8 Groups of Permutations

Often times members of a group act as functions, such as members of $GL(2, \mathbb{R})$ and the binary operation between members would be function composition. In this section we study groups whose elements are called *permutations*. Each permutation acts on a finite set.

Definition. *A **permutation** of a set A is a function $\phi : A \to A$ that is both 1-1 and onto.*

8.1 Permutation Groups

Suppose σ, τ are permutations on a set A. For $a \in A$, we define $(\sigma\tau)(a) = (\sigma \circ \tau)(a) = \sigma(\tau(a))$. It can be shown that $\sigma\tau$ is also 1-1 and onto, and hence, $\sigma\tau$ is a permutation.

We use the following notation. If $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 1$, we write

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

Theorem. *Let A be a nonempty set and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.*

Suppose $\sigma(a') = a$ and hence $\sigma^{-1}(a) = a'$. We use the notation ι for the identity permutation: $\iota(a) = a$.

Definition. *Let A be the finite set $\{1, 2, \ldots, n\}$. The group of all permutations of A is the **symmetric group** on n letters, denoted by S_n.*

Remark. $|S_n| = n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1.$

8.2 Two Important Examples

Example 1. *Consider S_3 with the following elements:*

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

All finite groups up to order 5 are abelian. The multiplication table for S_3 shows that S_3 is not abelian. Thus S_3 is the smallest nonabelian group.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

ρ_i stand for rotations, and μ_i stand for mirror images in bisector of angles.

*S_3 is also called the group D_3 of **symmetries of an equilateral triangle**. D_3 means the third dihedral group. The n^{th} **dihedral group** D_n is the group of symmetries of the regular n-gon.*

Example 2. *D_4 is the group of permutations for the ways two copies of a square can be placed, one covering the other, that is, D_4 is the group of symmetries of the square. D_4 is also called the octic group. D_4 has eight permutations.*

We may use ρ_i for rotations, μ_i for mirror images in perpendicular bisectors of sides, and δ_i for diagonal flips.

D_4	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

Note that D_4 is nonabelian. D_4 has three subgroups of order 4

$$\{\rho_0, \rho_2, \mu_1, \mu_2\}, \quad \{\rho_0, \rho_1, \rho_2, \rho_3\}, \quad \{\rho_0, \rho_2, \delta_1, \delta_2\}$$

and five subgroups of order 2

$$\{\rho_0, \mu_1\}, \quad \{\rho_0, \mu_2\}, \quad \{\rho_0, \rho_2\}, \quad \{\rho_), \delta_1\}, \quad \{\rho_0, \delta_2\}$$

8.3 Cayley's Theorem

By observing a table for every group, we see that every row and every column is a permutation of the elements of the group.

Theorem (Cayley's Theorem)**.** *Every group is isomorphic to a group of permutations.*

The proof of Cayley's theorem requires a definition and a lemma.

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

Lemma. *Let G, G' be groups and let $\phi : G \to G'$ be a 1-1 function such that $\forall x, y \in G, \phi(xy) = \phi(x)\phi(y)$. Then $\phi[G]$ is a subgroup of G' and ϕ provides an isomorphism of G with $\phi[G]$.*

Definition. *Let $\lambda_x : G \to G$ be defined by $\forall g \in G, \lambda_x(g) = xg$ (think of λ_x as left multiplication by x). The map $\phi : G \to S_G$ defined by $\forall x \in G, \phi(x) = \lambda_x$ is called the* ***left regular representation*** *of G. The right regular permutation is defined similarly.*

Example 3. *Suppose*

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$$

1. *Calculate $\tau^2\sigma$.*
2. *Compute $|\langle\sigma\rangle|$*

Example 4. *Determine whether $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x + 1$ is a permutation of $\mathbb{R}$.*

Example 5. *Let A be a set and let $\sigma \in S_A$. For a fixed $a \in A$, the set*

$$\mathcal{O}_{a,\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$$

is the ***orbit*** *of a* ***under*** *σ. Let $a, b \in A$ and $\sigma \in S_A$. Show that if $\mathcal{O}_{a,\sigma}$ and $\mathcal{O}_{b,\sigma}$ have an element in common, then $\mathcal{O}_{a,\sigma} = \mathcal{O}_{b,\sigma}$.*