

## **2.7 The integers**

Stephan Falke

September 20<sup>th</sup> 2006

## 2.7 The integers

In this section, we give a construction of the set  $\mathbb{Z}$  of integers, both positive and negative.

Call a pair  $(m, n)$  of natural numbers a DIFFERENCE. Then an integer will be an equivalence class of differences. Informally, the differences  $(m, n)$  and  $(p, q)$  are equivalent iff  $m - n = p - q$ . But this has no meaning since we cannot subtract natural numbers.

### Definition 2.7.1

Let  $\sim$  be the binary relation on  $\mathbb{N} \times \mathbb{N}$  defined by

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

### Proposition 2.7.2

The relation  $\sim$  is an equivalence relation on  $\mathbb{N} \times \mathbb{N}$ .

*Proof.*

reflexivity: Let  $(m, n) \in \mathbb{N} \times \mathbb{N}$ . Then,  $m + n = m + n$ , which clearly implies  $(m, n) \sim (m, n)$ .

symmetry: Let  $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$  such that  $(m, n) \sim (p, q)$ . Thus,  $m + q = p + n$ . But then  $p + n = m + q$  as well, i.e.,  $(p, q) \sim (m, n)$ .

transitivity: Let  $(m, n), (p, q), (s, t) \in \mathbb{N} \times \mathbb{N}$  such that  $(m, n) \sim (p, q)$  and  $(p, q) \sim (s, t)$ . Thus,  $m + q = p + n$  and  $p + t = q + s$ . But adding these two equations we get  $m + q + p + t = p + n + q + s$ . By cancellation for addition,  $m + t = n + s$ . But this shows  $(m, n) \sim (s, t)$ .  $\square$

### Definition 2.7.3

The set  $\mathbb{Z}$  of INTEGERS is the set  $(\mathbb{N} \times \mathbb{N})/\sim$  of all equivalence classes of differences.

### Example 2.7.4

1. The integer  $2_{\mathbb{Z}}$  is the equivalence class

$$[(2, 0)]_{\sim} = \{(2, 0), (3, 1), (4, 2), \dots\}$$

2. The integer  $-3_{\mathbb{Z}}$  is the equivalence class

$$[(0, 3)]_{\sim} = \{(0, 3), (1, 4), (2, 5), \dots\}$$

Next we want to define a suitable addition operation in  $\mathbb{Z}$ . Informally, we can add differences as follows:

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

Hence, we are tempted to define

$$[(m, n)]_{\sim} +_{\mathbb{Z}} [(p, q)]_{\sim} = [(m + p, n + q)]_{\sim}$$

In order for this to make sense on equivalence classes, we need the following.

**Proposition 2.7.5**

If  $(m, n) \sim (m', n')$  and  $(p, q) \sim (p', q')$  then  $(m + p, n + q) \sim (m' + p', n' + q')$ .

*Proof.* The hypothesis yields  $m + n' = m' + n$  and  $p + q' = p' + q$ . Then,  $m + n' + p + q' = m' + n + p' + q$  by adding the equations. But this means  $(m + p, n + q) \sim (m' + p', n' + q')$ .  $\square$

Thus, the definition of  $+_{\mathbb{Z}}$  does not depend on the members of the equivalence classes that are used. This property is called COMPATIBILITY OF  $+_{\mathbb{Z}}$  WITH  $\sim$ .

**Example 2.7.6**

$$\begin{aligned} 2_{\mathbb{Z}} +_{\mathbb{Z}} (-3_{\mathbb{Z}}) &= [(2, 0)]_{\sim} +_{\mathbb{Z}} [(0, 3)]_{\sim} \\ &= [(2 + 0, 0 + 3)]_{\sim} \\ &= [(2, 3)]_{\sim} \\ &= [(0, 1)]_{\sim} \\ &= -1_{\mathbb{Z}} \end{aligned}$$

**Proposition 2.7.7**

The operation  $+_{\mathbb{Z}}$  is associative and commutative.

*Proof.* Let  $a, b, c \in \mathbb{Z}$ . Then,  $a = [(m, n)]_{\sim}$ ,  $b = [(p, q)]_{\sim}$ ,  $c = [(s, t)]_{\sim}$ . Now,

$$\begin{aligned} (a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c &= ([(m, n)]_{\sim} +_{\mathbb{Z}} [(p, q)]_{\sim}) +_{\mathbb{Z}} [(s, t)]_{\sim} \\ &= [(m + p, n + q)]_{\sim} +_{\mathbb{Z}} [(s, t)]_{\sim} \\ &= [(m + p) + s, (n + q) + t]_{\sim} \\ &= [(m + (p + s), n + (q + t))]_{\sim} \quad \text{since } + \text{ is associative} \\ &= [(m, n)]_{\sim} +_{\mathbb{Z}} [(p + s, q + t)]_{\sim} \\ &= [(m, n)]_{\sim} +_{\mathbb{Z}} ([[(p, q)]_{\sim} +_{\mathbb{Z}} [(s, t)]_{\sim}) \\ &= a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c) \end{aligned}$$

Hence,  $+_{\mathbb{Z}}$  is associative.

Similarly,

## 2.7. THE INTEGERS

---

$$\begin{aligned}
 a +_{\mathbb{Z}} b &= [(m, n)]_{\sim} +_{\mathbb{Z}} [(p, q)]_{\sim} \\
 &= [(m + p, n + q)]_{\sim} \\
 &= [(p + m, q + n)]_{\sim} && \text{since } + \text{ is commutative} \\
 &= [(p, q)]_{\sim} +_{\mathbb{Z}} [(m, n)]_{\sim} \\
 &= b +_{\mathbb{Z}} a
 \end{aligned}$$

Thus,  $+_{\mathbb{Z}}$  is commutative.  $\square$

### Proposition 2.7.8

Let  $a, b, c \in \mathbb{Z}$ . If  $a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c$ , then  $a = b$ .

*Proof.* Let  $a = [(m, n)]_{\sim}$ ,  $b = [(p, q)]_{\sim}$ ,  $c = [(s, t)]_{\sim}$ . Assume  $a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c$ . Then,

$$\begin{aligned}
 a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c &\text{ implies } [(m, n)]_{\sim} +_{\mathbb{Z}} [(s, t)]_{\sim} = [(p, q)]_{\sim} +_{\mathbb{Z}} [(s, t)]_{\sim} \\
 &\text{ implies } [(m + s, n + t)]_{\sim} = [(p + s, q + t)]_{\sim} \\
 &\text{ implies } m + s + q + t = p + s + n + t \\
 &\text{ implies } m + q = p + n && \text{by cancellation for } + \\
 &\text{ implies } (m, n) \sim (p, q) \\
 &\text{ implies } [(m, n)]_{\sim} = [(p, q)]_{\sim} \\
 &\text{ implies } a = b
 \end{aligned}$$

$\square$

### Proposition 2.7.9

1.  $0_{\mathbb{Z}} = [(0, 0)]_{\sim}$  is the unique additive identity element for  $+_{\mathbb{Z}}$ , i.e.,

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

for all  $a \in \mathbb{Z}$ .

2. For any integer  $a$ , there exists a unique integer  $b$  such that

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

This  $b$  is called the ADDITIVE INVERSE of  $a$ . If  $a = [(m, n)]_{\sim}$  then its additive inverse is  $-a = -[(m, n)]_{\sim} = [(n, m)]_{\sim}$ .

*Proof.*

1. Let  $a = [(m, n)]_{\sim}$ . Then,  $a +_{\mathbb{Z}} 0_{\mathbb{Z}} = [(m, n)]_{\sim} +_{\mathbb{Z}} [(0, 0)]_{\sim} = [(m + 0, n + 0)]_{\sim} = [(m, n)]_{\sim} = a$ .

For uniqueness, assume there is an integer  $e$  such that  $a +_{\mathbb{Z}} e = a$  for all integers  $a$ . Then, in particular  $0_{\mathbb{Z}} +_{\mathbb{Z}} e = 0_{\mathbb{Z}}$ . Also, since  $0_{\mathbb{Z}}$  is an additive identity,  $e +_{\mathbb{Z}} 0_{\mathbb{Z}} = e$ . Now, using the commutativity of addition,  $e = 0_{\mathbb{Z}}$  follows.

2. Let  $a = [(m, n)]_{\sim}$ . Define  $b := [(n, m)]_{\sim}$ . Then,  $a +_{\mathbb{Z}} b = [(m, n)]_{\sim} +_{\mathbb{Z}} [(n, m)]_{\sim} = [(m + n, n + m)]_{\sim} = [(0, 0)]_{\sim} = 0_{\mathbb{Z}}$ .

For uniqueness, assume  $a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}$  and  $a +_{\mathbb{Z}} b' = 0_{\mathbb{Z}}$  for some  $b, b' \in \mathbb{Z}$ . Now,

$$b = b +_{\mathbb{Z}} 0_{\mathbb{Z}} = b +_{\mathbb{Z}} (a +_{\mathbb{Z}} b') = (b +_{\mathbb{Z}} a) +_{\mathbb{Z}} b' = 0_{\mathbb{Z}} + b' = b'$$

□

Using additive inverses, we can also define a subtraction operation on  $\mathbb{Z}$ .

**Definition 2.7.10**

Let  $a, b \in \mathbb{Z}$ . Then SUBTRACTION is defined as

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

Similarly to addition, we can also define a multiplication  $\cdot_{\mathbb{Z}}$  on  $\mathbb{Z}$  as follows:

$$[(m, n)]_{\sim} \cdot_{\mathbb{Z}} [(p, q)]_{\sim} := [(mp + nq, mq + np)]_{\sim}$$

This definition is informally motivated by the property

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

**Proposition 2.7.11**

The operation  $\cdot_{\mathbb{Z}}$  is compatible with  $\sim$ .

*Proof.* We need to show that  $(m, n) \sim (m', n')$  and  $(p, q) \sim (p', q')$  implies  $(mp + nq, mq + np) \sim (m'p' + n'q', m'q' + n'p')$ . Thus, let  $(m, n) \sim (m', n')$  and  $(p, q) \sim (p', q')$ . This means

$$m + n' = m' + n \tag{2.1}$$

$$p + q' = p' + q \tag{2.2}$$

Multiplying equation (2.1) by  $p$  gives

$$mp + n'p = m'p + np \tag{2.3}$$

Multiplying equation (2.2) by  $n'$  and reading it right-to-left gives

$$n'p' + n'q = n'p + n'q' \tag{2.4}$$

By adding equations (2.3) and (2.4) we obtain

$$mp + n'p + n'p' + n'q = m'p + np + n'p + n'q' \tag{2.5}$$

## 2.7. THE INTEGERS

---

Cancelling the common term  $n'p$  gives

$$mp + n'p' + n'q = m'p + np + n'q' \quad (2.6)$$

Similarly, we can multiply equation (2.1) by  $q$  and read it right-to-left, and we can multiply equation (2.2) by  $m'$ . This gives

$$m'q + nq = mq + n'q \quad (2.7)$$

$$m'p + m'q' = m'p' + m'q \quad (2.8)$$

Adding (2.7) and (2.8) gives

$$m'q + nq + m'p + m'q' = mq + n'q + m'p' + m'q \quad (2.9)$$

After cancelling the common term  $m'q$  we get

$$nq + m'p + m'q' = mq + n'q + m'p' \quad (2.10)$$

Finally, we add (2.6) and (2.10) to get

$$\begin{aligned} mp + n'p' + n'q + nq + m'p + m'q' &= \\ m'p + np + n'q' + mq + n'q + m'p' & \end{aligned} \quad (2.11)$$

The terms  $n'q$  and  $m'p$  are common and can be cancelled to get

$$mp + n'p' + nq + m'q' = np + n'q' + mq + m'p' \quad (2.12)$$

Reordering the terms gives

$$mp + nq + m'q' + n'p' = m'p' + n'q' + mq + np \quad (2.13)$$

But this means  $(mp + nq, mq + np) \sim (m'p' + n'q', m'q' + n'p')$   $\square$

### Proposition 2.7.12

The operation  $\cdot_{\mathbb{Z}}$  is associative, commutative, and distributive over  $+$ .

*Proof.* Let  $a = [(m, n)]_{\sim}$ ,  $b = [(p, q)]_{\sim}$ ,  $c = [(s, t)]_{\sim}$ . Then  $\cdot_{\mathbb{Z}}$  is commutative since

$$\begin{aligned} a \cdot_{\mathbb{Z}} b &= [(m, n)]_{\sim} \cdot_{\mathbb{Z}} [(p, q)]_{\sim} \\ &= [(mp + nq, mq + np)]_{\sim} \\ &= [(pm + qn, qm + pn)]_{\sim} \quad \text{since } \cdot \text{ is commutative} \\ &= [(pm + qn, pn + qm)]_{\sim} \quad \text{since } + \text{ is commutative} \\ &= [(p, q)]_{\sim} \cdot_{\mathbb{Z}} [(m, n)]_{\sim} \\ &= b \cdot_{\mathbb{Z}} a \end{aligned}$$

For associativity,

$$\begin{aligned} a \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c) &= [(m, n)]_{\sim} \cdot_{\mathbb{Z}} ([p, q]_{\sim} \cdot_{\mathbb{Z}} [(s, t)]_{\sim}) \\ &= [(m, n)]_{\sim} \cdot [(ps + qt, pt + qs)]_{\sim} \\ &= [(m(ps + qt) + n(pt + sq), m(pt + qs) + n(ps + qt))]_{\sim} \end{aligned}$$

and

$$\begin{aligned} (a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c &= ([m, n]_{\sim} \cdot_{\mathbb{Z}} [p, q]_{\sim}) \cdot_{\mathbb{Z}} [(s, t)]_{\sim} \\ &= [(mp + nq, mq + np)]_{\sim} \cdot [(s, t)]_{\sim} \\ &= [((mp + nq)s + (mq + np)t, (mp + nq)t + (mq + np)s)]_{\sim} \end{aligned}$$

By properties of addition and multiplication on  $\mathbb{N}$  these are the same, hence  $\cdot_{\mathbb{Z}}$  is associative.

Finally, for distributivity,

$$\begin{aligned} (a +_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c &= ([m, n]_{\sim} +_{\mathbb{Z}} [p, q]_{\sim}) \cdot_{\mathbb{Z}} [(s, t)]_{\sim} \\ &= [(m + p, n + q)]_{\sim} \cdot_{\mathbb{Z}} [(s, t)]_{\sim} \\ &= [(m + p)s + (n + q)t, (m + p)t + (n + q)s]_{\sim} \end{aligned}$$

and

$$\begin{aligned} (a \cdot_{\mathbb{Z}} c) +_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c) &= ([m, n]_{\sim} \cdot_{\mathbb{Z}} [(s, t)]_{\sim}) +_{\mathbb{Z}} ([p, q]_{\sim} \cdot_{\mathbb{Z}} [(s, t)]_{\sim}) \\ &= [(ms + nt, mt + ns)]_{\sim} +_{\mathbb{Z}} [(ps + qt, pt + qs)]_{\sim} \\ &= [(ms + nt + ps + qt, mt + ns + pt + qs)]_{\sim} \end{aligned}$$

By properties of addition and multiplication on  $\mathbb{N}$  these are the same, hence  $\cdot_{\mathbb{Z}}$  is distributive over  $+_{\mathbb{Z}}$ .  $\square$

There is a unique multiplicative identity, denoted  $1_{\mathbb{Z}}$ .

**Proposition 2.7.13**

$1_{\mathbb{Z}} = [(1, 0)]_{\sim}$  is the unique multiplicative identity element for  $\cdot_{\mathbb{Z}}$ , i.e.,

$$a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = a$$

for all  $a \in \mathbb{Z}$ .

*Proof.* Let  $a = [(m, n)]_{\sim}$ . Then we get  $a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = [(m, n)]_{\sim} \cdot_{\mathbb{Z}} [(1, 0)]_{\sim} = [(m \cdot 1 + n \cdot 0, m \cdot 0 + n \cdot 1)]_{\sim} = [(m, n)]_{\sim} = a$ .

For uniqueness, assume there is an integer  $e$  such that  $a \cdot_{\mathbb{Z}} e = a$  for all integers  $a$ . Then, in particular  $1_{\mathbb{Z}} \cdot_{\mathbb{Z}} e = 1_{\mathbb{Z}}$ . Also, since  $1_{\mathbb{Z}}$  is a multiplicative identity,  $e \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = e$ . Now, using the commutativity of  $\cdot_{\mathbb{Z}}$ , we obtain  $e = 1_{\mathbb{Z}}$ .  $\square$

**Proposition 2.7.14**

Let  $a \in \mathbb{Z}$ . Then  $a \cdot_{\mathbb{Z}} 0_{\mathbb{Z}} = 0_{\mathbb{Z}}$ .

*Proof.* Let  $a = [(m, n)]_{\sim}$ . Then

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

## 2.7. THE INTEGERS

---

We state the following without proof:

**Fact 2.7.15**

Let  $a, b \in \mathbb{Z}$  such that  $a \neq 0_{\mathbb{Z}}$  and  $b \neq 0_{\mathbb{Z}}$ . Then  $a \cdot_{\mathbb{Z}} b \neq 0_{\mathbb{Z}}$ .

**Fact 2.7.16**

Let  $a, b, c \in \mathbb{Z}$ . If  $a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c$  and  $c \neq 0_{\mathbb{Z}}$ , then  $a = b$ .