9 Finite Symmetric Groups

We study an important class of groups, namely the symmetric group on \( n \) symbols for some positive integer \( n \). Any finite group can be identified with a subgroup of some symmetric group.

**Definition 9.1.** Let \( X \) be a finite set. A permutation of \( X \) is a bijection from \( X \) onto \( X \).

For example, if \( X = \{1, 2, 3, 4, 5\} \) then the correspondence

\[
1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1, 4 \mapsto 4, 6 \mapsto 5,
\]

is a permutation of \( X \). We can express this particular permutation as

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
2 & 3 & 1 & 4 & 6 & 5
\end{pmatrix}
\]

**Theorem 9.1.** The set of all permutations of a finite set \( X \) is a group wrt composition of functions.

**Proof.** We show that composition of functions is a well-defined operation on \( X \), and leave the remainder of the proof as an exercise.

Let \( \alpha, \beta \) be permutations of \( X \). Given any \( z \in X \), there exists \( y \in X \) such that \( \beta(y) = z \), since \( \beta \) is onto.

Since \( \alpha \) is onto, there exists \( x \in X \) such that \( \alpha(x) = y \). Then

\[
\beta \circ \alpha(x) = \beta(\alpha(x)) = \beta(y) = z,
\]

so \( \beta \circ \alpha \) is onto.

If \( \beta \circ \alpha(x) = \beta \circ \alpha(y) \) for some \( x, y \in X \) then \( \alpha(x) = \alpha(y) \) since \( \beta \) is \( 1 \)-1, and hence \( x = y \) since \( \alpha \) is \( 1 \)-1. It follows that \( \beta \circ \alpha \) is both \( 1 \)-1 and onto, and is therefore a bijection by definition.

**Definition 9.2.** Let \( X \) be a finite set of size \( n \) for some positive integer \( n \). The group of permutations of \( X \) is denoted by \( S_n \) (or \( \text{Sym}(X) \)), and is called the symmetric group on \( n \) symbols (or letters).

We list the distinct permutations of \( S_3 \).

\[
\begin{pmatrix}
1 & 2 & 3 \\
1 & 2 & 3
\end{pmatrix}, \begin{pmatrix}
1 & 2 & 3 \\
1 & 3 & 2
\end{pmatrix}, \begin{pmatrix}
1 & 2 & 3 \\
3 & 2 & 1
\end{pmatrix}, \begin{pmatrix}
1 & 2 & 3 \\
2 & 1 & 3
\end{pmatrix}, \begin{pmatrix}
1 & 2 & 3 \\
2 & 3 & 1
\end{pmatrix}, \begin{pmatrix}
1 & 2 & 3 \\
3 & 1 & 2
\end{pmatrix}.
\]

Note that \( S_3 \) has exactly \( 3! = 6 \) different permutations. This holds in general:

**Theorem 9.2.** \( S_n \) has exactly \( n! \) distinct elements.

**Proof.** We simply count the number of different arrays

\[
\begin{pmatrix}
1 & 2 & 3 & \cdots & n \\
\sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n)
\end{pmatrix}
\]

where \( \sigma : \{1, 2, ..., n\} \rightarrow \{1, 2, ..., n\} \) represents a bijection. There are \( n \) ways to define \( \sigma(1) \). Once this symbol has been assigned there remains \( n-1 \) ways to determine \( \sigma(2) \), and thereafter \( n-2 \) ways to determine \( \sigma(3) \). Continuing with this argument we see that there are \( n! = n(n-1)(n-2) \cdots (3)(2)(1) \) different possible ways to define \( \sigma \).

Composition of permutations is computed from right to left. For example, if

\[
\alpha = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
5 & 1 & 2 & 3 & 4 & 6
\end{pmatrix}, \quad \beta = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
5 & 4 & 3 & 2 & 6 & 1
\end{pmatrix},
\]

then \( \beta \circ \alpha \) is given by

\[
\beta \circ \alpha = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
5 & 4 & 3 & 2 & 6 & 1
\end{pmatrix} \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
5 & 1 & 2 & 3 & 4 & 6
\end{pmatrix} = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
6 & 5 & 4 & 3 & 2 & 1
\end{pmatrix}
\]

In fact we adopt a more succinct notation to represent permutations.
Definition 9.3. Let $\sigma$ be the permutation that maps $a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_{k-1} \mapsto a_k, a_k \mapsto a_1$. We say that $\sigma$ is a $k$–cycle, and write $\sigma = (a_1a_2\ldots a_k)$.

The permutations $\alpha, \beta$ shown above are expressed as

$\alpha = (15432)(6) = (15432), \quad \beta = (156)(24)(3) = (156)(24)$.

A pair of cycles $(a_1a_2\ldots a_s), (b_1b_2\ldots b_t)$ are called disjoint if $a_i \neq b_j$ for any $i \in \{1, \ldots, s\}, j \in \{1, \ldots, t\}$. In general, composition of permutations is not commutative. For example, with $\alpha, \beta$ as before $\alpha \circ \beta = (14)(23)(56) \neq \beta \circ \alpha = (16)(25)(34)$. However, disjoint cycles do commute.

Theorem 9.3. Every permutation can be expressed as a product of pairwise disjoint cycles. Up to the order of the cycles, and inclusions or exclusions of $1$–cycles, this can be done in exactly one way.

So we have a type of unique factorization in $S_n$. The product of disjoint $k$–cycles can be compared to a product of relatively prime integers.

By convention, we denote the identity permutation by $(1)$. The inverse of a $k$–cycle can be expressed as follows:

$$(a_1a_2\ldots a_k)^{-1} = (a_1a_k)(a_2a_{k-1})\cdots(a_{k-1}a_2)(a_k)(a_1).$$

Composing any $k$–cycle with itself $k$ times results in the identity permutation. Then $(a_1a_2\ldots a_k)^{-1} = (a_1a_2\ldots a_k)^{k-1}$.

Example 9.1. Suppose we wish to solve the equation $((123)(326145))^3z = (152)$ for some permutation for some $z \in S_6$. We’ll start by simplifying the expression


Since (25) is its own inverse, we can solve this equation for unique $z$ as follows:

$$(25)z = (152) \Rightarrow z = (25)(152) = (12).$$

Given a positive integer $n > 1$, the set of permutations of $S_n$ that fixes an given symbol $a \in \{1, \ldots, n\}$ can be identified with $S_{n-1}$. For this reason we think of $S_t$ as being a subgroup of $S_n$ whenever $t \leq n$. In fact any finite group can be identified with a subgroup of $S_n$ for some positive integer $n$.

A $2$–cycle is called a transposition. Any $k$–cycle can be expressed as a product of $k - 1$ transpositions:

$$(a_1a_2\ldots a_k) = (a_1a_k)(a_2a_{k-1})\cdots(a_{k-1}a_2)(a_k)(a_1).$$

Although there may be more than one way to factorize a $k$–cycle as a product of transpositions that are not pairwise disjoint, any cycle (and hence any permutation) is either a product of an even number of transpositions, or of an odd number of transpositions, but not both. If a permutation can be expressed as a product of an even number of transpositions, we say that it is an even permutation. Otherwise we call it an odd permutation.

Theorem 9.4. Let $A_n$ be the set of all even permutations of $S_n$. Then $A_n$ is a subgroup of $S_n$.

Proof. The product of a pair of even permutations clearly results in another even permutation. If $\sigma = (a_1a_2)(a_3a_4)\cdots(a_{k-1}a_k)$ then $\sigma^{-1} = (a_{k-1}a_k)(a_{k-2}a_{k-1})\cdots(a_1a_2)$, which is also an even permutation. \qed

Consider the case $n = 4$. We list the elements of $A_4$:

<table>
<thead>
<tr>
<th>the identity</th>
<th>(12)(12)</th>
<th>(1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-cycles</td>
<td>(12)(13)</td>
<td>(123), (132), (124), (142), (134), (143), (234), (243)</td>
</tr>
<tr>
<td>disjoint 2-cycles</td>
<td>(12)(34)</td>
<td>(12)(34), (13)(24), (14)(23)</td>
</tr>
</tbody>
</table>

Note that there are exactly $4!/2 = 12$ elements in $A_4$. In fact, in general, $A_n$ has exactly $n!/2$ elements.

Another important subgroup of $S_4$ is $V_4$, the Klein Viergruppe:

$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\},$

it consists of the set of even permutations of $S_4$ that are products of a pair of disjoint $2$–cycles.

29