17. Symmetric groups

Fix an integer \( n > 1 \), and let \( S_n \) be the set of all bijective functions \( f : \{1, \ldots, n\} \to \{1, \ldots, n\} \). As discussed in Lecture 10, \( S_n \) is a group with respect to composition. The groups \( S_n \) are called symmetric groups, and elements of \( S_n \) are called permutations. Sometimes symmetric groups are also called permutation groups, but this is not an accurate terminology. Usually by permutation groups one means a subgroup of a symmetric group (thus, symmetric groups are special kinds of permutation groups).

We begin by computing the order of \( S_n \). By definition \(|S_n|\) is the number of ways to choose a bijective function \( f : \{1, \ldots, n\} \to \{1, \ldots, n\} \).

Note that \( f(1) \) could be any natural number from 1 to \( n \), so there are \( n \) ways to choose \( f(1) \); once \( f(1) \) is chosen, \( f(2) \) can be any number distinct from \( f(1) \), so there are \( n - 1 \) choices for \( f(2) \), then \( n - 2 \) choices for \( f(3) \) etc. Finally, we have just 1 choice for the last element \( f(n) \). Overall we have \( n(n - 1) \cdots 2 \cdot 1 = n! \) choices. Thus, \(|S_n| = n!|\).

17.1. Cycle decompositions. There are two standard ways to represent elements of \( S_n \). The first one is two-line notation introduced in Lecture 10. For instance, the element of \( S_6 \) defined by \( f(1) = 4, f(2) = 6, f(3) = 3, f(4) = 5, f(5) = 1 \) and \( f(6) = 2 \) has the following representation by two-line notation:

\[
f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ f(1) & f(2) & f(3) & f(4) & f(5) & f(6) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 5 & 1 & 2 \end{pmatrix}.
\]

The second representation is the cycle decomposition which we now define. Given \( f \in S_n \), the set \( \{1, 2, \ldots, n\} \) can be decomposed as a disjoint union of subsets such that \( f \) cyclically permutes elements of each subset. For instance, for the above element \( f \in S_6 \) there will be three such subsets: \( \{1, 4, 5\}, \{2, 6\} \) and 3 since \( f \) permutes elements 1, 2, 3, 4, 5, 6 as follows: 1 \( \overset{f}{\rightarrow} \) 4 \( \overset{f}{\rightarrow} \) 5 \( \overset{f}{\rightarrow} \) 1; 2 \( \overset{f}{\rightarrow} \) 6 \( \overset{f}{\rightarrow} \) 2 and 3 \( \overset{f}{\rightarrow} \) 3.

Symbolically we write \( f = (1, 4, 5)(2, 6)(3) \). The expression \( (1, 4, 5)(2, 6)(3) \) is called the cycle decomposition of \( f \), and the “parts” of this decomposition, namely \( (1, 4, 5), (2, 6) \) and \( (3) \), are called the cycles of \( f \).

Each element \( f \) can be recovered from its cycle decomposition: if we are given the cycle decomposition of some \( f \in S_n \) and \( i \in \{1, \ldots, n\} \), and we want to compute \( f(i) \), we first find the cycle which contains \( i \). If \( i \) is not the last element in its cycle (counting from left to right), then \( f(i) \) is the next
element in the same cycle, and if $i$ is the last element in its cycle, then $f(i)$ is the first element in the same cycle.

Note that the order of cycles in a cycle decomposition of a given element does not matter: for instance $(1, 4, 5)(2, 6)(3) = (2, 6)(1, 4, 5)(3)$. Also we can cyclically permute elements within each cycle, e.g. $(1, 4, 5) = (4, 5, 1) = (5, 1, 4)$. However, $(1, 4, 5) \neq (1, 5, 4)$.

Cycles of length 1 are called fixed points. For instance, the above $f$ has one fixed point, namely 3. It is a standard convention to omit fixed points from the cycle decomposition, that is, write $(1, 4, 5)(2, 6)$ instead of $(1, 4, 5)(2, 6)(3)$ (it is assumed that the missing elements are fixed).

17.2. **Products of disjoint cycles.** The expression like $(1, 4, 5)(2, 6)$ for an element of $S_6$ can be interpreted in two a priori different ways. First, we can think of it precisely as described above: $(1, 4, 5)(2, 6)$ is the element $f \in S_6$ whose cycle decomposition is $(1, 4, 5)(2, 6) = (1, 4, 5)(2, 6)(3)$. On the other hand, we can consider two other elements $g, h \in S_6$:

$$g = (1, 4, 5) = (1, 4, 5)(2)(3)(6)$$
$$h = (2, 6) = (2, 6)(1)(4)(3)(5).$$

Then one can also interpret $(1, 4, 5)(2, 6)$ as the product of $g$ and $h$ in $S_6$ (that is, the composition of $g$ and $h$). A natural question is whether these two interpretations are the same, that is, whether $f = gh$.

Fortunately, the answer to this question is yes, as one can check by straightforward verification in the above example (the proof in the general case is essentially the same).

**Definition.** An element $f \in S_n$ is called a cycle if the cycle decomposition of $f$ has just one cycle (excluding fixed points).

For instance, $(1, 4, 5) \in S_6$ is a cycle of length 3 and $(2, 6) \in S_6$ is a cycle of length 2 in $S_6$, while $(1, 4, 5)(2, 6)$ is not a cycle.

**Definition.** Two cycles $u = (i_1, \ldots, i_k)$ and $v = (j_1, \ldots, j_l)$ are called disjoint if no integer appears in both $u$ and $v$.

Equivalence of two possible interpretations of a cycle decomposition yields the following theorem:

**Theorem 17.1.** Any element of $S_n$ can be written as a product of disjoint cycles.

**Remark:** Here we allow the empty product which by convention represents the identity element $e \in S_n$.

Let us now see how to multiply two non-disjoint cycles.
Example 1. Let $f = (1,2,3,5,6)$ and $g = (1,2,3,6,4)$ be elements of $S_6$. Write $fg$ as a product of disjoint cycles (equivalently, find the cycle decomposition of $fg$).

We track the image of each element of $\{1,2,3,4,5,6\}$ under the composition $fg$ (recall that we first apply $g$ and then $f$). We have $1 \xrightarrow{g} 2 \xrightarrow{f} 3; 3 \xrightarrow{g} 6 \xrightarrow{f} 1$. This completes the first cycle of $fg$, namely $(1,3)$.

$2 \xrightarrow{g} 3 \xrightarrow{f} 5; 5 \xrightarrow{g} 5 \xrightarrow{f} 6; 6 \xrightarrow{g} 4 \xrightarrow{f} 4; 4 \xrightarrow{g} 1 \xrightarrow{f} 2$. Thus, the second cycle of $fg$ is $(2,5,6,4)$, and the final answer is $fg = (1,3)(2,5,6,4)$.

17.3. Orders of elements in $S_n$.

Claim 17.2. A cycle of length $k$ has order $k$ (as an element of $S_n$)

We do not give a formal proof of this result, but illustrate it using two examples (the second example essentially shows why the result is true in general).

Let $f = (1,3) \in S_4$. Then $f \neq e$, but $f^2 = (1,3)(1,3)$. Thus, $1 \xrightarrow{f} 3 \xrightarrow{f} 1$ and $3 \xrightarrow{f} 1 \xrightarrow{f} 3$, so $f^2$ fixes 1 and 3, and clearly $f^2$ must fix 2 and 4 (since $f$ fixes 2 and 4). Thus $f^2$ fixes every element of $\{1,2,3,4\}$, so $f^2 = e$.

Let $f = (1,3,4,6) \in S_6$. Note that $f^k$ will send each $i \in \{1,3,4,6\}$ to the element which appears $k$ positions to the right of $i$ (in the “cyclic sense”). Thus $f^2 = (1,4)(3,6), f^3 = (1,6,3,4)$ and $f^4 = e$.

Now let us see compute the order of an element which is not a cycle.

Example 2. Let $f = f_1 f_2 f_3 \in S_9$ where $f_1 = (1,3,4,6), f_2 = (2,7)$ and $f_3 = (5,8,9)$. Compute $o(f)$.

By definition of order, we need to find the smallest positive $n$ s.t. $f^n = e$.
We know by Claim 17.2 that $o(f_1) = 4, o(f_2) = 2$ and $o(f_3) = 3$.

Since $f_1, f_2$ and $f_3$ are disjoint cycles, it is clear that they commute with each other, so $f^n = (f_1 f_2 f_3)^n = f_1^n f_2^n f_3^n$ for every $n \in \mathbb{N}$. Also since $f_1, f_2$ and $f_3$ move different elements, it is clear that $f^n = e \iff f_1^n = f_2^n = f_3^n = e$. Thus, we are looking for the smallest positive $n$ such that $f_1^n = f_2^n = f_3^n = e$.

The following result is an immediate consequence of Theorem 13.1: if $g$ is an element of some group $G$ and $d = o(g)$ is finite, then for any $k \in \mathbb{N}$ we have $g^k = e \iff d \mid k$ (that is, a power of $g$ is equal to $e \iff$ the exponent is a multiple of the order of $g$). Applying this result in our situations, we get that $f_1^n = f_2^n = f_3^n = e \iff 4 = o(f_1) \mid n, 2 = o(f_2) \mid n$ and $3 = o(f_3) \mid n$.

By definition, the smallest $n$ with this property is $LCM(2,3,4) = 12$. 

Applying the same logic to an arbitrary element of $S_n$, we obtain the following theorem:

**Theorem 17.3.** Let $f \in S_n$, and suppose $f$ is a product of disjoint cycles of lengths $n_1, \ldots, n_r$. Then $o(f) = \text{LCM}(n_1, \ldots, n_r)$.

17.4. **Cayley’s Theorem.** In this section we prove the following remarkable theorem:

**Theorem 17.4** (Cayley’s Theorem). Let $G$ be a finite group of order $n$. Then $G$ is isomorphic to a subgroup of $S_n$.

**Remark:** A more general version of Cayley’s theorem (which can be proved by the same argument) asserts that any group $G$ is isomorphic to a subgroup of $\text{Sym}(G)$ (the group of all bijective functions from $G$ to itself). We restrict ourselves to finite groups primarily for notational simplicity.

**Proof.** First of all note that to prove the theorem it will be sufficient to construct an injective homomorphism $\varphi : G \to S_n$. Indeed, if $\varphi : G \to S_n$ is any homomorphism, we can also think of $\varphi$ as a homomorphism from $G$ to $\varphi(G)$ (recall from Lecture 16 that $\varphi(G)$ is always a subgroup), and $\varphi$ will be surjective as a map from $G$ to $\varphi(G)$. If the original $\varphi$ is also injective, it will still be injective as a map from $G$ to $\varphi(G)$; thus $\varphi$ will be an isomorphism from $G$ to $\varphi(G)$. Thus, $G$ is isomorphic to $\varphi(G)$, and by construction $\varphi(G)$ is a subgroup of $S_n$.

We define an injective homomorphism $\varphi : G \to S_n$ as follows. Denote the elements of $G$ by symbols $g_1, g_2, \ldots, g_n$ (the order does not matter). Take any element $g \in G$, and consider the sequence $gg_1, gg_2, \ldots, gg_n$ (note that this is precisely the $g$-row of the multiplication table of $G$). By Sudoku property the sequence $gg_1, gg_2, \ldots, gg_n$ contains the same elements as $g_1, g_2, \ldots, g_n$, but in a (possibly) different order. Formally this means that there exists a bijection $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ such that $gg_k = g_{f(k)}$ for all $1 \leq k \leq n$. We can think of $f$ as an element of $S_n$ (note that $f$ depends only of $g$), and define $\varphi : G \to S_n$ by $\varphi(g) = f$. In other words, we define $\varphi(g)$ to be the unique element of $S_n$ such that

$$gg_k = g_{\varphi(g)(k)} \text{ for all } 1 \leq k \leq n \quad (\ast \ast \ast)$$

It is important to understand the meaning of the expression $(\varphi(g))(k)$. First we apply $\varphi$ to $g$ to get an element of $S_n$ which in turn is a function from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$. Then we apply this function to an integer $k$, and the result is also an integer between 1 and $n$. 

We now prove that $\varphi$ given by (***), is an injective homomorphism. First we check that $\varphi$ is a homomorphism, that is, $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in S_n$. Note that both $\varphi(gh)$ and $\varphi(g)\varphi(h)$ are elements of $S_n$ (here $\varphi(g)\varphi(h)$ is the composition of $\varphi(g)$ and $\varphi(h)$), that is, functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$. By definition two functions are equal to each other if and only if they have the same value at every input, so we need to check the equality $(\varphi(gh))(k) = (\varphi(g)\varphi(h))(k)$ for every $k \in \mathbb{N}$.

By the definition of $\varphi$ in (***), we have $(gh)g_k = g_{(\varphi(gh))(k)}$. On the other hand, $hg_k = g_{(\varphi(h))(k)}$. Let $i = (\varphi(h))k$, so that $h g_k = g_i$. Applying (***), with $k$ replaced by $i$, we get $g g_i = g_{\varphi(g)(i)}$. Therefore, $(gh)h_k = g(h g_k) = g g_i = g_{\varphi(g)(i)} = g_{\varphi(g)((\varphi(h))k)} = g_{\varphi(g)(\varphi(h))(k)}$ (where the last step holds since $\varphi(g)\varphi(h)$ is the composition of $\varphi(g)$ and $\varphi(h)$, as functions).

Thus, we obtained two different expressions for $(gh)g_k$, and setting them equal to each other, we conclude that $g_{(\varphi(gh))(k)} = g_{(\varphi(g)\varphi(h))(k)}$, and therefore $(\varphi(gh))(k) = (\varphi(g)\varphi(h))(k)$, as desired.

Thus, we proved that $\varphi$ is a homomorphism. By Theorem 16.3, to prove that $\varphi$ is injective, it suffices to show that $\ker(\varphi) = \{e\}$. Since $\ker(\varphi)$ always contains $e$, we just need to show that $\varphi(g) = id$ forces $g = e_G$ (here $id$ is the identity permutation which is the identity element of $S_n$). So take any $g \in G$ such that $\varphi(g) = id$. This means that $(\varphi(g))(k) = k$ for all $k$, so $g g_k = g_{\varphi(g)(k)} = g_k$ for all $k$. Already knowing this equation for a single $k$ forces $g = e_G$ by cancellation law. Thus, $\ker(\varphi) = \{e\}$, so $\varphi$ is injective. \[\square\]

We shall now explicitly compute the homomorphism from the proof of Cayley’s theorem in a specific example.

**Example 3.** Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, and let $\varphi : G \to S_4$ the homomorphism from the proof of Cayley’s theorem. Compute $\varphi(G)$.

Let $g_1 = ([0], [0])$ be the identity element of $G$, and let $g_2, g_3$ and $g_4$ denote the other three elements (the order does not matter). By direct computation (or by an argument from Lecture 18), the multiplication table of $G$ is

<table>
<thead>
<tr>
<th></th>
<th>$g_1$</th>
<th>$g_2$</th>
<th>$g_3$</th>
<th>$g_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$g_1$</td>
<td>$g_1$</td>
<td>$g_2$</td>
<td>$g_3$</td>
<td>$g_4$</td>
</tr>
<tr>
<td>$g_2$</td>
<td>$g_2$</td>
<td>$g_3$</td>
<td>$g_4$</td>
<td>$g_1$</td>
</tr>
<tr>
<td>$g_3$</td>
<td>$g_3$</td>
<td>$g_4$</td>
<td>$g_1$</td>
<td>$g_2$</td>
</tr>
<tr>
<td>$g_4$</td>
<td>$g_4$</td>
<td>$g_1$</td>
<td>$g_2$</td>
<td>$g_3$</td>
</tr>
</tbody>
</table>
By definition, to determine $\varphi(g)$ in two-line notation, we simply look at the sequence of indices in the $g$-row of the multiplication table. Thus

\[
\begin{align*}
\varphi(g_1) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \\
\varphi(g_2) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \\
\varphi(g_3) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \\
\varphi(g_4) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.
\end{align*}
\]

Converting to the cycle notation, we get

\[
\varphi(g_1) = id, \quad \varphi(g_2) = (1, 2)(3, 4), \quad \varphi(g_3) = (1, 3)(2, 4), \quad \varphi(g_4) = (1, 4)(2, 3).
\]

Thus, we conclude that the four elements \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} form a subgroup of $S_4$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. This subgroup actually has a special name, the Klein 4-group.

17.5. **Book references.** The general references for the first 3 sections in lecture are [Pinter, Chapter 8] and [Gilbert, 4.1]. Cayley’s Theorem is proved at the end of [Pinter, Chapter 9] as well as [Gilbert, 4.2].