4. The integers, the rationals and the reals

One might have been forgiven, presented with the axioms for a complete ordered field, for wondering whether these axioms made sense. *Do* these axioms make sense? Is there such a thing as $\mathbb{R}$ after all?

One answer is that it is clear to our intuition that $\mathbb{R}$ *does* exist. But here we take a different approach, by constructing $\mathbb{R}$ within Set Theory. One could argue that the axioms of Set Theory—or rather, those we will be using (Pairs, Unions, Subset, Power Set, Infinity)—are more clearly true, to the intuition, than is the existence of a continuum.

But let's be clear about what we are doing. We will be constructing a complete ordered field; that is, proving that the axiomatisation of the reals we saw in the First Year, is consistent. Will the thing we build be "the" "true" real line? *As mathematicians*, we don't care, because we are accustomed to regarding isomorphic structures as being indistinguishable, and any complete ordered field is isomorphic to $\mathbb{R}$.* More compactly, we may say that mathematicians are more interested in what things do than in what they are.

In what follows, the proofs will be omitted. If you are feeling energetic, you could try supplying them.

4.1. The integers

First, we construct $\mathbb{Z}$ from ω. The difference between $\mathbb{Z}$ and ω is, of course, that in $\mathbb{Z}$, we can do subtraction. In $\mathbb{Z}$, we have to provide values for all expressions $m - n$, where m and n are natural numbers. That idea underlies the construction that follows, where the ordered pair $\langle m, n\rangle$ stands for $m - n$.

On $\omega \times \omega$, define a relation $\sim$ so that

$$\langle a, b\rangle \sim \langle c, d\rangle \quad \text{iff} \quad a + d = b + c.$$

(You would expect $a - b$ and $c - d$ to be equal, after all, if and only if $a + d = b + c$.)

We define $\mathbb{Z}$ to be the set of equivalence classes, and define the following structure on it.

1. We define $[\langle a, b\rangle] + [\langle c, d\rangle]$ to be $[\langle a + c, b + d\rangle]$. Of course, it is necessary to show that this is well-defined.

2. We define $[\langle a, b\rangle].[\langle c, d\rangle]$ to be $[\langle ac + bd, ad + bc\rangle]$. Again, one would have to show that this is well-defined.

3. We define the zero of $\mathbb{Z}$, $0_{\mathbb{Z}}$, to be $[\langle 0, 0\rangle]$.

4. We define the one of $\mathbb{Z}$, $1_{\mathbb{Z}}$, to be $[\langle 1, 0\rangle]$.

5. Additive inverses: we define $-[\langle a, b\rangle]$ to be $[\langle b, a\rangle]$.

6. Order: we say $[\langle a, b\rangle] \leq [\langle c, d\rangle]$ iff $a + d \leq b + c$.

It is then necessary to prove that $\mathbb{Z}$ is an integral domain with an order relation such that, if $a \leq b$ and $c \leq d$, then $a + b \leq c + d$, and $ac \leq bd$ provided a, $b \geq 0_{\mathbb{Z}}$, and that the map $\phi : n \mapsto [\langle n, 0\rangle]$ is an isomorphism between ω and the set of non-negative elements of $\mathbb{Z}$.

---

* Though that may not stop us wondering in our leisure hours.

4.2. The rationals

Given any integral domain, we may construct its *field of fractions*, essentially by providing values for all quotients a/b in the same spirit that we provided values for differences $m - n$ when we constructed $\mathbb{Z}$.

In the case of $\mathbb{Z}$, the construction goes as follows.

On $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_\mathbb{Z}\})$, define a relation $\sim$ as follows:

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

As before, we define $\mathbb{Q}$ to be the set of equivalence classes, and make the following definitions (and we will have proofs of well-definedness to do).

1. We define $[\langle a, b\rangle] + [\langle c, d\rangle]$ to be $[\langle ad + bc, bd\rangle]$.
2. We define $[\langle a, b\rangle].[\langle c, d\rangle]$ to be $[\langle ac, bd\rangle]$.
3. We define the zero of $\mathbb{Q}$, $0_\mathbb{Q}$, to be $[\langle 0_\mathbb{Z}, 1_\mathbb{Z}\rangle]$.
4. We define the one of $\mathbb{Q}$, $1_\mathbb{Q}$, to be $[\langle 1_\mathbb{Z}, 1_\mathbb{Z}\rangle]$.
5. Additive inverses: we define $-[\langle a, b\rangle]$ to be $[\langle -a, b\rangle]$.
6. Multiplicative inverses: if $a \neq 0_\mathbb{Z}$, then we define $\left([\langle a, b\rangle]\right)^{-1}$ to be $[\langle b, a\rangle]$.
6. Order: if b, $d > 0_\mathbb{Z}$, then we say $[\langle a, b\rangle] \leq [\langle c, d\rangle]$ iff $ad \leq bc$.

Now we must show that $\mathbb{Q}$ is an ordered field, and that the map $\psi : a \mapsto [\langle a, 1\rangle]$ is a one-to-one, order-preserving ring homomorphism from $\mathbb{Z}$ to $\mathbb{Q}$.

4.3. The reals

There are several ways to construct $\mathbb{R}$ from $\mathbb{Q}$, and which one seems most natural will depend on what aspect of the structure of $\mathbb{R}$ we are most interested in. The construction given here, that of *Dedekind cuts*, focuses on the fact that $\mathbb{R}$ is an ordered set.

We define a *Dedekind cut* to be a subset R of $\mathbb{Q}$ such that

a. $R \neq \varnothing$,

b. $R \neq \mathbb{Q}$,

c. For all $q \in R$, for all $r \leq q$, $r \in R$,

d. R has no greatest element.

Intuitively, for some real number x, R is the set of all rationals less than x.

We define $\mathbb{R}$ to be the set of all Dedekind cuts (which exists, by an application of the Subset Scheme to $\wp\mathbb{Q}$), and impose the following structure on it.

1. We define $0_\mathbb{R}$ to be the set of negative rational numbers.
2. We define $1_\mathbb{R}$ to be the set of all rationals less than $1_\mathbb{Q}$.
3. We define $R + S$ to be $\{r + s : r \in R,\, s \in S\}$. Of course, we must prove that this is a Dedekind cut.
4. We define $-R$ to be $\{-r : \exists s < r\,(s \notin R)\}$. We must, again, prove that is a Dedekind cut.

(It would seem more natural to define $-R$ to be the set $\{-r : r \notin R\}$. But then there's the problem that this set might have a greatest element, and so not be a Dedekind cut.)

5. We define $R.S$ by cases.

If R or S is equal to $\{q \in \mathbb{Q} : q < 0_\mathbb{Q}\}$, define $R.S$ to be $\{q \in \mathbb{Q} : q < 0_\mathbb{Q}\}$.

If this is not true, then there are five cases to consider, as follows.

If R or S is equal to $0_{\mathbb{R}}$, then $R.S$ is equal to $0_{\mathbb{R}}$.

Now suppose that neither R nor S is equal to $0_{\mathbb{R}}$.

If R and S both contain $0_{\mathbb{Q}}$, let T be the set of all products $r.s$ such that r, $s \geq 0_{\mathbb{Q}}$, $r \in R$ and $s \in S$. Define $R.S$ to be $T \cup \{q \in \mathbb{Q} : q \leq 0_{\mathbb{Q}}\}$.

If R does not contain $0_{\mathbb{Q}}$ but S does, define $R.S$ to be $-((-R).S)$.

If R contains $0_{\mathbb{Q}}$ but S does not, then define $R.S$ to be $-(R.(-S))$.

If neither R nor S contains $0_{\mathbb{Q}}$, define $R.S$ to be $(-R).(-S)$.

6. We define R^{-1} by cases, provided R is not equal to $0_{\mathbb{R}}$.

If $0_{\mathbb{Q}} \in R$, then we define R^{-1} to be the union of $\{q \in \mathbb{Q} : q \leq 0_{\mathbb{Q}}\}$ with $\{r^{-1} : \exists s < r\, (s \notin R)\}$.

If $0_{\mathbb{Q}} \notin R$, then by assumption there exists $s < 0_{\mathbb{R}}$ such that $s \notin R$. Find $r \in \mathbb{Q}$ such that $s < r < 0_{\mathbb{Q}}$ (for instance, $r = s/2$). Then $-r \in -R$, and, since $0_{\mathbb{Q}} < -r$, $0_{\mathbb{Q}} \in -R$ also. So, define R^{-1} to be $-(-R)^{-1}$.

7. Order: we say that $R \leq S$ iff $R \subseteq S$.

Finally, we must prove that $\mathbb{R}$ is a complete ordered field, and that the map $\chi : q \mapsto \{r \in \mathbb{Q} : r < q\}$ is an order-preserving field homomorphism from $\mathbb{Q}$ to $\mathbb{R}$.

The proof of completeness is extremely simple: if $\mathscr{S}$ is a bounded non-empty subset of $\mathbb{R}$, then its supremum is simply $\bigcup \mathscr{S}$.

4.4. The set-theoretic justification

Which axioms of Set Theory have we used?

Of course, we have used the Axiom of Infinity, which proves for us that ω exists. We have used the Subset Axiom Scheme often; for instance, $\mathbb{R}$ is the set of all elements of $\wp\mathbb{Q}$ satisfying a particular list of conditions; we use the Subset Axiom to derive $\mathbb{R}$ from $\wp\mathbb{Q}$. Of course we have used the Power Set Axiom, both explicitly, and not: we need the Power Set Axiom to show that $\omega \times \omega$ exists, for instance. We have also used the Axiom of Pairs and the Axiom of Unions.

But it is also interesting to notice what we have not used. We have not used the Axiom of Foundation. More significantly, we have not used the Replacement Axiom Scheme, or the Axiom of Choice.

This is significant because both the Axiom of Choice and the Replacement Axiom Scheme have been doubted by mathematicians. I may go into why, a bit later in term, when we have come to these axioms.