

Script 7

The Field Axioms

7.1 Journal

1/28: **Definition 7.1.** A **binary operation** on a set X is a function

$$f : X \times X \rightarrow X$$

We say that f is **associative** if

$$f(f(x, y), z) = f(x, f(y, z)) \quad \text{for all } x, y, z \in X$$

We say that f is **commutative** if

$$f(x, y) = f(y, x) \quad \text{for all } x, y \in X$$

An **identity element** of a binary operation f is an element $e \in X$ such that

$$f(x, e) = f(e, x) = x \quad \text{for all } x \in X$$

Remark 7.2. Frequently, we denote a binary operation differently. If $*$: $X \times X \rightarrow X$ is the binary operation, we often write $a * b$ in place of $*(a, b)$. We sometimes indicate this same operation by writing $(a, b) \mapsto a * b$.

Exercise 7.3. Rewrite Definition 7.1 using the notation of Remark 7.2.

Answer. A **binary operation** on a set X is a function

$$* : X \times X \rightarrow X$$

We say that $*$ is **associative** if

$$(x * y) * z = x * (y * z) \quad \text{for all } x, y, z \in X$$

We say that $*$ is **commutative** if

$$x * y = y * x \quad \text{for all } x, y \in X$$

An **identity element** of a binary operation $*$ is an element $e \in X$ such that

$$x * e = e * x = x \quad \text{for all } x \in X$$

□

Examples 7.4.

1. The function $+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ which sends a pair of integers (m, n) to $+(m, n) = m + n$ is a binary operation on the integers, called addition. Addition is associative, commutative, and has identity element 0.

2. The maximum of m and n , denoted $\max(m, n)$, is an associative and commutative binary operation on \mathbb{Z} . Is there an identity element for \max ?

Proof. Suppose for the sake of contradiction that there exists an identity element e for \max . But $\max(e - 1, e) = e \neq e - 1$, a contradiction. Therefore, no identity element exists for \max . \square

3. Let $\wp(Y)$ be the power set of a set Y . Recall that the power set consists of all subsets of Y . Then the intersection of sets, $(A, B) \mapsto A \cap B$, defines an associative and commutative binary operation on $\wp(Y)$. Is there an identity element for \cap ?

Proof. Clearly, $Y \in \wp(Y)$. By Script 1, $Y \cap A = A \cap Y = A$ where $A \subset Y$. Therefore, Y is an identity element for \cap . \square

Exercise 7.5. Find a binary operation on a set that is not commutative. Find a binary operation on a set that is not associative.

Proof. We will prove that the subtraction operation on the integers $(- : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z})$ is not commutative or associative. To prove that it's not commutative, Definition 7.1 tells us that it will suffice to show that $x - y \neq y - x$ for some $x, y \in \mathbb{Z}$. Since $2 - 1 = 1$ but $1 - 2 = -1$, we can see that $1, 2 \in \mathbb{Z}$ clearly meet this requirement. To prove that it's not associative, Definition 7.1 tells us that it will suffice to show that $(x - y) - z \neq x - (y - z)$ for some $x, y, z \in \mathbb{Z}$. Since $(3 - 2) - 1 = 0$ but $3 - (2 - 1) = 2$, we can see that $1, 2, 3 \in \mathbb{Z}$ clearly meet this requirement. \square

Exercise 7.6. Let X be a finite set, and let $Y = \{f : X \rightarrow X \mid f \text{ is bijective}\}$. Consider the binary operation of composition of functions, denoted $\circ : Y \times Y \rightarrow Y$ and defined by $(f \circ g)(x) = f(g(x))$ as seen in Definition 1.25. Decide whether or not composition is commutative and/or associative and whether or not it has an identity.

Proof. To prove that composition is not commutative, Definition 7.1 tells us that it will suffice to find a finite set X paired with two bijections in Y that do not commute. Let $X = \{1, 2, 3\}$ and consider the bijections $f : X \rightarrow X$ (defined by $f(1) = 2, f(2) = 3, f(3) = 1$) and $g : X \rightarrow X$ (defined by $g(1) = 1, g(2) = 3, g(3) = 2$). In this case, $f \circ g$ would be defined by $f(g(1)) = 2, f(g(2)) = 1$, and $f(g(3)) = 3$, but $g \circ f$ would be defined by $g(f(1)) = 3, g(f(2)) = 2$, and $g(f(3)) = 1$.

To prove that composition is associative, Definition 7.1 tells us that it will suffice to show that $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$. We may do this with the following algebra.

$$\begin{aligned} ((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) \\ &= f(g(h(x))) \\ &= f((g \circ h)(x)) \\ &= (f \circ (g \circ h))(x) \end{aligned}$$

With respect to any finite set X , there will always be a bijection $i : X \rightarrow X$ defined by $i(x) = x$. To prove that i is an identity element, Definition 7.1 tells us that it will suffice to show that for all $f \in Y$, $f \circ i = i \circ f = f$. We may do this with the following algebra.

$$\begin{aligned} (f \circ i)(x) &= f(i(x)) \\ &= f(x) \\ &= i(f(x)) \\ &= (i \circ f)(x) \end{aligned}$$

\square

Theorem 7.7. Identity elements are unique. That is, suppose that f is a binary operation on a set X that has two identity elements e and e' . Then $e = e'$.

Proof. Let $f : X \times X \rightarrow X$ be a binary operation on a set X with two identity elements e, e' . By Definition 7.1, we know that $f(e, e') = e$ and $f(e, e') = e'$. Since f is a well-defined function by definition, it must be that $e = f(e, e') = e'$. \square

Definition 7.8. A **field** is a set F with two binary operations on F called addition, denoted $+$, and multiplication, denoted \cdot , satisfying the following **field axioms**:

FA1 (Commutativity of Addition) For all $x, y \in F$, $x + y = y + x$.

FA2 (Associativity of Addition) For all $x, y, z \in F$, $(x + y) + z = x + (y + z)$.

FA3 (Additive Identity) There exists an element $0 \in F$ such that $x + 0 = 0 + x = x$ for all $x \in F$.

FA4 (Additive Inverses) For any $x \in F$, there exists $y \in F$ such that $x + y = y + x = 0$, called an additive inverse of x .

FA5 (Commutativity of Multiplication) For all $x, y \in F$, $x \cdot y = y \cdot x$.

FA6 (Associativity of Multiplication) For all $x, y, z \in F$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

FA7 (Multiplicative Identity) There exists an element $1 \in F$ such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in F$.

FA8 (Multiplicative Inverses) For any $x \in F$ such that $x \neq 0$, there exists $y \in F$ such that $x \cdot y = y \cdot x = 1$, called a multiplicative inverse of x .

FA9 (Distributivity of Multiplication over Addition) For all $x, y, z \in F$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

FA10 (Distinct Additive and Multiplicative Identities) $1 \neq 0$.

Exercise 7.9. Consider the set $\mathbb{F}_2 = \{0, 1\}$, and define binary operations $+$ and \cdot on \mathbb{F}_2 by

$$\begin{array}{cccc} 0 + 0 = 0 & 0 + 1 = 1 & 1 + 0 = 1 & 1 + 1 = 0 \\ 0 \cdot 0 = 0 & 0 \cdot 1 = 0 & 1 \cdot 0 = 0 & 1 \cdot 1 = 1 \end{array}$$

Show that \mathbb{F}_2 is a field.

Proof. To prove that \mathbb{F}_2 obeys FA1 from Definition 7.8, it will suffice to show that $0 + 0 = 0 + 0$, $0 + 1 = 1 + 0$, and $1 + 1 = 1 + 1$. The first and third of these are evidently true. For the second, we have $0 + 1 = 1 = 1 + 0$, so it is good, too.

To prove that \mathbb{F}_2 obeys FA2 from Definition 7.8, the following casework will suffice.

$$\begin{array}{ll} (0 + 0) + 0 = 0 = 0 + (0 + 0) & (0 + 0) + 1 = 1 = 0 + (0 + 1) \\ (0 + 1) + 0 = 1 = 0 + (1 + 0) & (1 + 0) + 0 = 1 = 1 + (0 + 0) \\ (0 + 1) + 1 = 0 = 0 + (1 + 1) & (1 + 1) + 0 = 0 = 1 + (1 + 0) \\ (1 + 0) + 1 = 0 = 1 + (0 + 1) & (1 + 1) + 1 = 1 = 1 + (1 + 1) \end{array}$$

To prove that \mathbb{F}_2 obeys FA3 from Definition 7.8, it will suffice to find an element $0 \in \mathbb{F}_2$ such that $x + 0 = 0 + x = x$. Since $0 + 0 = 0$, $1 + 0 = 0$, and with commutativity, it is clear that 0 is an additive identity in \mathbb{F}_2 .

To prove that \mathbb{F}_2 obeys FA4 from Definition 7.8, it will suffice to show that for all $x \in \mathbb{F}_2$, there exists a $y \in \mathbb{F}_2$ such that $x + y = y + x = 0$. For 0 , this object is 0 (since $0 + 0 = 0 + 0 = 0$), and for 1 , this object is 1 (since $1 + 1 = 1 + 1 = 0$).

To prove that \mathbb{F}_2 obeys FA5 from Definition 7.8, it will suffice to show that $0 \cdot 0 = 0 \cdot 0$, $0 \cdot 1 = 1 \cdot 0$, and $1 \cdot 1 = 1 \cdot 1$. The first and third of these are evidently true. For the second, we have $0 \cdot 1 = 0 = 1 \cdot 0$, so it is good, too.

To prove that \mathbb{F}_2 obeys FA6 from Definition 7.8, the following casework will suffice.

$$\begin{array}{ll} (0 \cdot 0) \cdot 0 = 0 = 0 \cdot (0 \cdot 0) & (0 \cdot 0) \cdot 1 = 0 = 0 \cdot (0 \cdot 1) \\ (0 \cdot 1) \cdot 0 = 0 = 0 \cdot (1 \cdot 0) & (1 \cdot 0) \cdot 0 = 0 = 1 \cdot (0 \cdot 0) \\ (0 \cdot 1) \cdot 1 = 0 = 0 \cdot (1 \cdot 1) & (1 \cdot 1) \cdot 0 = 0 = 1 \cdot (1 \cdot 0) \\ (1 \cdot 0) \cdot 1 = 0 = 1 \cdot (0 \cdot 1) & (1 \cdot 1) \cdot 1 = 1 = 1 \cdot (1 \cdot 1) \end{array}$$

To prove that \mathbb{F}_2 obeys FA7 from Definition 7.8, it will suffice to find an element $1 \in \mathbb{F}_2$ such that $x \cdot 1 = 1 \cdot x = x$. Since $0 \cdot 1 = 0$, $1 \cdot 1 = 1$, and with commutativity, it is clear that 1 is a multiplicative identity in \mathbb{F}_2 .

To prove that \mathbb{F}_2 obeys FA8 from Definition 7.8, it will suffice to show that for all $x \in \mathbb{F}_2$ such that $x \neq 0$, there exists a $y \in \mathbb{F}_2$ such that $x \cdot y = y \cdot x = 1$. For 1, this object is 1 (since $1 \cdot 1 = 1 \cdot 1 = 1$).

To prove that \mathbb{F}_2 obeys FA9 from Definition 7.8, the following casework will suffice.

$$\begin{array}{ll} 0 \cdot (0 + 0) = 0 = 0 \cdot 0 + 0 \cdot 0 & 0 \cdot (0 + 1) = 0 = 0 \cdot 0 + 0 \cdot 1 \\ 0 \cdot (1 + 0) = 0 = 0 \cdot 1 + 0 \cdot 0 & 1 \cdot (0 + 0) = 0 = 1 \cdot 0 + 1 \cdot 0 \\ 0 \cdot (1 + 1) = 0 = 0 \cdot 1 + 0 \cdot 1 & 1 \cdot (1 + 0) = 1 = 1 \cdot 1 + 1 \cdot 0 \\ 1 \cdot (0 + 1) = 1 = 1 \cdot 0 + 1 \cdot 1 & 1 \cdot (1 + 1) = 0 = 1 \cdot 1 + 1 \cdot 1 \end{array}$$

To prove that \mathbb{F}_2 obeys FA10 from Definition 7.8, it will suffice to show that $0 \neq 1$. Clearly this is true. \square

Theorem 7.10. *Suppose that F is a field. Then additive inverses are unique. This means: Let $x \in F$. If $y, y' \in F$ satisfy $x + y = 0$ and $x + y' = 0$, then $y = y'$.*

Proof. Let $x, y, y' \in F$ be such that $x + y = 0$ and $x + y' = 0$. From Definition 7.8, we have

$$y' + (x + y) = (y' + x) + y \quad \text{FA2}$$

$$y' + 0 = 0 + y \quad \text{FA4}$$

$$y' = y \quad \text{FA3}$$

\square

We usually write $-x$ for the additive inverse of x .

Corollary 7.11. *If $x \in F$, then $-(-x) = x$.*

Proof. Let $x \in F$. From Definition 7.8, we have

$$(x + (-x)) + (-(-x)) = x + ((-x) + (-(-x))) \quad \text{FA2}$$

$$0 + (-(-x)) = x + 0 \quad \text{FA4}$$

$$-(-x) = x \quad \text{FA3}$$

\square

Theorem 7.12. *Let F be a field, and let $a, b, c \in F$. If $a + b = a + c$, then $b = c$.*

Proof. Let $a, b, c \in F$ be such that $a + b = a + c$. By FA4 from Definition 7.8, there exists $-a \in F$ such that $-a + a = a + (-a) = 0$. Having established that $-a$ exists, we can prove from Definition 7.8 that

$$-a + (a + b) = -a + (a + c)$$

$$(-a + a) + b = (-a + a) + c \quad \text{FA2}$$

$$0 + b = 0 + c \quad \text{FA4}$$

$$b = c \quad \text{FA3}$$

\square

Theorem 7.13. *Let F be a field. If $a \in F$, then $a \cdot 0 = 0$.*

Proof. Let $a \in F$. From Definition 7.8, we have

$$a = a \cdot 1 \quad \text{FA7}$$

$$= a \cdot (1 + 0) \quad \text{FA3}$$

$$= a \cdot 1 + a \cdot 0 \quad \text{FA9}$$

$$= a + a \cdot 0 \quad \text{FA7}$$

$$0 = a \cdot 0 \quad \text{Theorem 7.12}$$

\square

2/2: **Theorem 7.14.** Suppose that F is a field. Then multiplicative inverses are unique. This means: Let $x \in F$. If $y, y' \in F$ satisfy $x \cdot y = 1$ and $x \cdot y' = 1$, then $y = y'$.

Proof. Let $x, y, y' \in F$ be such that $x \cdot y = 1$ and $x \cdot y' = 1$. From Definition 7.8, we have

$$(y \cdot x) \cdot y' = y \cdot (x \cdot y') \quad \text{FA6}$$

$$1 \cdot y' = y \cdot 1 \quad \text{FA8}$$

$$y' = y \quad \text{FA7}$$

□

We usually write x^{-1} or $\frac{1}{x}$ for the multiplicative inverse of x .

Corollary 7.15. If $x \in F$ and $x \neq 0$, then $(x^{-1})^{-1} = x$.

Proof. Let $x \in F \setminus \{0\}$. Then by FA8 from Definition 7.8, there exists $x^{-1} \in F$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$. It follows from Theorem 7.13 that $x^{-1} \neq 0$ (if $x^{-1} = 0$, then Theorem 7.13 would imply that $x \cdot x^{-1} = 0$, a contradiction). Thus, by FA8 from Definition 7.8 again, there exists $(x^{-1})^{-1} \in F$ such that $x^{-1} \cdot (x^{-1})^{-1} = (x^{-1})^{-1} \cdot x^{-1} = 1$. Having established that $(x^{-1})^{-1}$ exists, we can prove from Definition 7.8 that

$$(x \cdot x^{-1}) \cdot (x^{-1})^{-1} = x \cdot (x^{-1} \cdot (x^{-1})^{-1}) \quad \text{FA6}$$

$$1 \cdot (x^{-1})^{-1} = x \cdot 1 \quad \text{FA8}$$

$$(x^{-1})^{-1} = x \quad \text{FA7}$$

□

Theorem 7.16. Let F be a field, and let $a, b, c \in F$. If $a \cdot b = a \cdot c$ and $a \neq 0$, then $b = c$.

Proof. Let $a, b, c \in F$ be such that $a \cdot b = a \cdot c$ and $a \neq 0$. By FA8 from Definition 7.8, there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Having established that a^{-1} exists, we can prove from Definition 7.8 that

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c) \quad \text{FA6}$$

$$(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c \quad \text{FA8}$$

$$1 \cdot b = 1 \cdot c \quad \text{FA8}$$

$$b = c \quad \text{FA7}$$

□

Theorem 7.17. Let F be a field, and let $a, b \in F$. If $a \cdot b = 0$, then $a = 0$ or $b = 0$.

Proof. Let $a, b \in F$ be such that $a \cdot b = 0$, and suppose for the sake of contradiction that $a \neq 0$ and $b \neq 0$. It follows from the supposition by consecutive applications of FA8 from Definition 7.8 that a^{-1} and b^{-1} exist. Thus, from Definition 7.8, we have

$$b^{-1} \cdot (a \cdot b) = 0 = a^{-1} \cdot (a \cdot b) \quad \text{Theorem 7.13}$$

$$b^{-1} \cdot (b \cdot a) = 0 = a^{-1} \cdot (a \cdot b) \quad \text{FA5}$$

$$(b^{-1} \cdot b) \cdot a = 0 = (a^{-1} \cdot a) \cdot b \quad \text{FA6}$$

$$1 \cdot a = 0 = 1 \cdot b \quad \text{FA8}$$

$$a = 0 = b \quad \text{FA7}$$

But this contradicts the supposition that $a \neq 0$ and $b \neq 0$. □

Lemma 7.18. *Let F be a field. If $a \in F$, then $-a = (-1)a$.*

Proof. Let $a \in F$. From Definition 7.8, we have

$$\begin{aligned}
 0 &= 0 \cdot a && \text{Theorem 7.13} \\
 a + (-a) &= (1 + (-1)) \cdot a && \text{FA4} \\
 a + (-a) &= 1 \cdot a + (-1) \cdot a && \text{FA9} \\
 a + (-a) &= a + (-1)a && \text{FA7} \\
 -a &= (-1)a && \text{Theorem 7.12}
 \end{aligned}$$

□

Lemma 7.19. *Let F be a field. If $a, b \in F$, then $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$.*

Proof. Let $a, b \in F$. From Definition 7.8, we have

$$\begin{aligned}
 a \cdot (-b) &= a \cdot ((-1) \cdot b) && \text{Lemma 7.18} \\
 &= a \cdot (b \cdot (-1)) && \text{FA5} \\
 &= (a \cdot b) \cdot (-1) && \text{FA6} \\
 &= (-1) \cdot (a \cdot b) && \text{FA5} \\
 &= \boxed{-(a \cdot b)} && \text{Lemma 7.18} \\
 &= (-1) \cdot (a \cdot b) && \text{Lemma 7.18} \\
 &= ((-1) \cdot a) \cdot b && \text{FA6} \\
 &= \boxed{(-a) \cdot b} && \text{Lemma 7.18}
 \end{aligned}$$

□

Lemma 7.20. *Let F be a field. If $a, b \in F$, then $a \cdot b = (-a) \cdot (-b)$.*

Proof. Let $a, b \in F$. Thus, we have

$$\begin{aligned}
 (-a) \cdot (-b) &= -(-a) \cdot b && \text{Lemma 7.19} \\
 &= a \cdot b && \text{Corollary 7.11}
 \end{aligned}$$

□

Definition 7.21. An **ordered field** is a field F equipped with an ordering $<$ (satisfying Definition 3.1) such that also:

- (a) Addition respects the ordering: if $x < y$, then $x + z < y + z$ for all $z \in F$.
- (b) Multiplication respects the ordering: if $0 < x$ and $0 < y$, then $0 < x \cdot y$.

Definition 7.22. Suppose F is an ordered field and $x \in F$. If $0 < x$, we say that x is **positive**. If $x < 0$, we say that x is **negative**.

Lemma 7.23. *Let F be an ordered field, and let $x \in F$. If $0 < x$, then $-x < 0$. Similarly, if $x < 0$, then $0 < -x$.*

Proof. Let $x \in F$ be such that $0 < x$. Then by Definition 7.21a, $0 + (-x) < x + (-x)$. Consequently, from Definition 7.8, we have

$$\begin{aligned}
 -x &< x + (-x) && \text{FA3} \\
 -x &< 0 && \text{FA4}
 \end{aligned}$$

The proof is symmetric if $x < 0$.

□

Lemma 7.24. *Let F be an ordered field, and let $x, y, z \in F$.*

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

(b) *If $x < 0$ and $y < z$, then $x \cdot z < x \cdot y$.*

Proof of a. Let $x, y, z \in F$ be such that $x > 0$ and $y < z$. It follows from the latter condition by Definition 7.21a that $y + (-y) < z + (-y)$. Thus, by FA4 from Definition 7.8, we have $0 < z + (-y)$. This combined with the fact that $0 < x$ implies by Definition 7.21b that $0 < x \cdot (z + (-y))$. Consequently, from Definition 7.8, we have

$$\begin{aligned}
 0 &< x \cdot z + x \cdot (-y) && \text{FA9} \\
 0 &< x \cdot z + (-(x \cdot y)) && \text{Lemma 7.19} \\
 0 + x \cdot y &< (x \cdot z + (-(x \cdot y))) + x \cdot y && \text{Definition 7.21a} \\
 0 + x \cdot y &< x \cdot z + (-(x \cdot y) + x \cdot y) && \text{FA2} \\
 0 + x \cdot y &< x \cdot z + 0 && \text{FA4} \\
 x \cdot y &< x \cdot z && \text{FA3}
 \end{aligned}$$

□

Proof of b. Let $x, y, z \in F$ be such that $x < 0$ and $y < z$. It follows from the former condition by Lemma 7.23 that $0 < -x$. Thus, by Lemma 7.24a, $(-x) \cdot y < (-x) \cdot z$. Consequently, from Definition 7.8, we have

$$\begin{aligned}
 -(x \cdot y) &< -(x \cdot z) && \text{Lemma 7.19} \\
 -(x \cdot y) + (x \cdot y + x \cdot z) &< -(x \cdot z) + (x \cdot y + x \cdot z) && \text{Definition 7.21a} \\
 -(x \cdot y) + (x \cdot y + x \cdot z) &< -(x \cdot z) + (x \cdot z + x \cdot y) && \text{FA1} \\
 (-(x \cdot y) + x \cdot y) + x \cdot z &< (-(x \cdot z) + x \cdot z) + x \cdot y && \text{FA2} \\
 0 + x \cdot z &< 0 + x \cdot y && \text{FA4} \\
 x \cdot z &< x \cdot y && \text{FA3}
 \end{aligned}$$

□

Remark 7.25. An immediate consequence of this lemma is the fact that if x and y are both positive or both negative, their product is positive.

Lemma 7.26. *Let F be an ordered field, and let $x \in F$. Then $0 \leq x^2$. Moreover, if $x \neq 0$, then $0 < x^2$.*

Proof. We divide into two cases ($x = 0$ and $x \neq 0$). Suppose first that $x = 0$. Then by Theorem 7.13, $0 = 0 \cdot 0 = 0^2 = x^2$, as desired. Now suppose that $x \neq 0$. We divide into two cases again ($x > 0$ and $x < 0$). If $x > 0$, then by Lemma 7.24a, $x > 0$ and $0 < x$ imply that $x \cdot 0 < x \cdot x$, from which it follows by Theorem 7.13 that $0 < x^2$, as desired. On the other hand, if $x < 0$, then by Lemma 7.24b, $x < 0$ and $x < 0$ imply that $x \cdot 0 < x \cdot x$, from which it follows for the same reason as before that $0 < x^2$, as desired. Both cases together prove the first statement, while the second case alone proves the second statement. □

Corollary 7.27. *Let F be an ordered field. Then $0 < 1$.*

Proof. By FA10 from Definition 7.8, $1 \neq 0$. Thus, by Lemma 7.26, $0 < 1^2 = 1$, as desired. □

Theorem 7.28. *If F is an ordered field, then F has no first or last point.*

Proof. Suppose for the sake of contradiction that F has a first point a . By Corollary 7.27, we have that $0 < 1$, which implies by Lemma 7.23 that $-1 < 0$. It follows by Definition 7.21a that $-1 + a < 0 + a$. Thus, by FA3 from Definition 7.8, $-1 + a < a$. Since there exists an object in F (namely $-1 + a$) that is less than a , Definition 3.3 tells us that a is not the first point of F , a contradiction. □

Theorem 7.29. *The rational numbers \mathbb{Q} form an ordered field.*

Proof. To prove that \mathbb{Q} forms an ordered field, Definition 7.21 tells us that it will suffice to show that \mathbb{Q} forms a field; has an ordering $<$; satisfies $x + z < y + z$ if $x < y$ for all $z \in \mathbb{Q}$; and satisfies $0 < x \cdot y$ if $0 < x$ and $0 < y$. We will take this one constraint at a time.

To show that \mathbb{Q} forms a field, Definition 7.8 tells us that it will suffice to verify that \mathbb{Q} has two binary operations ($+$ and \cdot), and satisfies field axioms 1-10. Define $+$ and \cdot as in Definition 2.7. Under these definitions, parts a-i of Theorem 2.10 guarantee that \mathbb{Q} satisfies FA1-FA9, respectively. As to FA10, to verify that $\begin{bmatrix} 1 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, Exercise 2.6 tells us that it will suffice to confirm that $(1, 1) \approx (1, 0)$. But since $1 \cdot 0 = 0 \neq 1 = 1 \cdot 1$, Exercise 2.2e confirms that $(1, 1) \approx (1, 0)$, as desired.

\mathbb{Q} has an ordering by Exercise 3.9d, as desired.

To show that $x + z < y + z$ if $x < y$ for all $z \in \mathbb{Q}$, let $\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}, \begin{bmatrix} x \\ z \end{bmatrix}$ be arbitrary elements of \mathbb{Q} with positive denominators (we can choose these WLOG by Exercise 3.9b) and the first two satisfying $\begin{bmatrix} a \\ b \end{bmatrix} < \begin{bmatrix} c \\ d \end{bmatrix}$; we seek to verify that $\begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} x \\ z \end{bmatrix} < \begin{bmatrix} c \\ d \end{bmatrix} + \begin{bmatrix} x \\ z \end{bmatrix}$. Since $\begin{bmatrix} a \\ b \end{bmatrix} < \begin{bmatrix} c \\ d \end{bmatrix}$, we have by Exercise 3.9c that $ad < bc$. It follows by Script 0 that

$$\begin{aligned} ad &< bc \\ adzz &< bczz \\ adzz + bdxz &< bczz + bdxz \\ azdz + bxdz &< bczx + bzdx \\ (az + bx)(dz) &< (bz)(cz + dx) \end{aligned}$$

Thus, by Exercise 3.9c, $\begin{bmatrix} az+bx \\ bz \end{bmatrix} < \begin{bmatrix} cz+dx \\ dz \end{bmatrix}$. Therefore, by Definition 2.7, $\begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} x \\ z \end{bmatrix} < \begin{bmatrix} c \\ d \end{bmatrix} + \begin{bmatrix} x \\ z \end{bmatrix}$, as desired.

To show that $0 < x \cdot y$ if $0 < x$ and $0 < y$, let $\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}$ be arbitrary elements of \mathbb{Q} with positive denominators (which we can choose for the same reason as before) such that $\begin{bmatrix} 0 \\ 1 \end{bmatrix} < \begin{bmatrix} a \\ b \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix} < \begin{bmatrix} c \\ d \end{bmatrix}$; we seek to verify that $\begin{bmatrix} 0 \\ 1 \end{bmatrix} < \begin{bmatrix} a \\ b \end{bmatrix} \cdot \begin{bmatrix} c \\ d \end{bmatrix}$. Since $\begin{bmatrix} 0 \\ 1 \end{bmatrix} < \begin{bmatrix} a \\ b \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix} < \begin{bmatrix} c \\ d \end{bmatrix}$, we have by Exercise 3.9c that $0 \cdot b < 1 \cdot a$ and $0 \cdot d < 1 \cdot c$. It follows by Script 0 that $0 \cdot bd < 1 \cdot ac$. Thus, by Exercise 3.9c, $\begin{bmatrix} 0 \\ 1 \end{bmatrix} < \begin{bmatrix} ac \\ bd \end{bmatrix}$. Therefore, by Definition 2.7, $\begin{bmatrix} 0 \\ 1 \end{bmatrix} < \begin{bmatrix} a \\ b \end{bmatrix} \cdot \begin{bmatrix} c \\ d \end{bmatrix}$, as desired. \square