IT-24667
Md. Safayat Hossain

Assignment: Prove that the set of rational numbers $\mathbb{Q}$, equipped with two binary operations of addition and multiplication, forms a field.
or,
$\mathbb{Q} = \{ p/q \mid p, q \in \mathbb{Z}, q \neq 0 \}$, equipped with two binary operations,
Addition: $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$,
Multiplication: $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, forms a field.

proof: We verify the field axioms.

① Well-definedness of operations.
A rational numbers is an equivalence class of pairs (p, q) with $q \neq 0$ under $p/q = \frac{p'}{q'} \Leftrightarrow pq' = p'q$
The usual formulas

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + rq}{qs}, \quad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$$

respect this equivalence, so addition and multiplication are well defined on $\mathbb{Q}$.

② Closure: If $p/q, r/s \in \mathbb{Q}$ (with $q, s \neq 0$)
then $\frac{p}{q} + \frac{r}{s} = \frac{ps + rq}{qs} \in \mathbb{Q}, \quad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \in \mathbb{Q}$
Since integers are closed under "+" and "·" and $qs \neq 0$.

IT-24667
Md. Safayat Hossain

3. Associativity of "+" and ".": Associativity follows from associativity in $\mathbb{Z}$ and the formulas for sum/product of fractions; e.g. for addition compute both $\left(\frac{p}{q}+\frac{r}{s}\right)+\frac{t}{u}$ and $\frac{p}{q}+\left(\frac{r}{s}+\frac{t}{u}\right)$ and simplify to the Same fraction $\frac{psu+rqu+tqs}{qsu}$ and similarly for multiplication.

4. commutativity of "+" and ".": from commutativity in $\mathbb{Z}$:

$$\frac{p}{q}+\frac{r}{s}=\frac{ps+rq}{qs}=\frac{rq+ps}{sq}=\frac{r}{s}+\frac{p}{q}$$

and likewise. $\frac{p}{q}\cdot\frac{r}{s}=\frac{pr}{qs}=\frac{rp}{sq}=\frac{r}{s}\cdot\frac{p}{q}$

5. Identities:

Additive identity: $0=\frac{0}{1}$; For any $\frac{p}{q}$.

$$\frac{p}{q}+\frac{0}{1}=\frac{p.1+0.q}{q.1}=\frac{p}{q}$$

multiplicative identity: $1=\frac{1}{1}$; For any $\frac{p}{q}$

$$\frac{p}{q}\cdot\frac{1}{1}=\frac{p.1}{q.1}=\frac{p}{q}.$$

IT-24667
md. Safayat Hossain

6. Additive Inverse: For $\frac{p}{q} \in \mathbb{Q}$, the additive inverse is $-\frac{p}{q} = \frac{-p}{q}$ since

$$\frac{p}{q} + \frac{-p}{q} = \frac{pq + (-p)q}{q^2} = \frac{0}{q^2} = 0$$

7. Multiplicative Inverse (for nonzero elements):

If $\frac{p}{q} \in \mathbb{Q}$ and $\frac{p}{q} \neq 0$ then $p \neq 0$. The inverse is $\left(\frac{p}{q}\right)^{-1} = \left(\frac{q}{p}\right)$

and indeed $\frac{p}{q} \cdot \frac{q}{p} = \frac{pq}{qp} = 1$. (well-defined because if $\frac{p}{q} = \frac{p'}{q'}$ then also $\frac{q}{p} = \frac{q'}{p'}$)

8. Distributive law:

For any $\frac{p}{q}, \frac{r}{s}, \frac{t}{u} \in \mathbb{Q}$

$$\frac{p}{q}\left(\frac{r}{s} + \frac{t}{u}\right) = \frac{p}{q} \cdot \frac{ru + ts}{su} = \frac{p(ru + ts)}{qsu}$$

$$= \frac{pru + pts}{qsu}$$

$$= \frac{pr}{qs} + \frac{pt}{qu}$$

$$= \frac{p}{q} \cdot \frac{r}{s} + \frac{p}{q} \cdot \frac{t}{u}$$

so, multiplication distributes over addition.

All field axioms (closure, associativity, commutativity, identities, inverses and distributivity) hold, so $(\mathbb{Q}, +, \cdot)$ is a field.