Field Theory Examples

Jason Sass

July 2, 2023

Fields

Example 1. smallest field $(\mathbb{Z}_2, +, \cdot)$
$(\frac{\mathbb{Z}}{2\mathbb{Z}}, +, \cdot)$ is a field.

Proof. The structure $(\frac{\mathbb{Z}}{2\mathbb{Z}}, +, \cdot)$ is a commutative ring with unity $1 \neq 0$.
Since $1 \cdot 1 = 1$, then $1^{-1} = 1$, so 1 has a multiplicative inverse.
Hence, every nonzero element of $\frac{\mathbb{Z}}{2\mathbb{Z}}$ has a multiplicative inverse.
Therefore, $\frac{\mathbb{Z}}{2\mathbb{Z}}$ is a field. $\square$

Example 2. field of rational numbers $(\mathbb{Q}, +, \cdot)$
$(\mathbb{Q}, +, \cdot)$ is a field.
Additive identity is $0 = \frac{0}{1}$.
Additive inverse of $\frac{a}{b}$ is $-\frac{a}{b}$.
Multiplicative identity is $1 = \frac{1}{1}$.
Multiplicative inverse of $\frac{a}{b} \in \mathbb{Q}^*$ is $\frac{b}{a} \in \mathbb{Q}^*$.

Proof. Addition and multiplication are binary operations defined on the set of all rational numbers $\mathbb{Q}$.
Addition over $\mathbb{Q}$ is associative and commutative.
$\square$

Proof. We prove $0 \in \mathbb{Q}$ is a right additive identity.
Since 0 and 1 are integers and $1 \neq 0$, then $0 = \frac{0}{1} \in \mathbb{Q}$.
Observe that $\frac{a}{b} + 0 = \frac{a}{b}$ for all $\frac{a}{b} \in \mathbb{Q}$.
Since $0 \in \mathbb{Q}$ and $\frac{a}{b} + 0 = \frac{a}{b}$ for all $\frac{a}{b} \in \mathbb{Q}$, then $0 \in \mathbb{Q}$ is a right additive identity. $\square$

Proof. We prove for every $\frac{a}{b} \in \mathbb{Q}$ there is a right additive inverse $\frac{-a}{b} \in \mathbb{Q}$.
Let $\frac{a}{b} \in \mathbb{Q}$.
Then $a, b \in \mathbb{Z}$ and $b \neq 0$.
Since $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$.
Since $-a$ and b are integers and $b \neq 0$, then $\frac{-a}{b} \in \mathbb{Q}$.
Observe that $\frac{a}{b} + \frac{-a}{b} = 0$.
Since $\frac{-a}{b} \in \mathbb{Q}$ and $\frac{a}{b} + \frac{-a}{b} = 0$, then $\frac{-a}{b}$ is a right additive inverse of $\frac{a}{b}$.
Therefore, for every $\frac{a}{b} \in \mathbb{Q}$ there is a right additive inverse $\frac{-a}{b} \in \mathbb{Q}$. $\square$

Proof. Multiplication over $\mathbb{Q}$ is associative and commutative. $\square$

Proof. We prove $1 \in \mathbb{Q}$ is a right multiplicative identity.

Since 1 is an integer and $1 \neq 0$, then $\frac{1}{1} \in \mathbb{Q}$.

Since $\frac{1}{1} \in \mathbb{Q}$ and $\frac{a}{b} \cdot 1 = \frac{a}{b}$ for all $\frac{a}{b} \in \mathbb{Q}$, then $1 \in \mathbb{Q}$ is a right multiplicative identity. $\square$

Proof. We prove for every nonzero $\frac{a}{b} \in \mathbb{Q}$ there is a right multiplicative inverse $\frac{b}{a} \in \mathbb{Q}$.

Let $\frac{a}{b} \in \mathbb{Q}$ and $\frac{a}{b} \neq 0$.

Since $\frac{a}{b} \in \mathbb{Q}$, then $a, b \in \mathbb{Z}$ and $b \neq 0$.

Since $\frac{a}{b} \neq 0$ and $b \neq 0$, then $a \neq 0$, so $\frac{b}{a} \neq 0$.

Since $a, b \in \mathbb{Z}$ and $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

Since $b, a \in \mathbb{Z}$ and $a \neq 0$, then $\frac{b}{a} \in \mathbb{Q}$.

Observe that

$$\begin{aligned} \frac{a}{b} \cdot \frac{b}{a} &= \frac{ab}{ba} \\ &= \frac{ab}{ab} \\ &= 1. \end{aligned}$$

Thus, $\frac{a}{b} \cdot \frac{b}{a} = 1$, so $\frac{b}{a} \in \mathbb{Q}$ is a right multiplicative inverse.

Therefore, for every nonzero $\frac{a}{b} \in \mathbb{Q}$ there is a right multiplicative inverse $\frac{b}{a} \in \mathbb{Q}$. $\square$

Proof. We prove multiplication is left distributive over addition.

Since $\frac{m}{n}(\frac{p}{q} + \frac{r}{s}) = \frac{m}{n} \cdot \frac{p}{q} + \frac{m}{n} \cdot \frac{r}{s}$ for all $\frac{m}{n}, \frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$, then multiplication is left distributive over addition. $\square$

Proof. We prove multiplicative identity $1 \in \mathbb{Q}$ is distinct from additive identity $0 \in \mathbb{Q}$.

Since 0 and 1 are integers, then $1 \neq 0$.

Since $1 = \frac{1}{1} \in \mathbb{Q}$ and $0 = \frac{0}{1} \in \mathbb{Q}$, then $\frac{1}{1} \neq \frac{0}{1}$, so multiplicative identity is distinct from additive identity. $\square$

Proof. Since addition and multiplication are binary operations on $\mathbb{Q}$ and addition over $\mathbb{Q}$ is associative and commutative and $0 \in \mathbb{Q}$ is a right additive identity and for every $\frac{a}{b} \in \mathbb{Q}$ there is a right additive inverse $\frac{-a}{b} \in \mathbb{Q}$ and multiplication over $\mathbb{Q}$ is associative and commutative and $1 \in \mathbb{Q}$ is a right multiplicative identity and for every nonzero $\frac{a}{b} \in \mathbb{Q}$ there is a right multiplicative inverse $\frac{b}{a} \in \mathbb{Q}$ and multiplication is left distributive over addition and multiplicative identity $1 \in \mathbb{Q}$ is distinct from additive identity $0 \in \mathbb{Q}$, then $(\mathbb{Q}, +, \cdot)$ is a field. $\square$

Example 3. field of real numbers $(\mathbb{R}, +, \cdot)$

$(\mathbb{R}, +, \cdot)$ is a field.

Additive identity is 0.

Additive inverse of a is $-a$.

Multiplicative identity is 1.
Multiplicative inverse of $a \in \mathbb{R}^*$ is $\frac{1}{a} \in \mathbb{R}^*$.

Proof. TODO $\square$

Example 4. field of complex numbers $(\mathbb{C}, +, \cdot)$
$(\mathbb{C}, +, \cdot)$ is a field.
Additive identity is $0 = 0 + 0i$.
Let $a, b \in \mathbb{R}$.
Additive inverse of $z = a + bi$ is $-z = -a - bi$.
Multiplicative identity is $1 = 1 + 0i$.
Let $z \in \mathbb{C}^*$.
Multiplicative inverse of $z = |z|\text{cis }\theta$ is $z^{-1} = \frac{1}{z} = \frac{1}{|z|}\text{cis }(-\theta)$

Proof. TODO $\square$

Example 5. $\mathbb{Z}_p$ is a field when p is prime
Let $p \in \mathbb{Z}^+$.
If p is prime, then $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof. TODO $\square$

Example 6. Gaussian integers
Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
Then $(\mathbb{Z}[i], +)$ is an abelian group under complex addition.
$(\mathbb{Z}[i], +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$ known as the **Gaussian integers**.

Proof. TODO $\square$

Example 7. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field under addition and multiplication of $\mathbb{R}$.

Proof. TODO $\square$