# 1. Field and Order Axioms

Let's start by discussing the axioms for real numbers, which are the axioms for a field. We'll also discuss the axioms for the order $>$.

**Definition 1 (Law of Composition)**

A law of composition on some set $E$ is a map $\star : E \times E \to E$. That is, if $E$ is closed under $\star$ then $\star$ is a law of composition.

(Note: We often use $E$ to represent a general set. This notation is relatively commonplace; it comes from the French language, where the French term for set is *ensemble*.)

**Definition 2 (Field)**

A field $(K, +, \cdot)$ is a particular set $K$, equipped with two laws of composition (which we commonly denote as $+$ and $\cdot$), which meets a series of properties, or axioms. The axioms are as follows:

(a) $K$ must be closed under $+$ and $\cdot$. That is, for any $k_1, k_2 \in K$, we need $k_1 + k_2 \in K$ and $k_1 \cdot k_2 \in K$.

(b) $+$ and $\cdot$ must be commutative in $K$. That is, for any $k_1, k_2 \in K$, we need $k_1 + k_2 = k_2 + k_1$ and $k_1 \cdot k_2 = k_2 \cdot k_1$.

(c) $+$ and $\cdot$ must be associative in $K$. That is, for any $k_1, k_2, k_3 \in K$, we need $k_1 + (k_2 + k_3) = (k_1 + k_2) + k_3$ and $k_1 \cdot (k_2 \cdot k_3) = (k_1 \cdot k_2) \cdot k_3$.

(d) $K$ must have distributivity of $\cdot$ over $+$. That is, for any $k_1, k_2, k_3 \in K$, we need $k_1 \cdot (k_2 + k_3) = k_1 \cdot k_2 + k_1 \cdot k_3$.

(e) $+$ and $\cdot$ must have identities in $K$. That is, we must have some elements $i_+, i_\bullet \in K$ such that for all $k \in K$, $k + i_+ = k$ and $k \cdot i_\bullet = k$. We commonly denote $0 := i_+$ and $1 := i_\bullet$.

(f) $+$ and $\cdot$ must have inverses in $K$. That is, for any $k \in K$ we must have some elements $\overline{k}, \tilde{k} \in K$ such that $k + \overline{k} = 0$ and $k \cdot \tilde{k} = 1$. We commonly denote $-k := \overline{k}$ and $k^{-1} := \tilde{k}$.

(Note: We commonly use $K$ to represent a general field. This notation is also relatively commonplace; this time, it comes from the German language, where the German term *Körper* is used.)

A few common fields include $\mathbb{R}$, the set of real numbers; $\mathbb{C}$, the set of complex numbers; and, $\mathbb{Z}_p$, the subset of the integers $\{1, ..., p\}$ for some prime $p$, all under the typical definitions of addition and multiplication.

**Definition 3 (Ring)**

If you have some set $R$ paired with two laws of composition $+$ and $\cdot$, where $(R, +, \cdot)$ would be a field iff inverses existed for $\cdot$ and $\cdot$ was commutative, then we call $R$ a ring.

Here is a theorem to give you some exposure to proofs involving fields.

**Theorem 1 (Multiplication by Additive Identity)**

Let $(K, +, \cdot)$ be a field with additive identity $0$. For any $k \in K$, we have $0 \cdot k = 0$.

**Proof.**Observe that we can write $0 = 0 + 0$. Then $0 \cdot k = (0 + 0) \cdot k$. By commutativity, we get $k \cdot (0 + 0)$. Applying distributivity yields $0 \cdot k = k \cdot 0 + k \cdot 0$. Applying commutativity to the LHS yields $k \cdot 0 = k \cdot 0 + k \cdot 0$. We can add the additive inverse of $k \cdot 0$ to yield $0 = k \cdot 0$ as required. $\square$

Going forward, for convenience, we will often say "$K$ is a field" with the two laws of composition implied.
Now we shall define the order $>$ in $\mathbb{R}$.

**Definition 4 (The Order $>$)**

We define the order $>$ in $\mathbb{R}$ as the operator satisfying the following:

(a) $>$ satisfies the trichotomy property. That is, for all $a, b \in \mathbb{R}$, either $a > b$ or $b > a$ or $a = b$.

(b) $>$ is transitive. That is, for all $a, b, c \in \mathbb{R}$, if $a > b$ and $b > c$ then $a > c$.

(c) $>$ is additive. That is, for all $a, b, c \in \mathbb{R}$, if $a > b$ then $a + c > b + c$.

(d) $>$ is multiplicative. That is, for all $a, b, c \in \mathbb{R}$, given that $a > b$, if $c > 0$ then $ac > bc$, and if $0 > c$ then $bc > ac$.

We define $a < b$ to be equivalent to $b > a$.
(Note: We don't necessarily have the same orders for other fields. For instance, in $\mathbb{C}$, is $i$ greater than $1$ or $-i$? In $\mathbb{Z}_3$, is $2$ greater than $1$?)