6 Permutation Groups

Let $S$ be a nonempty set and $\mathcal{M}(S)$ be the collection of all mappings from $S$ into $S$. In this section, we will emphasize on the collection of all invertible mappings from $S$ into $S$. The elements of this set will be called permutations because of Theorem 2.4 and the next definition.

**Definition 6.1**

Let $S$ be a nonempty set. A one-to-one mapping from $S$ onto $S$ is called a **permutation**.

Consider the collection of all permutations on $S$. Then this set is a group with respect to composition.

**Theorem 6.1**

The set of all permutations of a nonempty set $S$ is a group with respect to composition. This group is called the **symmetric group on $S$** and will be denoted by $\text{Sym}(S)$.

**Proof.**

By Theorem 2.4, the set of all permutations on $S$ is just the set $\mathcal{I}(S)$ of all invertible mappings from $S$ to $S$. According to Theorem 4.3, this set is a group with respect to composition. ■

**Definition 6.2**

A group of permutations, with composition as the operation, is called a **permutation group on $S$**.

**Example 6.1**

1. $\text{Sym}(S)$ is a permutation group.
2. The collection $\mathcal{L}$ of all invertible linear functions from $\mathbb{R}$ to $\mathbb{R}$ is a permutation group with respect to composition. (See Example 4.4.) Note that $\mathcal{L}$ is
a proper subset of $\text{Sym}(\mathbb{R})$ since we can find a function in $\text{Sym}(\mathbb{R})$ which is not in $\mathcal{L}$, namely, the function $f(x) = x^3$. This example shows that, in general, a permutation group on $S$ needs not contain all the permutations on $S$. ■

**Example 6.2**

Let $S = \{1, 2, 3\}$. There are six permutations on $S$. We will represent these permutations using the *two-row form* as follows:

$$
\begin{align*}
\rho_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \rho_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \rho_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\
\rho_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, & \rho_5 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & \rho_6 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}
\end{align*}
$$

In composing permutations we always follow the same convention we use in composing any other mappings: read from right to left. Thus,

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

That is, $1 \to 3 \to 2, 2 \to 2 \to 1, 3 \to 1 \to 3$.

**Example 6.3**

Let $S = \{1, 2, 3\}$. Then $\text{Sym}(S) = \{\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6\}$, where the $\rho$'s are defined in Example 6.2. Let's construct the Cayley table for this group.

<table>
<thead>
<tr>
<th></th>
<th>$\rho_1$</th>
<th>$\rho_2$</th>
<th>$\rho_3$</th>
<th>$\rho_4$</th>
<th>$\rho_5$</th>
<th>$\rho_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rho_1$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
<td>$\rho_3$</td>
<td>$\rho_4$</td>
<td>$\rho_5$</td>
<td>$\rho_6$</td>
</tr>
<tr>
<td>$\rho_2$</td>
<td>$\rho_2$</td>
<td>$\rho_1$</td>
<td>$\rho_3$</td>
<td>$\rho_5$</td>
<td>$\rho_6$</td>
<td>$\rho_4$</td>
</tr>
<tr>
<td>$\rho_3$</td>
<td>$\rho_3$</td>
<td>$\rho_4$</td>
<td>$\rho_1$</td>
<td>$\rho_6$</td>
<td>$\rho_5$</td>
<td>$\rho_2$</td>
</tr>
<tr>
<td>$\rho_4$</td>
<td>$\rho_4$</td>
<td>$\rho_6$</td>
<td>$\rho_5$</td>
<td>$\rho_1$</td>
<td>$\rho_3$</td>
<td>$\rho_2$</td>
</tr>
<tr>
<td>$\rho_5$</td>
<td>$\rho_5$</td>
<td>$\rho_4$</td>
<td>$\rho_6$</td>
<td>$\rho_2$</td>
<td>$\rho_1$</td>
<td>$\rho_3$</td>
</tr>
<tr>
<td>$\rho_6$</td>
<td>$\rho_6$</td>
<td>$\rho_5$</td>
<td>$\rho_4$</td>
<td>$\rho_3$</td>
<td>$\rho_2$</td>
<td>$\rho_1$</td>
</tr>
</tbody>
</table>

Notice that the permutation

$$
\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}
$$

is the identity mapping of $\text{Sym}(S)$. Moreover,

$$
\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}
$$

2
Thus, the inverse of an element is obtained by reading from the bottom entry to the top entry rather than from top to bottom: if 1 appears beneath 3 in $\rho_2$ then 3 appears beneath 1 in $\rho_2^{-1}$.

We will denote the above group by $S_3$. In general, if $S = \{1, 2, \cdots, n\}$ then the symmetric group on $S$ will be denoted by $S_n$.

The number of elements of $S_n$ is found in the following theorem.

**Theorem 6.2**
The order of $S_n$ is $n!$, where $0! = 1! = 1$ and $n! = n(n-1)(n-2)\cdots2\cdot1$.

**Proof.**
The proof involves the following counting principle: If a decision consists of two steps, if the first step can be done in $r$ different ways and the second step can be done in $s$ different ways then the decision can be made in $rs$ different ways.

The problem of computing the number of elements of $S_n$ is the same as the problem of computing the number of different ways the integers $1, 2, \cdots, n$ can be placed in the $n$ blanks indicated (with each number used only once)

\[
\begin{pmatrix}
1 & 2 & 3 & \cdots & n \\
\_ & \_ & \_ & \cdots & 
\end{pmatrix}
\]

Filling the blanks from the left, we see that the first blank can be filled with $n$ different ways. Once this is completed, the second blank can be filled in $n-1$ ways, the third in $n-2$ ways and so on. Thus, by the principle of counting, there are $n(n-1)(n-2)\cdots2\cdot1 = n!$ ways of filling the blanks. In conclusion, $|S_n| = n!$.

Now, since $S_1 = \{(1)\}$ then $S_1$ with respect to composition is commutative. Similarly, since $(1)(12) = (12)(1)$ then $S_2 = \{(1), (12)\}$ is also Abelian. Unfortunately, this is not true anymore for $|S| > 2$.

**Theorem 6.3**
$S_n$ is non-Abelian for $n \geq 3$.

**Proof.**
All that we need to do here is to find two permutations $\alpha$ and $\beta$ in $S_n$ with $n \geq 3$ such that $\alpha \circ \beta \neq \beta \circ \alpha$. Indeed, consider the permutations

\[
\alpha = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & \cdots & n \\
1 & 3 & 2 & 4 & 5 & \cdots & n
\end{pmatrix}
\quad \text{and} \quad
\beta = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & \cdots & n \\
3 & 2 & 1 & 4 & 5 & \cdots & n
\end{pmatrix}
\]
Then
\[\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 2 & 3 & 1 & 4 & 5 & \cdots & n \end{pmatrix}\] and \[\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 3 & 1 & 2 & 4 & 5 & \cdots & n \end{pmatrix}\]
so that \(\alpha \circ \beta \neq \beta \circ \alpha\).

**Cycle Notation for Permutations**

The cycle notation for permutations can be thought as a condensed way to write permutations. Here is how it works.

Let \(\alpha \in S_n\) be the permutation
\[\alpha(a_1) = a_2, \alpha(a_2) = a_3, \cdots, \alpha(a_k) = a_1\]
and \(\alpha(a_i) = a_i\) for \(i = k + 1, \cdots, n\), where \(a_1, a_2, \cdots, a_n \in \{1, 2, 3, \cdots, n\}\).

That is, \(\alpha\) follows the circle pattern shown in Figure 6.1

[Diagram of cycle notation]

Such a permutation is called a *cycle of length* \(k\) or simply a *\(k\)-cycle*. We will write
\[\alpha = (a_1a_2a_3 \cdots a_k)\] (1)

Let us elaborate a little further on the notation employed in (1). The cycle notation is read from left to right, it says \(\alpha\) takes \(a_1\) into \(a_2\), \(a_2\) into \(a_3\), etc., and finally \(a_k\), the last symbol, into \(a_1\), the first symbol. Moreover, \(\alpha\) leaves all the other elements not appearing in the representation (1) fixed.

**Example 6.4**
The permutation
\[
\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 3 & 7 & 5 & 4 & 2 \end{pmatrix}
\]
can be represented as a 4-cycle
\[ \alpha = (2647). \]

Note that one can write the same cycle in many ways using this type of notation.

\[ \alpha = (2647) = (6472) = (4726) = (7264) \]

**Remark 6.1**

A k-cycle can be written in k different ways, since

\[ (a_1a_2 \ldots a_k) = (a_2a_3 \ldots a_k a_1) = \cdots = (a_k a_1 \ldots a_{k-1}). \]

**Example 6.5**

It is easy to write the inverse of a cycle. Since \( \alpha(a_k) = a_{k+1} \) implies \( \alpha^{-1}(a_{k+1}) = a_k \), we only need to reverse the order of the cyclic pattern. For example,

\[ (2647)^{-1} = (7462). \]

**Example 6.6**

Multiplication of cycles is performed by applying the right permutation first. Consider the product in \( S_5 \)

\[ (12)(245)(13)(125) \]

Reading from right to left

1 \( \mapsto \) 2 \( \mapsto \) 2 \( \mapsto \) 4 \( \mapsto \) 4

so 1 \( \mapsto \) 4.

Now

4 \( \mapsto \) 4 \( \mapsto \) 4 \( \mapsto \) 5 \( \mapsto \) 5

so 4 \( \mapsto \) 5.

Next

5 \( \mapsto \) 1 \( \mapsto \) 3 \( \mapsto \) 3 \( \mapsto \) 3

5
so $5 \mapsto 3$.
Then
$$3 \mapsto 3 \mapsto 1 \mapsto 1 \mapsto 2$$
so $3 \mapsto 2$.
Finally
$$2 \mapsto 5 \mapsto 5 \mapsto 2 \mapsto 1$$
so $2 \mapsto 1$. Since all the elements of $A = \{1, 2, 3, 4, 5\}$ have been accounted for, we have

**Remark 6.2**
A 1-cycle of $S_n$ is the identity of $S_n$ and is denoted by $\alpha$. Of course, $\alpha = (2) = (3) = \cdots = (n)$.

Now not all permutations are cycles; for example, the permutation
$$\alpha = \left( \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{array} \right)$$
is not a cycle. However, one can check easily that
$$\alpha = (123)(4567)$$
This suggests how we may extend the idea of cycles to cover all permutations.

**Definition 6.3**
If $\alpha$ and $\beta$ are two cycles, they are called disjoint if the elements moved by one are left fixed by the other, i.e., their cycle representations contain different elements of the set $S = \{1, 2, 3, \ldots, n\}$.

**Example 6.7**
The cycles $(124)$ and $(356)$ are disjoint whereas the cycles $(124)$ and $(346)$ are not since they have the number 4 in common.

**Theorem 6.4**
If $\alpha$ and $\beta$ are disjoint cycles then $\alpha \beta = \beta \alpha$. 

Proof.
Indeed, since the cycles $\alpha$ and $\beta$ are disjoint, each element moved by $\alpha$ is fixed by $\beta$ and vice versa. Let $\alpha = (a_1a_2\cdots a_s)$ and $\beta = (b_1b_2\cdots b_t)$ where $\{a_1, a_2, \ldots, a_s\} \cap \{b_1, b_2, \ldots, b_t\} = \emptyset$.

(i) Let $1 \leq k \leq s$. Then
$$ (\alpha\beta)(a_k) = \alpha(\beta(a_k)) = \alpha(a_k) = a_{k+1} $$
and
$$ (\beta\alpha)(a_k) = \beta(\alpha(a_k)) = \beta(a_{k+1}) = a_{k+1}. $$

(ii) Let $1 \leq k \leq t$. Then
$$ (\alpha\beta)(b_k) = \alpha(\beta(b_k)) = \alpha(b_{k+1}) = b_{k+1} $$
and
$$ (\beta\alpha)(b_k) = \beta(\alpha(b_k)) = \beta(b_k) = b_{k+1}. $$

(iii) Let $1 \leq m \leq n$ and $m \notin \{a_1, a_2, \ldots, a_s, b_1, b_2, \ldots, b_t\}$. Then
$$ (\alpha\beta)(m) = \alpha(\beta(m)) = \alpha(m) = m $$
and
$$ (\beta\alpha)(m) = \beta(\alpha(m)) = \beta(m) = m. $$
It follows from (i), (ii), and (iii) that $\alpha\beta = \beta\alpha$. $\blacksquare$

Theorem 6.5
Every permutation of $S_n$ is either a cycle or can be written uniquely, except for order of cycles or the different ways a cycle is written, as a product of disjoint cycles.

Proof.
The proof is by induction on $n$. If $n = 1$ then there is only one permutation, and it is the cycle $(1)$.
Assume that the result is valid for all sets with fewer than $n$ elements. We will prove that the result is valid for a set with $n$ elements.
Let $\sigma \in S_n$. If $\sigma = (1)$ then we are done. Otherwise there exists a positive integer $m$ such that $\sigma^{m-1}(1) \neq 1$ and $\sigma^m(1) = 1$. For example, if $\sigma =$
Let $(145) \in S_5$ then $m = 3$ since $\sigma(1) = 4, \sigma^2(1) = \sigma(\sigma(1)) = \sigma(4) = 5$, and $\sigma^3(1) = \sigma(\sigma^2(1)) = \sigma(5) = 1$.

Let $Q = \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{m-1}(1)\}$.

If $Q = \{1, 2, \ldots, n\}$ then $\sigma$ is the cycle $\sigma = (1\sigma(1)\sigma^2(1)\ldots\sigma^{m-1}(1))$. If $Q \neq S$, where $S = \{1, 2, \ldots, n\}$, then

$$\sigma = (1\sigma(1)\sigma^2(1)\ldots\sigma^{m-1}(1))\tau$$

where $\tau$ is a permutation on the set $S - Q = \{t \in S : t \notin Q\}$. Since this set has order smaller than $n$, then by the induction hypothesis $\tau$ can be written as a product of disjoint cycles, say, $\tau = \tau_1\tau_2\ldots\tau_k$. Thus,

$$\sigma = (1\sigma(1)\sigma^2(1)\ldots\sigma^{m-1}(1))\tau_1\tau_2\ldots\tau_k$$

But this says that $\sigma$ is expressed as a product of disjoint cycles. This completes the induction step, and establishes the result for all $n$.

**Example 6.8**

Let $S = \{1, 2, \ldots, 8\}$ and let

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

Start the first cycle with 1 and continue until we get back to 1, and then close the first cycle. Then start the second cycle with the smallest number not in the first cycle, continue until we get back to that number, and then close the second cycle, and so on to obtain

$$\alpha = (1245)(367)(8)$$

It is customary to omit such cycles as (8), i.e., elements left fixed by $\alpha$, and write $\alpha$ simply as

$$\alpha = (1245)(367)$$