Field axioms and proofs

samrmay

August 2023

Contents

1 Binary operators

1.1 Definitions

To get to the field axioms and consequences, we first define and characterize binary operators on sets.

Definition 1.1 *For set F, call operator $\circ$ a binary operator if it takes the form*

$$\circ : F \times F \to F \tag{1}$$

Definition 1.2 *For set F and binary operator $\circ$, call $\circ$ associative if $\forall\, x, y, z \in F$,*

$$(x \circ y) \circ z = x \circ (y \circ z) \tag{2}$$

and call $\circ$ commutative if $\forall\, x, y \in F$,

$$x \circ y = y \circ x \tag{3}$$

A word on notation. For binary operator $\circ$ we use $x \circ y$ to mean $\circ(x, y)$ because it is more familiar. Then $x \circ y \circ z$ is technically ill-defined, but practically allowed when $\circ$ is associative and commutative.

Definition 1.3 *For set F and binary operator $\circ$, if there is an element $x_0 \in F$ s.t. $\forall\, y \in F$,*

$$x_0 \circ y = y \circ x_0 = y \tag{4}$$

Call x_0 an identity of $\circ$ in F.

Definition 1.4 *For element $x \in F$ and binary operator $\circ$ on F, if there is an element y s.t.*

$$x \circ y = y \circ x = x_0 \tag{5}$$

where x_0 is an identity of $\circ$, call y the inverse of x (with respect to $\circ$)

1.2 Theorems about binary operators

Note that in Defn. 1.3 and 1.4, we did not assume these elements were unique in F or for element x respectively. Here, we show that this is always the case. For all of the below assume a set F and binary operator $\circ$ on F.

Theorem 1.5 *Uniqueness of binary identity*

If $x_1, x_2 \in F$ are identities of $\circ$, then

$$x_1 = x_2 \tag{6}$$

Ie. there is a unique identity element in F, generally denoted $\mathbb{1}$.

Pf.

$$x_1 = x_1 \circ x_2 \tag{7}$$
$$x_1 \circ x_2 = x_2 \tag{8}$$

Since both x_1, x_2 are identities. Therefore $x_1 = x_2$. ■

Theorem 1.6 *Uniqueness of inverse*

For element $x \in F$, if $y_1, y_2 \in F$ are both inverses of x wrt an associative $\circ$, then

$$y_1 = y_2 \tag{9}$$

Ie. the inverse of x is unique and generally denoted x^{-1}.

Pf.

$$x \circ y_1 = x \circ y_2 = \mathbb{1} \tag{10}$$
$$y_1 \circ (x \circ y_1) = y_1 \circ (x \circ y_2) \tag{11}$$
$$(y_1 \circ x) \circ y_1 = (y_1 \circ x) \circ y_2 \tag{12}$$
$$\mathbb{1} \circ y_1 = \mathbb{1} \circ y_2 \tag{13}$$
$$y_1 = y_2 \tag{14}$$

Where we used the fact that $\circ$ is associative explicitly.■

This proof hints at a more general "cancellation law" for associative binary operators.

Theorem 1.7 *Cancellation laws*

For $x, y, z \in F$ and associative binary operator $\circ$,

$$x \circ z = y \circ z \iff x = y \tag{15}$$
$$z \circ x = z \circ y \iff x = y \tag{16}$$

Pf.

Need to prove four different statements:

$x \circ z = y \circ z \implies x = y$

$$x \circ z = y \circ z \tag{17}$$
$$(x \circ z) \circ z^{-1} = (y \circ z) \circ z^{-1} \tag{18}$$
$$x \circ (z \circ z^{-1}) = y \circ (z \circ z^{-1}) \tag{19}$$
$$x \circ \mathbb{1} = y \circ \mathbb{1} \tag{20}$$
$$x = y \tag{21}$$

$x = y \implies x \circ z = y \circ z$ follows directly by substitution.

Similarly for the left case,

$z \circ x = z \circ y \implies x = y$

$$z \circ x = z \circ y \tag{22}$$
$$(z^{-1} \circ z) \circ x = (z^{-1} \circ z) \circ y \tag{23}$$
$$x = y \tag{24}$$

and $x = y \implies z \circ x = z \circ y$ similarly follows directly by substitution. ■

We can also make some statements about inverses

Theorem 1.8 *Double inverse law*

For $\forall\, f \in F$ and associative binary operator $\circ$,

$$(f^{-1})^{-1} = f \tag{25}$$

where f^{-1} is the inverse of f wrt $\circ$. Ie. the inverse of the inverse of f is itself.

Pf.

By definition of the inverse,

$$f^{-1} \circ (f^{-1})^{-1} = \mathbb{1} \tag{26}$$
$$f \circ (f^{-1} \circ (f^{-1})^{-1}) = f \circ \mathbb{1} \tag{27}$$
$$(f \circ f^{-1}) \circ (f^{-1})^{-1} = f \tag{28}$$
$$\mathbb{1} \circ (f^{-1})^{-1} = f \tag{29}$$
$$(f^{-1})^{-1} = f \tag{30}$$

2 Fields

Define a field $\mathcal{F} = (F, +, \cdot)$ as a set F together with two binary operations:

$$+ : F \times F \to F \tag{31}$$
$$\cdot : F \times F \to F \tag{32}$$

called addition and multiplication respectively, which have the following 9 properties. As above, we take $x+y$ to denote $+(x, y)$. Do not be fooled by the familiarity! These $+, \cdot$ are arbitrary operators and not necessarily familiar addition and multiplication on real numbers. See examples below.

For all below properties, assume a triple $(F, +, \cdot)$

Property 2.1 $+$ *is associative*

Ie. $\forall\ x, y, z \in F$,

$$(x + y) + z = x + (y + z) \tag{33}$$

Property 2.2 *Additive identity*

There exists an element $0_{\mathcal{F}} \in F$ *s.t.* $\forall\ f \in F$

$$f + 0_{\mathcal{F}} = 0_{\mathcal{F}} + f = f \tag{34}$$

By Thm.1.5, $0_{\mathcal{F}}$ is unique. We also denote simply as 0 where the field is unambiguous.

Property 2.3 *Additive inverse*

$\forall f \in F, \exists -f \in F$ *s.t.*

$$f + (-f) = (-f) + f = 1 \tag{35}$$

By Thm. 1.6, $-f$ is unique for each $f \in F$.

Property 2.4 $\cdot$ *is associative*

Ie. $\forall\ x, y, z \in F$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{36}$$

Property 2.5 $\cdot$ *is commutative*

Ie. $\forall\ x, y \in F$,

$$x \cdot y = y \cdot x \tag{37}$$

Property 2.6 *Multiplicative identity*

There exists an element in F $1_{\mathcal{F}}$ *s.t.* $\forall f \in F$

$$f \cdot 1_{\mathcal{F}} = 1_{\mathcal{F}} \cdot f = f \tag{38}$$

By Thm. 1.5, $1_{\mathcal{F}}$ is unique. We denote also by 1 where the field is unambiguous.

Property 2.7 *Multiplicative inverse*

$\forall f \in F \setminus \{0\}$, $\exists f^{-1} \in F$ *s.t.*

$$f \cdot f^{-1} = f^{-1} \cdot f = 1 \tag{39}$$

By Thm. 1.6, f^{-1} is unique. Note also that we do not assume 0 *does not* have an inverse, we simply do not assume that it does.

Property 2.8 *Distributivity across addition*

$\forall f_1, f_2, f_3 \in F$

$$f_1 \cdot (f_2 + f_3) = (f_1 \cdot f_2) + (f_1 \cdot f_3) \tag{40}$$

Property 2.9 *Zero-One law*

The multiplicative and additive inverses for a triple $\mathcal{F} = (F, +, \cdot)$ are distinct. Ie. $0_{\mathcal{F}} \neq \mathbb{1}_{\mathcal{F}}$

2.1 Consequences of field axioms

Many intuitive properties of ”normal” numbers, such as commutativity of addition, are not axioms but follow directly. Again, assume an arbitrary field $\mathcal{F} = (F, +, \cdot)$

Theorem 2.10 $+$ *is commutative Ie.* $\forall\, x, y \in F$,

$$x + y = y + x \tag{41}$$

Pf. By commutativity of multiplication,

$$(1 + x) \cdot (1 + y) = (1 + y) \cdot (1 + x) \tag{42}$$

$$\tag{43}$$

By distributivity across addition,

$$((1 + x) \cdot 1) + ((1 + x) \cdot y) = ((1 + y) \cdot 1) + ((1 + y) \cdot x) \tag{44}$$

$$((1 \cdot 1) + (x \cdot 1)) + ((1 \cdot y) + (x \cdot y)) = ((1 \cdot 1) + (y \cdot 1)) + ((1 \cdot x) + (y \cdot x)) \tag{45}$$

$$(1 + x) + (y + (x \cdot y)) = (1 + y) + (x + (x \cdot y)) \tag{46}$$

By cancellation laws (Thm. 1.7), associativity of addition, and commutativity of multiplication,

$$1 + ((x + y) + (x \cdot y)) = 1 + ((y + x) + (y \cdot x)) \tag{47}$$

$$(x + y) + (x \cdot y) = (y + x) + (x \cdot y) \tag{48}$$

$$x + y = y + x \tag{49}$$

■

Other properties, like multiplication by 0 and -1 are also consequences:

Theorem 2.11 $\forall\, f \in F$,

$$0 \cdot f = 0 \tag{50}$$

Pf.

$$f = f \tag{51}$$
$$1 \cdot f = f \tag{52}$$
$$(1 + 0) \cdot f = f \tag{53}$$
$$(1 \cdot f) + (0 \cdot f) = f + 0 \tag{54}$$
$$f + (0 \cdot f) = f + 0 \tag{55}$$
$$0 \cdot f = 0 \tag{56}$$

Where we used cancellation law in the last line. ■

Theorem 2.12 $\forall f \in F$,

$$-1 \cdot f = -f \tag{57}$$

Pf. By the above theorem and since -1 is the additive inverse of 1,

$$0 \cdot f = 0 \tag{58}$$
$$(1 + (-1)) \cdot f = 0 \tag{59}$$
$$(1 \cdot f) + (-1 \cdot f) = 0 \tag{60}$$
$$f + (-1 \cdot f) = 0 \tag{61}$$

Then $-1 \cdot f$ is the additive inverse of f by definition. ■