# 1 Semigroups and Group

## 1.1 Binary Operations. Semigroups

**Definition 1.** A *binary operation* on a nonempty set $S$ is any mapping of $S \times S$ into $S$.

So, with every ordered pair $(a, b)$ of elements of $S$ a binary operation on $S$ associates an element of $S$, uniquely determined by $a$ and $b$.This element is denoted by a symbol such as $a + b$, $a.b$, $ab$, $a\,O\,b$, etc. The requirement that the image of every element of $S \times S$ under the given mapping must belong to $S$, is referred to as the *closure property.* As a rule, we use the symbol $ab$ for the image of $(a, b)$ and any given binary operation; in doing this we follow the multiplicative notation. Occasionally we use the notation $a + b$ for the image of $(a, b)$; in doing this we follow the *additive notation.*

**Definition 2.** An element $e \in S$ is called a *left identity*, or a *right identity*, or a *twosided identity* for a given binary operation on $S$ iff $ea = a$, or $ae = a$, or $ea = ae = a$ holds, respectively, for every $a \in S$.

**Definition 3.**

(i) A binary operation on $S$ is called *associative*; or *commutative*, iff $(ab)c = a(bc)$ holds for all $a, b, c \in S$; or $ab = ba$ holds for all $a, b \in S$, respectively.

(ii) A *semigroup* is any nonempty set $S$ equipped with an associative binary operation.

(iii) A semigroup is called *abelian* (after N. H. Abel, 1802-1829) iff the binary operation is commutative (in addition to being associative).

**Example.** Addition, as well as multiplication of numbers, is a binary operation on each of the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}.\mathbb{C}$; each of these binary operations is associative and commutative. So each of the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is an abelian semigroup under addition, as Well as abelian semigroup under multiplication. Each of these sem groups under multiplication has a (unique) two-sided identity. viz. 1 The same is true for each of the semigroups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under addition, for 0 is the identity element for addition, but not for $\mathbb{N}$ because $0 \notin \mathbb{N}$.

*Remark.* There are some modem authors who include 0 among the natural numbers. We do not agree with practice because it is historically unjustified.

**Example.** Let $X$ be any non-empty set and $P(X)$ be the power set of $X$. Each of the mappings $(A, B) \to A \cup B, (A, B) \to A \cap B, (A, B) \to A \Delta B$, is an associative and commutative binary operation on $P(X)$. So $P(X)$ is an abelian semigroup under each of these binary operations. Each of these semigroups has a (unique) two-sided identity, viz. $\varnothing, X, \varnothing$, respectively. Thus, two distinct binary operations on a set may have the same identity element.

*Remark.* If a given binary operation has a two-sided identity $e$ then $e$ is the only two-sided identity for that binary operation.

**Example.** Let Map $(X)$ be the set all mappings of a nonempty set $X$ into itself. The composition of mappings is a binary operation on Map $(X)$, which is associative but in general not commutative. By Example 1.4.6 (p. 13) composition of mappings is a binary operation on Bij $(X)$, the subset of Map $(X)$ consisting of all bijective mappings $X$ onto itself. So, Map $(X)$, as well as Bij $(X)$, is a semigroup under the composition of mappings. Each of these semigroups has a (unique) twosided identity element, viz. $l_X$, the identity mapping on $X$.

**Example.** Let $M_n(D)$ be the set of all $n \times n$ matírices with entries in $D$, where $n > 1$ and $D$ is any of the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Addition of matrices, as well as multiplication of matrices, is a binary operation on $M_n(D)$, because $D$ is closed under addition and multiplication of numbers. Each of these semigroups under addition is abelian and has an identity element, viz. the zero matrix of order $n$. Each of the multiplicative semigroups is non-abelian, and has a (unique) twosided identity, viz. the identity matrix of order $n$.

**Example.** Show that the set S of all $2 \times 2$ matrices of the form $\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}$ with entries in $\mathbb{Z}$, is a nonabelian semigroup under multiplication of matrices. Show also that $S$ has no right identity, while every matrix of the form $\begin{bmatrix} 1 & b \\ 0 & 0 \end{bmatrix}$, where $b \in \mathbb{Z}$, is a left identity. The matrix product $\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x' & y' \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xx' & yy' \\ 0 & 0 \end{bmatrix}$ belongs to $S$, for all $x, x', y, y' \in \mathbb{Z}$. So $S$ is closed under multiplication of matrices. The associative law $(AB)C = A(BC)$ holds in $M_2(Z)$; so it holds in $S$, because $(AB)C$ and $A(BC)$ belong to $S$, wherever $A, B, C$ belong to $S$.
So $S$ is a semigroup under multiplication of matrices. S is nonabelian, because - for example - we have $\begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 0 & 0 \end{bmatrix}$ while $\begin{bmatrix} 3 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 9 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 6 & 9 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 6 & 7 \\ 0 & 0 \end{bmatrix}$ Suppose $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ is a right identity for $S$.
Since
$\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xa & xb \\ 0 & 0 \end{bmatrix}$, we should have $xa = x$ and $xb = y$.
But there is no fixed $b \in \mathbb{Z}$ such that $xb = y$ holds for all $x, y \in Z$.
Therefore $S$ has no right identity identity.
For any fixed $b \in \mathbb{Z}$, the matrix $\begin{bmatrix} 1 & b \\ 0 & 0 \end{bmatrix}$ belongs to $S$ and is a left identity for $S$, because $\begin{bmatrix} 1 & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} =$ $\begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix}$ holds for all $x, y \in \mathbb{Z}$. So $S$ has infinitely many left identities.

*Remark.* If for a given mapping on $S \times S$, the image does not always belong to $S$, then that mapping is not a binary operation on $S$.

For example, the set $S$ of all $2 \times 2$ matrices of the form $\begin{bmatrix} x & x \\ x & 0 \end{bmatrix}$ with entries in $\mathbb{Z}$, is not closed under multiplication of matrices, because $\begin{bmatrix} x & x \\ x & 0 \end{bmatrix} \begin{bmatrix} y & y \\ y & 0 \end{bmatrix} = \begin{bmatrix} 2xy & xy \\ xy & xy \end{bmatrix}$ does not belong to $S$, unless $xy = 0$ (that is, unless $x = 0$ or $y = 0$). So $S$ is not a semigroup under multiplication of matrices, even though multiplication of matrices in $M_2(\mathbb{Z})$, in particular of those in $S$, is associative.

It is of course possible that a set $S$ is closed under a given mapping on $S \times S$, but that binary operation is not associative. An example is subtraction on the set $\mathbb{Z}$; indeed $a - (b - c) = (a - b) - c$ holds only for $c = 0$. So $\mathbb{Z}$ is not a semigroup under subtraction.

At this stage it is desirable to formulate the definition of semigroup bypassing the notion of binary operation.

**Definition 4.** A nonempty set $S$ is called a *semigroup* under a mapping $(a, b) \to ab$ from $S \times S$ into $S$, iff the following properties (referred to *semigroup axioms*) hold:

1. $ab \in S$ for all $a, b \in S$(closure property)

2. $(ab)c = a(bc)$ for all $a, b, c \in S$ (associative law)

In Definition 3 (ii) the closure property was not expressly mentioned, because the notion of binary operation embodies the closure property. Even then it is desirable to list the closure property explicitly, because in a specific example this property has to be checked first.

**Definition 5.** Suppose $e$ is a *left*, or *right*, or a *two-sided identity* of a given semigroup $S$. Given $a \in S$, an element $a' \in S$ is called a *left*, or *right*, or a *two-sided inverse* of $a$ iff $a'a = e$, or $aa' = e$ or $a'a = aa' = e$, holds, respectively. $a$ is then called *left invertible*, or