Arkansas Tech University
MATH 4033: Elementary Modern Algebra
Dr. Marcel B. Finan

3 Binary Operations

We are used to addition and multiplication of real numbers. These operations combine two real numbers to generate a unique single real number. So we can look at these operations as functions on the set

$$\mathbb{R} \times \mathbb{R} = \{(a, b) : a \in \mathbb{R} \text{ and } b \in \mathbb{R}\}$$

defined by

$$\begin{array}{rccc} + & : & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & & (a, b) & \longrightarrow & a + b \end{array}$$

and

$$\begin{array}{rccc} \cdot & : & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & & (a, b) & \longrightarrow & a \cdot b \end{array}$$

These operations are examples of a binary operation. The general definition of a binary operation is as follows.

Definition 3.1
A **binary operation** on a set S is a mapping $*$ that assigns to each ordered pair of elements of S a uniquely determined element of S. That is, $* : S \times S \longrightarrow S$ is a mapping. The set S is said to be **closed** under the operation $*$.

The image $*(a, b)$ will be denoted by $a * b$.

Example 3.1
Addition and multiplication are binary operations on the set $\mathbb{Z}$ of integers so that this set is closed under these operations. However, $\mathbb{Z}$ is not closed under the operation of division since $1 \div 2$ is not an integer.■

Example 3.2
The "ordered pair" statement in Definition 3.1 is critical. For example, consider the binary operation $*$ defined on the set $\mathbb{N}$ by $a * b = a^b$. Then $2 * 3 = 2^3 = 8$ and $3 * 2 = 3^2 = 9$. That is, $2 * 3 \neq 3 * 2$.■

Example 3.3 *(Cayley's Tables)*
The idea of a binary operation is just a way to produce an element of a set from a given pair of ordered elements of the same set. In the case of a finite set we could list the rule in a table which we'll call a *multiplication table* or Cayley's table. For example, the following is the multiplication table of a binary operation $* : \{a, b\} \times \{a, b\} \longrightarrow \{a, b\}$.

*	a	b
a	a	b
b	b	a ■

In studying binary operations on sets, we tend to be interested in those operations that have certain properties which we discuss next.

Definition 3.2
A binary operation $*$ on a set S is said to be **associative** if it satisfies the associative law:

$$a * (b * c) = (a * b) * c$$

for all $a, b, c \in S$.

The associative property allows us to speak of $a * b * c$ without having to worry about whether we should find the answer to $a * b$ first and then that answer "multiplied" by c rather than evaluate $b * c$ first and then "multiply" a with that answer. Which ever way we process the expression we end up with the same element of the set. Note though that it does not say we can do the product in any order (i.e. $a * b$ and $b * a$ may not have the same value).

Example 3.4
1. The operations " $+$ " and $\cdot$ on $\mathbb{R}$ are associative.
2. The operation " $-$ " on $\mathbb{R}$ is not associative since $2 - (3 - 4) \neq (2 - 3) - 4$. (Notice that if the associative law fails for just one triple (a, b, c) then the operation is not associative).
3. The operation $*$ defined by $a * b = a^b$ on the set $\mathbb{N}$ is not associative since $2 * (3 * 2) = 512$ and $(2 * 3) * 2 = 64$.■

Definition 3.3
A binary operation $*$ on a set S is said to be **commutative** if it satisfies the condition:

$$a * b = b * a$$

for all $a, b, \in S$. In this case, the order in which elements are combined does not matter.

Remark 3.1
When a set with a binary operation is given by a Cayley's table then the operation is commutative if and only if equal elements appear in all positions that are symmetrically placed relative to the diagonal from upper left to lower right. That is, to check whether an operation defined by a Cayley's table is commutative, simply draw a diagonal line from upper left to lower right, and see if the table is symmetric about this line. For example, the operation $*$ defined by the table below is commutative.

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Example 3.5
The binary operations of addition and multiplication on $\mathbb{R}$ are both commutative. However, the binary operation of subtraction on $\mathbb{R}$ does not satisfy the commutative law since $5 - 7 \neq 7 - 5$.■

Example 3.6
The binary operation on $\mathbb{R}$ defined by $a * b = a + b - 1$ is commutative since

$$a * b = a + b - 1 = b + a - 1 = b * a.$$■

Example 3.7
Show that the binary operation on $\mathbb{R}$ defined by $a * b = 1 + ab$ is commutative but not associative.

Solution.
For any real numbers a and b we have $a * b = 1 + ab = 1 + ba = b * a$ where we used the fact that multiplication in $\mathbb{R}$ is commutative. Now, by letting $a = 0, b = 1$, and $c = -1$ then $a * (b * c) = a * 0 = 1$ and $(a * b) * c = 1 * c = 0$. Thus, $*$ is not associative.■

Definition 3.4
Let S be a set on which there is a binary operation $*$. An element e of this set is called a **left identity** if for all $a \in S$, we have $e * a = a$. Similarly, an element e is a **right identity** if $a * e = a$ for each $a \in S$.

Example 3.8
Given a binary operation on a set.

1. There might be left identities which are not right identities and vice-versa. For example, the operation $a * b = a$ on the set $\mathbb{R}$ has 2 as a right identity which is not a left identity. The set $\mathbb{R}$ with the operation $a * b = b$ has 2 as a left identity which is not a right identity.

2. There might be many left or right identity elements. The set $\mathbb{R}$ with the operation $a * b = a$, every number is a right identity. With the operation $a * b = b$, every number is a left identity.

3. There might be no left or right identity elements. For example, the set $\{2, 3, 4, \cdots\}$ has no left or right identity elements under the operation $a * b = a \cdot b$■

We tend to be familiar with the situation in which there is a unique identity. As soon as an operation has both a left and a right identity, they are necessarily unique and equal as shown in the next theorem.

Theorem 3.1
If S is a set with a binary operation $*$ that has a left identity element e_1 and a right identity element e_2 then $e_1 = e_2 = e$.

Proof.
Let $e_1 \in S$ be a left identity element and $e_2 \in S$ be a right identity element. Then

$$\begin{aligned} e_1 &= e_1 * e_2 (since\ e_2\ is\ a\ right\ identity) \\ &= e_2 (since\ e_1\ is\ a\ left\ identity) \end{aligned}$$ ■

Definition 3.5
An element which is both a right and left identity is called the **identity element**(Some authors use the term two sided identity.) Thus, an element is an identity if it leaves every element unchanged.

Remark 3.2
Note that an identity (left or right or both) for one operation does not have to be an identity for another operation. Think of addition and multiplication on the reals where the identities are 0 and 1 respectively.

Example 3.9
The operation $a * b = a + b - 1$ on the set of integers has 1 as an identity element since $1 * a = 1 + a - 1 = a$ and $a * 1 = a + 1 - 1 = a$ for all integer a.■

Example 3.10
Show that the operation $a * b = 1 + ab$ on the set of integers $\mathbb{Z}$ has no identity element.

Solution.
If e is an identity element then we must have $a * e = a$ for all $a \in \mathbb{Z}$. In particular, $1 * e = 1$. But this imply that $1 + e = 1$ or $e = 0$. Since $2 * 0 = 1 \neq 2$ then e does not exist.■

Whenever a set has an identity element with respect to a binary operation on the set, it is then in order to raise the question of inverses.

Definition 3.6
Suppose that an operation $*$ on a set S has an identity element e. Let $a \in S$. If there is an element $b \in S$ such that $a * b = e$ then b is called a **right inverse** of a. Similarly, if $b * a = e$ then b is called a **left inverse.**

Example 3.11
1. An element can have no left or right inverses. For example, the number 2 has no left or right inverse with respect to multiplication on the set of integers.

2. There might be a left inverse which is not a right inverse and vice versa. For example, consider the set $M(\mathbb{Z})$ of all functions from the set of integers into itself. Then the operation of composition is a binary operation on $M(\mathbb{Z})$. Consider the two functions $f(n) = 2n$ and

$$g(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ 4 & \text{if } n \text{ is odd} \end{cases}$$

Then $(g \circ f)(n) = n$ for all $n \in \mathbb{Z}$. That is, g is a left inverse of f. However, since

$$(f \circ g)(n) = \begin{cases} n & \text{if } n \text{ is even} \\ 8 & \text{if } n \text{ is odd} \end{cases}$$

then g is not a right inverse since $f \circ g \neq \iota_{\mathbb{Z}}$ ■

Suppose that an element $a \in S$ has both a left inverse and a right inverse with respect to a binary operation $*$ on S. Under what condition are the two inverses equal?

Theorem 3.2
Let S be a set with an associative binary operation $*$ and identity element e. Let $a, b, c \in S$ be such that $a * b = e$ and $c * a = e$. Then $b = c$.

Proof.
Indeed,

$$\begin{aligned} b &= e * b \\ &= (c * a) * b \\ &= c * (a * b) \\ &= c * e \\ &= c \ \blacksquare \end{aligned}$$

Definition 3.7
If a has both a left and right inverse then we say that a has **two-sided inverse** or simply an **inverse** element.

Example 3.12
Consider the operation $*$ on the set of integers defined by $a * b = a + b - 1$. We will show that each integer has an inverse under this operation. Indeed, let x be an integer. Let y be a right inverse of x. Then $x * y = 1$. That is, $x + y - 1 = 1$. Solving for y we find $y = -x + 2$. This is also a left inverse of x since $(-x + 2) * x = -x + 2 + x - 1 = 1$.■