

□ Prove that the set of rational numbers \mathbb{Q} , equipped with the two binary operations of addition and multiplication forms a field.

Soln : A set F with two binary operations $+$ and \cdot is a field if the following hold :

1. $(F, +)$ is an abelian (commutative) group :

- (a) closure under $+$,
- (b) associativity of $+$,
- (c) identity element 0 ,
- (d) additive inverses
- (e) commutativity of $+$

2. $(F \setminus \{0\}, \cdot)$ is an abelian group :

- (a) closure under \cdot
- (b) associativity of \cdot
- (c) identity element 1
- (d) inverse multiplicative for every non zero element
- (e) commutativity of \cdot

3. Distributivity : $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in F$

Finally, $0 \neq 1$ must hold (so the two ~~id~~ identities are distinct.)

Verification for \mathbb{Q} :

Every rational number can be written as $\frac{a}{b}$ with $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$.

1. $(\mathbb{Q}, +)$ is an abelian group.

• Closure under addition:

if $x = a/b$ and $y = c/d$ then

$$x+y = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

and $ad+bc$ and bd are integers with $bd \neq 0$

Thus $x+y \in \mathbb{Q}$

→ Associativity: addition of rationals is

associative because it follows from associativity of integer addition.

for rationals x, y, z $(x+y)+z = x+(y+z)$.

→ Additive Identity : 0 satisfies $x+0=x$ for every rational x .

→ Additive inverse : for $x = a/b$, the additive inverse is $-x = \frac{-a}{b}$, which is rational and satisfies $x+(-x)=0$.

→ Commutativity :

$$\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$$

Hence, $(\mathbb{Q}, +)$ is an abelian group.

2. $(\mathbb{Q} \setminus \{0\})$ is an abelian group

Closure under multiplication :

$$\text{with } x = \frac{a}{b}, y = \frac{c}{d}$$

$$x \cdot y = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

and ac, bd , are integers with $bd \neq 0$, So the product is in \mathbb{Q} . If neither x nor y is zero then $ac \neq 0$, so the product is non zero.

• Associativity : Multiplication of rationals is associative.

• Multiplicative identity : 1 satisfies $1 \cdot x = x$ for all $x \in \mathbb{Q}$

• Multiplicative inverse : For a non-zero rational

$x = \frac{a}{b}$ with $a \neq 0$, the inverse is b/a (an element of \mathbb{Q}) and $\frac{a}{b} \cdot \frac{b}{a} = 1$

• Commutativity : $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$ because integer multiplication is commutative. Thus $(\mathbb{Q} \setminus \{0\}, \cdot)$ is an abelian group.

3. Distributivity : For rationals $x = \frac{a}{b}$, $y = \frac{c}{d}$, $z = \frac{e}{f}$

$$x \cdot (y + z) = \frac{a}{b} \left(\frac{c}{d} + \frac{e}{f} \right) = \frac{a}{b} \cdot \frac{cf + de}{df} = \frac{acf}{bdf} + \frac{ade}{bdf}$$

$$= \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$$

$$= x \cdot y + x \cdot z$$

4. $0 \neq 1$

In \mathbb{Q} , 0 is $\frac{0}{1}$ and 1 is $\frac{1}{1}$. These are different rationals, so $0 \neq 1$. This prevents the degenerate one-element ring.

All field axioms hold for \mathbb{Q} : $(\mathbb{Q}, +)$ is an abelian group, $(\mathbb{Q} \setminus \{0\}, \cdot)$ is an abelian group, multiplication distributes over addition, and $0 \neq 1$. Therefore \mathbb{Q} with usual addition and multiplication is a field.