The Rational Numbers

Here we construct the field of rational numbers. Mindful of the fact that all new mathematical objects are built upon the foundation of previously constructed objects (which can ultimately be traced back to assumed notions and axioms), in this case we take $\mathbb{Z}$, the ring of integers, as our foundation. Recall that $\mathbb{Z}$ is a commutative ring—thus it satisfies all the ring axioms including commutativity, associativity and distributivity. It has an identity element 1 satisfying $1a = a$ for all $a \in \mathbb{Z}$. More than this, it is an *integral domain*: if $ab = 0$ then $a = 0$ or $b = 0$ (so $\mathbb{Z}$ has no zero divisors). All these properties are used when we construct $\mathbb{Q}$ from $\mathbb{Z}$. More than this, $\mathbb{Z}$ is an *ordered ring*: there is a binary relation '$<$' defined on $\mathbb{Z}$ satisfying such properties as $a < b \Rightarrow a+c < b+c$.

One may imagine that we are communicating with an intelligent alien who has understood everything about the integers; in particular the alien understands the notation we humans use, as well as the conceptual properties of the integers mentioned in the previous paragraph. The alien also understands basic logic and set theory, as these are previously laid foundations required in the construction of $\mathbb{Z}$. Our task is to precisely define the rationals to this alien. We must be precise: there are several points at which a little sloppiness would show the alien we have no idea what we're talking about. (It must be emphasized that this process is very different from the way we teach fractions to children, whose intuition substitutes for limited knowledge; here we instead teach by example and tell white lies, hoping that later their misconceptions about the rationals will be fixed up.)

Why are we doing this?

- First of all, this material clarifies those features of $\mathbb{Q}$ that our elementary school background takes for granted: it is here that we explain exactly what $\mathbb{Q}$ is and why it 'works' (in particular, why it is a field, in fact an ordered field). This is like two different answers to the question 'How does a car work?' The elementary school answer is 'Put the key in the ignition and turn it like this.' The deeper explanation requires an explanation of how an internal combustion engine works, the transmission, etc.
- Secondly, because the formal process by which one constructs $\mathbb{Q}$ from $\mathbb{Z}$ is exactly the same as the process by which one constructs the quotient field of an arbitrary integral domain (e.g. construct $F(x)$ from $F[x]$, or $F((x))$ from $F[[x]]$). And

- thirdly, the key ideas in this process arise in *much more general* constructions of new objects from old: $\mathbb{R}$ from $\mathbb{Q}$, $\mathbb{F}_p$ from $\mathbb{Z}$, $\mathbb{Q}_p$ from $\mathbb{Q}$, etc. So a thorough understanding of how $\mathbb{Q}$ is constructed from $\mathbb{Z}$, is the best preparation for understanding how other new number systems are constructed.

Before we can define addition or multiplication of fractions, or show how the ordering of factions works, we must define the *elements* of the set $\mathbb{Q}$, i.e. the rational numbers. The first subtlelty is the role of equivalent fractions: the fact that the expressions $\frac{3}{6}$ and $\frac{1}{2}$ represent the same rational number. We must understand a rational number as not a single formal expression of 'a over b'; rather, a rational number is an entire equivalence class of such pairs (a, b). Our intelligent alien understands equivalence relations and equivalence classes, as these are more basic notions founded in set theory. Let us review:

Equivalence Relations and Classes

Let S be any set. Let '$\sim$' be a binary relation on S: thus for all $a, b \in S$, either $a \sim b$ or $a \not\sim b$. Any such a binary relation amounts to a partition of $S^2 = \{(a, b) : a, b \in S\}$ into two such subsets: those pairs (a, b) that satisfy the relation '$\sim$' and those that don't. So if S has n elements, then S^2 has $|S^2| = n^2$ elements and 2^{n^2} subsets. So there are exactly $2^{|S|^2}$ binary relations on S. This formula works also in the infinite case; but a countably infinite set has uncountably manysubsets and uncountably many binary relations.

We say that $\sim$ is an *equivalence relation on* S if for all $a, b, c \in S$ we have

$a \sim a$ (i.e. '$\sim$' is *reflexive*);
$a \sim b \Leftrightarrow b \sim a$ (i.e. '$\sim$' is *symmetric*); and
$a \sim b \sim c \Rightarrow a \sim c$ (i.e. '$\sim$' is *transitive*).

For example, the relation '$<$' on $\mathbb{Z}$ is transitive but neither reflexive nor symmetric: it is not an equivalence relation.

Given an equivalence relation '$\sim$' on S, we obtain a partition of S into equivalence classes, as follows. The *equivalence class* of $a \in S$ is

$$[a] = [a]_\sim = \{x \in S : x \sim a\}.$$

Note that $[a] = [b] \Leftrightarrow a \sim b \Leftrightarrow a \in [b]$. The collection of all equivalence classes forms a *partition* of S:

$$S/\!\sim \;=\; \{[a] : a \in S\}.$$

Recall that a partition of a set S is a collection of nonempty subsets of S, which cover S (i.e. their union is all of S), and no two subsets in this collection overlap (i.e. they are mutually disjoint). It is easy to see that $S/{\sim}$ has this property:

$$\bigcup_{a \in S} [a] = S \qquad \text{and} \qquad [a] \cap [b] = \varnothing \ \text{ whenever } \ [a] \neq [b].$$

It is a straightforward exercise to check that having an equivalence relation on S, amounts to the same thing as having a partition of S. From an equivalence relation, the equivalence classes give us a partition; conversely, given a partition of S, we get an equivalence relation by saying two elements of S are equivalent iff they are in the same member of the partition.

The set of rational numbers

Every rational number must be represented using a *pair* of integers a, b with $b \neq 0$; we will use these integers for the numerator and the denominator. This motivates the following definition: Let S be the set of all pairs (a, b) of integers with $b \neq 0$; thus

$$S = \{(a, b) \,:\, a, b \in \mathbb{Z};\ b \neq 0\}.$$

Define a relation $\sim$ on S by

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

Let us check that '$\sim$' is transitive: assuming $(a, b) \sim (c, d) \sim (e, f)$, then $ad = bc$ and $cf = de$, so that

$$adf = bcf = bde, \quad \text{i.e.} \quad (af - be)d = 0.$$

Since $d \neq 0$ and $\mathbb{Z}$ has no zero divisors, we conclude that $af = be$, i.e. $(a, b) \sim (e, f)$. Similar arguments show that '$\sim$' is reflexive and symmetric, so it is an equivalence relation.

We now define the symbol $\frac{a}{b}$ to be the equivalence class of $(a, b) \in S$:

$$\tfrac{a}{b} = [(a, b)] = \{(x, y) \in S \,:\, ay = bx\}$$

and the set of rational numbers is the set of all such equivalence classes:

$$\mathbb{Q} \ = \ S/{\sim} \ = \ \left\{\tfrac{a}{b} \,:\, a, b \in \mathbb{Z};\ b \neq 0\right\} \ = \ \left\{[(a, b)] \,:\, a, b \in \mathbb{Z};\ b \neq 0\right\}.$$

Automatically we get $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. This test for equality of fractions is what we call 'cross-multiplication'.

Addition and Multiplication of Rational Numbers

In order for $\mathbb{Q}$ to be a number system, it must be more than an abstract set of elements; we must define addition and multiplication of elements of $\mathbb{Q}$. We do so as follows: given two elements $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, we define their sum and their product as

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

A subtle but important point here is that if $(a, b) \in S$ and $(c, d) \in S$, then $(ad+bc, bd) \in S$ and $(ac, bd) \in S$; otherwise the equivalence classes $\frac{ad+bc}{bd}$ and $\frac{ac}{bd}$ would not be defined. However, this is not enough to show that addition and multiplication in $\mathbb{Q}$ are well-defined; we must also show that sums and products do not depent upon the choice of representative from equivalence classes. To this end, suppose that $\frac{a'}{b'} = \frac{a}{b}$, i.e. $a'b = ab'$; then

$$(a'd+b'c)bd = (a'b)d^2 + b'bcd = (ab')d^2 + bb'cd = (ad+bc)b'd$$

so that

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

Thus the sum of two fractions is unchanged if the first fraction $\frac{a}{b}$ is replaced by an equivalent fraction $\frac{a'}{b'}$. A similar argument applies when the second term is replaced by an equivalent fraction; so the sum of two fractions is well-defined, independently of the choice of representatives. A similar (but easier) argument shows that the product of two fractions is well-defined.

The Rational Numbers form a Field

Next we show that $\mathbb{Q}$ is a field. Consider arbitrary elements $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$; then

$$\frac{a}{b} + \frac{0}{1} = \frac{a1+0b}{b1} = \frac{a}{b} \qquad \text{and} \qquad \frac{1}{1}\,\frac{a}{b} = \frac{1a}{1b} = \frac{a}{b}$$

so we have a zero element and an identity. Also

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-a)b}{bb} = \frac{0}{b^2} = \frac{0}{1}$$

since $01 = b^2 0$ in $\mathbb{Z}$. Also

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\,\frac{cf+de}{df} = \frac{a(cf+de)}{bdf} = \frac{acf+ade}{bdf} = \frac{acf+ade}{bdf}\,.$$

Cross-multiplying, we see that this is the same as

$$\tfrac{(acf+ade)b}{b^2df} \;=\; \tfrac{abcf+abde}{b^2df} \;=\; \tfrac{ac}{bd}+\tfrac{ae}{bf} \;=\; \tfrac{a}{b}\,\tfrac{c}{d}+\tfrac{a}{b}\,\tfrac{e}{f}\,,$$

so $\mathbb{Q}$ satisfies the distributive law. Similar computations show that both addition and multiplication in $\mathbb{Q}$ are ccommutative and associative.

Finally, we check that nonzero elements are invertible: Suppose that $\frac{a}{b} \neq \frac{0}{1}$. Cross-multiplying, this says that $a = a1 \neq b0 = 0$; so there is an element $(b, a) \in S$. We check that

$$\tfrac{a}{b}\,\tfrac{b}{a} \;=\; \tfrac{ab}{ba} \;=\; \tfrac{1}{1}$$

where the last equality is verified by cross-multiplication. Thus $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, and so $\mathbb{Q}$ is a field.

Embedding $\mathbb{Z}$ in $\mathbb{Q}$

A slight difficulty arises at this point: we want $\mathbb{Z}$ to be a subring of $\mathbb{Q}$, but currently this fails because elements of $\mathbb{Q}$ are equivalence classes of pairs of integers, whereas elements of $\mathbb{Z}$ are simply integers: thus strictly speaking, $\mathbb{Z}$ is not a subset of $\mathbb{Q}$. However, we check that the elements $\frac{a}{1} \in \mathbb{Q}$ form a subring isomorphic to $\mathbb{Z}$, and that is just as good. Formally, we define $\theta : \mathbb{Z} \to \mathbb{Q}$ by $a \mapsto \frac{a}{1}$ and check (easily) that θ is a ring homomorphism, and that θ is one-to-one so that

$$\theta(\mathbb{Z}) = \left\{ \tfrac{a}{1} \;:\; a \in \mathbb{Z} \right\} \subset \mathbb{Q}$$

is a subring isomorphic to $\mathbb{Z}$ as required. Now we simply regard a as an abbreviation for $\frac{a}{1}$.

The Ordering

Next, we would like an order relation '$<$' on $\mathbb{Q}$. Fortunately we have an order relation on $\mathbb{Z}$, which can be used to define the order relation on $\mathbb{Q}$. Consider two elements $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. We will assume that $b, d \geqslant 1$; for if $b < 0$ we may rewrite $\frac{a}{b}$ as $\frac{-a}{-b}$ so that its denominator becomes positive; and the same remarks apply to $\frac{c}{d}$. With this convention, we may define

$$\tfrac{a}{b} < \tfrac{c}{d} \quad \text{iff} \quad ad < bc.$$

Let's be careful: we need to check that this is well-defined, independent of the choice of equivalent fraction used to represent each equivalence class. We also need to check that if the fractions are integers, then this agrees with our previously defined ordering on $\mathbb{Z}$.

These are just more technical details to check, and none of them difficult. We will leave these details as an exercise.

Next we need to check that the ordering does what we expect: in particular if $\frac{a}{b} < \frac{c}{d}$ then we should have $\frac{a}{b} + \frac{e}{f} < \frac{c}{d} + \frac{e}{f}$; also that the product of two positive fractions is positive. We also need to verify the *trichotomy law*: given any two fractions $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, exactly one of the three possibilities

$$\tfrac{a}{b} < \tfrac{c}{d} \quad \text{or} \quad \tfrac{a}{b} = \tfrac{c}{d} \quad \text{or} \quad \tfrac{a}{b} > \tfrac{c}{d}$$

holds, where the last option is understood as another way of writing $\frac{c}{d} < \frac{a}{b}$.