9 The Construction of $\mathbb{Z}$

Basic idea

$$-1 = \{\langle 0,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \dots, \langle n, n+1\rangle, \dots\}$$
$$-5 = \{\langle 0,5\rangle, \langle 1,6\rangle, \langle 2,7\rangle, \dots, \langle n, n+5\rangle, \dots\}$$

Definition 9.1. Let $\sim$ be the binary relation on $\omega\times\omega$ defined by

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

Theorem 9.2. *$\sim$ is an equivalence relation on $\omega\times\omega$.*

Proof. Suppose that $\langle m,n\rangle \in \omega\times\omega$. Then $m+n = m+n$ and so $\langle m,n\rangle \sim \langle m,n\rangle$. Thus $\sim$ is reflexive.

Next suppose that $\langle m,n\rangle \sim \langle p,q\rangle$. Then $m+q = p+n$. Hence $p+n = m+q$ and so $\langle p,q\rangle \sim \langle m,n\rangle$. Thus $\sim$ is symmetric.

Finally suppose that $\langle m,n\rangle \sim \langle p,q\rangle$ and $\langle p,q\rangle \sim \langle r,s\rangle$. Then

$$\begin{aligned} m+q &= p+n \\ p+s &= r+q \end{aligned}$$

and so

$$m+q+p+s = p+n+r+q.$$

This implies

$$(m+s)+(p+q) = (r+n)+(p+q)$$

and so, by the Cancellation Law,

$$m+s = r+n.$$

Hence $\langle m,n\rangle \sim \langle r,s\rangle$ and so $\sim$ is transitive. □

Definition 9.3. The set $\mathbb{Z}$ of *integers* is defined by

$$\mathbb{Z} = \omega\times\omega/\sim$$

ie $\mathbb{Z}$ is the set of $\sim$–equivalence classes.

Notation For each $\langle m,n\rangle \in \omega\times\omega$, the corresponding $\sim$–equivalence class is denoted by $[\langle m,n\rangle]$.
eg

$$[\langle 0,3\rangle] = \{\langle 0,3\rangle, \langle 1,4\rangle, \langle 2,5\rangle, \dots\} \in \mathbb{Z}$$

Now we want to define an operation $+_{\mathbb{Z}}$ on $\mathbb{Z}$. [Note that

$$(m-n)+(p-q) = (m+p)-(n+q)$$

This suggests we make the following definition.]

Definition 9.4. We define the binary operation $+_{\mathbb{Z}}$ on $\mathbb{Z}$ by

$$[\langle m, n\rangle] +_{\mathbb{Z}} [\langle p, q\rangle] = [\langle m + p, n + q\rangle].$$

Lemma 9.5. *$+_{\mathbb{Z}}$ is well-defined.*

Proof. We must prove that if $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$, then $\langle m+p, n+q\rangle \sim \langle m' + p', n' + q'\rangle$. So suppose that $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$. Then

$$\begin{aligned} m + n' &= m' + n \\ p + q' &= p' + q \end{aligned}$$

and so

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

Hence $\langle m + p, n + q\rangle \sim \langle m' + p', n' + q'\rangle$. □

Theorem 9.6. *For all $a, b, c \in \mathbb{Z}$, we have that*

$$\begin{aligned} a +_{\mathbb{Z}} b &= b +_{\mathbb{Z}} a \\ (a +_{\mathbb{Z}} b) +_{\mathbb{Z}} &= a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c) \end{aligned}$$

Proof. We just check the first identity. (The proof of the second identity is similar.) Let $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$. Then

$$\begin{aligned} a +_{\mathbb{Z}} b &= [\langle m, n\rangle] +_{\mathbb{Z}} [\langle p, q\rangle] \\ &= [\langle m + p, n + q\rangle] \quad \text{Def of } +_{\mathbb{Z}} \\ &= [\langle p + m, q + n\rangle] \quad \text{Commutativity of + on } \omega \\ &= [\langle p, q\rangle] +_{\mathbb{Z}} [\langle m, n\rangle] \quad \text{Def of } +_{\mathbb{Z}} \\ &= b +_{\mathbb{Z}} a. \end{aligned}$$

□

Definition 9.7 (Identity element for addition).

$$0_{\mathbb{Z}} = [\langle 0, 0\rangle].$$

Theorem 9.8.

- *For all $a \in \mathbb{Z}$, $a +_{\mathbb{Z}} 0_{\mathbb{Z}} = a$.*
- *For any $a \in \mathbb{Z}$, there exists a* unique *$b \in \mathbb{Z}$ such that*

$$a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}.$$

Proof.

- Let $a = [\langle m, n\rangle]$. Then

$$\begin{aligned} a +_{\mathbb{Z}} 0_{\mathbb{Z}} &= [\langle m, n\rangle] +_{\mathbb{Z}} [\langle 0, 0\rangle] \\ &= [\langle m+0, n+0\rangle] \\ &= [\langle m, n\rangle] \\ &= a \end{aligned}$$

- Let $a = [\langle m, n\rangle]$. To see that there exists *at least* one such element, consider $b = [\langle n, m\rangle]$. Then

$$\begin{aligned} a +_{\mathbb{Z}} b &= [\langle m, n\rangle] +_{\mathbb{Z}} [\langle n, m\rangle] \\ &= [\langle m+n, n+m\rangle]. \end{aligned}$$

  Note that $m + n + 0 = 0 + n + m$. Hence

$$\begin{aligned} a +_{\mathbb{Z}} b &= [\langle m+n, n+m\rangle] \\ &= [\langle 0, 0\rangle] \\ &= 0_{\mathbb{Z}}. \end{aligned}$$

  To see that there exists *at most* one such element, suppose that $a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}$ and $a +_{\mathbb{Z}} b' = 0_{\mathbb{Z}}$. Then

$$\begin{aligned} b &= b +_{\mathbb{Z}} 0_{\mathbb{Z}} \\ &= b +_{\mathbb{Z}} (a +_{\mathbb{Z}} b') \\ &= (b +_{\mathbb{Z}} a) +_{\mathbb{Z}} b' \\ &= (a +_{\mathbb{Z}} b) +_{\mathbb{Z}} b' \\ &= 0_{\mathbb{Z}} +_{\mathbb{Z}} b' \\ &= b' \quad \square \end{aligned}$$

Definition 9.9. For any $a \in \mathbb{Z}$, $-a$ is the unique element of $\mathbb{Z}$ such that

$$a +_{\mathbb{Z}} (-a) = 0_{\mathbb{Z}}.$$

Definition 9.10. We define the binary operation $-_{\mathbb{Z}}$ on $\mathbb{Z}$ by

$$a -_{\mathbb{Z}} b = a +_{\mathbb{Z}} (-b).$$

Remark 9.11.

- Clearly $-_{\mathbb{Z}}$ is well-defined.

- From the above proof, if $a = [\langle m, n\rangle]$, then $-a = [\langle n, m\rangle]$.

[Next we want to define a multiplication operation on $\mathbb{Z}$. Note that

$$(m - n) \cdot (p - q) = mp + nq - (mq + np).$$

This suggests that we make the following definition.]

Definition 9.12. We define the binary operation $\cdot_{\mathbb{Z}}$ on $\mathbb{Z}$ by

$$[\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p, q\rangle] = [\langle mp + nq, mq + np\rangle].$$

Lemma 9.13. *$\cdot_{\mathbb{Z}}$ is well-defined.*

Proof. We must show that if $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$, then

$$\langle mp + nq, mq + np\rangle \sim \langle m'p' + n'q', m'q' + n'p'\rangle.$$

Tedious reading exercise, Enderton p. 96. □

Theorem 9.14. *For all $a, b, c \in \mathbb{Z}$, we have that*

$$a \cdot_{\mathbb{Z}} b = b \cdot_{\mathbb{Z}} a$$

$$(a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c = a \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c)$$
$$a \cdot_{\mathbb{Z}} (b +_{\mathbb{Z}} c) = a \cdot_{\mathbb{Z}} b +_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} c)$$

Proof. We just check the first equality. (The proofs of the other equalities are similar.) Let $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$. Then

$$\begin{aligned} a \cdot_{\mathbb{Z}} b &= [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle p, q\rangle] \\ &= [\langle mp + nq, mq + np\rangle] \end{aligned}$$

and

$$\begin{aligned} b \cdot_{\mathbb{Z}} a &= [\langle p, q\rangle] \cdot_{\mathbb{Z}} [\langle m, n\rangle] \\ &= [\langle pm + qn, pn + qm\rangle] \end{aligned}$$

Using the commutivity of addition and multiplication in ω we see that

$$mp + nq = pm + qn \quad \text{and} \quad mq + np = pn + qm.$$

Thus

$$a \cdot_{\mathbb{Z}} b = b \cdot_{\mathbb{Z}} a.$$ □

Definition 9.15 (Identity for multiplication).

$$1_{\mathbb{Z}} = [\langle 1, 0\rangle].$$

Theorem 9.16. *For all $a \in \mathbb{Z}$, $a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = a$.*

Proof. Let $a = [\langle m, n\rangle]$. Then

$$\begin{aligned} a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} &= [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle 1, 0\rangle] \\ &= [\langle m \cdot 1 + n \cdot 0, m \cdot 0 + n \cdot 1\rangle] \\ &= [\langle m, n\rangle] \\ &= a \quad \square \end{aligned}$$

Finally we want to define an order relation on $\mathbb{Z}$. [Note that

$$m - n < p - q \quad \text{iff} \quad m + q < p + n.$$

This suggests the following definition.]

Definition 9.17. We define the binary relation $<_{\mathbb{Z}}$ on $\mathbb{Z}$ by

$$[\langle m, n\rangle] <_{\mathbb{Z}} [\langle p, q\rangle] \quad \text{iff} \quad m + q < p + n.$$

Lemma 9.18. *$<_{\mathbb{Z}}$ is well-defined.*

Proof. Reading Exercise, Enderton p. 98. $\square$

Theorem 9.19. *$<_{\mathbb{Z}}$ is a linear order on $\mathbb{Z}$.*

Proof. First we prove that $<_{\mathbb{Z}}$ is transitive. Let $a = [\langle m, n\rangle]$, $b = [\langle p, q\rangle]$, and $c = [\langle r, s\rangle]$. Suppose that $a <_{\mathbb{Z}} b$ and $b <_{\mathbb{Z}} c$. Thus

$$\begin{aligned} m + q &< p + n \quad (1) \\ p + s &< r + q \quad (2) \end{aligned}$$

Using our earlier theorems, this implies that

$$\begin{aligned} m + q + s &< p + n + s \quad (3) \\ p + s + n &< r + q + n \quad (4) \end{aligned}$$

Using (3), (4), and the transitivity of $<$ on ω, we obtain

$$m + q + s < r + q + n \quad (5)$$

By our earlier theorem,

$$m + s < r + n$$

Hence $[\langle m, n\rangle] <_{\mathbb{Z}} [\langle r, s\rangle]$; ie $a <_{\mathbb{Z}} c$.

Next we prove trichotomy. Again let $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$. Then the following statements are equivalent:

(I) Exactly one of the following holds

$$a <_Z Zb, \quad a = b, \quad b <_{\mathbb{Z}} a$$

(II) Exactly one of the following holds

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

Clearly (II) follows from the fact that $<$ satisfies trichotomy on ω. Hence (I) also holds. □

Definition 9.20.
An integer $b \in \mathbb{Z}$ is *positive* iff $0_{\mathbb{Z}} <_{\mathbb{Z}} b$.
An integer $b \in \mathbb{Z}$ is *negative* iff $b <_{\mathbb{Z}} 0_{\mathbb{Z}}$.

Lemma 9.21. *For all $b \in \mathbb{Z}$, exactly one of the following holds:*

- *b is positive.*
- *b is negative*
- *$b = 0_{\mathbb{Z}}$.*

Proof. An immediate consequence of trichotomy for $<_{\mathbb{Z}}$. □

Exercise 9.22. For all $b \in \mathbb{Z}$, $b <_{\mathbb{Z}} 0_{\mathbb{Z}}$ iff $0_{\mathbb{Z}} <_{\mathbb{Z}} -b$.

Exercise 9.23. Suppose that $m, n \in \omega$ and that $m < n$. Then there exists $p \in \omega$ such that $n = m + p^+$. [Hint: argue by induction on p.]

Remark 9.24. Clearly ω is not *literally* a subset of $\mathbb{Z}$. However, $\mathbb{Z}$ does contain an "isomorphic copy" of ω

Definition 9.25. Let $E \colon \omega \to \mathbb{Z}$ be the function defined by

$$E(n) = [\langle n, 0 \rangle].$$

Theorem 9.26. *E is an injection of ω into $\mathbb{Z}$ which satisfies the following properties for all $m, n \in \omega$:*

(a) $E(m + n) = E(m) +_{\mathbb{Z}} E(n)$.

(b) $E(mn) = E(m) \cdot_{\mathbb{Z}} E(n)$.

(c) $m < n$ *iff* $E(m) <_{\mathbb{Z}} E(n)$.

Proof. First we prove that E is an injection. So suppose that $m, n \in \omega$. Then

$$\begin{aligned} E(m) = E(n) \quad &\text{implies} \quad [\langle m, 0\rangle] = [\langle n, 0\rangle] \\ &\text{implies} \quad \langle m, 0\rangle \sim \langle n, 0\rangle \\ &\text{implies} \quad m + 0 = n + 0 \\ &\text{implies} \quad m = n. \end{aligned}$$

Next we prove that (a) holds. Let $m, n \in \omega$. Then

$$\begin{aligned} E(m) +_{\mathbb{Z}} E(n) &= [\langle m, 0\rangle] +_{\mathbb{Z}} [\langle n, 0\rangle] \\ &= [\langle m + n, 0 + 0\rangle] \\ &= [\langle m + n, 0\rangle] \\ &= E(m + n). \end{aligned}$$

The proofs of (b) and (c) are similar. □

Theorem 9.27. *For all $b \in \mathbb{Z}$, exactly one of the following holds:*

(i) $b = 0_Z Z$

(ii) There exists $p \in \omega$ such that $b = E(p^+)$.

(iii) There exists $p \in \omega$ such that $b = -E(p^+)$.

Proof. Let $b = [\langle m, n\rangle]$. There are three cases to consider.

Case 1 If $m = n$, then $\langle m, n\rangle \sim \langle 0, 0\rangle$ and so $b = [\langle 0, 0\rangle] = 0_{\mathbb{Z}}$.

Case 2 If $m > n$, then there exists $p \in \omega$ such that $m = n + p^+$. It follows that $\langle m, n\rangle =\sim \langle p^+, 0\rangle$ and so $b = [\langle p^+, 0\rangle] = E(p^+)$.

Case 3 If $m < n$, then there exists $p \in \omega$ such that $n = m + p^+$. It follows that $\langle m, n\rangle =\sim \langle 0, p^+\rangle$ and so

$$b = [\langle 0, p^+\rangle] = -[\langle p^+, 0\rangle] = -E(p^+).$$

□

Theorem 9.28 (Cancellation Law for $\mathbb{Z}$). *(a) For any $a, b, c \in \mathbb{Z}$,*

$$a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c \quad \textit{implies} \quad a = b.$$

- *For any $a, b \in \mathbb{Z}$ and $0_{\mathbb{Z}} \neq c \in \mathbb{Z}$,*

$$a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c \quad \textit{implies} \quad a = b.$$

Proof. Reading Exercise Enderton, p. 99-100. □

Notation From now on, we write $+, \cdot, <, 0, 1$ instead of $+_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, <_{\mathbb{Z}}, 0_{\mathbb{Z}}, 1_{\mathbb{Z}}$. We also usually write ab instead of $a \cdot b$