0.1 The Rational Numbers

Assume Z, the integers, have arithmetic order. What is $\mathbb{Q}$? Perhaps it's the set: $\left\{ \frac{m}{n} \middle| m, n \in \mathbb{Z}, n \neq 0 \right\}$.

However, what does that fraction notation actually mean? When we first begin teaching fractions to children we talk about splitting things like cake into smaller pieces. If we have a whole cake made of 3 slices, we can give one person a slice so they have $\frac{1}{3}$ of the cake. If we have a cake of 6 slices, we could give them 2 slices instead. They would have $\frac{2}{6}$. These two fractions are equivalent though! We need more rigor (this is mathmematics of course).

We say that the fractions as equivalent ordered pairs $(1,3) \sim (2,6)$. These belong to the same **equivalence class**, $\left[\frac{1}{3}\right]$.

Definition (Rational Numbers)*:*
The **rational numbers**, $\mathbb{Q}$, is the set $\left\{ \frac{m}{n} \middle| m, n \in \mathbb{Z}, n \neq 0 \right\}$ where $\frac{m}{n}$ is an equivalence class of (m,n) with the relation $(m,n) \sim (p,q)$ if $mq = np$ and $q, n \neq 0$

Proof. Is $\sim$ an equivalence relation? Need to show $\sim$ reflextive, symmetric, and transitive.

Step 1 Reflective: Let $(p,q) \in \mathbb{Q}$. Show $(p,q) \sim (p,q)$
Since $ab = ba$, $(p,q) \sim (p,q)$ ✓

Step 2 Symmetry: Let $(p,q),(m,n) \in \mathbb{Q}$. Assume $(p,q) \sim (m,n)$. Show $(m,n) \sim (p,q)$.

$$\begin{aligned}(p,q) \sim (m,n) &\implies pn = qm \\ &\implies qm = pn \\ &\implies mq = np \\ &\implies (m,n) \sim (p,q) \checkmark\end{aligned}$$

Step 3 Transitive: Let $(p,q),(m,n),(a,b) \in \mathbb{Q}$. Assume $(p,q) \sim (m,n)$ and $(m,n) \sim (a,b)$. Show $(p,q) \sim (a,b)$.
Need cancellation law on $\mathbb{Z}$: if $ab = ac$ and $a \neq 0$ then $b = c$.
$(p,q) \sim (m,n) \implies pn = qm$ and $(m,n) \sim (a,b) \implies mb = na$

Case 1: $p = 0$

$$\begin{aligned}p = 0 &\implies pn = qm = 0 \\ &\implies m = 0 \text{ since } q \neq 0 \\ &\implies mb = na = 0 \\ &\implies a = 0 \text{ since } n \neq 0 \\ &\implies pb = qa = 0 \\ &\implies (p,q) \sim (a,b) \checkmark\end{aligned}$$

Case 2: $m = 0$
Similar to Case 1. ✓

Case 3: $p, m \neq 0$
Multiplying $pn = qm$ by ab: $ab(pn) = ab(qm)$.
$\implies na(pb) = mb(qa)$
$\implies pb = qa$ by cancellation law ($m \neq 0$ and $mb = na$) $\implies (p, q) \sim (a, b)$ ✓ □

0.1.1 Arithmetic (of Rationals)

Our definitions of arithmetic on $\mathbb{Q}$ be well-defined. For example, we could define addition as follows:

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

However,

$$\frac{1}{2} + \frac{1}{3} = \frac{2}{5}$$
$$\frac{2}{4} + \frac{3}{7} = \frac{3}{7}$$

$\dfrac{1}{2}$ and $\dfrac{2}{4}$ are in the same equivalent class, but $\frac{2}{5}$ and $\frac{3}{7}$ are not. This is not well-defined. We want a definition of addition <u>not dependent on our representatives chosen</u>.

Now, $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{0}{1}$. This is well-defined but not helpful.

Definition (Addition in $\mathbb{Q}$)*:*

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

If this well-defined?

Proof. Assume $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. Show $(ad + bc, bd) \sim (a'd' + b'c', b'd')$.
$(a, b) \sim (a', b') \implies ab' = ba'$
$(c, d) \sim (c', d') \implies cd' = dc'$

$$\begin{aligned} b'd'(ad + bc) &= b'd'ad + b'd'bc \\ &= (d'd)(ab') + (b'b)(cd') \\ &= (d'd)(ba') + (b'b)(dc') \\ &= (bd)(a'd') + (bd)(c'b') \\ &= bd(a'd' + c'b') \end{aligned}$$

$\implies (ad + bc, bd) \sim (a'd' + b'c', b'd')$ ✓ □

Definition (Multiplication in $\mathbb{Q}$)*:*

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

If this well-defined?

Proof. Assume $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. Show $(ac, bd) \sim (a'c', b'd')$.
$(a, b) \sim (a', b') \implies ab' = ba'$
$(c, d) \sim (c', d') \implies cd' = dc'$

$$\begin{aligned} acb'd' &= (ab')(cd') \\ &= (ba')(dc') \\ &= (a'c')(bd) \end{aligned}$$

$\implies (ac, bd) \sim (a'c', b'd')$ ✓ □

In what way does $\mathbb{Q}$ extend $\mathbb{Z}$?

The correspondence is $\frac{n}{1} \longleftrightarrow n$. Addition and multiplication is the same in $\mathbb{Q}$ as in $\mathbb{Z}$.

Note. We can define subtraction by adding the negative of a number (multiply by -1).

0.1.2 Order

Definition (Order)*:*
An **order** on a set S is a relation $<$ satisfying:

1. (Trichotomy) If $x, y \in S$, exactly one is true: $x < y$, $x = y$, $y < x$.
2. (Transitivity) If $x, y, z \in S$, $x < y$, and $y < z, x < z$.

Example:
In $\mathbb{Z}$, say $m < n$ if $n - m$ is positive, i.e. in $\mathbb{N}$.

Example:
In $\mathbb{Z} \times \mathbb{Z}$, say $(a, b) < (c, d)$ if $a < c$ or ($a = c$ or $b < d$). This is called the dictionary order.

Example:
In $\mathbb{Q}$, say $\frac{m}{n}$ is positive if $mn > 0$. This is well-defined.

Proof. Assume $(m, n) \sim (p, q)$ and $mn > 0$. Show $pq > 0$.
Suppose, to the contrary, $pq < 0$.

$$\begin{aligned} (m, n) \sim (p, q) &\implies mq = np \\ &\implies (mq)^2 = mqnp \end{aligned}$$

By assumption, $mnpq < 0$, a contradiction since $mn > 0$. Thus, $pq > 0$. □

So $\dfrac{a}{b} < \dfrac{c}{d}$ if $\dfrac{c}{d} + \dfrac{-a}{b}$ is positive.

Write $y > x$ for $x < y$ and $x <= y$ for $x < y$ or $x = y$.

Theorem 1. *$x^2 = 2$ has no solution in $\mathbb{Q}$.*

Proof (by contradiction). Assume x^2 has a solution in $\mathbb{Q}$, i.e. $x = \dfrac{p}{q}$ where $p, q \in \mathbb{Z}$.
Also assume p, q are in "lowest terms," i.e. they have no common factors. (We can do this using elements in the equivalence classes of $\mathbb{Q}$.)
So $\left(\dfrac{p}{q}\right)^2 = 2$, hence $p^2 = 2q^2$.
Then p^2 is even (divisible by 2).
Then p is even. (If p was odd, p^2 would be odd.)
So $p = 2m$ for some $m \in \mathbb{Z}$, hence $p^2 = 4m^2 = 2q^2$.
Then $2m^2 = q^2$.
Then q^2 is even, hence q is even.
This contradicts the fact that p, q are in "lowest terms." So, $x^2 = 2$ must have no solution in $\mathbb{Q}$. $\square$

0.1.3 Fields

Definition (Field)*:*
A **field** is a set F with two operations $+, \times$ satisfying axioms:

A1. F is closed under $+$. (Adding two things in the set gives you something in the set.)

A2. $+$ is commutative.

A3. $+$ is associative.

A4. F has an additive identity, call it 0.

A5. Every element has an additive inverse.

M1. F is closed under $\times$.

M2. $\times$ is commutative.

M3. $\times$ is associative.

M4. F has an additive identity, call it 1.

M5. Every element except 0 has an additive inverse.

D1. $\times$ distributes over $+$.

Example:
In $\mathbb{Q}$, the 0 element is $\left[\dfrac{0}{1}\right]$ and the 1 element is $\left[\dfrac{1}{1}\right]$.

Definition (Ordered Field)*:*
An **ordered field** is a field with an order s.t. order is preserved by field operations.

1. If $y < z$, then $x + y < x + z$.
2. If $y < z$ and $x > 0$, then $xy < xz$.

Note. $\mathbb{Z}$ is a ring not a field. There are no multiplicative inverses.
$\mathbb{Q}$ is an ordered field!