I.3.1. Fields

a) Show that the set of rational numbers $\mathbb{Q}$ forms a commutative field under the ordinary addition and multiplication of numbers.

b) Consider a set F with two elements, $F = \{\theta, e\}$. On F, define an operation "plus" (+), about which we assume nothing but the defining properties

$$\theta + \theta = \theta \quad , \quad \theta + e = e + \theta = e \quad , \quad e + e = \theta$$

Further, define a second operation "times" ($\cdot$), about which we assume nothing but the defining properties

$$\theta \cdot \theta = e \cdot \theta = \theta \cdot e = \theta \quad , \quad e \cdot e = e$$

Show that with these definitions (and **no** additional assumptions), F is a field.

(7 points)

Solution

a) $\mathbb{Q}$ is a group under addition with neutral element $0 \in \mathbb{Q}$:

(i) $q_1 + q_2 \in \mathbb{Q} \; \forall \; q_1, q_2 \in \mathbb{Q}$

(ii) Addition of rational numbers is associative and commutative

(iii) The number zero is an element of $\mathbb{Q}$, and $0 + q = q \; \forall \; q \in \mathbb{Q}$

(iv) Let $q \in \mathbb{Q}$. Then $\exists - q \; : \; q + (-q) = 0$. 1pt

Furthermore, $\mathbb{Q} \setminus \{0\}$ is a group under multiplication:

(i) $q_1 q_2 \in \mathbb{Q} \; \forall \; q_1, q_2 \in \mathbb{Q}$

(ii) Multiplication of rational numbers is associative and commutative

(iii) The number 1 is an element of $\mathbb{Q}$, and $1 \cdot q = q \; \forall \; q \in \mathbb{Q}$

(iv) Let $q \in \mathbb{Q} \setminus \{0\}$. Then $\exists q^{-1} \equiv 1/q \;:\; q \cdot q^{-1} = 1$

Finally, ordinary addition and multiplication on $\mathbb{Q}$ are distributive. $\Rightarrow \mathbb{Q}$ is a commutative field.

1pt

b) We need to show that F is a group under addition.

(i) $a + b \in F \; \forall \; a, b \in F$ by definition $\Rightarrow$ Closure ✓

(ii) $(\theta + e) + \theta = e + \theta = e = \theta + (e + \theta)$
$(e + e) + \theta = \theta + \theta = \theta = e + (e + \theta)$
$\Rightarrow$ "+" is associative 1pt

(iii) θ is the neutral element by definition

(iv) $-\theta = \theta$ and $-e = e$ by definition $\Rightarrow$ existence of an inverse ✓

(v) "+" is commutative by definition

$\Rightarrow F$ is an abelian group under "+" 1pt

We also need to show that $F \setminus \{\theta\}$ is a group under the multiplication "$\cdot$". But $F \setminus \{\theta\} = \{e\}$, and hence the group axioms are all fulfilled by definition. 1pt

Finally, we need to check the distributive laws. Since the multiplication is abelian we only need to show that

$$(a+b)\cdot c = a\cdot c + b\cdot c \ \forall a,b,c \in F \qquad (*)$$

(i) $c = \theta \Rightarrow (a+b)\cdot c = (a+b)\cdot\theta = a\cdot c + a\cdot b \ \forall\ a,b \in F$ 1pt

(ii) $c = e$. If either $a = \theta$ or $b = \theta$, $(*)$ holds.
If $a = b = e$, then $(e+e)\cdot e = \theta\cdot e = \theta$
and $e\cdot e + e\cdot e = \theta + \theta = \theta$

$\Rightarrow$ The distributive laws hold

$\Rightarrow$ F is a field. 1pt