Math 310
November 20, 2020 Lecture

Steven G. Krantz

November 11, 2020

Figure: This is your instructor.

The Axioms of a Field

The axioms of a field are as follows:

Definition:

A set S is called a *field* if it is equipped with a binary operation (usually called addition and denoted "+") and a second binary operation (usually called multiplication and denoted "·") such that the following axioms are satisfied:

A1. S is closed under addition: if $x, y \in S$, then $x + y \in S$.
A2. Addition is commutative: if $x, y \in S$, then $x + y = y + x$.
A3. Addition is associative: if $x, y, z \in S$, then

$$x + (y + z) = (x + y) + z.$$

A4. There exists an element, called 0, in S which is an additive identity: if $x \in S$, then $0 + x = x$.

A5. Each element of S has an additive inverse: if $x \in S$ then there is an element $-x \in S$ such that $x + (-x) = 0$.

M1. S is closed under multiplication: if $x, y \in S$, then $x \cdot y \in S$.
M2. Multiplication is commutative: if $x, y \in S$, then $x \cdot y = y \cdot x$.
M3. Multiplication is associative: if $x, y, z \in S$, then

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

M4. There exists an element, called 1, which is a multiplicative identity: if $x \in S$, then $1 \cdot x = x$.

M5. Each nonzero element of S has a multiplicative inverse: if $0 \neq x \in S$, then there is an element $x^{-1} \in S$ such that $x \cdot (x^{-1}) = 1$. The element x^{-1} is sometimes denoted by $1/x$.

D1. Multiplication distributes over addition: if $x, y, z \in S$, then $x \cdot (y + z) = x \cdot y + x \cdot z$.

The rational numbers $\mathbb{Q}$ form a field. So do the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. There are infinitely many other examples of fields.

Next we prove some properties of fields. We could just prove them for the rational numbers, but instead we establish the results for *all fields* at once.

Theorem:

Any field has the following properties:

(1) If $z + x = z + y$, then $x = y$.

(2) If $x + z = 0$, then $z = -x$ (the additive inverse is unique).

(3) $-(-y) = y$.

(4) If $y \neq 0$ and $y \cdot x = y \cdot z$, then $x = z$.

(5) If $y \neq 0$ and $y \cdot z = 1$, then $z = y^{-1}$ (the multiplicative inverse is unique).

(6) $\left(x^{-1}\right)^{-1} = x$.

(7) $0 \cdot x = 0$.

(8) If $x \cdot y = 0$, then either $x = 0$ or $y = 0$.

(9) $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$.

(10) $(-x) \cdot (-y) = x \cdot y$.

Proof:

To prove **(1)**, we write

$$z + x = z + y \Rightarrow (-z) + (z + x) = (-z) + (z + y)$$

and now Axiom A3 yields that this implies

$$((-z) + z) + x = ((-z) + z) + y.$$

Next, Axiom A5 yields that

$$0 + x = 0 + y$$

and hence, by Axiom A4,

$$x = y.$$

To prove **(7)**, we observe that

$$0 \cdot x = (0 + 0) \cdot x \, .$$

By Axiom M2, the right-hand side equals

$$x \cdot (0 + 0).$$

By Axiom D1, the last expression equals

$$x \cdot 0 + x \cdot 0,$$

which by Axiom M2 equals $0 \cdot x + 0 \cdot x$.

Thus, we have derived the equation

$$0 \cdot x = 0 \cdot x + 0 \cdot x.$$

Axioms A4 and A2 let us rewrite the left side as

$$0 \cdot x + 0 = 0 \cdot x + 0 \cdot x.$$

Finally, part **(1)** of the present theorem (which we have already proved) yields that

$$0 = 0 \cdot x,$$

which is the desired result.

To prove **(8)**, we suppose that $x \neq 0$. In this case, x has a multiplicative inverse x^{-1} and we multiply both sides of our equation by this element:

$$x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0.$$

By Axiom M3, the left side can be rewritten and we have

$$(x \cdot x^{-1}) \cdot y = x^{-1} \cdot 0.$$

Next, we rewrite the right side using Axiom M2:

$$(x \cdot x^{-1}) \cdot y = 0 \cdot x^{-1}.$$

Now Axiom M5 allows us to simplify the left side:

$$1 \cdot y = 0 \cdot x^{-1}.$$

We further simplify the left side using Axiom M4 and the right side using Part **(7)** of the present theorem (which we just proved) to obtain:

$$y = 0.$$

Thus we see that if $x \neq 0$ then $y = 0$. But this is logically equivalent with $x = 0$ or $y = 0$, as we wished to prove. [If you have forgotten why these statements are logically equivalent, write a truth table.] $\square$

Refer to Section 4.2 of the book for the notion of a strict, simple ordering.

Example:

The integers $\mathbb{Z}$ form a strictly, simply ordered set when equipped with the usual ordering. We can make this ordering precise by saying that $x < y$ if $y - x$ is a positive integer. For instance,

$$6 < 8 \quad \text{because} \quad 8 - 6 = 2 > 0.$$

Likewise,

$$-5 < -1 \quad \text{because} \quad -1 - (-5) = 4 > 0.$$

Observe that the same ordering works on the rational numbers.

If A is a strictly ordered set and a, b are elements, then we often write $a \leq b$ to mean that *either* $a < b$ *or* $a = b$.

When a field has an ordering which is compatible with the field operations, then a richer structure results:

Definition:

A field F is called an *ordered field* if F has a strict, simple ordering $<$ that satisfies the following addition properties:

(1) If $x, y, z \in F$ and if $y < z$, then $x + y < x + z$.

(2) If $x, y \in F, x > 0$, and $y > 0$, then $x \cdot y > 0$.

Again, these are familiar properties of the rational numbers: $\mathbb{Q}$ forms an ordered field. Some further properties of ordered fields may be proved from the axioms:

Theorem:

Any *ordered* field has the following properties:

(1) If $x > 0$ and $z < y$, then $x \cdot z < x \cdot y$.

(2) If $x < 0$ and $z < y$, then $x \cdot z > x \cdot y$.

(3) If $x > 0$, then $-x < 0$. If $x < 0$, then $-x > 0$.

(4) If $0 < y < x$, then $0 < 1/x < 1/y$.

(5) If $x \neq 0$, then $x^2 > 0$.

(6) If $0 < x < y$, then $x^2 < y^2$.

Proof: Again we prove just a few of these statements and leave the rest as exercises.

To prove **(1)**, observe that property **(1)** of ordered fields together with our hypothesis implies that

$$(-z) + z < (-z) + y.$$

Thus, using **A2**, we see that $y - z > 0$. Since $x > 0$, property **(2)** of ordered fields gives

$$x \cdot (y - z) > 0.$$

Finally,

$$x \cdot y = x \cdot [(y - z) + z] = x \cdot (y - z) + x \cdot z > 0 + x \cdot z$$

(by property **(1)** of ordered fields again). In conclusion,

$$x \cdot y > x \cdot z.$$

To prove **(3)**, begin with the equation

$$0 = -x + x.$$

Since $x > 0$, the right side is greater than $-x$. Thus $0 > -x$ as claimed. The proof of the other statement of **(3)** is similar.

To prove **(5)**, we consider two cases. If $x > 0$, then $x^2 \equiv x \cdot x$ is positive by property **(2)** of ordered fields. If $x < 0$, then $-x > 0$ (by part **(3)** of the present theorem, which we just proved) hence $(-x) \cdot (-x) > 0$. But part **(10)** of the last theorem guarantees that $(-x) \cdot (-x) = x \cdot x$ hence $x \cdot x > 0$. $\square$