# Constructing the Rationals

W. Patrick Hooper

December 3, 2018

Recall that the set of integers $\mathbb{Z}$ is the set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$. In these notes we will assume an understanding of $\mathbb{Z}$ and construct the rational numbers

$$\mathbb{Q} = \left\{ \frac{p}{q} : \ p, q \in \mathbb{Z} \quad \text{and} \quad q \neq 0 \right\}.$$

## 1. The integers

Let $S$ be a set. A *binary operation* on $S$ is a function of the form

$$b : S \times S \to S.$$

For example, addition and multiplication are binary operations on $\mathbb{Z}$.

A *commutative ring* is a set together with binary operations $+$ and $\cdot$ (which take as input an ordered pair of elements of $R$ and produce a new element of $R$) that satisfy the *commutative ring axioms*:

**A1.** $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$ ($+$ is associative).

**A2.** $a + b = b + a$ for all $a, b \in R$ ($+$ is commutative).

**A3.** There is an element $0 \in R$ so that $a + 0 = a$ for all $a \in R$ (0 is the additive identity).

**A4.** For each $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$ ($-a$ is the additive inverse of $a$).

**M1.** $a(bc) = (ab)c$ for all $a, b, c \in R$ ($\cdot$ is associative).

**M2.** $ab = ba$ for all $a, b \in R$ ($\cdot$ is commutative).

**M3.** There is an element $1 \in R$ so that $a \cdot 1 = a$ for all $a \in R$ (1 is the multiplicative identity).

**DL.** $a(b + c) = ab + ac$ for all $a, b, c \in R$ (distributive law).

The integers $\mathbb{Z}$ are an example of a commutative ring. Another example is the ring of $\mathbb{Z}[x]$ of polynomials in a variable $x$ with coefficients in $\mathbb{Z}$. A typical element of $\mathbb{Z}[x]$ is $3x^3 - 7x^2 + 9$, and multiplication and addition operate as you expect on $\mathbb{Z}[x]$.

The following mirror's Ross' Theorem 3.1:

**Theorem 1.** *Suppose $R$ is a commutative ring. Then*

**(i)** *$a + c = b + c$ implies $a = b$ for all $a, b \in R$;*

**(ii)** *$a \cdot 0 = 0$ for all $a \in R$;*

**(iii)** *$(-a)b = -ab$ for all $a, b \in R$;*

**(iv)** *$(-a)(-b) = ab$ for all $a, b \in R$.*

*Proof.* Proofs work the same as in Ross' proof of Theorem 3.1. Note that he uses the missing axiom **M4** to prove **(v)** and **(vi)**, which we don't include in our list. □

A commutative ring $R$ is called an *integral domain* if the following statement is true:

**ID.** $a \neq 0$ and $b \neq 0$ imply $ab \neq 0$ for all $a, b \in R$.

From basic facts about arithmetic, we know that $\mathbb{Z}$ is an integral domain. (It follows from order properties: $a > 0$ and $b > 0$ implies $ab > 0$, $a > 0$ and $b < 0$ implies $ab < 0$, etc.)

Statement **ID** is the contrapositive of statement **(vi)** of Ross' Theorem 3.1, and this statement implies statement **(v)** of Ross' Theorem:

**Proposition 2** (Cancellation in multiplication)**.** *Suppose $R$ is an integral domain. Then $ab = ac$ implies $b = c$ whenever $a, b, c \in R$ and $a \neq 0$.*

*Proof.* Suppose that $a \neq 0$ and $ab = ac$. Adding $-ac$ to both sides and using **A4** yields $ab + (-ac) = 0$. By **(iii)** and commutativity we have $-ac = a(-c)$. Thus, by **DL** we see

$$0 = ab + (-ac) = ab + a(-c) = a\big(b + -c\big).$$

By the contrapositive of **ID**, we see that since $a\big(b + -c\big) = 0$ we have either $a = 0$ or $b + -c = 0$. Since we already know $a \neq 0$, we must have $a + -c = 0$. Then by adding $c$ to both sides we see $a = c$. □

A *field* is a commutative ring $F$ which satisfies the additional axiom:

**M4.** For each $a \in F$ with $a \neq 0$, there is an element $a^{-1}$ such that $aa^{-1} = 1$.

The goal of this note is to construct the rationals $\mathbb{Q}$ from $\mathbb{Z}$ and to convince you that $\mathbb{Q}$ is a field.

## 2. Equivalence relations and "well-defined"

Let $S$ be a set. Recall that an equivalence relation $\sim$ on $S$ is a relation on $S$ which reflexive, symmetric, and transitive. Given $s \in S$, the *equivalence class* of $s$ is

$$[s] = \{t \in S : \ s \sim t\}.$$

Recall that $[s_1] = [s_2]$ if and only if $s_1 \sim s_2$.

Let $Q = S/\sim$ denote the set of equivalence classes on $Q$. Let $b : S \times S \to S$ be a binary operation. We say that $b$ determines *well-defined* binary operation on $Q$ if

$$s_1 \sim s_2 \quad \text{and} \quad t_1 \sim t_2 \quad \text{imply} \quad b(s_1, t_1) \sim b(s_2, t_2).$$

The reason to make this definition is the following:

**Proposition 3.** *If $b : S \times S \to S$ is well-defined on $Q$, then there is a* quotient binary operation

$$b_Q : Q \times Q \to Q$$

*that satisfies $b_Q([s],[t]) = [b(s,t)]$ for all $s, t \in S$.*

*Proof.* We need to explain that equal inputs produce equal outputs. Suppose $([s_1],[t_1]) = ([s_2],[t_2])$. We'll show that $[b(s_1,t_1)] = [b(s_2,t_2)]$.

Since $([s_1],[t_1]) = ([s_2],[t_2])$, we know $[s_1] = [s_2]$ and $[t_1] = [t_2]$ or equivalently $s_1 \sim s_2$ and $t_1 \sim t_2$. Since $b$ determines a well-defined action on $Q$, we know $b(s_1,t_1) \sim b(s_2,t_2)$. But this is equivalent to saying that $[b(s_1,t_1)] = [b(s_2,t_2)]$. Since by definition, $b_Q([s_1],[t_1]) = [b(s_1,t_1)]$ and $b_Q([s_2],[t_2]) = [b(s_2,t_2)]$, we have shown that the equal inputs produce equal outputs as desired. □

**Remark 4.** *We have defined equivalence for binary operations, but there are similar definitions for the notion of well-defined for functions from a set to itself. Sometimes we might want to involve more equivalence relations. For instance if $\sim$ is an equivalence relation on $A$ and $\approx$ is an equivalence relation on $B$, then a function $f : A \to B$ determines a* well-defined *function $f' : (A/\sim) \to (B/\approx)$ if $a_1 \sim a_2$ implies $f(a_1) \approx f(a_2)$.*

## 3. Construction of the set of rationals

We will now construct the set of rationals. Define the set

$$P = \{(p,q) \in \mathbb{Z} \times \mathbb{Z} : \ q \neq 0\} \subset \mathbb{Z} \times \mathbb{Z}. \tag{1}$$

Let $\sim$ to be the relation on $P$ defined so that

$$(a,b) \sim (c,d) \quad \text{if and only if} \quad ad = bc.$$

**Lemma 5.** *The relation $\sim$ is an equivalence relation on $P$.*

*Proof.* To see $\sim$ is reflexive, fix $(p,q) \in P$. By definition of $\sim$, $(p,q) \sim (p,q)$ if and only if $pq = qp$, which is true by commutativity of multiplication (axiom **M2**).

To see $\sim$ is symmetric, suppose $(a,b) \sim (c,d)$. This means that $ad = bc$. Again by commutativity of multiplication, we see $cb = da$. Again by definition of $\sim$, we therefore have $(c,d) \sim (a,b)$.

To see $\sim$ is transitive, suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then we have $ad = bc$ and $cf = de$. By multiplying by $f$ and $b$ respectively, we see

$$adf = bcf \quad \text{and} \quad bcf = bde.$$

Therefore we have $adf = bde$. By cancellation of multiplication (Proposition 2), since $d \neq 0$, we have $af = be$. Then by definition of $\sim$, we see that $(a,b) \sim (e,f)$. □

Formally, we define $\mathbb{Q}$ to be the collection of equivalence classes $P/\sim$.

**Remark 6.** *The set $P$ and the relation $\sim$ make sense for any commutative ring $R$. The proof of Lemma 5 works for any integral domain $R$. In this case, the quotient $P/\sim$ is called the* field of fractions *of the integral domain $R$. It is always a field when endowed with binary operations as described in the next subsection.*

## 4. Addition and multiplication of rationals

Let $P$ be as in (1). Let $\oplus$ denote the binary operation on $P$ defined by

$$(a, b) \oplus (c, d) = (ad + bc, bd).$$

**Proposition 7.** *The operation $\oplus$ induces a well-defined binary operation on $\mathbb{Q} = P/\sim$.*

*Proof.* Suppose that $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$. Define

$$(e_1, f_1) = (a_1, b_1) \oplus (c_1, d_1) \quad \text{and} \quad (e_2, f_2) = (a_2, b_2) \oplus (c_2, d_2).$$

We need to show that $(e_1, f_1) \sim (e_2, f_2)$.

Since $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$ we know

$$a_1 b_2 = b_1 a_2 \quad \text{and} \quad c_1 d_2 = d_1 c_2. \tag{2}$$

By definition of $\oplus$, we see that

$$e_1 = a_1 d_1 + b_1 c_1, \quad f_1 = b_1 d_1, \quad e_2 = a_2 d_2 + b_2 c_2, \quad \text{and} \quad f_2 = b_2 d_2.$$

To see that $(e_1, f_1) \sim (e_2, f_2)$ observe using

$$\begin{array}{rcll} e_1 f_2 & = & (a_1 d_1 + b_1 c_1)(b_2 d_2) & \\ & = & a_1 b_2 d_1 d_2 + b_1 b_2 c_1 d_2 & \text{by } \mathbf{DL} \text{ and } \mathbf{M2} \\ & = & b_1 a_2 d_1 d_2 + b_1 b_2 d_1 c_2 & \text{by (2)} \\ & = & (a_2 d_2 + b_2 c_2)(b_1 d_1) & \text{by } \mathbf{DL} \text{ and } \mathbf{M2} \\ & = & e_2 f_1. & \end{array}$$

Since $e_1 f_2 = e_2 f_1$ we see that $(e_1, f_1) \sim (e_2, f_2)$ as desired. □

We'll let $+$ denote the binary operation of $\mathbb{Q} = P/\sim$ induced by the binary $\otimes$. (See Proposition 3.)

Similarly, we define a binary operation $\odot$ on $P$ by

$$(a, b) \odot (c, d) = (ac, bd).$$

**Proposition 8.** *The binary operation $\odot$ induces a well-defined binary operation on $\mathbb{Q} = P/\sim$.*

*Proof.* Suppose that $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$. Define

$$(e_1, f_1) = (a_1, b_1) \dot{(} c_1, d_1) \quad \text{and} \quad (e_2, f_2) = (a_2, b_2) \odot (c_2, d_2).$$

We need to show that $(e_1, f_1) \sim (e_2, f_2)$.

Since $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$ we again get (2). This time we have

$$e_1 = a_1 c_1, \quad f_1 = b_1 d_1, \quad e_2 = a_2 c_2, \quad \text{and} \quad f_2 = b_2 d_2.$$

To see $(e_1, f_1) \sim (e_2, f_2)$ observe using (2) that

$$e_1 f_2 = a_1 b_2 c_1 d_2 = b_1 a_2 d_1 c_2 = e_2 f_1.$$

□

We'll let $\cdot$ denote the binary operation of $\mathbb{Q} = P/\sim$ induced by the binary $\otimes$.

## 5. The rationals form a field

We'll write $[p, q]$ to denote the $\sim$-equivalence class of $(p, q)$. We'll avoid writing $\frac{p}{q}$ because this would tempt us to use ordinary arithmetic properties. We are trying to prove that the usual things we want to do with rationals actually work for our definition of the rationals!

**Theorem 9.** *The rational numbers $\mathbb{Q} = P/\sim$ together with the binary operations $+$ and $\cdot$ form a field.*

*Proof.* **A1.** To see that addition is associative, let $[a, b], [c, d], [e, f] \in \mathbb{Q}$. Then

$$\big([a, b] + [c, d]\big) + [e, f] = [ad + bc, bd] + [e, f] = [(ad + bc)f + bde, bdf], \quad \text{and}$$

$$[a, b] + \big([c, d] + [e, f]\big) = [a, b] + [cf + de, df] = [adf + b(cf + de), bdf].$$

Observe that both coordinates coincide (using arithmetic properties of $\mathbb{Z}$).

**A2.** To see that addition is commutative, let $[a, b], [c, d] \in \mathbb{Q}$. Then

$$[a, b] + [c, d] = [ad + bc, bd] \quad \text{and} \quad [c, d] + [a, b] = [cb + ad, db].$$

By arithmetic properties of $\mathbb{Z}$, these coincide.

**A3.** We will show that $[0, 1]$ is the additive identity. Let $[a, b] \in \mathbb{Q}$. Then

$$[0, 1] + [a, b] = [0b + 1a, 1b] = [a, b].$$

**A4.** We will show that $[-a, b]$ is the negation $-[a, b]$. Let $[a, b] \in \mathbb{Q}$ be arbitrary. Then,

$$[a, b] + [-a, b] = [ab + (-a)b, b^2] = [0, b^2],$$

since $-(ab) = (-a)b$ algebraic properties of $\mathbb{Z}$ (namely **(iii)**). Now we observe that $[0, b^2] = [0, 1]$ since this is equivalent to $(0, b^2) \sim (0, 1)$ which we can see is true by definition of $\sim$ since $0 \cdot 1 = 0$ and $b^2 \cdot 0 = 0$.

**M1.** We will show that multiplication is associative. Let $[a, b], [c, d], [e, f] \in \mathbb{Q}$. Then

$$[a, b] \cdot ([c, d] \cdot [e, f]) = [a, b] \cdot [ce, df] = [ace, bdf], \quad \text{and}$$

$$([a, b] \cdot [c, d]) \cdot [e, f] = [ac, bd] \cdot [e, f] = [ace, bdf].$$

**M2.** We will show that multiplication is commutative. Let $[a, b], [c, d] \in \mathbb{Q}$. Then

$$[a, b] \cdot [c, d] = [ac, bd] = [ca, db] = [c, d] \cdot [a, b].$$

**M3.** We will show that $[1, 1]$ is the multiplicative identity. Let $[a, b] \in \mathbb{Q}$. Then

$$[1, 1] \cdot [a, b] = [1a, 1b] = [a, b].$$

**M4.** We will show that $[a, b]^{-1} = [b, a]$. To see this, observe

$$[a, b] \cdot [b, a] = [ab, ba].$$

We claim that $[ab, ba] = [1, 1]$ or equivalently that $(ab, ba) \sim (1, 1)$. To check this we need to see that $ab \cdot 1 = ba \cdot 1$ which is true by commutativity of multiplication in $\mathbb{Z}$.

**DL.** To see that the distributive law holds, let $[a, b], [c, d], [e, f] \in \mathbb{Q}$. Then

$$[a, b] \cdot ([c, d] + [e, f]) = [a, b] \cdot [cf + de, df] = [a(cf + de), bdf], \quad \text{and}$$

$$[a, b] \cdot [c, d] + [a, b] \cdot [e, f] = [ac, bd] + [ae, bf] = [acbf + bdae, bdbf].$$

We must show that $(a(cf + de), bdf) \sim (acbf + bdae, bdbf)$. We have

$$a(cf + de)bdbf = ab^2df(cf + de) \quad \text{and} \quad bdf(acbf + bdae) = ab^2df(cf + de)$$

as desired. □

Now that we have proven that $\mathbb{Q} = P/\sim$ forms a field, we introduce the usual notation. We will write $\frac{p}{q}$ to represent $[p, q]$ (the $\sim$-equivalence class of $(p, q) \in P$). Then addition and multiplication look as we expect:

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

Also since $(ab, ac) \sim (b, c)$ we have $\frac{ab}{ac} = \frac{b}{c}$.