Chapter 1

The Integers

1.1 The integers

Definition 1.1.1 (Integers). *An* integer *is an expression of the form a–b, where a and b are natural numbers. Two integers are considered to be equal, a–b = c–d, iff a + d = c + b. We let denote the set of all integers.*

Remark 1.1.2. *In the language of set theory, what we are doing here is starting with the space × of ordered pairs (a, b) of natural numbers. Then we place an equivalence relation ∼ on these pairs by declaring (a, b) ∼ (c, d) iff a + d = c + b. The set-theoretic interpretation of the symbol a–b is that it is the space of all pairs equivalent to (a, b) : a–b(c, d) ∈ × : (a, b) ∼ (c, d). However, this interpretation plays no role in how we manipulate the integers and we will not refer to it again. A similar set-theoretic interpretation can be given to the construction of the rational numbers later in this chapter, or the real numbers in the next chapter.*

Corollary 1.1.3. *The definition of equality on the integers is reflexive, symmetric, and transitive.*

i:ac:4.1.1. Let $(a, b), (c, d), (e, f) \in \times$. Since

$$a + b = a + b \qquad\qquad i : ac : 2.2.1$$
$$\implies a\text{–}b = a\text{–}b, \qquad\qquad i : 4.1.1$$

we know that i:4.1.1 is reflexive.

Next suppose that $a\text{–}b = c\text{–}d$. Then we have

$$a\text{–}b = c\text{–}d$$
$$\implies a + d = c + b \qquad\qquad i : 4.1.1$$
$$\implies c + b = a + d$$
$$\implies c\text{–}d = a\text{–}b. \qquad\qquad i : 4.1.1$$

Thus, i:4.1.1 is symmetric.

Finally suppose that $a\text{–}b = c\text{–}d$ and $c\text{–}d = e\text{–}f$. Then we have

$$(a\text{–}b = c\text{–}d) \wedge (c\text{–}d = e\text{–}f)$$
$$\Longrightarrow (a + d = c + b) \wedge (c + f = e + d) \qquad\qquad i : 4.1.1$$
$$\Longrightarrow (a + d + f = c + b + f) \wedge (c + f + b = e + d + b) \qquad i : 2.2.6$$
$$\Longrightarrow (a + f + d = c + f + b) \wedge (c + f + b = e + b + d) \qquad i : 2.2.4$$
$$\Longrightarrow a + f + d = e + b + d$$
$$\Longrightarrow a + f = e + b \qquad\qquad i : 2.2.6$$
$$\Longrightarrow a\text{–}b = e\text{–}f. \qquad\qquad i : 4.1.1$$

Thus, i:4.1.1 is transitive. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Definition 1.1.4. *The sum of two integers, $(a\text{–}b) + (c\text{–}d)$, is defined by the formula*

$$(a\text{–}b) + (c\text{–}d)(a + c)\text{–}(b + d).$$

The product of two integers, $(a\text{–}b) \times (c\text{–}d)$, is defined by

$$(a\text{–}b) \times (c\text{–}d)(ac + bd)\text{–}(ad + bc).$$

Lemma 1.1.5 (Addition and multiplication are well-defined)**.** *Let a, b, a', b', c, d be natural numbers. If $(a\text{–}b) = (a'\text{–}b')$, then $(a\text{–}b) + (c\text{–}d) = (a'\text{–}b') + (c\text{–}d)$ and $(a\text{–}b) \times (c\text{–}d) = (a'\text{–}b') \times (c\text{–}d)$, and also $(c\text{–}d) + (a\text{–}b) = (c\text{–}d) + (a'\text{–}b')$ and $(c\text{–}d) \times (a\text{–}b) = (c\text{–}d) \times (a'\text{–}b')$. Thus, addition and multiplication are well-defined operations (equal inputs give equal outputs).*

i:4.1.3. To prove that $(a\text{–}b) + (c\text{–}d) = (a'\text{–}b') + (c\text{–}d)$, we evaluate both sides as $(a + c)\text{–}(b + d)$ and $(a' + c)\text{–}(b' + d)$. Thus, we need to show that $a + c + b' + d = a' + c + b + d$. But since $(a\text{–}b) = (a'\text{–}b')$, we have $a + b' = a' + b$, and so by adding $c + d$ to both sides we obtain the claim.

Now we show that $(a\text{–}b) \times (c\text{–}d) = (a'\text{–}b') \times (c\text{–}d)$. We evaluate both sides to $(ac + bd)\text{–}(ad + bc)$ and $(a'c + b'd)\text{–}(a'd + b'c)$, so we have to show that $ac + bd + a'd + b'c = a'c + b'd + ad + bc$. But the left-hand side factors as $c(a + b') + d(a' + b)$, while the right-hand side factors as $c(a' + b) + d(a + b')$. Since $a + b' = a' + b$, the two sides are equal. The other two identities are proven similarly. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Corollary 1.1.6. *The integers $n\text{–}0$ behave in the same way as the natural numbers n; indeed one can check that $(n\text{–}0) + (m\text{–}0) = (n + m)\text{–}0$ and $(n\text{–}0) \times (m\text{–}0) = nm\text{–}0$. Furthermore, $(n\text{–}0)$ is equal to $(m\text{–}0)$ iff $n = m$. (The mathematical term for this is that there is an* isomorphism *between the natural numbers n and those integers of the form $n\text{–}0$.) Thus, we* may identify *the natural numbers with integers by setting $n \equiv n\text{–}0$; this does not affect our definitions of addition or multiplication or equality since they are consistent with each other. In particular, 0 is equal to $0\text{–}0$ and 1 is equal to $1\text{–}0$. Of course, if we set n equal to $n\text{–}0$, then it will also be equal to any other integer which is equal to $n\text{–}0$.*

i:ac:4.1.2. Let $n, m \in$. First, we show that $(n\text{–}0) + (m\text{–}0) = (n + m)\text{–}0$. This is true since

$$(n\text{–}0) + (m\text{–}0) = (n + m)\text{–}(0 + 0) \qquad\qquad i : 4.1.2$$
$$= (n + m)\text{–}0. \qquad\qquad i : 2.2.1$$

Next we show that $(n\text{--}0) \times (m\text{--}0) = nm\text{--}0$. This is true since

$$
\begin{aligned}
(n\text{--}0) \times (m\text{--}0) &= (nm + 0 \times 0)\text{--}(n \times 0 + 0 \times m) && i : 4.1.2 \\
&= (nm + 0)\text{--}(0 + 0) && i : 2.3.1, i : ac : 2.3.2 \\
&= nm\text{--}0. && i : 2.2.2
\end{aligned}
$$

Finally we show that $(n\text{--}0) = (m\text{--}0) \iff n = m$. This is true since

$$
\begin{aligned}
(n\text{--}0) &= (m\text{--}0) \\
\iff n + 0 &= m + 0 && i : 4.1.1 \\
\iff n &= m. && i : 2.2.1
\end{aligned}
$$

$\square$

Remark 1.1.7. *We can now define incrementation on the integers by defining $xx + 1$ for any integer x; this is of course consistent with our definition of the increment operation for natural numbers. However, this is no longer an important operation for us, as it has been now superceded by the more general notion of addition.*

Definition 1.1.8 (Negation of integers). *If $(a\text{--}b)$ is an integer, we define the negation $-(a\text{--}b)$ to be the integer $(b\text{--}a)$. In particular, if $n = n\text{--}0$ is a positive natural number, we can define its negation $-n = 0\text{--}n$.*

Corollary 1.1.9. *The definition of negation on the integers is well-defined.*

i:ac:4.1.3. Let $a, b, a', b' \in$ and $a\text{--}b = a'\text{--}b'$. Then we have

$$
\begin{aligned}
a\text{--}b &= a'\text{--}b' \\
\implies a + b' &= a' + b && i : 4.1.1 \\
\implies b' + a &= b + a' && i : 2.2.4 \\
\implies b'\text{--}a' &= b\text{--}a && i : 4.1.1 \\
\implies -(a'\text{--}b') &= -(a\text{--}b). && i : 4.1.4
\end{aligned}
$$

Thus, i:4.1.4 is well-defined. $\square$

Lemma 1.1.10 (Trichotomy of integers). *Let x be an integer. Then exactly one of the following three statements is true:*

1. *x is zero.*

2. *x is equal to a positive natural number n.*

3. *x is the negation $-n$ of a positive natural number n.*

i:4.1.5. We first show that at least one of (a), (b), (c) is true. By definition, $x = a\text{--}b$ for some natural numbers a, b. By i:2.2.13, we have three cases: $a > b$, $a = b$, or $a < b$. If $a > b$ then by i:2.2.12(f), $a = b + c$ for some positive natural number c, which means that $a\text{--}b = c\text{--}0 = c$, which is (b). If $a = b$, then $a\text{--}b = a\text{--}a = 0\text{--}0 = 0$, which is (a). If $a < b$,

then $b > a$, so that $b\text{–}a = n$ for some natural number n by the previous reasoning, and thus $a\text{–}b = -n$, which is (c). Now we show that no more than one of (a), (b), (c) can hold at a time. By i:2.2.7, a positive natural number is non-zero, so (a) and (b) cannot simultaneously be true. If (a) and (c) were simultaneously true, then $0 = -n$ for some positive natural n; thus $(0\text{–}0) = (0\text{–}n)$, so that $0 + n = 0 + 0$, so that $n = 0$, a contradiction. If (b) and (c) were simultaneously true, then $n = -m$ for some positive n, m, so that $(n\text{–}0) = (0\text{–}m)$, so that $n + m = 0 + 0$, which contradicts i:2.2.8. Thus, exactly one of (a), (b), (c) is true for any integer x.   □

Remark 1.1.11. *If n is a positive natural number, we call n a positive integer and $-n$ a negative integer. Thus, by i:4.1.5, every integer is positive, zero, or negative, but not more than one of these at a time.*

Remark 1.1.12. *One could well ask why we don't use i:4.1.5 to define the integers; i.e., why didn't we just say an integer is anything which is either a positive natural number, zero, or the negative of a natural number. The reason is that if we did so, the rules for adding and multiplying integers would split into many different cases (e.g., negative times positive equals negative; negative plus positive is either negative, positive, or zero, depending on which term is larger, etc.) and to verify all the properties would end up being much messier.*

Proposition 1.1.13 (Laws of algebra for integers). *Let x, y, z be integers. Then we have*

$$x + y = y + x$$
$$(x + y) + z = x + (y + z)$$
$$x + 0 = 0 + x = x$$
$$x + (-x) = (-x) + x = 0$$
$$xy = yx$$
$$(xy)z = x(yz)$$
$$x1 = 1x = x$$
$$x(y + z) = xy + xz$$
$$(y + z)x = yx + zx.$$

i:4.1.6. There are two ways to prove these identities. One is to use i:4.1.5 and split into a lot of cases depending on whether x, y, z are zero, positive, or negative. This becomes very messy. A shorter way is to write $x = (a\text{–}b), y = (c\text{–}d)$, and $z = (e\text{–}f)$ for some natural numbers a, b, c, d, e, f, and expand these identities in terms of a, b, c, d, e, f and use the algebra of the natural numbers. This allows each identity to be proven in a few lines.

We first show that $x + y = y + x$.

$$
\begin{aligned}
x + y &= (a\text{–}b) + (c\text{–}d) & \\
&= (a + c)\text{–}(b + d) & i : 4.1.2 \\
&= (c + a)\text{–}(d + b) & i : 2.2.4 \\
&= (c\text{–}d) + (a\text{–}b) & i : 4.1.2 \\
&= y + x.
\end{aligned}
$$

Thus, the addition on integers is commutative.

Next we show that $(x + y) + z = x + (y + z)$.

$$
\begin{aligned}
(x + y) + z &= ((a\text{–}b) + (c\text{–}d)) + (e\text{–}f) & \\
&= ((a + c)\text{–}(b + d)) + (e\text{–}f) & i : 4.1.2 \\
&= ((a + c) + e)\text{–}((b + d) + f) & i : 4.1.2 \\
&= (a + (c + e))\text{–}(b + (d + f)) & i : 2.2.5 \\
&= (a\text{–}b) + ((c + e)\text{–}(d + f)) & i : 4.1.2 \\
&= (a\text{–}b) + ((c\text{–}d) + (e\text{–}f)) & i : 4.1.2 \\
&= x + (y + z).
\end{aligned}
$$

Thus, the addition on integers is associative.

Next we show that $x + 0 = 0 + x = x$. Since the addition on integers is commutative, we know that $x + 0 = 0 + x$. So we only need to show that $x + 0 = x$.

$$
\begin{aligned}
x + 0 &= (a\text{–}b) + (0\text{–}0) & i : ac : 4.1.2 \\
&= (a + 0)\text{–}(b + 0) & i : 4.1.2 \\
&= a\text{–}b & i : 2.2.2 \\
&= x.
\end{aligned}
$$

Thus, 0 is the additive identity on integers.

Next we show that $x + (-x) = (-x) + x = 0$. Since the addition on integers is commutative, we know that $x + (-x) = (-x) + x$. So we only need to show that $x + (-x) = 0$.

$$
\begin{aligned}
x + (-x) &= (a\text{–}b) + (b\text{–}a) & i : 4.1.4 \\
&= (a + b)\text{–}(b + a) & i : 4.1.2 \\
&= (a + b)\text{–}(a + b) & i : 2.2.4 \\
&= 0\text{–}0 & i : 4.1.1 \\
&= 0. & i : ac : 4.1.2
\end{aligned}
$$

Thus, the additive inverse of integer x is $-x$.

Next we show that $xy = yx$.

$$
\begin{aligned}
xy &= (a\text{–}b) \times (c\text{–}d) & \\
&= (ac + bd)\text{–}(ad + bc) & i : 4.1.2 \\
&= (ca + db)\text{–}(da + cb) & i : 2.3.2 \\
&= (ca + db)\text{–}(cb + da) & i : 2.2.4 \\
&= (c\text{–}d) \times (a\text{–}b) & i : 4.1.2 \\
&= yx.
\end{aligned}
$$

Thus, the multiplication on integers is commutative.

Next we show that $(xy)z = x(yz)$.

$$
\begin{aligned}
(xy)z & \\
&= ((a\text{–}b) \times (c\text{–}d)) \times (e\text{–}f) & \\
&= ((ac + bd)\text{–}(ad + bc)) \times (e\text{–}f) & i : 4.1.2 \\
&= ((ac + bd)e + (ad + bc)f)\text{–}((ac + bd)f + (ad + bc)e) & i : 4.1.2 \\
&= ((ac)e + (bd)e + (ad)f + (bc)f)\text{–}((ac)f + (bd)f + (ad)e + (bc)e) & i : 2.3.4 \\
&= (a(ce) + b(de) + a(df) + b(cf))\text{–}(a(cf) + b(df) + a(de) + b(ce)) & i : 2.3.5 \\
&= (a(ce) + a(df) + b(cf) + b(de))\text{–}(a(cf) + a(de) + b(ce) + b(df)) & i : 2.2.4 \\
&= (a(ce + df) + b(cf + de))\text{–}(a(cf + de) + b(ce + df)) & i : 2.3.4 \\
&= (a\text{–}b) \times ((ce + df)\text{–}(cf + de)) & i : 4.1.2 \\
&= (a\text{–}b) \times ((c\text{–}d) \times (e\text{–}f)) & i : 4.1.2 \\
&= x(yz). &
\end{aligned}
$$

Thus, the multiplication on integers is associative.

Next we show that $x1 = 1x = x$. Since the multiplication on integers is commutative, we know that $x1 = 1x$. So we only need to show that $x1 = x$.

$$
\begin{aligned}
x1 &= (a\text{–}b) \times (1\text{–}0) & i : ac : 4.1.2 \\
&= (a1 + b0)\text{–}(a0 + b1) & i : 4.1.2 \\
&= (a + 0)\text{–}(0 + b) & i : ac : 2.3.2, i : ac : 2.3.4 \\
&= a\text{–}b & i : 2.2.1, i : 2.2.2 \\
&= x.
\end{aligned}
$$

Thus, 1 is the multiplicative identity on integers.

Next we show that $x(y + z) = xy + xz$.

$$
\begin{aligned}
x(y + z) &= (a\text{–}b) \times ((c\text{–}d) + (e\text{–}f)) & \\
&= (a\text{–}b) \times ((c + e)\text{–}(d + f)) & i : 4.1.2 \\
&= (a(c + e) + b(d + f))\text{–}(a(d + f) + b(c + e)) & i : 4.1.2 \\
&= (ac + ae + bd + bf)\text{–}(ad + af + bc + be) & i : 2.3.4 \\
&= (ac + bd + ae + bf)\text{–}(ad + bc + af + be) & i : 2.2.4 \\
&= ((ac + bd)\text{–}(ad + bc)) + ((ae + bf)\text{–}(af + be)) & i : 4.1.2 \\
&= (a\text{–}b) \times (c\text{–}d) + (a\text{–}b) \times (e\text{–}f) & i : 4.1.2 \\
&= xy + xz.
\end{aligned}
$$

Thus, the multiplication and addition on integers are left distributive.

Finally we show that $(y + z)x = yx + zx$.

$$
\begin{aligned}
(y + z)x &= x(y + z) & \text{(multiplication is commutative)} \\
&= xy + xz & \text{(multiplication and addition are left distributive)} \\
&= yx + zx. & \text{(multiplication is commutative)}
\end{aligned}
$$

Thus, the multiplication and addition on integers are right distributive. □

Remark 1.1.14. *The set of nine identities in i:4.1.6 have a name; they are asserting that the integers form a* commutative ring. *(If one deleted the identity $xy = yx$, then they would only assert that the integers form a* ring*). Note that some of these identities were already proven for the natural numbers, but this does not automatically mean that they also hold for the integers because the integers are a larger set than the natural numbers. On the other hand, this proposition supercedes many of the propositions derived earlier for natural numbers.*

Corollary 1.1.15. *We now define the operation of* subtraction $x - y$ *of two integers by the formula*

$$x - y x + (-y).$$

We do not need to verify the substitution axiom for this operation, since we have defined subtraction in terms of two other operations on integers, namely addition and negation, and we have already verified that those operations are well-defined.
   One can easily check now that if a and b are natural numbers, then

$$a - b = a + -b = (a\text{--}0) + (0\text{--}b) = a\text{--}b,$$

and so a–b is just the same thing as $a - b$. Because of this we can now discard the – notation, and use the familiar operation of subtraction instead. (As remarked before, we could not use subtraction immediately because it would be circular.)

Corollary 1.1.16. *Let x, y be integers. Then $-x = (-1)x$ and $-xy = (-x)y = x(-y)$.*

i:ac:4.1.5. Let $x = (a\text{--}b)$ where $a, b \in$. Then we have

$$
\begin{aligned}
-x &= (b\text{--}a) & & i : 4.1.4 \\
&= (1b\text{--}1a) & & i : ac : 2.3.4 \\
&= (0 + 1b)\text{--}(0 + 1a) & & i : 2.2.1 \\
&= (0a + 1b)\text{--}(0b + 1a) & & i : 2.3.1 \\
&= (0\text{--}1) \times (a\text{--}b) & & i : 4.1.2 \\
&= (-1) \times (a\text{--}b) & & i : 4.1.4 \\
&= (-1)x.
\end{aligned}
$$

So we can use i:4.1.6 to show that

$$
\begin{aligned}
-xy &= (-1)(xy) & & \text{(from the proof above)} \\
&= ((-1)x)y & & i : 4.1.6 \\
&= (-x)y & & \text{(from the proof above)} \\
&= (-1)(yx) & & i : 4.1.6 \\
&= ((-1)y)x & & i : 4.1.6 \\
&= (-y)x & & \text{(from the proof above)} \\
&= x(-y). & & i : 4.1.6
\end{aligned}
$$

$\square$

Corollary 1.1.17. *Let x be an integer. Then $x = -(-x)$.*

i:ac:4.1.6. Let $x = (a\text{–}b)$ where $a, b \in$. Then we have

$$
\begin{aligned}
-(-x) &= -(b\text{–}a) & i &: 4.1.4 \\
&= (a\text{–}b) & i &: 4.1.4 \\
&= x.
\end{aligned}
$$

$\square$

Corollary 1.1.18. *Let x, y be integers. Then $(-x)(-y) = xy$.*

i:ac:4.1.7. We have

$$
\begin{aligned}
(-x)(-y) &= ((-1)x)(-y) & i &: ac : 4.1.5 \\
&= (-1)(x(-y)) & i &: 4.1.6 \\
&= -(x(-y)) & i &: ac : 4.1.5 \\
&= x(-(-y)) & i &: ac : 4.1.5 \\
&= xy. & i &: ac : 4.1.6
\end{aligned}
$$

$\square$

Corollary 1.1.19. *Let x, y be integers. Then we have $x = -x \iff x = 0$ and $x - y = 0 \iff x = y$.*

i:ac:4.1.8. First, we show that $x = -x \iff x = 0$. Let $x = a\text{–}b$ for some $a, b \in$. Then we have

$$
\begin{aligned}
& x = -x \\
\iff & a\text{–}b = b\text{–}a & i &: 4.1.4 \\
\iff & a + a = b + b & i &: 4.1.1 \\
\iff & 2a = 2b & i &: 2.3.1 \\
\iff & a = b & i &: 2.3.7 \\
\iff & a + 0 = 0 + b & i &: 2.2.1, i : 2.2.2 \\
\iff & a\text{–}b = 0\text{–}0 & i &: 4.1.1 \\
\iff & x = 0. & i &: ac : 4.1.2
\end{aligned}
$$

Now we show that $x - y = 0 \iff x = y$. Let $x = a\text{–}b$ and $y = c\text{–}d$ for some $a, b, c, d \in$. Then we have

$$
\begin{aligned}
& x - y = x + (-y) = 0 & i &: ac : 4.1.4 \\
\iff & (a\text{–}b) + (d\text{–}c) = 0\text{–}0 & i &: ac : 4.1.2, i : 4.1.4 \\
\iff & (a + d)\text{–}(b + c) = 0\text{–}0 & i &: 4.1.2 \\
\iff & a + d + 0 = b + c + 0 & i &: 4.1.1 \\
\iff & a + d = b + c & i &: 2.2.2 \\
\iff & a + d = c + b & i &: 2.2.4 \\
\iff & a\text{–}b = c\text{–}d & i &: 4.1.1 \\
\iff & x = y.
\end{aligned}
$$

$\square$

Proposition 1.1.20 (Integers have no zero divisors)**.** *Let a and b be integers such that $ab = 0$. Then either $a = 0$ or $b = 0$ (or both).*

i:4.1.8. Suppose for the sake of contradiction that $(a \neq 0) \wedge (b \neq 0)$. By i:4.1.5 we can split into four cases:

- a is positive and b is positive. Then by i:2.2.7,i:ac:4.1.2, we know that a, b are positive natural numbers. But by i:2.3.3, we must have $(a = 0) \vee (b = 0)$, a contradiction.

- a is negative and b is positive. Then by i:4.1.4, $-a$ is positive and we have

$$
\begin{aligned}
(-a)b &= ((-1)a)b & i : ac : 4.1.5 \\
&= (-1)(ab) & i : 4.1.6 \\
&= (-1)0 \\
&= 0. & i : 4.1.2
\end{aligned}
$$

  Using the same argument as in the first case, we see that $(-a = 0) \vee (b = 0)$. But by i:ac:4.1.6,i:ac:4.1.8, we know that $-a = 0 \implies -(-a) = a = -0 = 0$. Thus, we have $(a = 0) \vee (b = 0)$, a contradiction.

- a is positive and b is negative. We can use the same argument as the second case and switch the role of a, b to derive $(b = 0) \vee (a = 0)$. But again this contradicts $(a \neq 0) \wedge (b \neq 0)$.

- a is negative and b is negative. Then by i:4.1.4, $-a$ and $-b$ are positive. By i:ac:4.1.7, we know that $(-a)(-b) = ab$. This means $(-a = 0) \vee (-b = 0)$. Using the same argument as in the second case, we have $(a = 0) \vee (b = 0)$, a contradiction.

From all cases above, we derived contradiction. Thus, we must have $(a = 0) \vee (b = 0)$. $\square$

Corollary 1.1.21 (Cancellation law for integers)**.** *If a, b, c are integers such that $ac = bc$ and c is non-zero, then $a = b$.*

i:4.1.9. We have

$$
\begin{aligned}
& ac = bc \\
\implies & ac + (-bc) = bc + (-bc) = 0 & i : 4.1.6 \\
\implies & ac + (-b)c = 0 & i : ac : 4.1.5 \\
\implies & (a + (-b))c = 0 & i : 4.1.6 \\
\implies & (a + (-b) = 0) \vee (c = 0) & i : 4.1.8 \\
\implies & a + (-b) = 0 & (c \neq 0) \\
\implies & a = b. & i : ac : 4.1.8
\end{aligned}
$$

$\square$

Definition 1.1.22 (Ordering of the integers)**.** *Let n and m be integers. We say that n is greater than or equal to m, and write $n \geq m$ or $m \leq n$, iff we have $n = m + a$ for some natural number a. We say that n is strictly greater than m, and write $n > m$ or $m < n$, iff $n \geq m$ and $n \neq m$.*

Lemma 1.1.23 (Properties of order)**.** *Let a, b, c be integers.*

1. *$a > b$ iff $a - b$ is a positive natural number.*

2. *(Addition preserves order) If $a > b$, then $a + c > b + c$.*

3. *(Positive multiplication preserves order) If $a > b$ and c is positive, then $ac > bc$.*

4. *(Negation reverses order) If $a > b$, then $-a < -b$.*

5. *(Order is transitive) If $a > b$ and $b > c$, then $a > c$.*

6. *(Order trichotomy) Exactly one of the statements $a > b$, $a < b$, or $a = b$ is true.*

i:4.1.11(a). We have

$$
\begin{aligned}
& a > b \\
\Longleftrightarrow\ & (\exists m \in:\ a = b + m) \wedge (a \neq b) && i : 4.1.10 \\
\Longleftrightarrow\ & \exists m \in:\ a - b = m \neq 0 && i : 4.1.6 \\
\Longleftrightarrow\ & a - b \text{ is a positive natural number.} && i : 2.2.7
\end{aligned}
$$

$\square$

i:4.1.11(b). We have

$$
\begin{aligned}
& a > b \\
\Longrightarrow\ & (\exists m \in:\ a = b + m) \wedge (a \neq b) && i : 4.1.10 \\
\Longrightarrow\ & (\exists m \in:\ a + c = b + m + c) \wedge (a + c \neq b + c) && i : 4.1.3 \\
\Longrightarrow\ & (\exists m \in:\ a + c = b + c + m) \wedge (a + c \neq b + c) && i : 4.1.6 \\
\Longrightarrow\ & a + c > b + c. && i : 4.1.10
\end{aligned}
$$

$\square$

i:4.1.11(c). We have

$$
\begin{aligned}
& a > b \\
\Longrightarrow\ & \exists m \in:\ (a - b = m) \wedge (m > 0) && i : 4.1.11[a] \\
\Longrightarrow\ & \exists m \in:\ ((a - b)c = ac - bc = mc) \wedge (m > 0) && i : 4.1.3, i : 4.1.6 \\
\Longrightarrow\ & \exists m \in:\ (ac - bc = mc) \wedge (mc > 0c = 0) && i : 2.3.1, i : 2.3.6 \\
\Longrightarrow\ & ac > bc. && i : 4.1.11[a]
\end{aligned}
$$

$\square$

i:4.1.11(d). We have

$$\begin{aligned}
&a > b \\
\implies\ &\exists m \in: (a - b = m) \land (m > 0) && i : 4.1.11[a] \\
\implies\ &\exists m \in: (-(-a) - b = m) \land (m > 0) && i : ac : 4.1.6 \\
\implies\ &\exists m \in: ((-b) - (-a) = m) \land (m > 0) && i : ac : 4.1.4, i : 4.1.6 \\
\implies\ &-b > -a. && i : 4.1.11[a]
\end{aligned}$$

□

i:4.1.11(e). We have

$$\begin{aligned}
&(a > b) \land (b > c) \\
\implies\ &\exists m, n \in: (a = b + m) \land (b = c + n) \land (m > 0) \land (n > 0) && i : 4.1.11[a] \\
\implies\ &\exists m, n \in: (a = c + n + m) \land (m > 0) \land (n > 0) && i : 4.1.3 \\
\implies\ &\exists m, n \in: (a = c + n + m) \land (n + m > 0) && i : 2.2.8 \\
\implies\ &a > c. && i : 4.1.11[a]
\end{aligned}$$

□

i:4.1.11(f). By i:4.1.5, $a - b$ can be exactly one of the following three statements:

- $a - b = 0$. Then by i:ac:4.1.8, we have $a = b$.

- $a - b$ is a positive natural number. Then by i:4.1.11(a), we have $a > b$.

- $a - b = -n$ where n is a positive natural number. Then we have

$$\begin{aligned}
&a - b = -n \\
\iff\ &-(a - b) = -(-n) && i : ac : 4.1.3 \\
\iff\ &b - a = n, && i : 4.1.4, i : ac : 4.1.6
\end{aligned}$$

  and by i:4.1.11(a), we have $b > a$. By i:4.1.10, we have $b > a \iff a < b$.

Thus, we conclude that exactly one of the statements $a = b$, $a > b$, or $a < b$ is true. □

Corollary 1.1.24. *Let $m, n \in$. We define the following eight subsets of :*

$$\begin{aligned}
_{\leq n}i \in&: i \leq n; & _{<n}i \in&: i < n; & ^{+}{}_{>0}; \\
_{\geq n}i \in&: i \geq n; & _{>n}i \in&: i > n; & ^{-}{}_{<0}; \\
_{m \leq n}i \in&: m \leq i \leq n; & _{m<n}i \in&: m < i < n.
\end{aligned}$$

In particular, we have $=_{\geq 0}$.

Exercises

4.1.1 Verify that the definition of equality on the integers is both reflexive and symmetric.

i:ex:4.1.1. See i:ac:4.1.1.   □

4.1.2 Show that the definition of negation on the integers is well-defined in the sense that if $(a\text{–}b) = (a'\text{–}b')$, then $-(a\text{–}b) = -(a'\text{–}b')$ (so equal integers have equal negations).

i:ex:4.1.2. See i:ac:4.1.3.   □

4.1.3 Show that $(-1) \times a = -a$ for every integer a.

i:ex:4.1.3. See i:ac:4.1.5.   □

4.1.4 Prove the remaining identities in i:4.1.6.

i:ex:4.1.4. See i:4.1.6.   □

4.1.5 Prove i:4.1.8.

i:ex:4.1.5. See i:4.1.8.   □

4.1.6 Prove i:4.1.9.

i:ex:4.1.6. See i:4.1.9.   □

4.1.7 Prove i:4.1.11.

i:ex:4.1.7. See i:4.1.11.   □

4.1.8 Show that the principle of induction (i:2.5) does not apply directly to the integers. More precisely, give an example of a property $P(n)$ pertaining to an integer n such that $P(0)$ is true, and that $P(n)$ implies $P(n)$ for all integers n, but that $P(n)$ is not true for all integers n. Thus, induction is not as useful a tool for dealing with the integers as it is with the natural numbers. (The situation becomes even worse with the rational and real numbers, which we shall define shortly.)

i:ex:4.1.8. For the sake of contradiction, we claim that $n+1 > 0$ for all $n \in$. We use i:2.5 to prove the claim. For $n = 0$, by i:4.1.10, we know that $(0+1 = 1) \wedge (1 \neq 0) \implies 1 > 0$. So the base case holds. Suppose inductively that $n + 1 > 0$ for some $n \in$. Then for $n+1$, we need to show that $(n+1)+1 > 0$. By the induction hypothesis, we know that $n + 1 > 0$. Then by i:4.1.11(b), we have $(n + 1) + 1 > 0 + 1 = 1$. Since $(n + 1) + 1 > 1$ and $1 > 0$, by i:4.1.11(e), we have $(n + 1) + 1 > 0$. This closes the induction.

Now let $n = -1$. By i:4.1.6, we have $(-1)+1 = 0$. But by i:4.1.10, this means $-1 > 0$, which implies $0 > 1$ by i:4.1.11(b). This contradict to $0 < 1$. Thus, one can not use induction on the integers as it is with the natural numbers.   □