Script 7

The Field Axioms

7.1 Journal

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

$$f : X \times X \to X$$

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 $* : X \times X \to X$ 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

$$* : X \times X \to X$$

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

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

$\square$

Examples 7.4.

1. *The function $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ 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. □

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 $\cap$. □

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 ($- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$) 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. □

Exercise 7.6. Let X be a finite set, and let $Y = \{f : X \to X \mid f \text{ is bijective}\}$. Consider the binary operation of composition of functions, denoted $\circ : Y \times Y \to Y$ 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 $f : X \to X$ (defined by $f(1) = 2$, $f(2) = 3$, $f(3) = 1$) and $g : X \to X$ (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 $i : X \to X$ 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.

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

□

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 $f : X \times X \to X$ 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 $e = f(e, e') = e'$. ☐

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.

$$\begin{aligned}
&0 \cdot (0+0) = 0 = 0 \cdot 0 + 0 \cdot 0 & \qquad & 0 \cdot (0+1) = 0 = 0 \cdot 0 + 0 \cdot 1 \\
&0 \cdot (1+0) = 0 = 0 \cdot 1 + 0 \cdot 0 & & 1 \cdot (0+0) = 0 = 1 \cdot 0 + 1 \cdot 0 \\
&0 \cdot (1+1) = 0 = 0 \cdot 1 + 0 \cdot 1 & & 1 \cdot (1+0) = 1 = 1 \cdot 1 + 1 \cdot 0 \\
&1 \cdot (0+1) = 1 = 1 \cdot 0 + 1 \cdot 1 & & 1 \cdot (1+1) = 0 = 1 \cdot 1 + 1 \cdot 1
\end{aligned}$$

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. □

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

$$\begin{aligned}
y' + (x+y) &= (y'+x) + y && \text{FA2} \\
y' + 0 &= 0 + y && \text{FA4} \\
y' &= y && \text{FA3}
\end{aligned}$$

□

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

$$\begin{aligned}
(x + (-x)) + (-(-x)) &= x + ((-x) + (-(-x))) && \text{FA2} \\
0 + (-(-x)) &= x + 0 && \text{FA4} \\
-(-x) &= x && \text{FA3}
\end{aligned}$$

□

Corollary 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 $a + b = a + c$. From Definition 7.8, we have

$$\begin{aligned}
b &= b + 0 && \text{FA3} \\
&= b + (a + (-a)) && \text{FA4} \\
&= (b + a) + (-a) && \text{FA2} \\
&= (a + b) + (-a) && \text{FA1} \\
&= (a + c) + (-a) && \text{Substitute} \\
&= (c + a) + (-a) && \text{FA1} \\
&= c + (a + (-a)) && \text{FA2} \\
&= c + 0 && \text{FA4} \\
&= c && \text{FA3}
\end{aligned}$$

□

Corollary 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

$$\begin{aligned} a &= a \cdot 1 && \text{FA7} \\ &= a \cdot (1+0) && \text{FA3} \\ &= a \cdot 1 + a \cdot 0 && \text{FA9} \\ &= a + a \cdot 0 && \text{FA7} \\ 0 &= a \cdot 0 && \text{Corollary 7.12} \end{aligned}$$

□