Appendix C: the rational numbers

Here we define the rational numbers and give their fundamental properties. For brevity we denote multiplication of integers by justaposition, as is usually done.

Let $A = \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$. We define a relation $\sim$ on A as follows:

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

This definition and succeeding ones are well-motivated if you think of (a, b) as being $\frac{a}{b}$ intuitively.

Lemma C1. *$\sim$ is an equivalence relation on A.*

Proof. Reflexivity: If $(a, b) \in A$, then $ab = ba$, so $(a, b) \sim (a, b)$.

Symmetry: Assume that $(a, b) \sim (c, d)$. Thus $ad = bc$, so $cb = da$, and hence $(c, d) \sim (a, b)$.

Transitivity: Assume that $(a, b) \sim (c, d) \sim (e, f)$. Thus $ad = bc$ and $cf = de$. Hence $adf = bcf = bde$, so $0 = adf - bde = d(af - be)$. Since $d \neq 0$, it follows that $af - be = 0$, and hence $af = be$. This shows that $(a, b) = (e, f)$. □

We let $\mathbb{Q}'$ be the set of all equivalence classes under $\sim$.

Proposition C2. *There is a binary operation $+$ on $\mathbb{Q}'$ such that for any $(a, b), (c, d) \in A$, $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$.*

Proof. First note that if $(a, b), (c, d) \in A$, then $bd \neq 0$, so that at least the pair $(ad + bc, bd)$ is in A. Now let

$$\begin{aligned} R = \{(x, y) : &\text{ there exist } (a, b), (c, d) \in A \text{ such that} \\ &x = ([(a, b)], [(c, d)]) \text{ and } y = [(ad + bc, bd)]\}. \end{aligned}$$

We claim that R is a function. For, suppose that $(x, y), (x, z) \in R$. Then we can choose $(a, b), (c, d), (a', b'), (c', d') \in A$ such that $x = ([(a, b)], [(c, d)])$, $y = [(ad + bc, bd)]$, $x = ([(a', b')], [(c', d')])$, and $y = [(a'd' + b'c', b'd')]$. so $([(a, b)], [(c, d)]) = ([(a', b')], [(c', d')])$, hence $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$, hence $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, hence

$$ab' = ba' \tag{1}$$

$$cd' = dc' \tag{2}$$

Hence

$$\begin{aligned} (ad + bc)b'd' &= adb'd' + bcb'd' \\ &= ab'dd' + cd'bb' \\ &= ba'dd' + dc'bb' \quad \text{by (1), (2)} \\ &= a'd'bd + b'c'bd \\ &= (a'd' + b'c')bd, \end{aligned}$$

and hence $(ad+bc, bd) \sim (a'd'+b'c', b'd')$. Thus $y = [(ad+bc, bd)] = [(a'd'+b'c', b'd')] = y'$. This proves that R is a function. The proposition is now clear. □

Proposition C3. *If $x, y, z \in \mathbb{Q}'$, then*
(i) $x + (y + z) = (x + y) + z$.
(ii) $x + y = y + x$.

Proof. Let $x = [(a, b)]$, $y = [(c, d)]$, and $z = [(e, f)]$. Then

$$\begin{aligned}
x + (y + z) &= [(a, b)] + ([(c, d)] + [(e, f)]) \\
&= [(a, b)] + [(cf + de, df)] \\
&= [(adf + b(cf + de), bdf)]; \\
(x + y) + z &= ([(a, b)] + [(c, d)]) + [(e, f)] \\
&= [(ad + bc, bd)] + [(e, f)] \\
&= [((ad + bc)f + bde, bdf)] \\
&= [(adf + bcf + bde, bdf)] \\
&= x + (y + z); \\
x + y &= [(a, b)] + [(c, d)] \\
&= [(ad + bc, bd)] \\
&= [(cb + da, db)] \\
&= [(c, d)] + [(a, b)] \\
&= y + x.
\end{aligned}$$

□

Now we define $0' = [(0, 1)]$.

Proposition C4. *$x + 0' = x$ for any $x \in \mathbb{Q}$. Moreover, for any $x \in \mathbb{Q}'$ there is a $y \in \mathbb{Q}'$ such that $x + y = 0'$.*

Proof. Let $x = [(a, b)]$. Then

$$\begin{aligned}
x + 0' &= [(a, b)] + [(0, 1)] \\
&= [(a \cdot 1 + b \cdot 0, b \cdot 1)] \\
&= [(a, b)] \\
&= x.
\end{aligned}$$

Next, let $y = [(-a, b)]$. Then

$$x + y = [(a, b)] + [(-a, b)] = [(ab + b(-a), bb)] = [(0, bb)] = [(0, 1)].$$

Here the last equality holds because $0 \cdot 1 = 0 = bb \cdot 0$. □

The following two facts are proved as in appendix B, proof of B6 and B7.

Proposition C5. *If r is an element of $\mathbb{Q}'$ such that $x + r = x$ for all $x \in \mathbb{Q}'$, then $r = 0'$.*

Proposition C6. *If $x, y, z \in \mathbb{Q}'$ and $x + y = 0' = x + z$, then $y = z$.*

These are all of the properties of $+$ that we need.

Proposition C7. *There is a binary operation $\cdot$ on $\mathbb{Q}'$ such that for all $(a, b), (c, d) \in A$, $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$.*

Proof. First note that if $(a, b), (c, d) \in A$, then $bd \neq 0$, so that $(ac, bd) \in A$. Now let

$$\begin{aligned} R = \{(x, y) :\ &\text{there exist } (a, b), (c, d) \in A \text{ such that} \\ &x = ([(a, b)], y = [(c, d)]),\ \text{and } z = [(ac, bd)]\}. \end{aligned}$$

We claim that R is a function. For, suppose that $(x, y), (x, z) \in R$. Then we can choose $(a, b), (c, d), (a', b'), (c', d') \in A$ such that $x = ([(a, b)], [(c, d)])$, $y = [(ac, bd)]$, $x = ([(a', b')], [(c', d')])$, and $z = [(a'c', b'd')]$. So $([(a, b)], [(c, d)]) = ([(a', b')], [(c', d')])$, and hence $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$, hence $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, hence $ab' = ba'$ and $cd' = dc'$. Hence

$$\begin{aligned} &acb'd' = ab'cd' = ba'dc' = bda'c', \\ &\text{hence } (ac, bd) \sim (a'c', b'd'), \\ &\text{hence } y = [(ac, bd)] = [(a'c', b'd')] = z. \end{aligned}$$

So R is a function, and the conclusion is clear. □

Proposition C8. *For any $x, y, z \in \mathbb{Q}'$ we have*
(i) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
(ii) $x \cdot y = y \cdot x$.
(iii) $x \cdot (y + z) = x \cdot y + x \cdot z$.

Proof. Write $x = [(a, b)]$, $y = [(c, d)$, and $z = [(e, f)]$. Then

$$\begin{aligned} x \cdot (y \cdot z) &= [(a, b)] \cdot ([(c, d)] \cdot [(e, f)]) \\ &= [(a, b)] \cdot [(ce, df)] \\ &= [(ace, bdf)] \\ &= [(ac, bd)] \cdot [(e, f)] \\ &= ([(a, b)] \cdot [(c, d)]) \cdot [(e, f)] \\ &= (x \cdot y) \cdot z; \\ x \cdot y &= [(a, b)] \cdot [(c, d)] \\ &= [(ac, bd)] \\ &= [(ca, db)] \\ &= [(c, d)] \cdot [(a, b)] \\ &= y \cdot x; \\ x \cdot (y + z) &= [(a, b)] \cdot ([(c, d)] + [(e, f)]) \end{aligned}$$

$$
\begin{aligned}
&= [(a,b)] \cdot [(cf+de, df)] \\
&= [(a(cf+de), bdf)] \\
&= [(acf+ade, bdf)]; \\
x \cdot y + x \cdot z &= [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)] \\
&= [(ac, bd)] + [(ae, bf)] \\
&= [(acbf + bdae, bdbf)].
\end{aligned}
$$

Thus for the distributive law (iii) we just need to show that $[(acf+ade, bdf)] = [(acbf + bdae, bdbf)]$, or equivalently that $(acf+ade, bdf) \sim (acbf + bdae, bdbf)$, or equivalently that $(acf+ade)bdbf = bdf(acbf + bdae)$. This last statement is proved as follows:

$$(acf+ade)bdbf = abbcdff + abbddef \text{ and } bdf(acbf + bdae) = abbcdff + abbddef. \quad \square$$

Next, we define $1' = [(1,1)]$.

Proposition C9. *Let $x \in \mathbb{Q}'$.*
(i) $x \cdot 1' = x$.
(ii) If $x \neq 0'$ then there is a unique $y \in \mathbb{Q}'$ such that $x \cdot y = 1'$.

Proof. Write $x = [(a,b)]$. Then $x \cdot 1' = [(a,b)] \cdot [(1,1)] = [(a,b)] = x$. For (ii), assume that $x \neq 0'$. Thus $[(a,b)] \neq [(0,1)]$, so $a \cdot 1 \neq b \cdot 0$, i.e., $a \neq 0$. Let $y = [(b,a)]$. Then $x \cdot y = [(a,b)] \cdot [(b,a)] = [(ab, ba)]$, and this is equal to $[(1,1)] = 1'$ since $ab1 = ba1$. Suppose that also $x \cdot z = 1'$. Write $z = [(c,d)]$. then $[(1,1)] = x \cdot z = [(a,b)] \cdot [(c,d)] = [ac, bd)$, and so $ac = bd$, and hence $y = [(b,a)] = [(c,d)] = z$. $\square$

We turn to the order of the rationals. In general outline, we follow the procedure used for the integers.

First we define the set P of positive rationals:

$$P = \{[(a,b)] \in \mathbb{Q}' : ab > 0\}.$$

As for the similar definition for integers, this definition says that if $ab > 0$ then $[(a,b)] \in P$, but does not say anything about the converse, so we prove this converse:

Proposition C10. $[(a,b)] \in P$ *iff* $ab > 0$.

Proof. As mentioned, $\Leftarrow$ holds by definition. Now assume that $[(a,b)] \in P$. This means that there is a $[(c,d)] \in \mathbb{Q}'$ such that $[(a,b)] = [(c,d)]$ and $cd > 0$. So $(a,b) \sim (c,d)$, and hence $ad = bc$. Hence $adbd = bcbd$. Now we need the following little general fact:

(1) If $x \in \mathbb{Z}$ and $x \neq 0$, then $xx > 0$.

In fact, we have $x > 0$ or $-x > 0$ by B13(i) and the definition of $<$ for integers, so by B14(v), $xx > 0$ or $xx = (-x)(-x) > 0$, as desired in (1).

Now by (1) and B14(v) we have $abdd = bcbd > 0$. In particular, $ab \neq 0$. If $ab < 0$, then $abdd < 0dd = 0$, contradiction. So $ab > 0$. $\square$

Proposition C11. *Suppose that $r, s \in \mathbb{Q}'$.*

(i) If $r \neq 0'$, then $r \in P$ or $-r \in P$, but not both.

(ii) If $r, s \in P$, then $r + s \in P$.

(iii) If $r, s \in P$, then $r \cdot s \in P$.

Proof. Let $r = [(a, b)]$ and $s = [(c, d)]$.

(i): Assume that $r \neq 0'$. Then $ab \neq 0$, since $ab = 0$ would imply that $a = 0$ (since $b \neq 0$), and so $(a, b) = (0, b) \sim (0, 0)$ and hence $r = [(a, b)] = [(0, 0)] = 0'$, contradiction. If $ab > 0$, then $r \in P$, and if $-(ab) > 0$, then $(-a)b > 0$, so $-r = [(-a, b)] \in P$. Thus $r \in P$ or $-r \in P$. Suppose that $r \in P$ and $-r \in P$. Thus $ab > 0$ and $(-a)b > 0$, contradiction.

(ii): Suppose that $r, s \in P$. Then $ab > 0$ and $cd > 0$. Now $r + s = [(ad + bc, bd)]$, and $(ad + bc)bd = abdd + bbcd$. By (1) in the proof of C10, $dd > 0$ and $bb > 0$. Hence by properties of integers, $abdd + bbcd > 0$.

(iii): Suppose that $r, s \in P$. Then $ab > 0$ and $cd > 0$. Now $rs = [(ac, bd)]$ and $acbd = abcd > 0$. □

Now we can define the order: $a < b$ iff $b - a \in P$. The main properties of $<$ are given in the following proposition.

Proposition C12. *Let $x, y, z \in \mathbb{Q}'$. Then*

(i) $x \not< x$.

(ii) If $x < y < z$, then $x < z$.

(iii) $x < y$, $x = y$, or $y < x$.

(iv) $x < y$ iff $x + z < y + z$.

(v) If $0' < x$ and $0' < y$, then $0' < x \cdot y$.

(vi) If $0' < z$, then $x < y$ implies that $x \cdot z < y \cdot z$.

Proof. (i): $x - x = 0'$, so (i) follows from C11(i).

(ii): Assume that $x < y < z$. So $y - x \in P$ and $z - y \in P$. Hence $z - x = (z - y) + y - x) \in P$ by C11(ii), so $x < z$.

(iii): We have $x = y$ or $x - y \in P$ or $y - x \in P$, so (iii) follows.

(iv): $x < y$ iff $y - x \in P$ iff $(y + z) - (x + z) \in P$ iff $x + z < y + z$.

(v): This is immediate from C11(iii).

(vi): Assume that $0' < z$ and $x < y$. So $z, y - x \in P$, so by C11(iii), $y \cdot z - x \cdot z = z \cdot (y - x) \in P$, and so $x \cdot z < y \cdot z$. □

This finishes the main construction of the rational numbers. There are still two things to do, though: identify the integers among the rationals, and make a replacement so that the integers are a subset of the rationals.

For every integer a we define $f(a) = [(a, 1)]$.

Proposition C13. *f is an isomorphism of $\mathbb{Z}$ into $\mathbb{Q}'$. That is, f is an injection, and for any $a, b \in \mathbb{Z}$ we have $f(a + b) = f(a) + f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$.*

Proof. Suppose that $f(a) = f(b)$. Thus $[(a, 1)] = [(b, 1)]$, hence $(a, 1) \sim (b, 1)$, hence $a = a1 = 1b = b$. So f is an injection.

Now suppose that $a, b \in \mathbb{Z}$. Then

$$f(a) + f(b) = [(a,1)] + [(b,1)] = [(a1 + 1b, 1)] = [(a+b,1)] = f(a+b);$$
$$f(a) \cdot f(b) = [(a,1)] \cdot [(b,1)] = [(ab,1)] = f(ab).$$ □

Proposition C14. $\mathbb{Z} \cap \mathbb{Q}' = \emptyset$.

Proof. To show that $\omega \cap \mathbb{Q}' = \emptyset$ it suffices to show that each element of $\mathbb{Q}'$ is infinite. If $[(a,b)] \in \mathbb{Q}'$, then $(ca, cb) \in [(a,b)]$ for every $c \in \mathbb{Z}$, and $cb \neq db$ for $c \neq d$, and so $(ca, cb) \neq (da, db)$ for $c \neq d$; hence $[(a,b)]$ is infinite.

Now suppose that $x \in \mathbb{Z} \cap \mathbb{Q}'$ with $x \notin \omega$. Temporarily denote the equivalence relation used to define $\mathbb{Z}'$ by $\equiv$. Then there exist $m, n \in \omega$ such that $x = [(m,n)]_{\equiv}$, and there exists $(a,b) \in A$ such that $x = [(a,b)]_{\sim}$. Then $(a,b) \sim (2a, 2b)$, so also $[(2a,2b)]_{\sim} = [(a,b)]_{\sim} = x = [(m,n)]_{\equiv}$. Hence $(a,b), (2a,2b) \in [(m,n)]_{\equiv}$, and it follows that $(a,b) \equiv (2a,2b)$. So $a + 2b = b + 2a$, and hence $a = b$. Then $(0,0) \equiv (a,b)$, so $(0,0) \in [(a,b)]_{\equiv} = [(a,b)]_{\sim}$, and we infer that $(0,0) \in A$, contradiction. □

We can now proceed very much like for $\mathbb{Z}$ and $\mathbb{Z}'$. We define $\mathbb{Q} = (\mathbb{Q}' \backslash \mathrm{rng}(f)) \cup \mathbb{Z}$. There is a one-one function $g : \mathbb{Q} \to \mathbb{Q}'$, defined by $g([(a,b)]) = [(a,b)]$ if $[(a,b)] \in \mathbb{Q}' \backslash \mathrm{rng}(f)$, and $g(a) = f(a)$ for $a \in \mathbb{Z}$. Clearly g is a bijection. Now the operations $+'$ and $\cdot'$ are defined on $\mathbb{Q}$ as follows. For any $a, b \in \mathbb{Q}$,

$$a +' b = g^{-1}(g(a) + g(b));$$
$$a \cdot' b = g^{-1}(g(a) \cdot g(b)).$$

moreover, we define $a <' b$ iff $g(a) < g(b)$. With these definitions, g becomes an isomorphism of $\mathbb{Q}$ onto $\mathbb{Q}'$. Namely, if $a, b \in \mathbb{Q}$, then

$$g(a +' b) = g(g^{-1}(g(a) + g(b))) = g(a) + g(b);$$
$$g(a \cdot' b) = g(g^{-1}(g(a) \cdot g(b))) = g(a) \cdot g(b);$$
$$a <' b \quad \text{iff} \quad g(a) < g(b).$$

Moreover, the operations $+'$ and $\cdot'$ on $\mathbb{Z}$ coincide with the ones defined in appendix C, since if $a, b \in \mathbb{Z}$, then

$$a +' b = g^{-1}(g(a) + g(b)) = g^{-1}(f(a) + f(b)) = g^{-1}(f(a+b)) = a + b;$$
$$a \cdot' b = g^{-1}(g(a) \cdot g(b)) = g^{-1}(f(a) \cdot f(b)) = g^{-1}(f(a \cdot b)) = a \cdot b;$$
$$\begin{aligned} a <' b \quad &\text{iff} \quad g(a) < g(b) \\ &\text{iff} \quad f(a) < f(b) \\ &\text{iff} \quad a < b. \end{aligned}$$

All of the properties above, like the associative, commutative, and distributive laws, hold for $\mathbb{Z}$ since g is an isomorphism. Of course we use $+, \cdot, <$ now rather than $+', \cdot', <'$.