# Section 8: Symmetric and Permutation Groups

**Definition 0.1.** Let $A$ be a set. A **permutation** of a set is a function $\phi : A \to A$ that is both one-to-one and onto.

**Example 0.2.** In the worksheet on Friday, you explored permutations of the set $\{1, 2, 3, 4, 5\}$.

Defining permutations as functions that are both one-to-one and onto, we know (or perhaps, used to know) that the composition of two functions that are one-to-one and onto is again one-to-one and onto. So, we can define a *binary operation* on the set of permutations as the composition of two functions. If $\sigma : A \to A$ is a permutation and $\tau : A \to A$ is another permutation, $\sigma\tau = \sigma \circ \tau : A \to A$ is again a permutation, gotten by *first* doing $\tau$ and *second* doing $\sigma$.

We can also see that there is an identity permutation, namely the identity function $\iota : A \to A$ given by $\iota(a) = a$ for all $a \in A$. And, because a permutation $\sigma : A \to A$ is a function that is one-to-one and onto, there exists an inverse function $\sigma^{-1} : A \to A$, defined as the function such that $\sigma^{-1}(a) = a'$, where $a'$ is the unique element such that $a = \sigma(a')$.

With this information in hand, we can define the **permutation** or **symmetric** group.

**Definition 0.3.** 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 and is called the **permutation group** of $A$.

**Definition 0.4.** If $A = \{1, 2, \ldots, n\}$, then we call $S_A$ the $n^{th}$ **symmetric group** and denote it by $S_n$.

**Theorem 0.5.** *$S_n$ has $n!$ elements.*

We will spend most of our time discussing $S_n$. First of all, how can we write elements in $S_n$? There are two standard notations. Back to our worksheet about $S_5$, let's say I laid tiles on the grid

| | | | | |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

as follows:

| | | | | |
|---|---|---|---|---|
| 4 | 2 | 5 | 3 | 1 |

What happened?

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

where the top entry indicates the position and the bottom entry indicates what element moved to that position. You can consider $\sigma$ as the function that assigns an element to each spot of the grid: $\sigma(1) = 4$, $\sigma(2) = 2$, and so on. Now, what happens if I want to compose this with the permutation

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}?$$

Depending on the order, I could get two possible answers. Let's compute $\sigma\tau$. What is $\sigma\tau(1)$? Well, $\sigma\tau(1) = \sigma(\tau(1)) = \sigma(3) = 5$, and I could compute this for each element to get:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

Let's do the other way. What is $\tau\sigma$?

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}.$$

Note: these are *not* the same. In fact, we can prove the following theorem:

**Theorem 0.6.** *For $n \geq 3$, $S_n$ is not abelian.*

*Proof.* It suffices to show this for $S_3$. Given any permutation $\sigma \in S_3$, we can consider $\sigma$ as a permutation in $S_n$ by just applying $\sigma$ to the first three elements and doing nothing to the remaining $n - 3$.

So, we just need to find two elements $\sigma$ and $\tau$ in $S_3$ such that $\sigma\tau \neq \tau\sigma$. There are many choices, but here is one:

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

□

We have also already seen $S_3$ in another context: the group of symmetries of the triangle! (Remember, we could get every permutation of the elements $\{1, 2, 3\}$ with some symmetry operation of the triangle?) This is related to another important group.

**Definition 0.7.** The **dihedral group** $D_n$ is the group of symmetries of the regular $n$-gon. It has $2n$ elements. If $R$ is rotation by $360/n$ degrees clockwise and $F$ is flipping across the vertical axis, then $D_n = \{E, R, R^2, \ldots, R^{n-1}, F, FR, FR^2, \ldots, FR^{n-1}\}$ subject to the relations $R^n = F^2 = E$ and $RF = FR^{n-1}$.

**Theorem 0.8.** *$D_n$ is a subgroup of $S_n$.*

*Proof.* Label the vertices of the $n$-gon $1, 2, \ldots, n$ and consider each element of $D_n$ as a permutation by the given action on the vertices. (So, a rotation is the permutation $\begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 3 & \ldots & 1 \end{pmatrix}$.) By construction, $D_n$ is closed under composition, contains the identity, and contains the inverses. □

In more generality, we can actually show that *any group* is isomorphic to a subgroup of a permutation group. To do this, we will introduce a few more definitions.

**Definition 0.9.** Let $f : A \to B$ be a function and let $H$ be a subset of $A$. The **image** of $H$ under $f$ is the set $f[H] = \{f(h) \mid h \in H\}$.

**Definition 0.10.** Let $G$ and $G'$ be groups. A **homomorphism** is a function $\phi : G \to G'$ such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

In the context of what we already know, an *isomorphism* is a homomorphism that is also one-to-one and onto.

**Theorem 0.11** (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of a permutation group.*

We will prove this next time!