A Rational Construction

John McCuan

January 30, 2020

Here we construct the rational numbers following Gunning's *An Introduction to Analysis*. We begin with the totally ordered ring of integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

noting that $\mathbb{Z}$ is not a field because the nonzero elements

$$\mathbb{Z}^* = \{\pm 1, \pm 2, \pm 3, \ldots\}$$

do not all have multiplicative inverses. One does have, however, that $\mathbb{Z}^*$ is closed under multiplication and has a (multiplicative) identity, so $\mathbb{Z}^*$ is a monoid, and $\mathbb{Z}$ is a ring, and integral domain in fact and a unique factorization domain. The construction of an injection

$$\phi : \mathbb{Z} \to \mathbb{Q}$$

of the integers $\mathbb{Z}$ into the set of **rational numbers** $\mathbb{Q}$, which will be defined below, essentially involves appending to $\mathbb{Z}$ the multiplicative inverses of the nonzero elements in $\mathbb{Z}^*$, i.e., fractions $1/n$, and then making sure we keep the ring structure (closure under the operations in particular).

Without further adieu then, we note that Gunning's construction may again be thought of in two steps

$$\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}^* \to (\mathbb{N}_0 \times \mathbb{Z}^*)/\sim \; = \; \mathbb{Q}$$

where $\mathbb{Z} \times \mathbb{Z}^* = \{(m, n) : m \in \mathbb{Z} \text{ and } n \in \mathbb{Z}^*\}$ is the Cartesian product (of $\mathbb{Z}$ and $\mathbb{Z}^*$) and "$\sim$" is a certain equivalence relation. The pair (m, n) represents the fraction m/n, and we should introduce equivalence classes for each such fraction containing $(-m)/(-n)$ and $(ma)/(na)$ for every nonzero integer a. This is accomplished as follows:

We say $(m,n) \sim (r,s)$ if the familiar condition

$$\frac{m}{n} = \frac{r}{s}$$

holds. Of course, we can't say this yet, so what we really say is

$$(m,n) \sim (r,s) \qquad \Longleftrightarrow \qquad ms = nr. \tag{1}$$

Therefore, elements of $\mathbb{Q}$ (rational numbers) initially have the rather unappealing form

$$[(m,n)] = \{(r,s) \in \mathbb{Z} \times \mathbb{Z}^* : ms = nr\}$$

with the integers $n \in \mathbb{Z}$ taking the form

$$[(n,1)].$$

Here are the important results to prove:

Theorem 1 *$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ is a* **field** *under the operations*

$$[(m,n)] + [(r,s)] = [(sm+nr, ns)] \qquad \text{and} \qquad [(m,n)][(r,s)] = [(mr,ns)]$$

with additive and multiplicative identity

$$[(0,1)] \qquad \text{and} \qquad [(1,1)]$$

respectively, and for which the additive and multiplicative inverses of $[(m,n)]$ are

$$[(-m,n)] \qquad \text{and} \qquad [(n,m)]$$

respectively, with the latter being well-defined only when $m \neq 0$ or equivalently $[(m,n)] \neq [(0,1)]$. Furthermore, $\mathbb{Q}$ is a **totally ordered field** *with order determined by the positives*

$$\{[(m,n)] \in \mathbb{Q} : m,n \in \mathbb{N}\}$$

which determine the partition

$$\{[(-m,n)] \in \mathbb{Q} : m,n \in \mathbb{N}\} \cup \{[(0,1)]\} \cup \{[(m,n)] \in \mathbb{Q} : m,n \in \mathbb{N}\}.$$

Theorem 2 *$\phi : \mathbb{Z} \to \mathbb{Q}$ by $\phi(n) = [(n,1)]$ is an order preserving injection which is also a ring homomorphism. That is,*

$$\phi(m+n) = \phi(m) + \phi(n), \text{ and}$$
$$\phi(mn) = \phi(m)\phi(m) \text{ for all } m,n \in \mathbb{Z}.$$

As in the case of construction of $\mathbb{Z}$ from $\mathbb{N}_0$ or $\mathbb{N}$, once the construction is satisfactorily executed, the unappealing notation of equivalence classes in $\mathbb{Q}$ is "forgotten" and we write $n = n/1$ for $\phi(n)$, we write $\mathbb{Z}$ for $\phi(\mathbb{Z})$ (we write $\mathbb{N}$ for $\phi(\mathbb{N}) = \phi \circ \nu_0(\mathbb{N})$ etc.), and we write

$$\frac{m}{n} \qquad \text{for} \qquad [(m,n)].$$

One particular aspect of (the representation of) rational numbers should be observed with respect to the positioning of "signs" and verified, namely,

$$-[(m,n)] = [(-m,n)] = [(m,-n)] \qquad \text{corresponding to} \qquad -\frac{m}{n} = \frac{-m}{n} = \frac{m}{-n}.$$

It follows in particular that $[(-m,-n)] = [(m,n)]$ for $m,n \in \mathbb{N}$, so we can always assume the numerator and denominator of a positive rational are positive integers. Thus, if we write

$$\mathbb{Q}^+ = \{m/n \in \mathbb{Q} : m,n \in \mathbb{N}\}$$

there is no essential ambiguity.

Incompleteness of $\mathbb{Q}$

Among the most important arithmetic results in $\mathbb{Q}$ is a negative one.

Definition 1 *A subset A in a partially ordered set X is* **bounded above** *if there is an element $x \in X$ for which*

$$a \leq x \qquad \textit{for all } a \in A.$$

It may be that the **set of all upper bounds** B for a set A in a given set X, that is

$$B = \{x \in X : a \leq x \text{ for all } a \in A\},$$

is empty. If $B \neq \phi$, we say A is bounded above. If A is bounded above, it may be that $B \cap A = \phi$. If $B \cap A \neq \phi$, then $B \cap A = \{a_{\max}\}$ is a singleton, and we write

$$a_{\max} = \max A.$$

Definition 2 *If A is a subset of a partially ordered set X, then A is* **bounded below** *if there is an element $x \in X$ for which*

$$x \leq a \qquad \textit{for all } a \in A.$$

If a set A is bounded below and $A \cap L = \{a_{\min}\}$ where L is the set of all lower bounds of A, then the element $a_{\min}$ is called the **minimum** of A, and we write $\min A = a_{\min}$. Whenver A is bounded above, the set of upper bounds B is bounded below.

Definition 3 *If X is a partially ordered set in which every subset A which is bounded above has a set of upper bounds B with a well-defined minimum $\min B$, then X is said to be* **complete** *or to have the* **least upper bound property**.

Here is the negative result:

Theorem 3 *$\mathbb{Q}$ is not complete. There are sets in $\mathbb{Q}$ which are bounded above and have no least upper bound. There are sets in $\mathbb{Q}$ which are bounded below and have no greatest lower bound.*

Exercise 1 *Show $A = \{a \in \mathbb{Q} : a^2 \leq 2\}$ is bounded above, but the set*

$$B = \{x \in \mathbb{Q} : a \leq x \text{ for every } a \in A\}$$

does not have a well-defined minimum.

This deficiency may be viewed as the fundamental motivation for extending the rational field to the field or **real numbers** $\mathbb{R}$.

Here is a solution to the exercise above: First if $3/2 < a$ for $a \in A$, then $2 < 9/4 < a^2$ which is a contradiction, so $3/2$ is an upper bound for A.

Assume (BWOC) that $m/n = \min B$. Notice that $m/n > 1$ since $1 \in A$ (and in fact, $5/4 > 1$ is also in A). In particular, this means $m \neq 1$. On the other hand, since $1 < m/n < 3/2$, we know

1. We can assume $m, n \in \mathbb{N}$, and
2. $m/n \notin \mathbb{N}$, so $n \neq 1$.

By the unique factorization of natural numbers, there are unique primes $p_1 < p_2 < \cdots < p_k$ and for each p_j, $j = 1, \ldots, k$ there is a unique power $a_j \in \mathbb{N}$ such that

$$m = \prod_{j=1}^{k} p_j^{a_j}. \tag{2}$$

Similarly, there are unique primes $q_1 < q_2 < \cdots < q_\ell$ and for each q_j, $j = 1, \ldots, \ell$ there is a unique power $b_j \in \mathbb{N}$ such that

$$n = \prod_{j=1}^{\ell} q_j^{b_j}. \tag{3}$$

We claim, furthermore, that $(m/n)^2 = m^2/n^2 = 2$. If $(m/n)^2 < 2$, then we claim there is **another** rational number $a \in A$ for which $a > m/n$ contradicting the fact that $m/n = \min B$. In fact, this follows from another important property of the rational numbers:

Theorem 4 *(Archimedian Property of $\mathbb{Q}$) The field $\mathbb{Q}$ is an* **Archimedian field**, *that is, given any $\gamma \in \mathbb{Q}$, there is some integer $N \in \mathbb{N}$ for which $\gamma < N$.*

This result is also phrased in the following equivalent way:

Corollary 1 *(Archimedian Property of $\mathbb{Q}$) Given any positive $\gamma \in \mathbb{Q}$, there is some integer $N \in \mathbb{N}$ for which $1/N < \gamma$.*

Proof: $1/\gamma \in \mathbb{Q}$, so by the (first) Archimedian property, there is some $N \in \mathbb{N}$ with $1/\gamma < N$. Therefore, $0 < 1/N < \gamma$. $\square$

Returning to our consideration of m/n, we wish to find an integer $N \in \mathbb{N}$ for which $a = m/n + 1/N \in A$. That is,

$$\left(\frac{m}{n} + \frac{1}{N}\right)^2 < 2.$$

In other words we want to show

$$\left(\frac{m}{n}\right)^2 + 2\,\frac{m}{n}\,\frac{1}{N} + \frac{1}{N^2} < 2. \tag{4}$$

This seems plausible since we can choose N very large, or equivalently, $1/N$ very small. There is an obvious small positive number which should be of use to us, namely,

$$\gamma_1 = 2 - \left(\frac{m}{n}\right)^2.$$

Thus, we may start by assuming, i.e., choosing $N \in \mathbb{N}$ according to the second Archimedian property so that $1/N < \gamma_1$. This may not be good enough however, so we observe that for any $K \in \mathbb{N}$, we may also take $N \in \mathbb{N}$ so that

$$\frac{1}{N} < \gamma_2 = \frac{1}{K}\left[2 - \left(\frac{m}{n}\right)^2\right].$$

Rearranging this inequality gives

$$\left(\frac{m}{n}\right)^2 + \frac{K}{N} < 2.$$

Comparing this expression to the desired inequality (4), we see we can obtain what we want if

$$2\,\frac{m}{n}\,\frac{1}{N}+\frac{1}{N^2}<\frac{K}{N}.$$

Rearranging this inequality, we see it is equivalent to

$$2mN+n<KnN \qquad \text{or} \qquad \frac{1}{N}<\frac{Kn-2m}{n}.$$

Let us consider the plausibility of this inequality. By the first Archimedian property, we may choose $K\in\mathbb{N}$ so that $K>2m/n$. Then $(Kn-2m)/n>0$, and we may choose N by the second Archimedean property so that

$$\frac{1}{N}<\gamma=\min\left\{\frac{1}{K}\left[2-\left(\frac{m}{n}\right)^2\right],\frac{Kn-2m}{n}\right\}. \tag{5}$$

Reversing our preliminary calculations, we have from (5) that

$$\frac{1}{N}<\frac{Kn-2m}{n}.$$

It follows from this that

$$2\,\frac{m}{n}\,\frac{1}{N}+\frac{1}{N^2}<\frac{K}{N}.$$

Hence,

$$\left(\frac{m}{n}\right)^2+2\,\frac{m}{n}\,\frac{1}{N}+\frac{1}{N^2}<\left(\frac{m}{n}\right)^2+\frac{K}{N}.$$

However, it also follows from (5) that

$$\frac{K}{N}<2-\left(\frac{m}{n}\right)^2.$$

Thus, (4) holds as desired, and we have our contradiction. We have shown $(m/n)^2\geq 2$.

We now consider the possibility that $(m/n)^2>2$. If this happens, we claim there is **another upper bound** $b\in B$ with $b<m/n$, again contradicting the assumption that $m/n=\min B$. Taking $b=m/n-1/N$, we proceed with a preliminary calculation to establish

$$\left(\frac{m}{n}\right)^2-2\,\frac{m}{n}\,\frac{1}{N}+\frac{1}{N^2}>2. \tag{6}$$

This time the appropriate N is easier to find. We may choose K large enough so that $Kn - 2m > 0$. Then it will always be the case for any $N \in \mathbb{N}$ that

$$N > -\frac{n}{Kn - 2m} \qquad \text{and consequently} \qquad -2\,\frac{m}{n}\,\frac{1}{N} + \frac{1}{N^2} > -\frac{K}{N}.$$

Then, taking $N \in \mathbb{N}$ so that

$$\frac{1}{N} < \frac{1}{K}\left[\left(\frac{m}{n}\right)^2 - 2\right].$$

It then follows that

$$\left(\frac{m}{n}\right)^2 - \frac{K}{N} > 2$$

so that

$$\left(\frac{m}{n} - \frac{1}{N}\right)^2 > \left(\frac{m}{n}\right)^2 - \frac{K}{N} > 2.$$

Now, if $a \in A$ satisfies $a \geq b = m/n - 1/N$, then $a^2 > b^2 > 2$, and we have a contradiction. This means b is an upper bound for A as desired, and we have the final contradiction showing $(m/n)^2 = 2$.

Finally, we return to the prime factor decompositions of m and n given in (2) and (3). From these we have

$$p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} = 2q_1^{2b_1} q_2^{2b_2} \cdots + q_\ell^{2b_\ell}. \tag{7}$$

This means $2 \big| m = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k}$, and since 2 is the smallest prime, we must have $p_1 = 2$. By the cancellation rule in $\mathbb{Q}$, we can obtain from (7) the equation

$$2^{2a_1 - 1} p_2^{2a_2} \cdots p_k^{2a_k} = q_1^{2b_1} q_2^{2b_2} \cdots + q_\ell^{2b_\ell}.$$

The same reasoning now implies $2 \big| q$ and

$$2^{2a_1 - 1} p_2^{2a_2} \cdots p_k^{2a_k} = 2^{2b_1} q_2^{2b_2} \cdots + q_\ell^{2b_\ell}.$$

This contradicts unique prime factorization since the power $2a_1 - 1$ of 2 on the left is odd while the power $2b_1$ of 2 on the right is even. $\square$

The solution of the exercise above contains a proof of the fact that there is no rational number m/n for which $(m/n)^2 = 2$. It differs from most proofs of this fact in not assuming the fraction m is in lowest terms.

Reduction of Fractions to Lowest Terms

There is also an important consequence of the unique factorization in $\mathbb{N}$ and $\mathbb{Z}$ for the fractions in $\mathbb{Q}$. Each fraction may be **uniquely reduced to lowest terms**. We attempt to clarify this question of representation or notation here.

There was already nominally some ambiguity of notation in $\mathbb{Z}$ since $-(-n)$ and n are the same integer. The ambiguity with standard notation for fractions is much more noticable in $\mathbb{Q}$ since

$$\frac{mq}{nq} = \frac{m}{n}$$

whenever $m/n \in \mathbb{Q}$ and $q \in \mathbb{Z}^*$.

The main facts may be stated as follows:

Theorem 5 *(reduced form for positive rationals) Given $m/n \in \mathbb{Q}^+$, exactly one of the following three conditions holds:*

1. *There exist unique prime numbers $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_\ell$, with*

   $$\{p_1, p_2, \ldots, p_k\} \cap \{q_1, q_2, \ldots, q_\ell\} = \phi,$$

   and for each prime p_j $j = 1, 2, \ldots, k$, there is a unique power $a_j \in \mathbb{N}$ and for each prime q_j, $j = 1, 2, \ldots, \ell$, there is a unique power $b_j \in \mathbb{N}$ such that

   $$\frac{m}{n} = \frac{\prod_{j=1}^{k} p_j^{a_j}}{\prod_{j=1}^{k} q_j^{b_j}}. \tag{8}$$

   Notice this equality should not be interpreted to mean $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ or that $n = q_1^{b_1} q_2^{b_2} \cdots q_\ell^{b_\ell}$ but rather in the sense of equality in $\mathbb{Q}$ expressed by (1).

2. *$m/n \in \mathbb{N}$ in the same sense of (1), i.e., so that there is some unique $q \in \phi(\mathbb{N})$ such that $m = qn$.*

3. *There is some unique $q \in \mathbb{N}\backslash\{1\}$ such that*

   $$\frac{m}{n} = \frac{1}{q}. \tag{9}$$

In the first and third cases, the expressions on the right in (8) and (9) are said to represent m/n in **lowest terms**. *In the second case, m/n is represented by the integer q in lowest terms.*

Any two nonzero integers p and q are said to be **relatively prime** if their greatest common divisor[1] in $\mathbb{N}$ is 1. Note that in the first case the products

$$\prod_{j=1}^{k} p_j^{a_j} \qquad \text{and} \qquad \prod_{j=1}^{k} q_j^{b_j}$$

are relatively prime.

Theorem 6 *(reduced form for rationals) Given $m/n \in \mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, exactly one of the following four conditions holds:*

1. *There exist unique prime numbers $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_\ell$ in $\mathbb{N}$, with*
$$\{p_1, p_2, \ldots, p_k\} \cap \{q_1, q_2, \ldots, q_\ell\} = \phi,$$
and for each prime p_j $j = 1, 2, \ldots, k$, there is a unique power $a_j \in \mathbb{N}$ and for each prime q_j, $j = 1, 2, \ldots, \ell$, there is a unique power $b_j \in \mathbb{N}$ such that
$$\frac{m}{n} = \frac{\prod_{j=1}^{k} p_j^{a_j}}{\prod_{j=1}^{k} q_j^{b_j}}. \tag{10}$$

2. *There exist unique prime numbers $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_\ell$ in $\mathbb{N}$, with*
$$\{p_1, p_2, \ldots, p_k\} \cap \{q_1, q_2, \ldots, q_\ell\} = \phi,$$
and for each prime p_j $j = 1, 2, \ldots, k$, there is a unique power $a_j \in \mathbb{N}$ and for each prime q_j, $j = 1, 2, \ldots, \ell$, there is a unique power $b_j \in \mathbb{N}$ such that
$$\frac{m}{n} = \frac{-\prod_{j=1}^{k} p_j^{a_j}}{\prod_{j=1}^{k} q_j^{b_j}}. \tag{11}$$

3. *$m/n \in \mathbb{Z}^*$ in the sense that there is some unique $q \in \phi(\mathbb{Z}^*)$ such that $m = qn$.*

4. *There is some unique $q \in \mathbb{Z}\backslash\{0, \pm 1\}$ such that*
$$\frac{m}{n} = \frac{1}{q}. \tag{12}$$

[1]Recall that the **greatest common divisor** is always defined to be an integer in $\mathbb{N}$ even when $p, q \in \mathbb{Z}^*$.

Again, in the first, second and fourth cases, the expressions on the right in (10), (11), and (12) are said to represent m/n in **lowest terms**. *In the third case, m/n is represented by the integer q in lowest terms.*

Again in the first and second cases the products

$$\prod_{j=1}^{k} p_j^{a_j} \qquad \text{and} \qquad \prod_{j=1}^{k} q_j^{b_j}$$

are relatively prime.

1 Countability of $\mathbb{Q}$

As a final application of the fact that any rational number may be uniquely reduced to lowest terms, we give a short proof that the rationals are countable.[2] It is enough to find an injection $f : \mathbb{Q}\backslash\{0\} \to \mathbb{N}$. It is easy to check that if $p/q = r/s \in \mathbb{Q}\backslash\{0\}$ with both fractions p/q and r/s in lowest terms, then $p = r$ and $q = s$. Also, we know that in this form, we may assume $p \in \mathbb{Z}\backslash\{0\}$ and $q \in \mathbb{N}$. Consequently, $f : \mathbb{Q} \to \mathbb{N}$ by

$$f(p/q) = \begin{cases} 2^p 3^q & \text{if } p > 0, \\ 2^p 3^q 5 & \text{if } p < 0 \end{cases}$$

(where p/q is in lowest terms) is well-defined. Furthermore, if $f(p/q) = f(r/s)$, then

$$2^p 3^q = 2^r 3^s, \qquad 2^p 3^q 5 = 2^r 3^s, \qquad 2^p 3^q = 2^r 3^s 5, \qquad \text{or} \qquad 2^p 3^q 5 = 2^r 3^s 5.$$

In the first case and the last case $p = r$ and $q = s$ by the unique prime factorization of the integer $2^p 3^q$. In the second and third cases, we get a contradiction of the unique factorization of the integers $2^r 3^s$ and $2^p 3^q$ respectively. The only possible conclusion is

$$f(p/q) = f(r/s) \qquad \Longrightarrow \qquad p/q = r/s.$$

That is, f is injective. $\square$

As a final note, it is much easier and technically correct to show the rationals are countable in this manner than by using something like the "hand-waving" argument Gunning gives (originally due to Cantor) that a countable union of countable sets is countable (Theorem 1.4 of § 1.1). It is also much more difficult to give an actual

[2] I learned this proof from Simarpreet Kareer, a student in my Spring 2020 analysis course.

enumeration of the rationals, that is a bijection $f : \mathbb{N} \to \mathbb{Q}$. All three of the following results/problems present some difficulties with regard to giving an elegant precise proof.

Exercise 2 *Give an explicit enumeration of the rationals.*

Theorem 7 *The countable union of countable sets is countable.*

Theorem 8 *The Cartesian product of countable sets is countable.*

Actually, the countability of the Cartesian product is susceptible to the $(m, n) \mapsto 2^m 3^n$ argument above, but to give an explicit enumeration is trickier, though it seems easier to write down a bijection from the integer lattice $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ than the inverse.