Appendix B: the integers

In this appendix we define and develop the main properties of the integers. The development is based upon Chapter 6, in which properties of natural numbers were given. At the end of that chapter a sketch of the construction of integers was given, and we now give full details.

Let $A = \omega \times \omega$. We define a relation $\sim$ on A by setting, for any $m, n, p, q \in \omega$,

$$(m, n) \sim (p, q) \quad \text{iff} \quad m + q = n + p.$$

This definition is motivated by thinking of (m, n) as representing, in some sense, $m - n$.

Lemma B1. *$\sim$ is an equivalence relation on A.*

Proof. For reflexivity, given $m, n \in \omega$ we want to show that $(m, n) \sim (m, n)$. By definition, this means that we want to show that $m+n = n+m$. This is given by 6.14(iv).

For symmetry, assume that $(m, n) \sim (p, q)$; we want to show that $(p, q) \sim (m, n)$. The assumption means, by definition, that $m + q = n + p$. Hence $p + n = q + m$ by 6.14(iv) again. Hence $(p, q) \sim (m, n)$. [In the definition, replace m, n, p, q by p, q, m, n respectively.]

For transitivity, assume that $(m, n) \sim (p, q) \sim (r, s)$. Thus $m + q = n + p$ and $p + s = q + r$. Hence $m + q + s = n + p + s = n + q + r$, so using 6.15(iii) we get $m + s = n + r$, so that $(m, n) \sim (r, s)$. □

We now let $\mathbb{Z}'$ be the collection of all equivalence classes under $\sim$. Elements of $\mathbb{Z}'$ are denoted by $[(m, n)]$ with $m, n \in \omega$.

For the purposes of this appendix, we treat binary operations on $\mathbb{Z}'$ as functions mapping $\mathbb{Z}' \times \mathbb{Z}'$ into $\mathbb{Z}'$.

Proposition B2. *There is a binary operation $+$ on $\mathbb{Z}'$ such that for any $m, n, p, q \in \omega$, $[(m, n)] + [(p, q)] = [(m + p, n + q)]$.*

Proof. Let

$$R = \{(x, y) : \text{there exist } m, n, p, q \in \omega \text{ such that } x = ([(m, n)], [(p, q)]) \text{ and } y = [(m + p, n + q)]\}.$$

We claim that R is a function. For, assume that $(x, y), (x, z) \in R$. Then we can choose $m, n, p, q, m', n', p', q' \in \omega$ such that the following conditions hold:

(1) $x = ([(m, n)], [(p, q)])$;

(2) $y = [(m + p, n + q)]$;

(3) $x = ([(m', n')], [(p', q')])$;

(4) $z = [(m' + p', n' + q')]$.

From (1) and (3) we get $[(m, n)] = [(m', n')]$ and $[(p, q)] = [(p', q')]$, hence $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$, hence $m + n' = n + m'$ and $p + q' = q + p'$. Hence

$$m + p + n' + q' = m + n' + p + q' = n + m' + q + p' = n + q + m' + p',$$

from which it follows that $(m+p, n+q) \sim (m'+p', n'+q')$, hence $[(m+p, n+q)] = [(m'+p', n'+q')]$, hence $y = z$ by (2) and (4). This shows that R is a function.

Knowing that R is a function, the definition of R then says that for any $m, n, p, q \in \omega$, $([(m,n)], [(p,q)])$ is in the domain of R, and $R(([(m,n)], [(p,q)])) = [(m+p, n+q)]$. This is as desired in the proposition. □

Proposition B3. *The operation $+$ on $\mathbb{Z}'$ is associative and commutative. That is, if $x, y, z \in \mathbb{Z}'$, then $x + (y + z) = (x + y) + z$ and $x + y = y + x$.*

Proof. For any $a, b, c, d, e, f \in \omega$ we have

$$\begin{aligned}
[(a,b)] + ([(c,d)] + [(e,f)]) &= [(a,b)] + [(c+e, d+f)] \\
&= [(a+c+e, b+d+f)] \\
&= [(a+c, b+d)] + [(e,f)] \\
&= ([(a,b)] + [(c,d)]) + [(e,f)]; \\
[(a,b)] + [(c,d)] &= [(a+c, b+d)] \\
&= [(c+a, d+b)] \\
&= [(c,d)] + [(a,b)].
\end{aligned}$$

□

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

Proposition B4. *For any $a, b \in \omega$, $[(a,b)] + 0' = [(a,b)]$.* □

Proposition B5. *For any $x \in \mathbb{Z}'$ there is a $y \in \mathbb{Z}'$ such that $x + y = 0'$.*

Proof. Let $x \in \mathbb{Z}'$; hence there are $a, b \in \omega$ such that $x = [(a,b)]$. Let $y = [(b,a)]$. Then $x + y = [(a,b)] + [(b,a)] = [(a+b, b+a)] = [(0,0)] = 0'$. □

There are little group-theoretic facts that say that $0'$ and y above are unique:

Proposition B6. *If z is an element of $\mathbb{Z}'$ such that $x + z = x$ for all $x \in \mathbb{Z}'$, then $z = 0'$.*

Proof. $z = 0' + z$ (by B4) $= 0'$ (by assumption). □

Proposition B7. *If $x, y, z \in \mathbb{Z}'$ and $x + y = 0' = x + z$, then $y = z$.*

Proof. $y = 0' + y = x + z + y = z + x + y = z + 0' = z$. □

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

Proposition B8. *There is a binary operation $\cdot$ on $\mathbb{Z}'$ such that for all $m, n, p, q \in \omega$, $[(m,n)] \cdot [(p,q)] = [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)]$.*

Proof. Let

$$\begin{aligned}
R = \{(x,y) &: \text{there exist } m, n, p, q \in \omega \text{ such that} \\
&x = ([(m,n)], [(p,q)]) \text{ and } y = [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)]\}.
\end{aligned}$$

We claim that R is a function. For, assume that $(x, y), (x, z) \in R$. Then we can choose $m, n, p, q, m', n', p', q' \in \omega$ such that the following conditions hold:

(1) $x = ([(m, n)], [(p, q)])$;

(2) $y = [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)]$;

(3) $x = ([(m', n')], [(p', q')])$;

(4) $z = [(m' \cdot p' + n' \cdot q', m' \cdot q' + n' \cdot p')]$.

From (1) and (3) we get $[(m, n)] = [(m', n')]$ and $[(p, q)] = [(p', q')]$, hence $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$, hence $m + n' = n + m'$ and $p + q' = q + p'$. Hence

(1) $$m \cdot p + m \cdot q' + n \cdot q + n \cdot p' = m \cdot q + m \cdot p' + n \cdot p + n \cdot q'.$$

Also,

(2) $$m \cdot p' + n' \cdot p' + n \cdot q' + m' \cdot q' = n \cdot p' + m' \cdot p' + m \cdot q' + n' \cdot q'.$$

Hence

$$\begin{aligned} &m \cdot p + n \cdot q + m' \cdot q' + n' \cdot p' + m \cdot p' + n \cdot q' \\ &\quad = m \cdot p + n \cdot q + m \cdot p' + n' \cdot p' + n \cdot q' + m' \cdot q' \\ &\quad = m \cdot p + n \cdot q + n \cdot p' + m' \cdot p' + m \cdot q' + n' \cdot q' \quad \text{by (2)} \\ &\quad = m \cdot p + m \cdot q' + n \cdot q + n \cdot p' + m' \cdot p' + n' \cdot q' \\ &\quad = m \cdot q + m \cdot p' + n \cdot p + n \cdot q' + m' \cdot p' + n' \cdot q' \quad \text{by (1)} \end{aligned}$$

Considering the first side of the top equation and the last part, we can cancel $m \cdot p'$ and $n \cdot q'$ by 6.15(iii), and we get

$$m \cdot p + n \cdot q + m' \cdot q' + n' \cdot p' = m \cdot q + n \cdot p + m' \cdot p' + n' \cdot q',$$

which easily yields $y = z$.

Thus R is a function, and this clearly proves the proposition. □

Proposition B9. *Let $x, y, z \in \mathbb{Z}'$. Then*

(i) $x \cdot y = y \cdot x$.

(ii) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(iii) $x \cdot (y + z) = x \cdot y + x \cdot z$.

Proof. Write $x = [(m, n)]$, $y = [(p, q)$, and $z = [(r, s)]$. Then

$$\begin{aligned} x \cdot y &= [(m, n)] \cdot [(p, q)] \\ &= [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)] \\ &= [(p \cdot m + q \cdot n, p \cdot n + q \cdot m)] \\ &= [(p, q)] \cdot [(m, n)] \end{aligned}$$

$$
\begin{aligned}
&= y \cdot x; \\
x \cdot (y \cdot z) &= [(m,n)] \cdot ([(p,q)] \cdot [(r,s)]) \\
&= [(m,n)] \cdot [(p \cdot r + q \cdot s, p \cdot s + q \cdot r)] \\
&= [(m \cdot p \cdot r + m \cdot q \cdot s + n \cdot p \cdot s + n \cdot q \cdot r, \\
&\quad m \cdot p \cdot s + m \cdot q \cdot r + n \cdot p \cdot r + n \cdot q \cdot s)]; \\
(x \cdot y) \cdot z &= ([(m,n)] \cdot [(p,q)]) \cdot [(r,s)] \\
&= [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)] \cdot [(r,s)] \\
&= [(m \cdot p \cdot r + n \cdot q \cdot r + m \cdot q \cdot s + n \cdot p \cdot s, \\
&\quad m \cdot p \cdot s + n \cdot q \cdot s + m \cdot q \cdot r + n \cdot p \cdot r)] \\
&= x \cdot (y \cdot z) \quad \text{by the above;} \\
x \cdot (y + z) &= [(m,n)] \cdot ([(p,q)] + [(r,s)]) \\
&= [(m,n)] \cdot [(p + r, q + s)] \\
&= [(m \cdot p + m \cdot r + n \cdot q + n \cdot s, m \cdot q + m \cdot s + n \cdot p + n \cdot r)]; \\
x \cdot y + x \cdot z &= [(m,n)] \cdot [(p,q)] + [(m,n)] \cdot [(r,s)] \\
&= [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)] + [(m \cdot r + n \cdot s, m \cdot s + n \cdot r)] \\
&= [(m \cdot p + n \cdot q + m \cdot r + n \cdot s, m \cdot q + n \cdot p + m \cdot s + n \cdot r)] \\
&= x \cdot (y + z) \quad \text{by the above.}
\end{aligned}
$$

□

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

Proposition B10. *$1' \cdot x = x$ and $0' \cdot x = 0'$ for all $x \in \mathbb{Z}'$.*

Proof. Take any $x \in \mathbb{Z}$; say that $x = [(m,n)]$. Then

$$1' \cdot x = [(1,0)] \cdot [(m,n)] = [(1 \cdot m + 0 \cdot m, 1 \cdot n + 0 \cdot m)] = [(m,n)] = x,$$

as desired.

For the second statement, note that $x \cdot 0' + x = x \cdot 0' + x \cdot 1' = x \cdot (0' + 1') = x \cdot 1' = x$, so $x \cdot 0' = 0'$. □

Proposition B11. *If $x, y \in \mathbb{Z}'$ and $x \cdot y = 0'$, then $x = 0'$ or $y = 0'$.*

Proof. Write $x = [(m,n)]$ and $y = [(p,q)]$. Now $x \cdot y = [(m,n)] \cdot [(p,q)] = [m \cdot p + n \cdot q, m \cdot q + n \cdot p)]$ and also $x \cdot y = 0' = [0,0)]$, so $(m \cdot p + n \cdot q, m \cdot q + n \cdot p) \sim (0,0)$, so

$$m \cdot p + n \cdot q = m \cdot q + n \cdot p. \tag{1}$$

Suppose that $x \neq 0'$; we will show that $y = 0'$, which will prove the proposition. Thus $[(m,n)] = x \neq 0' = [(0,0)]$, so $m \neq n$. Hence $m < n$ or $n < m$.

Case 1. $m < n$. Then there is a nonzero natural number s such that $m + s = n$. Substituting this into (1) we get

$$
\begin{aligned}
m \cdot p + n \cdot q &= m \cdot p + (m + s) \cdot q \\
&= m \cdot p + m \cdot q + s \cdot q \quad \text{and} \\
m \cdot q + n \cdot p &= m \cdot q + (m + s) \cdot p \\
&= m \cdot q + m \cdot p + s \cdot p,
\end{aligned}
$$

and hence

$$m \cdot p + m \cdot q + s \cdot q = m \cdot q + m \cdot p + s \cdot p.$$

Then by 6.15(iii) we get $s \cdot q = s \cdot p$, and 6.20(viii) yields $q = p$. Hence $(p, q) \sim (0, 0)$, so $y = [(p, q)] = [(0, 0)] = 0'$.

Case 2. $n < m$. This is very similar to case 1. There is a nonzero natural number s such that $n + s = m$. Substituting this into (1) we get

$$\begin{aligned} m \cdot p + n \cdot q &= (n + s) \cdot p + n \cdot q \\ &= n \cdot p + s \cdot p + n \cdot q; \\ m \cdot q + n \cdot p &= (n + s) \cdot q + n \cdot p \\ &= n \cdot q + s \cdot q + n \cdot p, \end{aligned}$$

and hence

$$n \cdot p + s \cdot p + n \cdot q = n \cdot q + s \cdot q + n \cdot p.$$

Then by 6.15(iii) we get $s \cdot p = s \cdot q$, and 6.20(viii) yields $p = q$. Hence $(p, q) \sim (0, 0)$, so $y = [(p, q)] = [(0, 0)] = 0'$. □

This is all of the arithmetic properties of $\mathbb{Z}'$ that is needed. Now we introduce the order. First we only define the collection of positive elements:

$$P = \{[(m, n)] : m, n \in \omega \text{ and } m > n\}.$$

Note that this really means

$$P = \{x : \text{there exist } m, n \in \omega \text{ such that } x = [(m, n)] \text{ and } m > n\}.$$

Proposition B12. *For any $m, n \in \omega$, $[(m, n)] \in P$ iff $m > n$.*

Proof. $\Leftarrow$: true by definition. $\Rightarrow$: Suppose that $[(m, n)] \in P$. Choose $p, q \in \omega$ such that $p > q$ and $[(m, n)] = [(p, q)]$. Thus $(m, n) \sim (p, q)$, so $m + q = n + p$. If $m \leq n$, then by 6.17,

$$m + q \leq n + q < n + p = m + q,$$

contradiction. Hence $m < n$. □

Proposition B13. *For any $a, b \in \mathbb{Z}'$ we have:*
(i) If $a \neq 0'$, then $a \in P$ or $-a \in P$, but not both.
(ii) If $a, b \in P$, then $a + b \in P$.
(iii) If $a, b \in P$, then $a \cdot b \in P$.

Proof. Let $a = [(m, n)]$ and $b = [(p, q)]$. For (i), since $0' = [(0, 0)]$ we see that if $a \neq [(0, 0)]$ then $(m, n) \not\sim (0, 0)$ and so $m \neq n$. If $m < n$, then $-a = [(n, m)] \in P$. If $m > n$, then $a \in P$. If $a, -a \in P$, then by B12, $m < n$ and $n < m$, contradiction.

(ii): Assume that $a, b \in P$. Then by B12, $m > n$ and $p > q$. Clearly then $m+p > n+q$ by 6.17, so $a + b = [(m + p, n + q)] \in P$.

(iii): Assume that $a, b \in P$. Then by B12, $m > n$ and $p > q$. Write $n + s = m$ and $q + t = p$, with $s, t \neq 0$. Hence $s \cdot t \neq 0$. Now

$$(*) \qquad a \cdot b = [(m, n)] \cdot [(p, q)] = [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)].$$

Now

$$\begin{aligned} m \cdot q + n \cdot p + s \cdot t &= m \cdot q + n \cdot (q + t) + s \cdot t \\ &= m \cdot q + n \cdot q + n \cdot t + s \cdot t \\ &= m \cdot q + n \cdot q + (n + s) \cdot t \\ &= m \cdot q + n \cdot q + m \cdot t \\ &= m \cdot (q + t) + n \cdot q \\ &= m \cdot p + n \cdot q, \end{aligned}$$

and so $m \cdot q + n \cdot p < m \cdot p + n \cdot q$, so that $a \cdot b \in P$ by $(*)$ and B12. □

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

Proposition B14. *Let $x, y, z \in \mathbb{Z}'$. 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 B13(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 6.13(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 B13(iii).
(vi): Assume that $0' < z$ and $x < y$. So $z, y - x \in P$, so by B13(iii), $y \cdot z - x \cdot z = z \cdot (y - x) \in P$, and so $x \cdot z < y \cdot z$. □

This finishes our treatment of $\mathbb{Z}'$. Now we need to relate it to ω, and define our final version $\mathbb{Z}$ of the integers.

For any $m \in \omega$ let $f(m) = [(m, 0)]$.

Proposition B15. *f is a one-one function mapping ω into $\mathbb{Z}$. Moreover, for any $m, n \in \omega$ we have*
(i) $f(m + n) = f(m) + f(n)$.
(ii) $f(m \cdot n) = f(m) \cdot f(n)$.
(iii) $m < n$ iff $f(m) < f(n)$.

Proof. Suppose that $f(m) = f(n)$. Thus $[(m,0)] = [(n,0)]$, so $(m,0) \sim (n,0)$, hence $m + 0 = 0 + n$, hence $m = n$. So f is one-one. Next,

$$\begin{aligned}
f(m+n) &= [(m+n,0)] = [(m,0)] + [(n,0)] = f(m) + f(n);\\
f(m \cdot n) &= [(m \cdot n, 0)] = [(m \cdot n + 0 \cdot 0, m \cdot 0 + 0 \cdot n)] = [(m,0)] \cdot [(n,0)] = f(m) \cdot f(n)\\
f(m) < f(n) \quad &\text{iff} \quad [(m,0)] < [(n,0)]\\
&\text{iff} \quad m + 0 < 0 + n\\
&\text{iff} \quad m < n.
\end{aligned}$$

□

We have now identified a part of $\mathbb{Z}'$ which acts like the natural numbers. We now want to apply the replacement process given in 3.20 to officially define $\mathbb{Z}$. It turns out, though, that we do not need to use the general procedure of 3.20, since $\omega \cap \mathbb{Z}' = \emptyset$:

Proposition B16. $\omega \cap \mathbb{Z}' = \emptyset$.

Proof. Suppose that $m \in \omega \cap \mathbb{Z}'$. Choose $n, p \in \omega$ such that $m = [(n,p)]$. But $[(n,p)]$ is an infinite set, since it contains all of the pairs $(n,p), (n+1, p+1), (n+2, p+2), \ldots$, contradiction. □

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

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

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

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

Moreover, the operations $+'$ and $\cdot'$ on ω coincide with the ones defined in Chapter 6, since if $m, n \in \omega$, then

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

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 $+', \cdot', <'$.