Algebraic Structures

Ji, Yong-hyeon

February 17, 2025

We cover the following topics in this note.

- Group, Ring, Field
- Module, Vector Space, Algebra

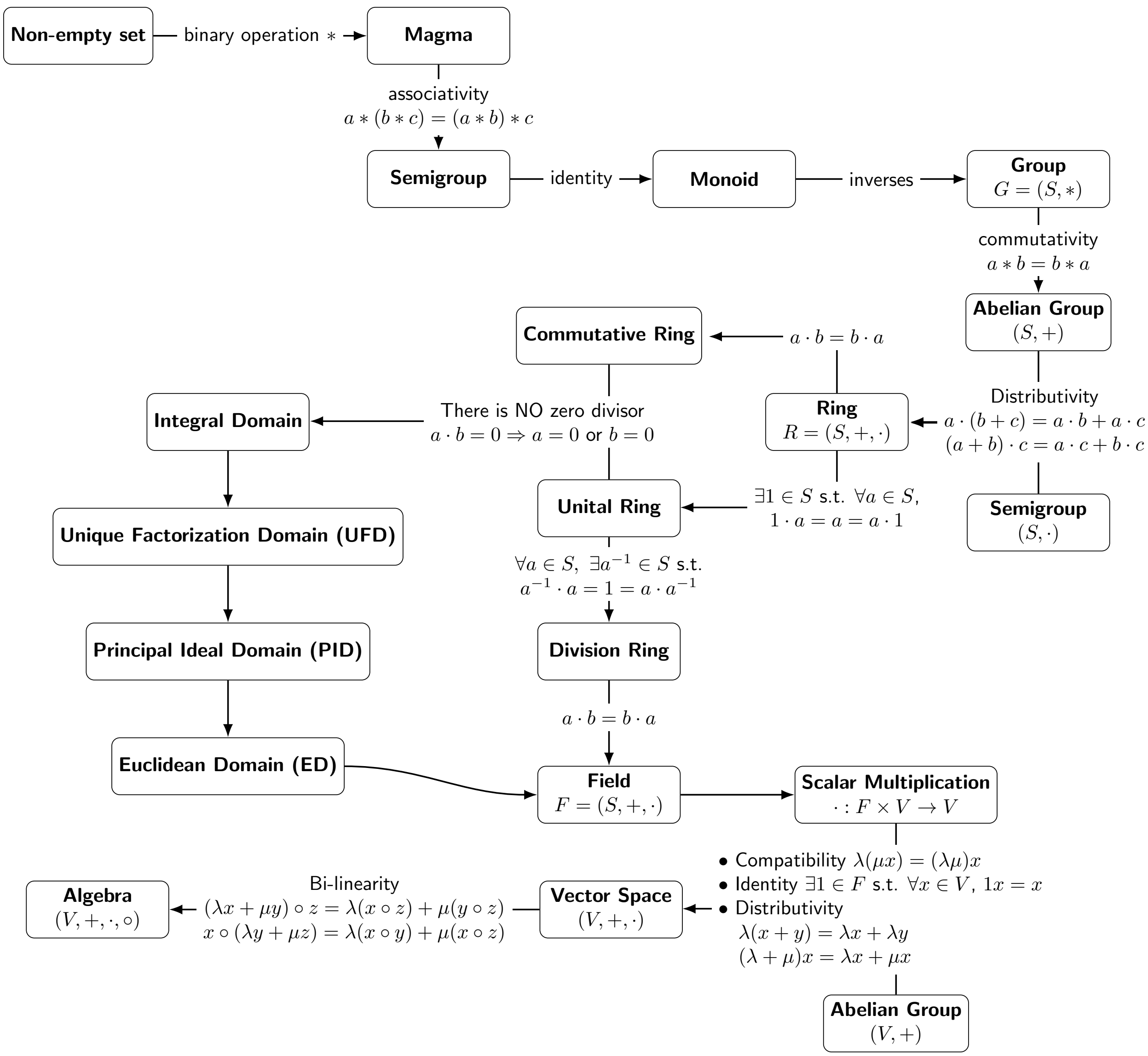

Figure 1: Algebraic Structures

Binary Operation

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

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

which assigns to each ordered pair $(a, b) \in S \times S$ an element $*(a, b) = a * b \in S$.

$$\boxed{S \times S} \;\text{—}\; (a, b) \longrightarrow \boxed{*} \;\text{—}\; a * b \longrightarrow \boxed{S}$$

Example 1. A binary operation on a set S is a rule that assigns to every ordered pair $(a, b) \in S$ an element $a * b \in S$.

- (*Addition on Integers*) Let $S = \mathbb{Z}$ and define

  $$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (a, b) \mapsto +(a, b) = a + b.$$

  This rule is a binary operation because the sum of any two integers is an integer.

- (*Maximum of Two Real Numbers*) Let $S = \mathbb{R}$ and define

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

  For any two real numbers, their maximum is again a real number, so this is a valid binary operation.

Semi-group

Definition. A **semigroup** is an algebraic structure $(S, *)$ where:

(i) $S \neq \varnothing$;

(ii) $* : S \times S \longrightarrow S$ is a binary operation that is *associative*: for all $a, b, c \in S$,

$$(a * b) * c \;=\; a * (b * c).$$

Example 2. A semigroup $(S, *)$ is a set S together with a binary operation $*$ that is associative.

- (*Positive Integers under Addition*) Let $S = \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ and define addition as the operation. For $a, b, c \in \mathbb{Z}^+$,

  $$(a + b) + c = a + (b + c).$$

  and the sum of two positive integers is again a positive integer.

- (*The Set* $\{0, 1\}$ *under Multiplication*) We consider the set

  $$S = \{0, 1\} \quad (\text{or } \mathbb{Z}_2 \text{ or } \mathbb{F}_2)$$

  and define binary operation $\times : S \times S \longrightarrow S$ by the usual multiplication of numbers. That is, $\forall a, b \in S$,

  $$a \times b = \begin{cases} 0 & : a = 0 \text{ or } b = 0 \\ 1 & : a = 1 \text{ and } b = 1 \end{cases}.$$

  The multiplication table for S is

$\times$	0	1
0	0	0
1	0	1

  We check that $(S, \times)$ is a semigroup:

  – Closure: For $a, b \in S$, the product $a \times b$ is either 0 or 1; hence $a \times b \in S$.

  – Associativity: The operation is associative.

  Note that $(S, \times)$ is in fact a *monoid* since there is the multiplicative identity 1 s.t.

  $$1 \times a = a = a \times 1 \quad \text{for all } a \in S.$$

- (*Singular Matrices under Matrix Multiplication*) Let

$$S := \left\{A \in M_{n\times n}(\mathbb{R}) : \det(A) = 0\right\}, \text{ the set of all } n \times n \text{ singular matrices over } \mathbb{R},$$

  the set of all $n \times n$ singular matrices over $\mathbb{R}$, and define the operation as matrix multiplication.

  - Closure: If A and B are singular, then $\det(AB) = \det(A)\det(B) = 0$; hence, AB is singular.
  - Associativity: Matrix multiplication is associative.

  Since the identity matrix (which is non-singular) is not in S, this semigroup does not have an identity element.

Monoid

Definition. A **monoid** is a semigroup $(S, *)$ that contains the *identity element*. That is, there exists the element $e \in S$ such that for all $a \in S$.

$$e * a \;=\; a \;=\; a * e.$$

Example 3. A monoid is a semigroup that also has an identity element.

- (Nonnegative Integers under Addition) Let $S = \mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$ and define addition on $\mathbb{Z}_{\geq 0}$.

  - Associativity: Addition is associative.
  - Identity: The element $0 \in \mathbb{Z}_{\geq 0}$ is the identity since

$$0 + a = a + 0 = a \quad \text{for each } a \in \mathbb{Z}_{\geq 0}.$$

- (All Square Matrices under Multiplication) Let $S = M_n(\mathbb{R})$, the set of all $n \times n$ matrices with real entries, and define the operation as matrix multiplication.

  - Associativity: Matrix multiplication is associative.
  - Identity: The identity matrix I_n (with ones on the diagonal and zeros elsewhere) satisfies

$$I_n A = A = A I_n \quad \text{for all } A \in M_n(\mathbb{R}).$$

Group

Definition. A **group** is a monoid $(S, *)$ in which every element has the *inverse*. That is, for all $a \in S$, there exists the element $b \in S$ such that

$$a * b = e = b * a.$$

Such $b \in S$ is called an *inverse* of a, and is commonly denoted $b = a^{-1}$.

Remark 1. A **group** is an algebraic structure $(G, *)$ satisfying the following axioms:

(G0) (Closure) $\forall a, b \in G,\ a * b \in G$;

(G1) (Associativitiy) $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$;

(G2) (Identity) $\exists e \in G : \forall a \in G,\ a * e = a = e * a$;

(G3) (Inverse) $\forall a \in G,\ \exists a^{-1} \in G : a^{-1} * a = e = a * a^{-1}$.

Example 4. A group $(G, *)$ is a monoid in which every element has the inverse.

- (Integers under Addition) Let $G = \mathbb{Z}$ and define addition on $\mathbb{Z}$.
  - Associativity: Addition is associative;
  - Identity: The integer 0 is the identity;
  - Inverse: For every $a \in \mathbb{Z}$, the element $-a \in \mathbb{Z}$ is its inverse since $a + (-a) = 0 = (-a) + a$.

  This group is abelian because addition is commutative.

- (Bijections under Composition) Let X be a nonempty set. Consider the set

  $$G = \mathcal{F} := \left\{ f \in X^X : f \text{ is a bijection} \right\}.$$

  Define the binary operation $\circ$ as the composition of functions. The structure $(\mathcal{F}, \circ)$ forms a group:
  - Associativity: Composition is associative.
  - Identity: $\mathrm{id}_X : X \to X,\ x \mapsto x$ for all $x \in X$.
  - Inverse: Every bijection f has an inverse function f^{-1}.

- (General Linear Group) Let

$$G = GL(n, \mathbb{R}) = \left\{A \in M_n(\mathbb{R}) : \det(A) \neq 0\right\},$$

with the operation of matrix multiplication.

  - Associativity: Matrix multiplication is associative.
  - Identity: The identity matrix I_n is the identity.
  - Inverse: Every matrix in $GL(n, \mathbb{R})$ is invertible. This group is generally non-abelian.

Remark 2. A group $(G, *)$ is called an **abelian group** (or **commutative group**) if the binary operation $*$ is *commutative*; that is, for all $a, b \in G$,

$$a * b = b * a,$$

Example 5 (Lie-bracket)**.** Let $\mathfrak{g}$ be a vector space over a field F. A **Lie bracket** on $\mathfrak{g}$ is a bilinear map

$$\begin{array}{rcccl} [\cdot,\cdot] & : & \mathfrak{g} \times \mathfrak{g} & \longrightarrow & \mathfrak{g} \\ & & (x, y) & \longmapsto & [x, y] = xy - yx \end{array}.$$

Then, for all $x, y, z \in \mathfrak{g}$,

$$\begin{aligned} [x, [y, z]] &= [x, yz - zy] = x(yz - zy) - (yz - zy)x = xyz - xzy - yzx + zyx, \\ [[x, y], z] &= [xy - yx, z] = (xy - yx)z - z(xy - yx) = xyz - yxz - zxy + zyx. \end{aligned}$$

Thus, Lie bracket is *not* associative.

Left and Right Cancellation

Proposition 1. *Let G be a group, and let $a, b, c, d \in G$. Let $e \in G$ is the identity of G.*

(1) (Left Cancellation) $ca = cb \implies a = b$.

(2) (Right Cancellation) $ac = bc \implies a = b$.

(3) $ab = e \iff ba = e$

Proof. (1) $ca = cb \implies c^{-1}(ca) = c^{-1}(cb) \implies (c^{-1}c)a = (c^{-1}c)b \implies ea = eb \implies a = b$.

(2) $ac = bc \implies (ac)c^{-1} = (bc)c^{-1} \implies a(cc^{-1}) = b(cc^{-1}) \implies ae = be \implies a = b$.

(3) $(\Rightarrow)$ $ab = e \implies a^{-1}(ab) = a^{-1}e \implies b = a^{-1} \implies ba = e$

$(\Leftarrow)$ $ba = e \implies b^{-1}(ba) = b^{-1}e \implies a = b^{-1} \implies ab = e$

□

Uniqueness of Identity and Inverse

Proposition 2. *Let G be a group.*

(1) The identity $e \in G$ is unique.

(2) For each $a \in G$, the inverse $a^{-1} \in G$ is unique.

Proof. (1) Let e, e' are identities of G. Then

$$e \underset{e' \text{ is an identity of } G}{\boxed{=}} ee' \underset{e \text{ is an identity of } G}{\boxed{=}} e'.$$

(2) Let a_1^{-1}, a_2^{-1} are inverses of $a \in G$. Then

$$aa_1^{-1} = aa_2^{-1} \implies a_1^{-1} = a_2^{-1} \quad \text{by left cancellation law.}$$

□

Ring

Definition. A **ring** is an algebraic structure $(R, +, \cdot)$ where:

(i) $(R, +)$ is an abelian group with identity element 0: that is, for all $a, b, c \in R$:

- Associativity: $(a + b) + c = a + (b + c)$;
- Commutativity: $a + b = b + a$;
- Identity: There exists $0 \in R$ such that $a + 0 = a$;
- Inverse: For every $a \in R$, there exits an element $-a \in R$ with $a + (-a) = 0$.

(ii) $(R, \cdot)$ is a semigroup; that is, multiplication is *associative*:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all } a, b, c \in R.$$

(iii) Distributivity (Compatibility):
Multiplication is distributive over addition; that is, for all $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Some authors require the existence of a multiplicative identity (an element $1 \in R$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$); if so, the ring is called a ring with unity.

Example 6.

- (The Integers $\mathbb{Z}$) Consider $R = \mathbb{Z}$ with the usual addition and multiplication.
  - $(\mathbb{Z}, +)$ is an abelian group (with identity 0).
  - Multiplication is associative.
  - The distributive laws hold, i.e., $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in \mathbb{Z}$.

  This ring is also commutative and has a multiplicative identity 1.

- (Polynomial Ring $\mathbb{C}[x]$) Let $R = \mathbb{C}[x]$, the set of all polynomials in x with complex coefficients.
  - $(\mathbb{C}[x], +)$ is an abelian group (with the zero polynomial 0 as the identity).
  - Polynomial multiplication is associative.
  - The distributive laws hold, i.e., $f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x)$ and $(f(x) + g(x))h(x) = f(x)h(x) + g(x)h(x)$ for all $f(x), g(x), h(x) \in \mathbb{C}[x]$.

  This ring is also commutative and has a multiplicative identity 1 (the constant polynomial 1).

Field

Definition. A **field** an algebraic structure $(F, +, \cdot)$ such that

(i) $(F, +)$ is an abelian group with additive identity element 0;

(ii) $(F \setminus \{0\}, \cdot)$ is a commutative group with multiplicative identity element 1, where $0 \neq 1$;

(iii) Distributivity: Multiplication is distributive over addition; that is, for all $a, b, c \in F$,

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

A field F is a commutative division ring.

Remark 3. A field is the smallest algebraic structure in which we can perform all the arithmetic operations $+, -, \times, \div$ (division by nonzero element), so in particular every nonzero element must a the multiplicative inverse.

Example 7. A field is a commutative ring with unity in which every nonzero element is invertible under multiplication.

- (The Real Numbers $\mathbb{R}$) Let $F = \mathbb{R}$ with the usual addition and multiplication.
  - $(\mathbb{R}, +)$ is an abelian group (with 0 as the additive identity)
  - $(\mathbb{R} \setminus \{0\}, \cdot)$ is an commutative group (with 1 as the multiplicative identity)
  - Multiplicative distributes over addition.

- (Finite Field $\mathbb{Z}_p$) Let p be a prime number and define

$$\mathbb{Z}_p := \{0, 1, \ldots, p-1\},$$

  with addition and multiplication defined modulo p.
  - $(\mathbb{Z}_p, +)$ is an abelian group with the additive identity 0.
  - $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ is a commutative group with the multiplicative identity 1 since every nonzero element has a unique inverse module p[1].
  - The distributive laws hold.

[1] By Bézout's identity, for $a, b \in \mathbb{Z}$, $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = \gcd(a, b)$. Let p be a prime. Then for any integer $a \in \mathbb{Z}$, $\exists x, y$ s.t. $ax + py = \gcd(a, p) = 1$, and so $ax \equiv 1 \pmod{p}$.

Module

Definition. Let R be a ring with unity 1_R. An R-**module** is an structure $(M, +, \cdot)$ consisting of an abelian group $(M, +)$ together with a scalar multiplication $\cdot : R \times M \longrightarrow M$ that satisfies the following axioms for all $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$:

(i)[a] $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$

(ii)[b] $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

(iii)[c] $(r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$

(iv)[d] $1_R \cdot m = m$.

[a] Distributivity over Module Addition
[b] Distributivity over Ring Addition
[c] Associativity of Scalar Multiplication
[d] Unital Property (if R is unital)

Remark 4. Consider R-module $(M, +, \cdot)$. Let $m \in M$. Since $0_R = 0_R + 0_R$, we have

$$0_R \cdot m = (0_R + 0_R) \cdot m = 0_R \cdot m + 0_R \cdot m.$$

Then

$$0_R \cdot m - 0_R \cdot m = 0_R \cdot m + 0_R \cdot m - 0_R \cdot m,$$

and so $0_M = 0_R \cdot m + 0_M$, i.e., $0_M = 0_R \cdot m$.

Vector Space

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

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

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

(iii) The following axioms hold: for all $a, b \in F$ and $u, v \in V$,

  (a) $a \cdot (u + v) = a \cdot u + a \cdot v$.

  (b) $(a + b) \cdot v = a \cdot v + b \cdot v$.

  (c) $a \cdot (b \cdot v) = (ab) \cdot v$.

  (d) $1_F \cdot v = v$ where 1_F denotes the multiplicative identity in F.

In other words, we say V is a vector space over a field F if V is a F-module

Algebra over a Field

Definition. Let F be a field. An F-**algebra** is a quadruple $(V, +, \cdot, \circ)$ where

(i)[a] $(V, +)$ is an abelian group (with additive identity 0).

(ii)[b] $(V, +, \cdot)$ is an F-vector space. That is, for all $x, y \in V$ and $\lambda, \mu \in F$,

- $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$,
- $(\lambda + \mu)x = \lambda \cdot x + \lambda \cdot x$,
- $(\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x)$,
- $1_F \cdot x = x$.

(iii)[c] There is a binary operation

$$\circ : V \times V \to V,$$

which is F-bilinear. That is, for all $x, y, z \in V$ and all $\lambda \in F$,

$$(\lambda x + y) \circ z = \lambda(x \circ z) + (y \circ z),$$
$$x \circ (\lambda y + z) = \lambda(x \circ y) + (x \circ z).$$

[a] Abelian Group Structure
[b] Vector Space Structure
[c] Algebra Multiplication

An algebra $(V, \circ)$ over a ring F, where F is a field and the F-module is a vector space.

References

[1] 수학의 즐거움, Enjoying Math. “수학 공부, 기초부터 대학원 수학까지, 13. 대수학 : 군, 환, 체, 가군, 벡터공간, 대수의 정의” YouTube Video, 27:06. Published October 7, 2019. URL: `https://www.youtube.com/watch?v=6DP6UQ2sPus`.