The Field Axioms

A *field* is a set F with binary operations $+$ ("plus") and $\cdot$ ("times") that obey the following axioms:

1. **Basic algebraic laws**

   Law of closure: If $a, b \in F$ then $a + b$ and $a \cdot b$ are both in F.

   Commutative Law: If $a, b \in F$ then $a + b = b + a$ and $a \cdot b = b \cdot a$.

   Associative Law: If $a, b, c \in F$ then

   $$a + (b + c) = (a + b) + c \quad \text{and} \quad a(bc) = (ab)c$$

   (we write multiplication without the "dot" whenever we feel like it).

   Distributive Law: If $a, b, c \in F$ then $a(b + c) = ab + ac$.

2. **Existence of identities:** There exist elements 0 and 1 in F such that for every $a \in F$: $0 + a = a$ and $1 \cdot a = a$ (we call 0 and 1 respective the "additive identity" and the "multiplicative identity").

   Remark: *Both these identity elements are unique.* For example, suppose some element $b \in F$ is an additive identity, i.e., $b + a = a$ for each $a \in F$. Then $0 + b = b$ by the definition of 0, while $b + 0 = 0$ by the property hypothesized for b. Summarizing, and using the commutative law:

   $$b = 0 + b = b + 0 = 0$$

   hence 0 is the only additive identity. Similar arguments establish the uniqueness of the multiplicative identity (an exercise, which I hope you'll work out!).

3. **Existence of inverses**

   Additive inverse: If $a \in F$ then there exists an element $b \in F$ such that $a + b = 0$ (we call b an "additive inverse" of a).

   Multiplicative inverse: If $a \in F$ and $a \neq 0$ then there exists an element b in F such that $a \cdot b = 1$.

Remarks

(a) It's the existence of the multiplicative inverse that distinguishes the integers $\mathbb{Z}$ from the rational numbers $\mathbb{Q}$ or the real numbers $\mathbb{R}$. Among the integers, only 1 has a multiplicative inverse *in* $\mathbb{Z}$.

(b) *Additive and multiplicative inverses are unique.* To see this for additive inverses, suppose b and b' are additive inverses for $a \in F$. Then $0 = a + b'$, so adding b to both sides:

$$\begin{aligned} b + 0 &= b + (a + b') \\ &= (b + a) + b' \quad \text{(Associate law of addition)} \\ &= 0 + b' \quad \text{(Commutative law of addition and ``}b\text{ an add. inverse of }a\text{'')} \\ &= b' \quad \text{(since 0 is the additive identity).} \end{aligned}$$

Thus a has only one additive inverse. We call this "$-a$".

Similarly, if $a \in F$ is not 0 then a has only one multiplicative inverse (another exercise I hope you'll do); we call this one a^{-1}, or $\frac{1}{a}$.

(c) *Examples:* We've already called attention to the fields $\mathbb{R}$ of real numbers and $\mathbb{Q}$ of rational numbers. Here are two others:

- *Quadratic extensions of the rationals.* We'll just think about one of these—you can easily supply other examples. Let $\mathbb{Q}(\sqrt{2})$ denote the set of all real numbers of the form $a + b\sqrt{2}$, where a and b are rational. Then it's easy to check that $\mathbb{Q}(\sqrt{2})$ is closed under ordinary addition and multiplication, and obeys all the axioms for a field, except possibly for the existence of multiplicative inverses. But this too is true, and I leave it to you as an exercise to prove it.
- *The field $\mathbb{C}$ of complex numbers.* We write each element of this field as $a + bi$ where a and b are real numbers and i is the "imaginary" element whose defining property is $i^2 = -1$. We define addition and multiplication in the obvious way, but for multiplication we always reduce powers of i to either 1, i, $-i$ or -1 using the equation $i^2 = -1$. Note that, in the spirit of the previous example, you can think of $\mathbb{C}$ as the "quadratic extension" $\mathbb{R}(i)$ of the real field.
- *The "binary field."* This is the two-element set $\mathbb{Z}_2 = \{0, 1\}$, with operations defined like this: $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$, $0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0$, and $1 \cdot 1 = 1$.

  Exercise: check that $\mathbb{Z}_2$ is a field. In particular, identify the additive and multiplicative identities and inverses.

Ordered Fields

An *ordered field* is a field on which there is defined on pairs of elements a relation "$<$" that obeys the following axioms:

Trichotomy: For each pair of elements $a, b \in F$, exactly one of these conditions holds: $a < b$, $\quad b < a$, $\quad$ or $\quad a = b$.

Transitivity: If $a, b, c \in F$ with $a < b$ and $b < c$ then $a < c$.

Additivity: If $a, b \in F$ with $a < b$, then $a + c < b + c$ for every $c \in F$.

Multiplicativity: If $a, b \in F$ with $a < b$ then:

- $ac < bc$ whenever $c \in F$ with $c > 0$, and
- $bc < ac$ whenever $c \in F$ with $c < 0$

Examples. The field $\mathbb{R}$ of real numbers, with its usual order, is an ordered field, as is the field $\mathbb{Q}$ of rational numbers with the order it inherits from the reals.

Proposition (Example 1.2 of our text): *If F is an ordered field then $a^2 =: a \cdot a > 0$ for every non-zero $a \in F$.*

Proof. Either $a < 0$ or $a > 0$ by Trichotomy. If $a > 0$ then $a^2 = a \cdot a > 0$ by the first multiplicative property. If $a < 0$ then the result follows in similar fashion from the second multiplicative property. □

Corollary. *In any ordered field:* $-1 < 0 < 1$.

Proof. $1 \neq 0$, hence $1 = 1^2 > 0$ by the Proposition. By additivity

$$-1 = -1 + 0 < -1 + 1 = 0$$

which completes the proof. □

Corollary. *There's no way to make $\mathbb{Z}_2$ into an ordered field.*

Proof. Suppose there's an ordering "<" on $\mathbb{Z}_2$ that *does* make it into an ordered field. Then by the previous Corollary, $0 < 1$, so by additivity $1 = 0 + 1 < 1 + 1 = 0$, i.e., both $0 < 1$ and $1 < 0$, which contradicts the trichotomy axiom. So such an ordering can't exist. □

Extra Credit Problem. Verify that the complex numbers $\mathbb{C}$, with their usual addition and multiplication, form a field. Then show that *there's no way to make $\mathbb{C}$ into an ordered field.*