Algebraic Systems

A set G together with a binary operation $+ : G \times G \to G$ is called a **group** provided the following hold.

(1) $(a + b) + c = a + (b + c)$ for all $a, b, \& c$ in G.
(2) There exists $0 \in G$ such that $a + 0 = 0 + a = a$ for all $a \in G$.
(3) For all $a \in G$ there exists a $-a \in G$ such that $a + -a = 0$.

If in addition $a+b = b+a$ for a and b in G then G is a **commutative** or **abelian group**.

Examples. $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}/n, +)$, $(\mathbb{R} - \{0\}, \cdot)$, $(2 \times 2\,\text{matrices}, +)$, but not $(2 \times 2\,\text{matrices}, \cdot)$, yet $(2 \times 2\,\text{matrices with } \det \neq 0, \cdot)$ is a group.

A set R together with two binary operations $+$ and $\cdot$ from $R \times R$ to R is called a **ring** provided the following hold.

(1) $(R, +)$ is an abelian group.
(2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, \& c$ in R.
(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, \& c$ in R.
(4) $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, \& c$ in R.

If there exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$ then R is a **ring with a unit**.

If $a \cdot b = b \cdot a$ for all a and b in R then R is a **commutative ring**.

Examples. $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$. $(2 \times 2\,\text{matrices}, +, \cdot)$, { polynomials }, $(\mathbb{Z}/n, +, \cdot)$.

A set F together with two binary operations $+$ and $\cdot$ from $F \times F$ to F is called a **field** provided the following hold.

(1) $(F, +, \cdot)$ is a commutative ring with a unit.
(2) $(F - \{0\}, \cdot)$ is an abelian group.

Examples. $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, but not $(\mathbb{Z}, +, \cdot)$. $(\mathbb{Z}/n, +, \cdot)$ is a field iff n is prime.

A field F is **ordered** provided there exists a order relation $<$ such that that following properties hold for all $x, y, z \in F$.

(1) $x < y \;\&\; y < z \implies x < z$.
(2) One and only one of the following are true: $x < y$, $x = y$, $y < x$.
(3) $x < y \implies x + z < y + z$.
(4) If $x > 0$ and $y > 0$, then $xy > 0$.

Examples. $\mathbb{R}$ and $\mathbb{Q}$ are ordered fields. $\mathbb{C}$ cannot be given an order. Niether can finite fields.

Let $(V, \oplus)$ be an abelian group and let $(F, +, \cdot)$ be a field. Then V is a **vector space** over F if there is a binary operation $\odot : F \times V \to V$, called **scalar multiplication** where the following hold.

(1) $1 \odot v = v$ for all $v \in V$.
(2) $(r \cdot s) \odot v = r \odot (s \odot v)$ for all r and s in F and v in V.
(3) $r \odot (v \oplus w) = (r \odot v) \oplus (r \odot w)$ for all $r \in F$, v and w in V.
(4) $(r + s) \odot v = (r \odot v) \oplus (s \odot v)$

The elements of V are called **vectors**. The elements of F are called **scalars**.