Algebraic Structures

Ji, Yong-hyeon

February 8, 2025

We cover the following topics in this note.

- Group, Ring, Field
- Vector Space, Module

Binary Operation

Definition. Let S be a nonempty set. A **binary operation on** S is a function

$$* : S \times S \to S,$$

which satisfies $*(a, b) \in S$ for all $a, b \in S$. In other words, for every ordered pair $(a, b) \in S \times S$, the element $*(a, b)$ is uniquely determined and belongs to S.

Semi-group

Definition. An algebraic structure $(S, *)$ is called a **semigroup** if and only if:

(i) $S \neq \emptyset$,

(ii) $* : S \times S \to S$ is a binary operation on S,

(iii) $*$ is *associative*, i.e.,

$$\forall\, x, y, z \in S, \quad (x * y) * z = x * (y * z).$$

Monoid

Definition. A **monoid** is a semigroup $(S, *)$ such that

$$\exists\, e \in S : \ \forall\, x \in S,\ e * x = x = x * e.$$

The element $e \in S$ is called the *identity element* with respect to the operation $*$.

Group

Definition. A *group* is a monoid $(S, *)$ in which every element has an *inverse*:

$$\forall x \in S,\ \exists y \in S:\ x * y = e \wedge y * x = e.$$

For each $x \in S$, any element $y \in S$ is called an *inverse* of x, and is commonly denoted $y = x^{-1}$.

Module

Definition. Let R be a ring with unity and M be a set. A *module* over R is a structure $(M, +, \cdot)$ satisfying:

(*) $M \neq \varnothing$.

(*) $(M, +)$ is an abelian group with identity element $0 \in M$.

(*) $\cdot : R \times M \to M$ is a function called *scalar multiplication*.

(*) The following axioms hold:

$$\forall r \in R,\ \forall m, n \in M:\quad r \cdot (m + n) = r \cdot m + r \cdot n,$$

$$\forall r, s \in R,\ \forall m \in M:\quad (r + s) \cdot m = r \cdot m + s \cdot m,$$

$$\forall r, s \in R,\ \forall m \in M:\quad (rs) \cdot m = r \cdot (s \cdot m),$$

$$\forall m \in M:\quad 1_R \cdot m = m,$$

where 1_R denotes the multiplicative identity in R.

Thus, formally,

$$(M, +, \cdot) \text{ is a module over } R \iff$$

$$\left[\begin{array}{l} M \neq \varnothing, \\ (M, +) \text{ is an abelian group with identity } 0, \\ \cdot : R \times M \to M, \\ \forall r \in R,\ \forall m, n \in M:\quad r \cdot (m + n) = r \cdot m + r \cdot n, \\ \forall r, s \in R,\ \forall m \in M:\quad (r + s) \cdot m = r \cdot m + s \cdot m, \\ \forall r, s \in R,\ \forall m \in M:\quad (rs) \cdot m = r \cdot (s \cdot m), \\ \forall m \in M:\quad 1_R \cdot m = m. \end{array}\right]$$

Vector Space

Definition. Let F be a field. A *vector space* over F is a structure $(V, +, \cdot)$ satisfying:

(i) $V \neq \emptyset$.

(ii) $(V, +)$ is an abelian group with identity element $0 \in V$.

(iii) $\cdot : F \times V \to V$ is a function called *scalar multiplication*.

(iv) The following axioms hold:

$$\forall a, b \in F,\ \forall u, v \in V: \quad a \cdot (u + v) = a \cdot u + a \cdot v,$$

$$\forall a, b \in F,\ \forall v \in V: \quad (a + b) \cdot v = a \cdot v + b \cdot v,$$

$$\forall a, b \in F,\ \forall v \in V: \quad a \cdot (b \cdot v) = (ab) \cdot v,$$

$$\forall v \in V: \quad 1_F \cdot v = v,$$

where 1_F denotes the multiplicative identity in F.

Thus, formally,

$$(V, +, \cdot) \text{ is a vector space over } F \iff$$

$$\left[\begin{array}{l} V \neq \emptyset, \\ (V, +) \text{ is an abelian group with identity } 0, \\ \cdot : F \times V \to V, \\ \forall a, b \in F,\ \forall u, v \in V: \quad a \cdot (u + v) = a \cdot u + a \cdot v, \\ \forall a, b \in F,\ \forall v \in V: \quad (a + b) \cdot v = a \cdot v + b \cdot v, \\ \forall a, b \in F,\ \forall v \in V: \quad a \cdot (b \cdot v) = (ab) \cdot v, \\ \forall v \in V: \quad 1_F \cdot v = v. \end{array}\right]$$

1 Introduction

Algebraic structures are defined by sets equipped with one or more operations that satisfy specified axioms. These axioms guarantee, for example, that equations involving the operations behave in predictable ways. In this article we examine how the equation

$$a * b = c$$

(or its suitable variant) is interpreted in each context. We provide examples showing:

- In a *semigroup* the operation is associative and closed,
- In a *monoid* an identity element exists,
- In a *group* every element has an inverse (yielding unique solutions),
- In a *module* equations can involve both the additive structure and scalar multiplication over a ring,
- In a *vector space* (a module over a field) the additional invertibility of nonzero scalars facilitates solving linear equations.

2 Semigroups

Definition 1 (Semigroup)**.** A *semigroup* is a pair $(S, *)$ where S is a nonempty set and

$$* : S \times S \to S$$

is a binary operation satisfying the associativity axiom:

$$\forall\, a, b, c \in S, \quad (a * b) * c = a * (b * c).$$

In a semigroup the equation

$$a * b = c$$

illustrates that the result is always an element of S (closure), and the grouping of operations is unambiguous (associativity). However, since there is no guarantee of an identity or inverses, solving for one variable given the others may not be possible or unique.

Example 1 (Addition on $\mathbb{N}$)

Let $S = \mathbb{N} = \{1, 2, 3, \dots\}$ and define $*$ as addition. Then:

$$3 + b = 7 \quad \Longrightarrow \quad b = 4,$$

provided that $7 \geq 3$. Note that if we choose $a = 5$ and $c = 3$, no solution exists in $\mathbb{N}$.

Example 2 (String Concatenation)

Let S be the set of all nonempty strings over a fixed alphabet and define $*$ as concatenation. For instance, with

$$a = \text{“Hello”}, \quad b = \text{“World”},$$

we have

$$a * b = \text{“HelloWorld”}.$$

In this semigroup, while concatenation is associative and closed, an equation like

$$a * x = c,$$

may have multiple or no solutions because the decomposition of c is not necessarily unique.

3 Monoids

Definition 2 (Monoid)**.** A *monoid* is a semigroup $(M, *)$ that contains an *identity element* e satisfying:

$$\forall\, a \in M, \quad a * e = e * a = a.$$

In a monoid the equation

$$a * b = c$$

may be interpreted using the identity. However, without the existence of inverses, “solving” such equations (i.e., undoing the operation) is not always possible.

Example 1 (Nonnegative Integers $\mathbb{N}_0$ Under Addition)

Let $M = \mathbb{N}_0 = \{0, 1, 2, \dots\}$ with addition and 0 as the identity. Then:

$$3 + b = 7 \quad \Longrightarrow \quad b = 4.$$

Conversely, if $a = 8$ and $c = 5$, there is no $b \in \mathbb{N}_0$ satisfying

$$8 + b = 5,$$

since subtraction may lead out of $\mathbb{N}_0$.

Example 2 (Strings Including the Empty String)

Let M be the set of all finite strings over an alphabet including the empty string ε, with concatenation as the operation. The empty string acts as the identity:

$$\varepsilon * s = s * \varepsilon = s.$$

For the equation

$$\text{“Hi”} * x = \text{“HiThere”},$$

one solution is

$$x = \text{“There”}.$$

Again, note that the lack of invertibility means that not every such equation is guaranteed to have a solution.

4 Groups

Definition 3 (Group)**.** A *group* is a monoid $(G, *)$ in which every element has an inverse. That is,

$$\forall\, a \in G, \quad \exists\, a^{-1} \in G \text{ such that } a * a^{-1} = a^{-1} * a = e.$$

In a group the equation

$$a * b = c$$

has the additional property that a unique solution exists for any one of the variables. This is because the existence of inverses allows us to “undo” the operation.

Example 1 (Integers Under Addition)

Let $G = \mathbb{Z}$ with addition. Given

$$a + b = c,$$

for any $a, c \in \mathbb{Z}$ the unique solution for b is

$$b = c - a.$$

For example, if $3 + b = 7$, then $b = 7 - 3 = 4$.

Example 2 (Nonzero Real Numbers Under Multiplication)

Consider the group $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ with multiplication. The equation

$$a \cdot b = c,$$

has the unique solution

$$b = \frac{c}{a},$$

since every nonzero real number a has an inverse $a^{-1} = \frac{1}{a}$. For instance, if $2 \cdot b = 8$, then $b = \frac{8}{2} = 4$.

5 Modules

Definition 4 (Module)**.** Let R be a ring with unity. A *module* over R is a triple $(M, +, \cdot)$ where:

(i) $(M, +)$ is an abelian group (with identity 0),

(ii) $\cdot : R \times M \to M$ is scalar multiplication,

(iii) The following axioms hold for all $r, s \in R$ and $m, n \in M$:

$$r \cdot (m + n) = r \cdot m + r \cdot n,$$

$$(r + s) \cdot m = r \cdot m + s \cdot m,$$

$$(rs) \cdot m = r \cdot (s \cdot m),$$

$$1_R \cdot m = m.$$

In a module, equations may involve both the additive structure and scalar multiplication. For example, the equation

$$r \cdot x = m$$

asks for an element $x \in M$ such that when scaled by $r \in R$ the result is m.

Example 1 (The $\mathbb{Z}$-Module $\mathbb{Z}$)

View $\mathbb{Z}$ as a module over itself. Consider:

$$2 \cdot x = 6.$$

Since scalar multiplication in a $\mathbb{Z}$-module is just ordinary multiplication, the solution is $x = 3$. In contrast, the equation

$$2 \cdot x = 5$$

has no solution in $\mathbb{Z}$ because 5 is not an even number.

Example 2 (A Linear Equation in $\mathbb{Z}^2$)

Let $M = \mathbb{Z}^2$ be a $\mathbb{Z}$-module and consider the equation

$$2 \cdot (x_1, x_2) + 3 \cdot (y_1, y_2) = (8, 11).$$

This expands to the system of linear Diophantine equations:

$$2x_1 + 3y_1 = 8, \quad 2x_2 + 3y_2 = 11.$$

Solutions exist if and only if each coordinate equation is consistent in $\mathbb{Z}$.

6 Vector Spaces

Definition 5 (Vector Space)**.** Let F be a field. A *vector space* over F is a module $(V, +, \cdot)$ satisfying the module axioms (with F replacing R) and, importantly, where every nonzero scalar in F is invertible.

Equations in a vector space benefit from both the additive structure and the rich scalar multiplication properties provided by the field.

Example 1 (Vector Addition in $\mathbb{R}^2$)

Let $V = \mathbb{R}^2$. Consider the equation

$$v + w = z.$$

If

$$v = (1, 2) \quad \text{and} \quad z = (4, 7),$$

then solving for w gives

$$w = z - v = (4 - 1, 7 - 2) = (3, 5).$$

Example 2 (Scalar Multiplication in $\mathbb{R}^2$)

In the vector space $V = \mathbb{R}^2$, consider the equation

$$c \cdot v = w,$$

with $v = (2, 3)$ and $w = (4, 6)$. Since scalar multiplication is defined coordinate-wise and c is a scalar from $\mathbb{R}$, we obtain

$$c = \frac{4}{2} = 2,$$

which is unique because nonzero scalars in a field are invertible.

7 Conclusion

The equation $a * b = c$ (or its variants) encapsulates different aspects of algebraic structures:

- In a **semigroup**, closure and associativity guarantee that the operation is well-defined.
- In a **monoid**, the presence of an identity element allows for the natural "do-nothing" solution.
- In a **group**, every equation has a unique solution thanks to the existence of inverses.
- In a **module** and a **vector space**, additional structure from scalar multiplication enables the formulation and solution of linear equations.

These examples highlight how the abstract axioms influence the process of solving equations in each setting, providing a concrete interpretation of the algebraic structures.

8 Semigroups

Definition 6 (Semigroup)**.** A *semigroup* is a set S together with a binary operation

$$* : S \times S \to S,$$

which is associative:

$$\forall\, a, b, c \in S, \quad (a * b) * c = a * (b * c).$$

In a semigroup, the equation

$$a * b = c$$

always yields an element $c \in S$ (closure), and the grouping of operations is unambiguous (associativity). However, there is no requirement for an identity or inverses, so solving such equations (i.e., "undoing" the operation) may not be feasible or unique.

Example 1 (Non-empty Strings under Concatenation)**.** Let S be the set of all non-empty finite strings over a fixed alphabet (e.g., $\{a, b, c, \dots\}$), and define the operation $*$ as concatenation. For any strings $s, t \in S$, the concatenation $s * t$ is again a non-empty string, and concatenation is associative:

$$(s * t) * u = s * (t * u).$$

Since the empty string is excluded, there is no identity element. Thus, $(S, *)$ is a semigroup.

Example 2 (Positive Integers (Excluding 1) under Multiplication)**.** Define

$$S = \{n \in \mathbb{N} : n \geq 2\},$$

and let the operation $*$ be ordinary multiplication. Since

$$a * b = ab \in S \quad \text{for all } a, b \geq 2,$$

and multiplication is associative, $(S, \times)$ is a semigroup. Note that the multiplicative identity 1 is not in S, so no identity element exists.

9 Monoids

Definition 7 (Monoid)**.** A *monoid* is a semigroup $(M, *)$ that contains an identity element e such that

$$\forall\, a \in M, \quad e * a = a * e = a.$$

In a monoid the equation

$$a * b = c$$

can sometimes be "undone" by using the identity element—but without inverses, one cannot generally solve for an unknown.

Example 3 (Natural Numbers with Zero under Addition)**.** Let

$$M = \mathbb{N}_0 = \{0, 1, 2, \dots\},$$

with the operation $+$. Since addition is associative, and 0 serves as the identity element (because $0 + a = a + 0 = a$), $(\mathbb{N}_0, +)$ is a monoid. Notice that aside from 0, no element has an additive inverse in $\mathbb{N}_0$.

Example 4 (All Finite Strings (Including the Empty String) under Concatenation)**.** Let M be the set of all finite strings over a fixed alphabet, *including* the empty string ε. Define the operation as concatenation. The empty string ε acts as the identity since

$$\varepsilon * s = s * \varepsilon = s,$$

for every string s. Thus, $(M, *)$ is a monoid. This example is non-trivial because the set M is infinite and diverse in structure.

10 Groups

Definition 8 (Group)**.** A *group* is a monoid $(G, *)$ in which every element has an inverse. That is,

$$\forall\, a \in G, \quad \exists\, a^{-1} \in G \text{ such that } a * a^{-1} = a^{-1} * a = e.$$

In a group every equation of the form

$$a * b = c$$

can be uniquely solved for any one variable by "canceling" with the inverse.

Example 5 (Integers under Addition)**.** Let

$$G = \mathbb{Z},$$

with the operation $+$. The identity element is 0 (since $a + 0 = 0 + a = a$ for all $a \in \mathbb{Z}$), and every integer a has the inverse $-a$ (because $a + (-a) = 0$). Hence, $(\mathbb{Z}, +)$ is a group. For example, the equation

$$3 + b = 7$$

has the unique solution $b = 7 - 3 = 4$.

Example 6 (The Symmetric Group S_3)**.** The symmetric group S_3 is the set of all permutations of

three objects, with the operation being composition of functions. The identity permutation (which leaves all elements fixed) serves as the identity element. Every permutation in S_3 has an inverse (its inverse permutation), and composition is associative. Since S_3 is non-abelian (the order of composition matters), it provides a non-trivial example of a finite group.

11 Modules

Definition 9 (Module)**.** Let R be a ring with unity. An *R-module* M is an abelian group $(M, +)$ equipped with a scalar multiplication

$$\cdot : R \times M \to M,$$

satisfying, for all $r, s \in R$ and $m, n \in M$:

$$r \cdot (m + n) = r \cdot m + r \cdot n, \quad (r + s) \cdot m = r \cdot m + s \cdot m,$$

$$(rs) \cdot m = r \cdot (s \cdot m), \quad 1_R \cdot m = m.$$

In modules, equations may involve both the additive structure and the action of scalars from the ring R.

Example 7 ($\mathbb{Z}^2$ as a $\mathbb{Z}$-Module)**.** Let

$$M = \mathbb{Z}^2 = \{(a, b) \mid a, b \in \mathbb{Z}\},$$

with vector addition defined componentwise and scalar multiplication by an integer k given by

$$k \cdot (a, b) = (ka, kb).$$

Since $\mathbb{Z}^2$ is an abelian group under addition and the scalar multiplication satisfies the module axioms over the ring $\mathbb{Z}$, it forms a non-trivial $\mathbb{Z}$-module.

Example 8 ($\mathbb{Z}_6$ as a $\mathbb{Z}$-Module)**.** Let

$$M = \mathbb{Z}_6 = \{\, [0], [1], [2], [3], [4], [5] \,\},$$

the integers modulo 6, with addition modulo 6. Every abelian group is naturally a $\mathbb{Z}$-module via the operation

$$k \cdot [a] = [ka],$$

with the usual multiplication of integers followed by reduction modulo 6. Thus, $\mathbb{Z}_6$ is a non-trivial, finite $\mathbb{Z}$-module.

12 Vector Spaces

Definition 10 (Vector Space)**.** Let F be a field. A *vector space* V over F is an F-module (i.e., an abelian group $(V, +)$ with a scalar multiplication $\cdot : F \times V \to V$) satisfying all the module axioms, where every nonzero scalar has a multiplicative inverse.

In vector spaces the availability of multiplicative inverses for scalars (when nonzero) ensures that linear equations have unique solutions.

Example 9 ($\mathbb{R}^3$)**.** Let

$$V = \mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\},$$

with the usual vector addition and scalar multiplication. This three-dimensional vector space over $\mathbb{R}$ is a classic example where the equation

$$v + w = u$$

has a unique solution for any one of the vectors when the other two are known.

Example 10 (The Space of Polynomials $P_2(\mathbb{R})$)**.** Let

$$V = P_2(\mathbb{R}) = \{\, a_0 + a_1 x + a_2 x^2 \mid a_0, a_1, a_2 \in \mathbb{R} \,\},$$

the set of all real polynomials of degree at most 2. With polynomial addition and scalar multiplication defined in the usual way, $P_2(\mathbb{R})$ forms a vector space over $\mathbb{R}$. This space is non-trivial and is widely used in approximation theory and other applications.

13 Conclusion

We have presented two non-trivial, concrete examples for each of the algebraic structures considered:

- **Semigroups:** non-empty strings under concatenation and positive integers (excluding 1) under multiplication.
- **Monoids:** natural numbers (including zero) under addition and all finite strings (including the empty string) under concatenation.
- **Groups:** the group of integers under addition and the symmetric group S_3.
- **Modules:** $\mathbb{Z}^2$ and $\mathbb{Z}_6$ as $\mathbb{Z}$-modules.
- **Vector Spaces:** the three-dimensional real space $\mathbb{R}^3$ and the space of polynomials $P_2(\mathbb{R})$.

In each case, the underlying operation ensures that equations such as $a * b = c$ are well defined, and the additional axioms (e.g., existence of an identity or inverses) dictate the nature of solution methods within that structure.

References

[1] 수학의 즐거움, Enjoying Math. "수학 공부, 기초부터 대학원 수학까지, 13. 대수학 : 군, 환, 체, 가군, 벡터공간, 대수의 정의" YouTube Video, 25:57. Published October 7, 2019. URL: https://www.youtube.com/watch?v=6DP6UQ2sPus.