2. The Symmetric Groups

Among the royalty of the group world are the symmetric groups.

Definition 2.1. Let \( n \geq 1 \). The symmetric group \( S_n \) is the group of all bijective (=1-1 and onto) functions from the set \( \{1, 2, \ldots, n\} \) to itself with the group multiplication being composition of functions. More succinctly, \( S_n \) is the group of permutations of \( \{1, 2, \ldots, n\} \).

It is common to use Greek letters for the elements of the symmetric group. Let’s check that \( S_n \) satisfies the axioms of Definition 1.1. First \( S_n \) is non-empty because it contains the identity function \( \text{id} : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \). Let’s write \( X = \{1, 2, \ldots, n\} \). If \( \sigma \) and \( \tau \) are permutations of \( X \), so is their composition \( \sigma \tau = \sigma \circ \tau \), which means first apply the permutation \( \tau \) then apply \( \sigma \), so we do have a well-defined multiplication.

Not all books adopt the convention that \( \sigma \tau \) means first do \( \tau \) then \( \sigma \); for example, P.M. Cohn’s book *Algebra* uses the opposite convention).

Lemma 2.2. \( |S_n| = n! \).

Proof. We must count the number of permutations of \( X = \{1, 2, \ldots, n\} \). There are \( n \) choices for where to send 1, then \( n-1 \) choices for where to send 2, and so on, giving a total of \( n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1 = n! \) choices. \( \square \)

Notation. We need some good (=short) notation to denote the various elements of \( S_n \). Here’s an example. The permutation \( \sigma \in S_9 \) defined by

\[
\sigma(1) = 1, \sigma(2) = 5, \sigma(3) = 7, \sigma(4) = 8, \sigma(5) = 2, \\
\sigma(6) = 4, \sigma(7) = 6, \sigma(8) = 9, \sigma(9) = 3,
\]

is denoted by

\[
\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 8 & 2 & 4 & 6 & 9 & 3 \end{pmatrix}.
\]

Example 2.3. Let’s write out the elements in \( S_3 \). There is

\[
e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},
\]

\[
\sigma \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},
\]

\[
\sigma \tau \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau \sigma \tau.
\]

Notice that \( S_3 \) is not abelian. \( \diamond \)

Let \( \sigma \in S_n \). The orbit of \( i \in \{1, 2, \ldots, n\} \) under the action of \( \sigma \in S_n \) is \( \{i, \sigma(i), \sigma^2(i), \ldots\} \). Obviously \( \{1, 2, \ldots, n\} \) is the disjoint union of its orbits under \( \sigma \).

Cycle notation. We can improve our notation by agreeing to write

\[
(a \, b \, c \, \ldots \, z) := \begin{pmatrix} a & b & c & \ldots & z \\ b & c & \ldots & z & a \end{pmatrix}.
\]
A permutation of this form is called a cycle. With our convention that \( \sigma \tau \) means first do \( \tau \) then \( \sigma \), we have \((12)(23) = (123)\). For example,

\[
\begin{pmatrix}
123 & 456 & 789 \\
157 & 824 & 693
\end{pmatrix}
= (25)(3764893).
\]

The length of the cycle \((abc \ldots z)\) is the cardinality of \(\{a, b, c, \ldots, z\}\). A cycle of length \(k\) is called a \(k\)-cycle. A 2-cycle is called a transposition.

A cycle can be written in different ways: e.g., \((123) = (231) = (312)\).

The following two important observations are easily proved.

**Lemma 2.4.** The order of a cycle is its length.

**Lemma 2.5.** The inverse of a cycle \((ab \ldots yz)\) is the cycle \((zy \ldots ba)\).

Two cycles \(\sigma\) and \(\tau\) are disjoint if they can be written as \(\sigma = (abc \ldots z)\) and \(\tau = (ab'c' \ldots z')\) with \(\{a, b, c, \ldots, z\} \cap \{a', b', c', \ldots, z'\} = \emptyset\). Disjoint cycles commute with each other.

**Lemma 2.6.** Every element of \(S_n\) can be written as a product of disjoint cycles in a unique way up to order.

**Proof.** Let \(\sigma \in S_n\). Write \(\{1, 2, \ldots, n\}\) as the disjoint union of its \(\sigma\)-orbits, say \(O_1 \cup \cdots \cup O_m\). Let \(\tau_i\) be the cycle that is the identity on all \(O_j\) other than \(O_i\) and acts on \(O_i\) as does \(\sigma\): thus, if \(a \in O_i\), then \(\tau_i = (a \sigma(a), \sigma^2(a) \ldots)\). Then \(\sigma = \tau_1 \cdots \tau_m\).

**Lemma 2.7.** Every permutation can be written as a product of transpositions.

**Proof.** Every cycle is a product of transpositions because, for example, \((12 \ldots m - 1 m) = (1 m)(1 m - 1) \cdots (13)(12)\). But every permutation is a product of cycles, so the result follows.

Lemma 2.7 can be read as saying that \(S_n\) is generated by transpositions. However, one can be efficient and generate it with just \(n - 1\) transpositions. Show that \(S_n = \langle (12), (23), \ldots, (n - 1 n)\rangle\); here and elsewhere the notation \(\langle x, y, \ldots, z \rangle\) is used to denote the smallest subgroup containing the elements \(x, y, \ldots, z\); we call it the subgroup generated by \(x, y, \ldots, z\).

**Some Exercises.**

1. Show that \(gHg^{-1}\) is a subgroup whenever \(H\) is.
2. How many elements are there in \(gHg^{-1}\)?
3. Define a relation \(\sim\) on \(G\) by \(x \sim y\) if \(x = gyy^{-1}\) for some \(g \in G\). Show this is an equivalence relation: i.e., show the relation is symmetric (meaning that \(x \sim x\)), reflexive (meaning that \(x \sim y\) implies \(y \sim x\)), and transitive (meaning that \(x \sim y\) and \(y \sim z\) implies \(x \sim z\)).
4. Suppose that \(X\) is a set with an equivalence relation \(\sim\). For each \(x \in X\), we write

\[
[x] := \{y \in X \mid y \sim x\}
\]

and call this the equivalence class of \(x\). Show that \(X\) is the disjoint union of its equivalence classes.
5. Let \(H\) be a subgroup of \(G\). Define a relation \(\sim\) on \(G\) such that \(x \sim y\) if \(x = yh\) for some \(h \in H\). Show this is an equivalence relation. What are the equivalence classes (they already turned up in this class and were given a special name)? How many elements are there in each equivalence class?
6. The center of a group is $Z(G) := \{ z \in G \mid zg = gz \text{ for all } g \in G \}$. Show that $Z(G)$ is a subgroup of $G$.
7. Show that the conjugacy class $C(x)$ consists of just one element if and only if $x \in Z(G)$.
8. Prove that the order of a cycle in $S_n$ is equal to its length.
9. Prove that the inverse of a cycle $(ab \ldots yz)$ is $(zy \ldots ba)$.
11. Show that $S_n = \langle (12), (23), \ldots, (n-1\ n) \rangle$.
12. Show that $xH = Hx$ if and only if $xHx^{-1} = H$. 