A Brief Introduction to Algebraic Systems

1 Groups

Definition 1.1: A Group is a non-empty set \( G \), along with a binary operation, \( * \), such that for \( a, b, c \in G \),

\[
\begin{align*}
\text{G-1)} & \quad a * b \in G \quad \text{(closure)} \\
\text{G-2)} & \quad (a * b) * c = a * (b * c) \quad \text{(associative)} \\
\text{G-3)} & \quad \text{There exists a unique element } e \in G \text{ such that } a * e = e * a = a, \quad \text{for every } a \in G. \\
& \quad \text{(identity)} \\
\text{G-4)} & \quad \text{For every } a \in G, \text{ there exists a unique element } a^{-1} \in G \text{ such that } a * a^{-1} = a^{-1} * a = e. \\
& \quad \text{(inverse)}
\end{align*}
\]

Definition 1.2: A group \( G \) is said to be abelian or (commutative) if \( a * b = b * a \), for all \( a, b \in G \).

Remark 1.1: A non-empty set \( S \) is called a semi-group if the binary operation “*” satisfies axioms G-1 and G-2 only.

2 Rings

Definition 2.1 A Ring is a non-empty set \( R \) with two binary operations: “+” and “*”, such that

\[
\begin{align*}
\text{R-1)} & \quad \text{R forms an abelian group under the operation +, i.e., for all } a, b, c \in R, \\
& \quad \text{i) } a + b \in R \\
& \quad \text{ii) } a + b = b + a \\
& \quad \text{iii) } (a + b) + c = a + (b + c) \\
& \quad \text{iv) There is a unique identity element } 0 \in R \text{ such that } a + 0 = a \quad \text{for every } a \in R. \\
& \quad \text{v) There exists a unique } -a \in R \text{ such that } a + (-a) = 0 \quad \text{for every } a \in R. \\
\text{R-2)} & \quad \text{R forms a semi-group under the operation *}, \text{ i.e.,} \\
& \quad \text{i) } a * b \in R \\
& \quad \text{ii) } (a * b) * c = a * (b * c)
\end{align*}
\]
R-3) The operation $\ast$ is distributive with respect to $\oplus$, i.e., for $a, b, c \in \mathcal{R}$,

\[
\begin{align*}
  a \ast (b + c) &= a \ast b + a \ast c \\
  (b + c) \ast a &= b \ast a + c \ast a.
\end{align*}
\]

Definition 2.2

- A **Commutative Ring** is a ring $\mathcal{R}$ that satisfies the commutative law with respect to the operation “$\ast$”.

- A **Ring with Unity** is a ring $\mathcal{R}$ that has an identity element $e$ with respect to the operation “$\ast$”.

- A **Division Ring** or (Skew Field) is a ring with all its non-zero elements forming a group under “$\ast$” operation, i.e., there exists an inverse $a^{-1} \in \mathcal{R}$ for all $a \neq 0, a \in \mathcal{R}$.

3 Fields

**Definition 3.1:** A **Field** $\mathcal{K}$ is a commutative ring in which set of non-zero elements form a group under “$\ast$” operation.

In other words, a field $\mathcal{K}$ is an abelian group with 0 as its identity under “$+$” operation, and $\mathcal{K} - \{0\}$ forms an abelian group with $e$ as its identity under the “$\ast$” operation satisfying the distributive law: $a \ast (b + c) = a \ast b + a \ast c$ and $(a + b) \ast c = a \ast c + b \ast c$ for all $a, b, c \in \mathcal{K}$.

4 Vector Spaces

**Definition 4.1:** A non-empty set $\mathcal{V}$ is said to be a **Vector Space** over a field $\mathcal{K}$ if it consists of a set of elements termed “vectors” and two binary operations: “$\oplus$”, a vector addition, and “$\cdot$”, a scalar multiplication, such that for $\vec{u}, \vec{v}, \vec{w} \in \mathcal{V}$ and $\alpha, \beta \in \mathcal{K}$,

\[
\begin{align*}
  \text{V-1)} \quad &\vec{u} \oplus \vec{v} \in \mathcal{V} \quad \text{(closure)} \\
  \text{V-2)} \quad &\vec{u} \oplus \vec{v} = \vec{v} \oplus \vec{u} \quad \text{(commutative)} \\
  \text{V-3)} \quad &\text{For all } \vec{u} \in \mathcal{V}, \text{ there exists a unique } \vec{0} \in \mathcal{V} \text{ such that } \vec{u} \oplus \vec{0} = \vec{u}. \\
  \text{V-4)} \quad &\vec{u} \oplus (-\vec{u}) = \vec{0} \quad \text{for every } \vec{u} \in \mathcal{V}. \\
  \text{V-5)} \quad & (\vec{u} \oplus \vec{v}) \oplus \vec{w} = \vec{u} \oplus (\vec{v} \oplus \vec{w}) \quad \text{(associative)} \\
  \text{V-6)} \quad &\alpha \cdot \vec{u} \in \mathcal{V} \\
  \text{V-7)} \quad &\alpha \cdot (\beta \cdot \vec{u}) = (\alpha \cdot \beta) \cdot \vec{u} \quad \text{("\cdot" is associative).} \\
  \text{V-8)} \quad &\vec{e} \cdot \vec{u} = \vec{u} \quad \text{for all } \vec{u} \in \mathcal{V}, \text{ where } \vec{e} \text{ is the identity element of } \mathcal{K} \text{ under "$\ast$"}. \]
V-9) \( \alpha \cdot (\vec{u} \oplus \vec{v}) = \alpha \cdot \vec{u} + \alpha \cdot \vec{v} \)

V-10) \( (\alpha + \beta) \cdot \vec{u} = \alpha \cdot \vec{u} + \beta \cdot \vec{u} \)

**Remark 4.1:** The vector space \( V \) forms an abelian group under the vector addition \( \oplus \).

**Remark 4.2** An \( n \)-dimensional vector space \( V \) over a field \( K \) consists of \( n \)-tuples of elements in the field \( K \), which can be written as

\[
\vec{u} = (u_1, u_2, \ldots, u_n)^T \\
\vec{v} = (v_1, v_2, \ldots, v_n)^T, \quad \forall \, \vec{u}, \vec{v} \in V
\]

where \( u_1, \ldots, u_n, v_1, \ldots, v_n \in K \).

The vector addition, \( \oplus \), is defined by

\[
\vec{u} \oplus \vec{v} = (u_1, u_2, \ldots, u_n) \oplus (v_1, v_2, \ldots, v_n) \\
= (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n)
\]

where the \( + \) operator is the \( + \) operator in \( K \).

And the identity for vector addition \( \oplus \) is \( \vec{0} = (0, \ldots, 0)^T \). The scalar multiplication, \( \cdot \), is defined by

\[
\alpha \cdot \vec{u} = (\alpha \ast u_1, \alpha \ast u_2, \ldots, \alpha \ast u_n)^T, \quad \text{for} \quad \alpha \in K
\]

where the \( \ast \) operator is the \( \ast \) operator in \( K \). One can verify that the vector addition and scalar mutiplication defined above satisfy axioms V-1) to V-10). We usually write \( V = K^n \) for this case, where \( K \) is usually \( \mathbb{R} \) or \( \mathbb{C} \).

5 **Algebras**

**Definition 5.1:** An *Algebra* over a field \( K \), is a set \( A \), which is a vector space over \( K \) along with a vector multiplication, \( \otimes \), such that for \( a, b, c \in A \) and \( \lambda \in K \),

A-1) \( a \otimes b \in A \)

A-2) \( \lambda \cdot (a \otimes b) = (\lambda \cdot a) \otimes b = a \otimes (\lambda \cdot b) \)

A-3) \( a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c \) and \( (a \oplus b) \otimes c = a \otimes c \oplus b \otimes c \)

**Remark 5.1:** If \( (a \otimes b) \otimes c = a \otimes (b \otimes c) \) holds for all \( a, b \in A \), then \( A \) is called an associative algebra.

6 **References:**
