Assignment - 03

Md. Samim Hossain
IT-24635

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

We take the rational numbers $\mathbb{Q}$ to be the set of equivalence classes of ordered pairs (a,b) with $a,b \in \mathbb{Z}$ and $b' \neq 0$, where $(a,b) \sim (a',b')$ if $ab' = a'b$. We identify the class of (a,b) with the usual fraction $\frac{a}{b}$.

Define addition and multidication in the usual way:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

for $b \neq 0$, $d \neq 0$. Below, we show these operations make $\mathbb{Q}$ a field.

1. The operations are well-defined

We must check that if $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ then $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ and $\frac{ac}{bd} = \frac{a'c'}{b'd'}$

(P.T.O.)

From $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ we have $ab' = a'b$

and $cd' = c'd$ compute

$$(ad+bc)\,b'd' = (ab')(dd') + (bc)(b'd') = (a'b)(dd') + (bc)(b'd')$$

and similarly expand the right-hand numerator times

$bdb'd'$. Rearranging and using $ab' = a'b$, $cd' = c'd$.

Shows both cross-products are equal, therefore

the sums (and similarly the products) represent the

same equivalence class. So addition and multiplication

are well-defined.

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

Take any $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$.

- closure $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ is a rational

number since $bd \neq 0$...

⊛ Associativity : follows from associativity of integer addition.

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+e(bd)}{(bd)f}$$

and a similar expansion for $\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$; both give the same numerator by associativity / commutativity of integers operations.

⊛ Identity : $0=\frac{0}{1}$ satisfies $\frac{a}{b}+0=\frac{a}{b}$

⊛ Inverse : additive inverse of $\frac{a}{b}$ is $-\frac{a}{b}=\frac{-a}{b}$

because $\frac{a}{b}+\frac{-a}{b}=\frac{0}{b}=0$.

⊛ Commutativity : $\frac{a}{b}+\frac{c}{d}=\frac{bc+ad}{bd}=\frac{c}{d}+\frac{a}{b}$

Thus $(\mathbb{Q},+)$ is a abelian group.

3. Multiplication on $\mathbb{Q}/\{0\}$ is an abelian group (except we first show ring axioms)

⊛ closure : product $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$ is rational since $bd\neq 0$

(iv) Associativity and commutativity: follow from associativity and commutativity of integer multiplication:

$$\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f} = \frac{ac}{bd}\cdot\frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)}$$

$$= \frac{a}{b}\cdot\frac{ce}{df} = \frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right)$$

(v) Multiplicative identity: $1 = \frac{1}{1}$ satifies $\frac{a}{b}\cdot 1 = \frac{a}{b}$

(vi) Distributive: for addition and multiplication,

$$\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right) = \frac{a}{b}\cdot\frac{cf+ed}{df} = \frac{a(cf+ed)}{bdf}$$

$$= \frac{acf+aed}{bdf} = \frac{ac}{bd}+\frac{ae}{bf} = \frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f},$$

using integer distributivity.

So $\mathbb{Q}$ is a commutative ring with unity 1.

4. Multiplicative inverse exist for nonzero rationals

Take a nonzero rational $\frac{a}{b}$ (so $a \neq 0$, $b \neq 0$). Its multiplicative inverse is $\frac{b}{a}$ because

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = 1$$

We also must check this inverse is well-defined: If

$\frac{a}{b} = \frac{a'}{b'}$ and $a \neq 0$, then $ab' = a'b$.

Multiplying both sides by $1/(aa')$ is informal but the correct check is $\frac{b}{a} = \frac{b'}{a'}$ if and only if $ba' = b'a$; but from $ab' = a'b$ we get exactly $ba' = b'a$, so inverse agree for different representatives. (Thus the operation of taking $\frac{a}{b} \mapsto \frac{b}{a}$ is well-defined on equivalence classes.)

5. Nontriviality: $0 \neq 1$

clearly $\frac{0}{1} \neq \frac{1}{1}$ because if $0 \cdot 1 = 1 \cdot 1$ then $0 = 1$, contradicting the integer's properties. So the field is not the zero ring.

(P.T.O.)

Putting the pieces together : $\mathbb{Q}$ with the usual addition and multiplication is a commutative ring with unity in which every non zero element has a multiplicative inverse. Therefore $\mathbb{Q}$ is a field.