A “group” is a nonempty set with a binary operation that combines two elements of set into one element of the set, that satisfies certain Axioms.

We will introduce the notion of a group by way of an example.

Example. For \( T = \{1, 2, 3\} \), a bijective function \( f \) from \( T \) to \( T \) can be represented by an array:

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

Recall from Math 290 that we called a bijective function of a set to itself a permutation of that set.

Because the cardinality of \( T \) is 3, there are precisely \( 3! = 6 \) permutations of \( T \).

We let \( S_3 \) be the set of all bijection functions from \( T \) to \( T \); the set \( S_3 \) consists of

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

Since we know that the composition of two bijective functions is a bijective function, we have a binary operation on the set \( S_3 \) of permutations of \( T \).

If \( f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \) and \( g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \), then \( f \circ g \) is the permutation of \( T \) given by

\[
(f \circ g)(1) = f(g(1)) = f(2) = 3,
(f \circ g)(2) = f(g(2)) = f(3) = 2,
(f \circ g)(3) = f(g(3)) = f(1) = 1.
\]

Thus the bijection \( f \circ g \) of \( T \) is the permutation

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

We may also determine \( f \circ g \) using the arrays for \( f \) and \( g \):

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

The set \( S_3 \) is closed under the binary operation of composition of functions.

Because composition of functions is in general associative,

\[(f \circ g) \circ h = f \circ (g \circ h),\]
the composition of the permutations in $S_3$ is associative.

With respect to the algebraic operation of composition on $S_3$, the element

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \in S_3$$

acts like an “identity” for composition:

$$I \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} f(1) & f(2) & f(3) \\ f(1) & f(2) & f(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix},$$

and

$$f \circ I = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

Since every bijection function has an inverse function, every element $f \in S_3$ has an inverse $g \in S_3$ which satisfies

$$f \circ g = I, \ g \circ f = I.$$

For instance, for

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

we have

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$$

and

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I.$$

Recall that in general the composition of functions is not always commutative, and this is the case for some of the elements of $S_3$:

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

and

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

We can now give the formal and abstract definition of a “group.”

**Definitions.** A group is a nonempty set $G$ equipped with a binary operation $*$ that satisfies the following Axioms.

1. **Closure:** If $a \in G$ and $b \in G$, then $a * b \in G$.
2. **Associativity:** $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
3. There exists an element $e \in G$ (called the identity element) such that $a * e = a = e * a$ for all $a \in G$.
4. For each $a \in G$, there exists an element $d \in G$ (called the inverse of $a$) such that $a * d = e = d * a$. 
A group $G$ is called abelian if it also satisfies this Axiom:

5. Commutativity: $a * b = b * a$ for all $a, b \in G$.

We call a group that does not satisfy Axiom 5 a nonabelian group.

A group $G$ is said to be finite if it has a finite number of elements; for such we say that the order of $G$ is the cardinality $|G|$, and also say that $G$ has finite order.

A group with infinitely many elements is said to have infinite order.

**Examples.**

(a) The set $S_3$ of permutations of $T = \{1, 2, 3\}$ is a nonabelian group of order $|S_3| = 6$.

(b) The set $S_n$ of permutations of $T = \{1, 2, \ldots, n\}$ is a nonabelian group of order $n!$.

(c) For any set $T$ with infinitely many elements, the set of permutations $A(T)$ with the usual composition of functions is a nonabelian group of infinite order.

(d) The set $\mathbb{Z}$ with the usual addition is an abelian group of infinite order.

(e) The set $\mathbb{Z}_n$ with the usual addition is an abelian group of finite order.

(f) The set $M(\mathbb{R})$ with the usual addition is an abelian group of infinite order.

(g) The set of invertible matrices in $M(\mathbb{R})$ with the usual multiplication is a nonabelian group of infinite order.

**Example.** Determine whether the subset $G = \{2, 4, 6, 8\}$ of $\mathbb{Z}_{10}$ equipped with the binary operation $a * b = ab$ is a group.

Axiom 1. We construct the table for the binary operation $*$ on $G$:

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>4</td>
</tr>
</tbody>
</table>

This shows that $G$ is closed under $*$.

Axiom 2. Since $G$ is a subring of $\mathbb{Z}_{10}$ and $a * b$ is the multiplication of $\mathbb{Z}_{10}$, then $a * b$ is associative.

Axiom 3. From the table, the element $e = 6$ satisfies $a * 6 = a = 6 * a$ for all $a \in G$.

Axiom 4. From the table, we see that each element of $G$ has an inverse:

- $2 * 8 = 6 = 8 * 2$,
- $4 * 4 = 6 = 4 * 4$,
- $6 * 6 = 6 = 6 * 6$,
- $8 * 2 = 6 = 2 * 8$.

So $G$ is a group. Is it abelian?

Axiom 5. From the table (it being symmetric), the group $G$ satisfies $a * b = b * a$.

The order of the abelian group $G$ is $|G| = 4$. 