1 The Definition of a Field

Definition 1.1. A *field* is a set $\mathbb{F}$ with two binary operations on $\mathbb{F}$ called addition, denoted $+$, and multiplication, denoted $\cdot$, satisfying the following *field axioms*:

FA0 **(Closure under Addition)** For all $x, y \in \mathbb{F}$, the sum $x + y$ is contained in $\mathbb{F}$

FA0 **(Closure under Multiplication)** For all $x, y \in \mathbb{F}$, the product $x \cdot y$ is contained in $\mathbb{F}$.

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

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

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

FA4 **(Additive Inverses)** For any $x \in \mathbb{F}$, there exists $y \in \mathbb{F}$ such that $x + y = y + x = 0$.
The element y is called the *additive inverse* of x and written $-x$.

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

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

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

FA8 **(Multiplicative Inverses)** For any $x \in \mathbb{F}$ such that $x \neq 0$, there exists $y \in \mathbb{F}$ such that $x \cdot y = y \cdot x = 1$.
The element y is called the *multiplicative inverse* of x and denoted x^{-1} or $\frac{1}{x}$.

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

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

FA0 is really a consequence of what it means to say that the operations of addition and multiplication are defined on $\mathbb{F}$, so "closure under addition" and "closure under multiplication" are usually not listed as axioms – but we have included them here as a reminder that they must always hold.

FA10 excludes one-element sets from being fields.

Definition 1.2. A field $\mathbb{F}$ is a *finite field* if $\mathbb{F}$ is a finite set.

2 Examples of Fields

Which of the sets (with their usual notion of addition and multiplication) are fields? Which are finite fields?

- Integers $\mathbb{Z}$
- Rational numbers $\mathbb{Q}$
- Real numbers $\mathbb{R}$
- Nonnegative reals $\mathbb{R}_{\geq 0}$
- Complex numbers $\mathbb{C}$
- 3×3 matrices $M_3(\mathbb{R})$ with entries in $\mathbb{R}$
- 3×3 invertible matrices $GL_3(\mathbb{R})$ with entries in $\mathbb{R}$
- $\mathbb{Z}/p\mathbb{Z}$ for p prime
- $\mathbb{Z}/n\mathbb{Z}$ for n composite
- $(\mathbb{Z}/n\mathbb{Z})^\times$ units modulo n
- Polynomials $\mathbb{Q}[x]$ in x with rational coefficients

3 Properties of Fields

Theorem 3.1. *Identity elements are unique. This means:*

1. *If* 0 *and* $0'$ *both satisfy* $0 + x = x + 0 = x$ *and* $0' + x = x + 0' = x$ *for all* x *in* $\mathbb{F}$*, then* $0 = 0'$*.*
2. *If* 1 *and* $1'$ *both satisfy* $x \cdot 1 = 1 \cdot x = x$ *and* $x \cdot 1' = 1' \cdot x = x$ *for all* x *in* $\mathbb{F}$*, then* $1 = 1'$*.*

Theorem 3.2. *Additive and multiplicative inverses are unique. This means for any* x *in* $\mathbb{F}$*,*

1. *If* $y, y' \in \mathbb{F}$ *satisfy* $x + y = 0$ *and* $x + y' = 0$*, then* $y = y'$*.*
2. *If* $y, y' \in \mathbb{F}$ *satisfy* $x \cdot y = 1$ *and* $x \cdot y' = 1$*, then* $y = y'$*.*

This theorem justifies our referring to "the" additive inverse and "the" multiplicative inverse of x, and using the notation $-x$ and x^{-1} or $\frac{1}{x}$ to refer to a specific uniquely-determined element.

Theorem 3.3. *If* $x \in \mathbb{F}$*, then* $-(-x) = x$*.*

Theorem 3.4. *If* $x \in \mathbb{F}$ *and* $x \neq 0$*, then* $(x^{-1})^{-1} = x$*.*

Theorem 3.5. *Let* $\mathbb{F}$ *be a field, and let* $a, b, c \in \mathbb{F}$*. If* $a + b = a + c$*, then* $b = c$*.*

Theorem 3.6. *Let* $\mathbb{F}$ *be a field, and let* $a, b, c \in \mathbb{F}$*. If* $a \cdot b = a \cdot c$ *and* $a \neq 0$*, then* $b = c$*.*

This is a crucial property of fields: we can divide by (or cancel) any nonzero element.

Theorem 3.7. *Let* $\mathbb{F}$ *be a field. If* $a \in \mathbb{F}$*, then* $a \cdot 0 = 0$*.*

Theorem 3.8. *Let* $\mathbb{F}$ *be a field, and let* $a, b \in \mathbb{F}$*. If* $a \cdot b = 0$*, then* $a = 0$ *or* $b = 0$*.*
In particular, fields have no (nonzero) zero divisors.