_n$ is a product of three-cycles for $n \geq 3$.
- $A_n \trianglelefteq S_n$, since $[S_n : A_n] = \frac{n!}{n!/2} = 2$.
- For $n \geq 5$, A_n is the only nontrivial normal subgroup of S_n.
- For $n \neq 4$, A_n is simple group. (Abel Theorem)
- For $n = 4$, $(1) \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$

Alternating Groups

- A_4 has no element of order 6. (This shows that the converse of the Lagrange's theorem need not always hold.)
-

$$\begin{aligned} A_4 / V_4 &= \{\sigma V_4 \mid \sigma \in A_4\} \\ &= \{(1)\, V_4, (123)\, V_4, (132)\, V_4\} \end{aligned}$$

where

$$\begin{aligned} (1)\, V_4 &= V_4 \\ (123)\, V_4 &= \{(123), (134), (243), (142)\} \\ (132)\, V_4 &= \{(132), (234), (124), (143)\}. \end{aligned}$$