MATH 162, SHEET 6: THE FIELD AXIOMS

Jeffrey Zhang IBL Script 6 Journal

We will formalize the notions of addition and multiplication in structures called fields. A field with a compatible order is called an ordered field. We will see that $\mathbb{Q}$ and $\mathbb{R}$ are both examples of ordered fields.

Definition 6.1. A *binary operation* on a set X is a function

$$f\colon X \times X \longrightarrow X.$$

We say that f is *associative* if:

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

We say that f is *commutative* if:

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

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

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

Remark 6.2. Frequently, we denote a binary operation differently. If $* : X \times X \longrightarrow X$ 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 6.3. Rewrite Definition 6.1 using the notation of Remark 6.2.

Proof. A binary operation on a set X is a function $f : X \times X \to X$. We say that f is associative if $(x * y) * z = x * (y * z)$ for all $x, y, z \in X$. We say that f is commutative if $(x * y) = (y * x)$ for $x, y \in X$. An identity element of a binary operation f is an element $e \in X$ such that $x * e = e * x = x$ for all $x \in X$. $\square$

Examples 6.4.

1. The function $+\colon \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ 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?

3. Let $P(Y)$ 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 $P(Y)$. Is there an identity element for $\cap$?

Proof. 2. There is no identity element for $\max(m, n)$ on $\mathbb{Z}$. Suppose there exists an identity element e such that $\max(x, e) = x$ for all $x, e \in \mathbb{Z}$. Then $e - 1 \in Z$, $\max(e, e-1) = e$, so e is not the identity element.
3. Let $P(Y)$ be the power set of a set Y. The identity element then is Y itself, because for all sets X such that $X \in P(Y)$, $X \subset Y$ so $X \cap Y = Y$. □

Exercise 6.5. Find a binary operation on a set that is not commutative. Find a binary operation on a set that is not associative.

Proof. Let $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be defined such that $f(x, y) = x - y$. We know that $1, 2, 3 \in \mathbb{R}$. $f(2, 1) = 2 - 1 = 1$, while $f(1, 2) = 1 - 2 = -1$. $1 \neq -1$ so f is not commutative. Similarly, we have that $f(f(3, 2), 1) = (3 - 2) - 1 = 0$, $f(3, f(2, 1)) = 3 - (2 - 1) = 2$. $0 \neq 2$, so f is also not associative. □

Exercise 6.6. Let X be a finite set, and let $Y = \{f : X \longrightarrow X \mid f \text{ is bijective}\}$. Consider the binary operation of composition of functions, denoted $\circ : Y \times Y \longrightarrow Y$ and defined by $(f \circ g)(x) = f(g(x))$. Decide whether or not composition is commutative and/or associative and whether or not it has an identity.

Proof. Let X be a finite set and $Y = \{f : X \to X \mid \text{f is bijective}\}$. Let $f, g \in Y$, $X = \{a, b, c\}$ such that $f(a) = b$, $f(b) = a$, $f(c) = c$, $g(a) = a$, $g(b) = c$, $g(c) = b$ and $a \neq b$, $b \neq c$, $a \neq c$. Through inspection it can be seen that f, g are injective and surjective and thus bijective by Definition 1.20. So we have that $(f \circ g)(a) = f(g(a)) = b$ and $(g \circ f)(a) = g(f(a)) = c$. $b \neq c$, so we know that composition is not commutative.
Let $p, q, r \in Y$ be arbitrary. Then we have that $((p \circ q) \circ r)(a) = p(q(r(a)))$. Similarly, $(p \circ (q \circ r))(a) = p(q(r(a)))$. p, q, r are arbitrary, so we have that composition is associative. The identity element for composition is the function f defined such that $f(x) = x$. □

Theorem 6.7. *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 have two identity elements e, e'. Then by 6.1, $f(e, e') = f(e', e) = e$. Similarly, $f(e', e) = f(e, e') = e$. So $e = e'$. □

Definition 6.8. 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 $x + y = y + x = 0$.

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 $x \cdot y = y \cdot x = 1$.

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 6.9. 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. Axiom 1: $\mathbb{F}_2$ only has two elements, so $x = 1, y = 0$. Then $0 + 1 = 1 + 0 = 1$, so Axiom 1 holds.
Axiom 2: There are two cases, $x = 1, y = 0, z = 1$ and $x = 1, y = 0, z = 0$ (the other cases are covered by commutativity of addition. $(1 + 0) + 1 = 1 + (0 + 1) = 1 + 1 = 0$. $(1 + 0) + 0 = 1 + (0 + 0) = 1 + 0 = 1$. So Axiom 2 holds.
Axiom 3: $0 \in \mathbb{F}_2$, 0 is the additive identity. $1 + 0 = 1$ and $0 + 0 = 0$ so for all $x \in \mathbb{F}_2$, $x + 0 = x$. Axiom 3 holds.
Axiom 4: The additive inverse of $x \in \mathbb{F}_2$ is x. $1 + 1 = 0, 0 + 0 = 0$ so Axiom 4 holds.
Axiom 5: $\mathbb{F}_2$ has two elements. Let $x = 1, y = 0$ then $1 \cdot 0 = 0 \cdot 1 = 0$. So Axiom 5 holds.
Axiom 6: Similarly to Axiom 2 there are two cases. Let $x = 1, y = 0, z = 1$, then $(1 \cdot 0) \cdot 1 = 1 \cdot (0 \cdot 1) = 0$. $(1 \cdot 0) \cdot 0 = 1 \cdot (0 \cdot 0) = 0$. So Axiom 6 holds.
Axiom 7: The multiplicative identity is 1. $0 \cdot 1 = 0$, $1 \cdot 1 = 1$, so $x \cdot 1 = x$ for all $x \in \mathbb{F}_2$. So Axiom 7 holds.
Axiom 8: The multiplicative inverse of $x \in \mathbb{F}_2$ is x. $1 \cdot 1 = 1$, so Axiom 8 holds.

Axiom 9: For x, y, z, if $x = 1$, then Axiom 9 obviously holds because $1 \cdot (y + z) = y + z$ and $1 \cdot y + 1 \cdot z = y + z$. If $x = 0$, then $0 \cdot y = 0$ for any $y \in \mathbb{F}_2$. (Note: $1 \cdot 0 = 0$, $0 \cdot 0 = 0$). So $0 \cdot (y + z) = 0$ and $0 \cdot y = 0$ and $0 \cdot z = 0$, so $0 = 0 + 0$, so Axiom 9 holds.
Axiom 10: The definition of $\mathbb{F}_2$ implies that $1 \neq 0$, so Axiom 10 holds. □

Theorem 6.10. *Suppose that F is a field. Then additive and multiplicative inverses are unique. This means:*

1. *Let $x \in F$. If $y, y' \in F$ satisfy $x + y = 0$ and $x + y' = 0$, then $y = y'$.*

   Proof. $x + y = x + y'$
   $(x + y) + (-x) = (x + y') + (-x)$ Axiom 4
   $0 + y = 0 + y'$ Axiom 1, 2, 4
   $y = y'$ Axiom 3

   □

2. *Let $x \in F$. If $y, y' \in F$ satisfy $x \cdot y = 1$ and $x \cdot y' = 1$, then $y = y'$.*

   Proof. $x \cdot y = x \cdot y'$
   $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (x \cdot y')$ Axiom 8
   $1 \cdot y = 1 \cdot y'$ Axiom 6, 8
   $y = y'$ Axiom 7 □

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

Corollary 6.11. *If $x \in F$, then $-(-x) = x$.*

Proof. Let $x \in F$, then $(-x) \in F$ and $(-(-x)) \in F$. $(-x) + (-(-x)) = 0$, so $(-x)$ is the additive inverse of both x and $(-(-x))$. By Theorem 6.10 then, $x = (-(-x))$. □

Corollary 6.12. *If $x \in F$ and $x \neq 0$, then $(x^{-1})^{-1} = x$.*

Proof. Let $x \in F$ such that $x \neq 0$. Then x^{-1} exists and $(x^{-1})^{-1}$ exists. So x^{-1} is the multiplicative inverse of both x and $(x^{-1})^{-1}$, so $x = (x^{-1})^{-1}$. □

Theorem 6.13. *Let F be a field, and let $a, b, c \in F$. If $a + b = a + c$, then $b = c$.*

Proof. Let F be a field, $a, b, c \in F$ such that $a + b = a + c$. Then we have
$a + b = a + c$
$(a + b) + (-a) = (a + c) + (-a)$ Axiom 4
$0 + b = 0 + c$ Axiom 1,2,4
$b = c$ Axiom 3 □

Theorem 6.14. *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. $a \cdot b = a \cdot c$
$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$ Axiom 8
$1 \cdot b = 1 \cdot c$ Axiom 6,8
$b = c$ Axiom 7 □

Theorem 6.15. *Let F be a field. If $a \in F$, then $a \cdot 0 = 0$.*

Proof. $a \cdot 0 = a \cdot (0 + 0)$ Axiom 3
$a \cdot 0 = (a \cdot 0) + (a \cdot 0)$ Axiom 9
$(a \cdot 0) + (-(a \cdot 0)) = ((a \cdot 0) + (a \cdot 0)) + (-(a \cdot 0))$ Axiom 2,4
$0 = (a \cdot 0) + 0$ Axiom 4
$a \cdot 0 = 0$ Axiom 3 □

Theorem 6.16. *Let F be a field, and let $a, b \in F$. If $a \cdot b = 0$, then $a = 0$ or $b = 0$.*

Proof. Let $a \cdot b = 0$. If $a = 0$, then we are done. So let $a \neq 0$, then a^{-1} exists (Multiplicative identity)
$a \cdot b = 0$
$a \cdot b = a \cdot 0$ Theorem 6.15
$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot 0)$ Axiom 8
$1 \cdot b = 1 \cdot 0$ Axiom 6,8
$b = 0$ Axiom 7
So we have that if $a \neq 0$, then $b = 0$. So $a = 0$ or $b = 0$. □

Lemma 6.17. *If $a, b \in F$, then $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$.*

Proof. $a \cdot 0 = 0$ Theorem 6.15
$a \cdot (1 + (-1)) = 0$ Axiom 4, 7
$(a \cdot 1) + (a \cdot (-1)) = 0$ Axiom 9
$a + (a \cdot (-1)) = 0$ Axiom 7
$(-a) + (a + (a \cdot (-1))) = (-a) + 0$ Axiom 4
$0 + (a \cdot (-1)) = (-a) + 0$ Axiom 2,4
$a \cdot (-1) = (-a)$ Axiom 3.
We now have Lemma 1 that $a \cdot (-1) = (-a)$.
$a \cdot (-b) = a \cdot (b \cdot (-1))$ Lemma 1
$a \cdot (-b) = (a \cdot b) \cdot (-1)$ Axiom 6
$a \cdot (-b) = -(a \cdot b)$ Lemma 1
Similarly from:
$a \cdot (-b) = (a \cdot b) \cdot (-1)$
$a \cdot (-b) = (a \cdot (-1)) \cdot b$ Axiom 5,6
$a \cdot (-b) = (-a) \cdot b$ Lemma 1
So we have that $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$. □

Lemma 6.18. *If $a, b \in F$, then $a \cdot b = (-a) \cdot (-b)$.*

Proof. $a, b \in F$, so $a \cdot b \in F$ and $-(a \cdot b) \in F$.
$(a \cdot b) + (-(a \cdot b)) = 0$ Axiom 4
$(a \cdot b) = -(-(a \cdot b))$ Corollary 6.11
$(a \cdot b) = -((-a) \cdot b)$ Lemma 6.17
$(a \cdot b) = (-a) \cdot (-b)$ Lemma 6.17 $\square$

Next, we discuss the notion of an ordered field.

Definition 6.19. An *ordered field* is a field F equipped with an ordering $<$ such that:

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

Definition 6.20. 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*.

For the remaining theorems, assume F is an ordered field.

Lemma 6.21. *If $0 < x$, then $-x < 0$. Similarly, if $x < 0$, then $0 < -x$.*

Proof. Let $0 < x$.
$(-x) + 0 < (-x) + x$ Axiom 4
$(-x) < 0$ Axiom 3,4.
Let $x < 0$.
$x + (-x) < 0 + (-x)$ Axiom 4
$0 < (-x)$ Axiom 3,4 $\square$

Lemma 6.22. *Let $x, y, z \in F$.*

1. *If $x > 0$ and $y < z$, then $xy < xz$.*

   Proof. Let $x > 0, y < z$. Let $z + (-y) = a$ for $a \in F$ such that $0 < a$. It follows then that $z = y + a$ and $y = y + 0$. Then we have $x > 0$, $a > 0$, so $xa > 0$.
   $0 < xa$
   $xy + 0 < xy + xa$
   $xy < x(y + a)$ Axiom 3,9
   $xy < xz$ (Substituting $z = y + a$) $\square$

2. *If $x < 0$ and $y < z$ then $xz < xy$.*

   Proof. Let $x < 0, y < z$. Let $z + (-y) = a$ for $a \in F$ such that $0 < a$. So we have that $z = y + a$. $x < 0$, so by Lemma 6.21 we have that $0 < -x$. $0 < a$ and $0 < (-x)$ so we have $0 < (-x)a$.
   $0 < (-x)a$
   $0 < -(xa)$ Lemma 6.17. We have $0 < -(xa)$, so by Lemma 6.21 again, we have $xa < 0$.

$xa < 0$
$xa + xy < 0 + xy$
$x(y + a) < xy$ Axiom 1,3,9
$xz < xy$ (Substituting $z = y + a$) $\square$

Lemma 6.23. *If $x \in F$, then $0 \leq x^2$. Moreover, if $x \neq 0$, then $0 < x^2$.*

Proof. Let $x \in F$. We have three cases, $x < 0, x = 0, x > 0$.
If $x < 0$, then by Lemma 6.21, $0 < (-x)$. Then $0 < (-x)\cdot(-x)$ by Definition 6.19, so $0 \leq x^2$.
If $x = 0$, then by Theorem 6.16, $x \cdot x = 0$, so $0 \leq x^2$.
If $x > 0$, then by Definition 6.19, $x \cdot x > 0$ so $x^2 \leq 0$.
So we have that $x^2 \leq 0$ for $x \in F$. $\square$

Corollary 6.24. $0 < 1$.

Proof. We know that $1 \in F$ and that $1 \neq 0$ by Axiom 10, so we have that $0 < 1^2$ by Lemma 6.23. $1^2 = 1 \cdot 1 = 1$, so $0 < 1$. $\square$

Theorem 6.25. *If F is an ordered field, then F has no first or last point.*

Proof. Assume that F has a first point $a \in F$. Then $\forall x \in F$, $a < x$. We have that $0 < 1$ from Corollary 6.24, so $-1 < 0$ by Lemma 6.21. It follows then that $(-1) + a < 0 + a$. By Axiom 3, we have then that $(-1) + a < a$, and we know $((-1) + a) \in F$, so this is a contradiction to a being the first point of F. So F has no first point.
Assume that F has a last point $b \in F$. By Corollary 6.24, $0 < 1$, so $0 + b < 1 + b$. It follows then by Axiom 3 that $b < 1 + b$, and we know $(1 + b) \in F$ so this is a contradiction to b being the last point of F. So F has no last point. $\square$