Algebraic Structures

Blake A. Farman

1 Binary Operations

Definition 1.1 Binary Operation. Assume X is a set. A **binary operation on** X is a function $*\colon X \times X \to X$.

As a matter of convenience, we typically write $x_1 * x_2$ instead of $*(x_1, x_2)$. ◊

Definition 1.2 Associative Binary Operation. We say a binary operation, $*$, on a set, X, is **associative** if for all $x_1, x_2, x_3 \in X$,

$$(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3).$$

◊

Definition 1.3 Commutative Binary Operation. We say a binary operation, $*$, on a set, X, is **commutative** if for all $x_1, x_2 \in X$,

$$x_1 * x_2 = x_2 * x_1.$$

We say a binary operation is **non-commutative** if it is not a commutative operation. ◊

Example 1.4 For any of the familiar sets of numbers

- The natural numbers, $\mathbb{N}$,
- The integers, $\mathbb{Z}$,
- The rationals, $\mathbb{Q}$,
- The reals, $\mathbb{R}$,
- The complex numbers, $\mathbb{C}$

the familiar arithmetic operations $+$ and $\times$ are associative, commutative operations. □

Definition 1.5 Assume Σ is a set. A **word** with letters from Σ is a string consisting of elements from Σ.

We write Σ^* for the set of all possible words with letters from Σ. Note that this set contains the **empty word**, ε. ◊

Example 1.6 Let $\Sigma = \{0, 1\}$. A word with letters from Σ is a string of 0's and 1's, such as

$$1010101010110011111.$$

We can define the concatenation operation on the words of Σ by joining the two strings together to form a single word. The result of concatenating the words $w_1 = 01010$ and $w_2 = 01011100$ is

$$w_1 w_2 = 0101001011100$$

Note that this operation is ***non-commutative***:

$$w_2 w_1 = 0101110001010 \neq 0101001011100 = w_1 w_2$$

□

Definition 1.7 Identity. We say a binary operation, $*$, on a set, X, has an **identity** if there exists an element $e \in X$ such that for all $x \in X$,

$$e * x = x \qquad \text{and} \qquad x * e = x$$

◊

Example 1.8

- The operation $+$ on one of the usual number systems $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ has identity 0 because for all numbers x, $x + 0 = x = 0 + x$.
- The operation $+$ on one of the usual number systems $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ has identity 1 because for all numbers x, $x \times 1 = x = 1 \times x$.
- The operation of concatenation on words has the empty string, ε, as its identity.

□

Definition 1.9 Inverse. Assume $*$ is a binary operation on the set X with identity $e \in X$. We say $x \in X$ has an **inverse** (with respect to $*$) if there exists $y \in X$ such that

$$x * y = e \qquad \text{and} \qquad y * x = e$$

For a general operation, we typically write x^{-1} for the inverse of x. If the operation is addition, then we write $-x$ instead. ◊

Example 1.10 For each of the number systems except the natural numbers $(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$, the operation $+$ admits an inverse for every element x, which is just the negative $-x$.

For the number systems $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, the operation $\times$ also admits an inverse for every non-zero element, x. In the reals (hence also the rationals), the inverse is $x^{-1} = 1/x$. For the complex numbers, the inverse is slightly more complicated:

$$(a + bi)^{-1} = \frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a - bi}{a^2 - (bi)^2} = \frac{a - bi}{a^2 + b^2}$$

□

2 Monoids

Definition 2.1 Monoid. A **monoid** is a set, M, equipped with a binary operation $*\colon M \times M \to M$ that is associative and has an identity, e_M. ◊

Example 2.2

- The binary operation $+$ endows each of the number systems $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ with the structure of an additive monoid.
- The binary operation $\times$ endows each of the number systems $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ with the structure of a multiplicative monoid.

- The concatenation operation endows Σ^* with the structure of a multiplicative monoid, where we think of concatenation, $w_1 w_2$, playing the role of multiplication.

□

3 Groups

Definition 3.1 Group. A set G equipped with an operation $*$ is a **group** if

1. G is a Monoid under $*$, andevery $g \in G$ has an inverse under $*$

If the operation is commutative, then we say the group is **abelian**. ◊

Example 3.2 All of the usual number systems are groups under addition except for $\mathbb{N}$ because the positive integers *do not* have inverses that are elements of $\mathbb{N}$. For example, for all $n \in \mathbb{N}$,

$$1 + n \geq 1 + 0 = 1 > 0$$

implies that 1 does not have an inverse in $\mathbb{N}$. Since addition is commutative, we say that each of $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are additive abelian groups. □

Example 3.3 For each of the number systems, multiplication *never* provides a group structure. This is because each one contains the additive identity 0, which does not have an inverse. We can prove this by contradiction: Assume for contradiction 0 has a multiplicative inverse. Then

$$1 = 0 \times 0^{-1} = 0$$

a contradiction.

However, if we remove the additive identity, then we do obtain a group structure for $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ under multiplication. These are commonly referred to as the **multiplicative group of units** $\mathbb{Q}^\times$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$. Note these are all examples of abelian groups. □

4 Rings

Definition 4.1 Ring. A set A equipped with two operations $+$ and $\times$ is said to be a **ring** if

1. A is an abelian group under $+$,
2. A is a monoid under $\times$,
3. These two structures are *compatible* in the sense that for all $a_1, a_2, a_3 \in A$,

$$a_1 \times (a_2 + a_3) = a_1 \times a_2 + a_1 \times a_3, \text{ and}$$
$$(a_1 + a_2) \times a_3 = a_1 \times a_3 + a_2 \times c_2$$

We say A is a **commutative ring** if the operation $\times$ is commutative. ◊

Definition 4.2 Field. A set F equipped with two operations $+$ and $\times$ is said to be a **field** if $(F, +\times)$ is a ring and $(F \setminus \{0\}, \times)$ is a group. ◊

Remark 4.3 The condition that $(F \setminus \{0\}, \times)$ is a group just ensures that every non-zero element of F has a multiplicative inverse.

Example 4.4 All of the number systems except $\mathbb{N}$ form rings under addition and multiplication. This follows from the fact that multiplication distributes over addition. This means $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are all commutative rings.

The ring $(\mathbb{Z}, +, \times)$ is *not* a field because, for example, the multiplicative inverse of 2 is $1/2 \notin \mathbb{Z}$. However, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are all fields. $\square$