

2.3 The Integers as an Ordered Ring

Sections 2.1 and 2.2 built $\mathbb{Z}$ as a set of classes with well-defined operations $+$, $\cdot$ and $-$, but we do not yet know which laws they obey. This section collects the laws of school algebra into one definition, a **commutative ring**, and checks them for $\mathbb{Z}$ by reducing each to a law of $\mathbb{N}$. Then it orders $\mathbb{Z}$ and derives the rules for inequalities from axioms alone: from here on, an inequality about integers is proved, never read off a picture.

2.3.1 The laws of a ring

Expanding brackets or moving a term across an equation uses a short list of laws: sums and products may be reordered and regrouped, 0 and 1 do nothing, every element has a negative, and products distribute over sums. The list holds in $\mathbb{Z}$, it will hold in $\mathbb{Q}$, and a result proved from the list alone holds wherever the list does. It deserves a name.

A commutative ring is a set where you may add, subtract and multiply by the usual rules; a field is one where you may also divide by anything non-zero.

Definition 2.3.1. Commutative Ring, Field

A **commutative ring** is a set R with two functions, **addition** $+: R \times R \rightarrow R$ and **multiplication** $\cdot: R \times R \rightarrow R$ (written $a \cdot b = ab$), such that clauses (F1)–(F7) and (F9) of the following list hold; clause (F8) is used only for fields.

- (F1) $a + b = b + a$ **for all** $a, b \in R$.
- (F2) $(a + b) + c = a + (b + c)$ **for all** $a, b, c \in R$.
- (F3) **There is** an element $0 \in R$ with $a + 0 = a$ **for every** $a \in R$.
- (F4) **For every** $a \in R$ there is an element $-a \in R$ with $a + (-a) = 0$.
- (F5) $(ab)c = a(bc)$ **for all** $a, b, c \in R$.
- (F6) $ab = ba$ **for all** $a, b \in R$.
- (F7) **There is** an element $1 \in R$ with $a \cdot 1 = a$ **for every** $a \in R$.
- (F8) **For every non-zero** $a \in R$ there is an element $a^{-1} \in R$ with $aa^{-1} = 1$.
- (F9) $a(b + c) = ab + ac$ **for all** $a, b, c \in R$.

A **field** is a commutative ring in which, **in addition**, $1 \neq 0$ and (F8) holds. We write $a - b := a + (-b)$, and in a field $a/b := ab^{-1}$ for $b \neq 0$.

In words: (F1)–(F4) say that addition is commutative and associative, with a neutral element 0 and negatives; (F5)–(F7) say the first three things about multiplication; (F9) links the two and lets us expand brackets. (F8) asks for inverses of **non-zero** elements only, and only in a field. The notations $-a$ and a^{-1} anticipate that these elements are unique, which we prove below. These are the axioms (F1)–(F9) of the linear-algebra companion, Chapter 0, and of the ordered fields of *Analysis on the Real Line*, Chapter 1, in the same numbering, except that there (F7) includes $1 \neq 0$.

Examples.

- $\mathbb{Z}$, with the operations of Definition 2.2.1: the next theorem.
- **The zero ring** $R := \{0\}$, with $0 + 0 := 0$, $0 \cdot 0 := 0$ and $1 := 0$. Every axiom other than (F8) is an equation in R , and every such equation reads $0 = 0$. So R is a commutative

ring, with $1 = 0$, and not a field. This degenerate ring is why several results below assume $1 \neq 0$.

A non-example by minimal change. The set $\mathbb{N}$, with its addition and multiplication from Chapter 1, satisfies (F1)–(F3), (F5)–(F7) and (F9), by Theorem 1.5.3 and Definition 1.5.1 (a). Only (F4) fails, at $a = 1$: $1 + x = x + 1 \neq 0$ for every $x \in \mathbb{N}$, by Theorem 1.5.3 (b) and Corollary 1.5.2. That one missing clause is why $\mathbb{Z}$ had to be built.

Why these clauses. No axiom says that $ab = 0$ forces $a = 0$ or $b = 0$: that is true in $\mathbb{Z}$ but fails in other commutative rings (the warning below), so it must be proved where it holds. The condition $1 \neq 0$ is kept out of the ring axioms, so that the zero ring is a ring, and put into the field axioms, so that $\{0\}$, where (F8) holds vacuously, is not a field.

Warning. A commutative ring may have **zero divisors**: non-zero a, b with $ab = 0$. The integers modulo 6 of *Sets, Relations, and Cardinality*, Section 2.5 (built there from the school integers, with well-defined operations by *Sets, Relations, and Cardinality*, Proposition 2.5.5) form a commutative ring: each of (F1)–(F7) and (F9) passes from the school integers to classes through representatives, a check we do not need and do not carry out here. In this ring $[2] \neq [0]$ and $[3] \neq [0]$, yet $[2][3] = [6] = [0]$. So “ $ab = 0$, hence $a = 0$ or $b = 0$ ” is not a consequence of (F1)–(F9). In an **ordered** ring it is a theorem, proved later in this section from the order axioms.

2.3.2 The integers form a commutative ring

To prove a law for classes, write each side through representatives (Definition 2.2.1) and compare the two pairs of natural numbers: if they are equal, or related by $\sim$ (*Sets, Relations, and Cardinality*, Theorem 2.5.1 (b)), the classes are equal. We call this move **reduce to the level below**: a statement about classes becomes an identity in $\mathbb{N}$, which Chapter 1 has proved.

Theorem 2.3.1. The Integers Form a Commutative Ring

$\mathbb{Z}$, with the addition, multiplication and negation of Definition 2.2.1, is a commutative ring, with zero $[(0, 0)]$ and one $[(1, 0)]$, and in it $1 \neq 0$.

Idea. The operations are functions by Proposition 2.2.2, so only the eight laws remain. On representatives each side of a law is the class of an explicit pair, and we compare the pairs in $\mathbb{N}$. Only associativity of multiplication is laborious; it is written out below the table.

Proof. By Proposition 2.2.2, $+$ and $\cdot$ are functions $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$. Let $x, y, z \in \mathbb{Z}$; by *Sets, Relations, and Cardinality*, Definition 2.5.4, $x = [(a, b)]$, $y = [(c, d)]$, $z = [(e, f)]$ with $a, \dots, f \in \mathbb{N}$. By Definition 2.2.1, each side of each axiom is the class of the pair shown in the table. “Equal” means the same pair of natural numbers, by Theorem 1.5.3 and Definition 1.5.1 (a), (b). “Related” means related by $\sim$ (Definition 2.1.1: $(p, q) \sim (r, s)$ means $p + s = q + r$), so the classes agree by *Sets, Relations, and Cardinality*, Theorem 2.5.1 (b).

Axiom	left side, as a pair	right side, as a pair	why the classes agree
(F1) $x + y = y + x$	$(a + c, b + d)$	$(c + a, d + b)$	equal: $+$ is commutative on $\mathbb{N}$
(F2) $(x + y) + z = x + (y + z)$	$((a + c) + e, (b + d) + f)$	$(a + (c + e), b + (d + f))$	equal: $+$ is associative on $\mathbb{N}$
(F3) $x + [(0, 0)] = x$	$(a + 0, b + 0)$	(a, b)	equal: $m + 0 = m$
(F4) $x + (-x) = [(0, 0)]$	$(a + b, b + a)$	$(0, 0)$	related: $(a + b) + 0 = (b + a) + 0$
(F5) $(xy)z = x(yz)$	see below	see below	equal, after expanding (below)
(F6) $xy = yx$	$(ac + bd, ad + bc)$	$(ca + db, cb + da)$	equal: $\cdot$ and $+$ are commutative
(F7) $x \cdot [(1, 0)] = x$	$(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)$	(a, b)	equal: $n \cdot 1 = n$, $n \cdot 0 = 0$, $n + 0 = 0 + n = n$
(F9) $x(y + z) = xy + xz$	$(a(c + e) + b(d + f), a(d + f) + b(c + e))$	$((ac + bd) + (ae + bf), (ad + bc) + (af + be))$	equal: distribute, then reorder the four terms

For (F5), write $xy = [(g, h)]$ with $g := ac + bd$, $h := ad + bc$. Then $(xy)z = [(ge + hf, gf + he)]$, and in $\mathbb{N}$

$$\begin{aligned} ge + hf &= ace + bde + adf + bcf, \\ gf + he &= acf + bdf + ade + bce. \end{aligned}$$

On the other side, $yz = [(ce + df, cf + de)]$, and $x(yz)$ is the class of the pair whose coordinates are

$$\begin{aligned} a(ce + df) + b(cf + de) &= ace + adf + bcf + bde, \\ a(cf + de) + b(ce + df) &= acf + ade + bce + bdf. \end{aligned}$$

Both first coordinates are sums of ace , adf , bcf , bde , and both second coordinates of acf , ade , bce , bdf , so the pairs are equal (Theorem 1.5.3 (b)–(g)).

Finally, $1 \neq 0$: if $[(1, 0)] = [(0, 0)]$, then $1 = 0$ by Proposition 2.1.2 (b). But $0 < 1$ in $\mathbb{N}$ (Theorem 1.6.1 (d)), and $<$ is irreflexive (Theorem 1.6.1 (a)), so $1 \neq 0$. This proves the theorem. ■

Seven of the eight rows end in “equal”. Only (F4) needs $\sim$: the pair $(a + b, b + a)$ records “ $(a + b) - (b + a)$ ”, which is zero, without performing the subtraction, and that is the whole point of passing to classes.

Remark. The zero and one of this ring are $[(0, 0)] = \iota(0)$ and $[(1, 0)] = \iota(1)$ (Proposition 2.2.3), so after the identification of Section 2.2 they are the natural numbers 0 and 1. With $a - b := a + (-b)$, the formula $[(a, b)] = \iota(a) + (-\iota(b))$ of Proposition 2.2.3 reads $[(a, b)] = a - b$ for $a, b \in \mathbb{N}$: the subtraction the pair recorded is now performed in $\mathbb{Z}$.

What the definition does not list must be derived, and the derivations work in every commutative ring at once.

Proposition 2.3.2. Algebra in a Commutative Ring

Let R be a commutative ring, and let $a, b \in R$.

- (a) The elements 0 and 1 of (F3) and (F7) are unique, the element $-a$ of (F4) is unique, and $-(-a) = a$.
- (b) $a \cdot 0 = 0$.
- (c) $(-a)b = a(-b) = -(ab)$ and $(-a)(-b) = ab$.
- (d) $(a + b)^2 = a^2 + 2ab + b^2$, where $x^2 := xx$ and $2 := 1 + 1$.

Idea. To show that something equals 0, or $-(ab)$, show that it satisfies the **defining equation** of that element and let uniqueness, part (a), finish.

Proof.

- (a) Suppose 0 and $0'$ both satisfy (F3). Then $0' = 0' + 0 = 0 + 0' = 0$, by (F3) for 0, (F1), and (F3) for $0'$. Likewise, if 1 and $1'$ both satisfy (F7), then $1' = 1' \cdot 1 = 1 \cdot 1' = 1$, by (F7) and (F6). Next, suppose $a + b = 0$ and $a + c = 0$. Then

$$\begin{aligned} b &= b + 0 = b + (a + c) = (b + a) + c \\ &= (a + b) + c = 0 + c = c + 0 = c, \end{aligned}$$

by (F3), the second hypothesis, (F2), (F1), the first hypothesis, (F1) and (F3). So $-a$ is the **only** element whose sum with a is 0. Finally, $(-a) + a = a + (-a) = 0$ by (F1) and (F4), so a satisfies the defining equation of $-(-a)$, and uniqueness gives $-(-a) = a$.

- (b) Let $z := a \cdot 0$. By (F3) and (F9), $z = a(0 + 0) = a \cdot 0 + a \cdot 0 = z + z$. Adding $-z$ to both sides,

$$0 = z + (-z) = (z + z) + (-z) = z + (z + (-z)) = z + 0 = z,$$

by (F4), the equation $z = z + z$, (F2), (F4) and (F3). So $a \cdot 0 = 0$.

- (c) By (F6) and (F9), $ab + (-a)b = b(a + (-a)) = b \cdot 0 = 0$, the last step by (b). So $(-a)b$ satisfies the defining equation of $-(ab)$, and (a) gives $(-a)b = -(ab)$. By (F6) also $a(-b) = (-b)a = -(ba) = -(ab)$. Hence $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$, using the first identity, the second, and (a).
- (d) By (F9) and (F6), $(a + b)(a + b) = (a + b)a + (a + b)b = a^2 + ba + ab + b^2$, and $ba + ab = ab \cdot 1 + ab \cdot 1 = ab(1 + 1) = 2ab$ by (F6), (F7) and (F9). Regrouping by (F1) and (F2) gives $(a + b)^2 = a^2 + 2ab + b^2$. ■

The argument of (a) with multiplication shows that in a **field** a non-zero a has only one inverse: if $ab = 1$ and $ac = 1$, then $b = b \cdot 1 = b(ac) = (ba)c = (ab)c = 1 \cdot c = c$, by (F7), (F5) and (F6). So a^{-1} , and with it a/b , names a single element. And (b) explains the zero ring: if $1 = 0$ in a commutative ring, then $a = a \cdot 1 = a \cdot 0 = 0$ for every a , so the ring is $\{0\}$.

2.3.3 Ordered rings

The integers carry an order tied to the operations: adding the same number to both sides keeps an inequality, and a product of positives is positive. We want every rule for inequalities to follow from a short list of axioms, as for equations. The list is the order axioms (O1)–(O4) of *Analysis on the Real Line*, Chapter 1, with “field” relaxed to “commutative ring”.

An ordered ring is a ring with a strict order that adding respects, in which a product of positives is positive.

Definition 2.3.2. Ordered Ring, Ordered Field

An **ordered commutative ring** is a commutative ring R (Definition 2.3.1) together with a relation $<$ on R such that, **for all** $a, b, c \in R$:

- (O1) (trichotomy) **exactly one** of $a < b$, $a = b$, $b < a$ holds;
- (O2) (transitivity) if $a < b$ and $b < c$, then $a < c$;
- (O3) (addition) if $a < b$, then $a + c < b + c$;
- (O4) (multiplication) if $0 < a$ and $0 < b$, then $0 < ab$.

An **ordered field** is a field that is an ordered commutative ring. We write $b > a$ for $a < b$, and $a \leq b$ for “ $a < b$ or $a = b$ ” (likewise $b \geq a$). An element a is **positive** if $a > 0$, **negative** if $a < 0$, and **non-negative** if $a \geq 0$.

In words: any two elements compare in exactly one way, so $a < a$ never holds; comparisons chain; we may add the same element to both sides; and (O4), the only clause about multiplication, speaks only of **positive** elements.

The degenerate case: the zero ring $\{0\}$ with the **empty** relation is an ordered commutative ring. Only the middle option of (O1) holds, and (O2)–(O4) are vacuous. There $1 = 0$, so any rule concluding $1 > 0$ must assume $1 \neq 0$.

Checking (O1)–(O4) directly means handling pairs of elements. It is easier to say which elements are positive and let $a < b$ mean that $b - a$ is positive. The next proposition says which “positive sets” give an order, and that every order arises so. We call the move **order from a positive set**.

Proposition 2.3.3. Order from a Positive Set

Let R be a commutative ring and $P \subseteq R$ a subset such that:

- (P1) if $a, b \in P$, then $a + b \in P$ and $ab \in P$;
- (P2) **for every** $a \in R$, **exactly one** of $a \in P$, $a = 0$, $-a \in P$ holds.

Define $a < b$ to mean $b - a \in P$. Then $(R, <)$ is an ordered commutative ring (Definition 2.3.2), and $P = \{a \in R : a > 0\}$.

Conversely, if $(R, <)$ is an ordered commutative ring, then $P := \{a \in R : a > 0\}$ satisfies (P1) and (P2), and for all $a, b \in R$, $a < b$ holds if and only if $b - a \in P$.

The labels (P1), (P2) are local; they are not the clauses of a partition (*Sets, Relations, and Cardinality*, Section 2.5) or Peano’s axioms (Chapter 1).

Idea. Each order axiom is a statement about one difference. (O1) is (P2) applied to $b - a$, since $-(b - a) = a - b$. (O2) is closure under sums, since $(c - b) + (b - a) = c - a$. (O3) holds since $(b + c) - (a + c) = b - a$. (O4) is closure under products. The algebra is uniqueness of negatives.

Proof. We first record three identities in R , for $a, b, c \in R$:

$$\begin{aligned} -(b - a) &= a - b, & (c - b) + (b - a) &= c - a, \\ (b + c) - (a + c) &= b - a. \end{aligned}$$

For the first, $(b - a) + (a - b) = (b + (-b)) + ((-a) + a) = 0$ by (F1), (F2), (F4), and [Proposition 2.3.2](#) (a) gives the identity. The second is regrouping by (F1)–(F4). For the third, $(a + c) + ((-a) + (-c)) = 0$ likewise, so $-(a + c) = (-a) + (-c)$ by [Proposition 2.3.2](#) (a), and the c 's cancel. Also $-0 = 0$ (as $0 + 0 = 0$), so $a - 0 = a$; and $b - a = 0$ if and only if $b = a$: one direction is (F4), and $b - a = 0$ gives $b = (b - a) + a = 0 + a = a$.

Now let P satisfy (P1), (P2), and let $a < b$ mean $b - a \in P$.

(O1) Apply (P2) to $b - a$: exactly one of $b - a \in P$, $b - a = 0$, $-(b - a) \in P$ holds. By the facts above, these say $a < b$, $a = b$ and $a - b \in P$, that is, $b < a$. So exactly one of the three holds.

(O2) If $b - a \in P$ and $c - b \in P$, then $c - a = (c - b) + (b - a) \in P$ by (P1).

(O3) If $b - a \in P$, then $(b + c) - (a + c) = b - a \in P$.

(O4) Since $a - 0 = a$, we have $0 < a$ if and only if $a \in P$. So $0 < a$ and $0 < b$ give $a, b \in P$, hence $ab \in P$ by (P1), that is, $0 < ab$. The same equivalence says $P = \{a \in R : a > 0\}$.

Conversely, let $(R, <)$ be an ordered commutative ring and $P := \{a : a > 0\}$. If $a < b$, then $a + (-a) < b + (-a)$ by (O3), that is, $0 < b - a$. If $0 < b - a$, then $0 + a < (b - a) + a = b$ by (O3), that is, $a < b$. This is the last claim. For (P1), let $a, b > 0$. Then $0 + b < a + b$ by (O3), so $0 < b < a + b$ and $a + b > 0$ by (O2); and $ab > 0$ by (O4). For (P2), let $a \in R$. By (O1) exactly one of $0 < a$, $a = 0$, $a < 0$ holds, and by the last claim $a < 0$ holds exactly when $0 - a = -a$ is in P . This proves the proposition. ■

So an order on a commutative ring is the same thing as a positive set. For $\mathbb{Z}$, the natural one is the classes $[(a, b)]$ with $b < a$. Section 2.1 warned that “ $b < a$ ” is a statement about **one** representative; we now check that it is a statement about the class.

2.3.4 The order of the integers

Definition 2.3.3. Order on the Integers

Let $S := \{(a, b) \in \mathbb{N} \times \mathbb{N} : b < a\}$, and

$$P_{\mathbb{Z}} := \{[(a, b)] : (a, b) \in S\} \subseteq \mathbb{Z}.$$

For $x, y \in \mathbb{Z}$, define $x < y$ to mean $y - x \in P_{\mathbb{Z}}$.

Well-definedness. By Theorem 2.2.1 (c), with $X = \mathbb{N} \times \mathbb{N}$, it suffices that $(a, b) \sim (a', b')$ and $b < a$ imply $b' < a'$. Write $a = b + k$ with $k \neq 0$ (Proposition 1.6.3 (a)). Then $a + b' = b + a'$ reads $(b' + k) + b = a' + b$ (Theorem 1.5.3 (b), (c)), and canceling b (Proposition 1.6.3 (b)) gives $a' = b' + k$, so $b' < a'$. Hence, for **every** pair,

$$[(a, b)] \in P_{\mathbb{Z}} \iff b < a.$$

So “positive” may be tested on any representative, as Section 2.1’s warning required.

Examples. $[(5, 2)] \in P_{\mathbb{Z}}$, since $2 < 5$; this is the integer 3. $[(2, 5)] \notin P_{\mathbb{Z}}$ and $[(4, 4)] \notin P_{\mathbb{Z}}$, since neither $5 < 2$ nor $4 < 4$. To compare $x = [(3, 5)]$ and $y = [(4, 1)]$: $y - x = [(4, 1)] + [(5, 3)] = [(9, 4)]$, and $4 < 9$, so $x < y$, as “ $-2 < 3$ ” leads us to expect. The degenerate pair $(0, 0)$ is not in S , so $0 \notin P_{\mathbb{Z}}$: zero is not positive.

Quick check. Is $[(7, 10)] < [(2, 4)]$?

Solution. Compute $[(2, 4)] - [(7, 10)] = [(2, 4)] + [(10, 7)] = [(12, 11)]$ by Definition 2.2.1. Since $11 < 12$, the difference lies in $P_{\mathbb{Z}}$, so yes: $[(7, 10)] < [(2, 4)]$, which is $-3 < -2$.

Recall from Section 2.2 that $\mathbb{Z}_{>0} := \{n \in \mathbb{N} : n \neq 0\}$, a set of natural numbers, inside $\mathbb{Z}$ through the identification $n = \iota(n)$. The next theorem shows that it is exactly the set of positive integers.

Theorem 2.3.4. The Integers Form an Ordered Ring

$\mathbb{Z}$, with the operations of Definition 2.2.1 and the relation $<$ of Definition 2.3.3, is an ordered commutative ring, and its positive elements are exactly $P_{\mathbb{Z}}$. Moreover:

- (a) for $m, n \in \mathbb{N}$, $\iota(m) < \iota(n)$ if and only if $m < n$;
- (b) $\mathbb{N} = \{x \in \mathbb{Z} : x \geq 0\}$, and $\mathbb{Z}_{>0} = \{x \in \mathbb{Z} : x > 0\}$;
- (c) (**discreteness**) there is no $k \in \mathbb{Z}$ with $0 < k < 1$; hence, for $m, n \in \mathbb{Z}$ with $m < n$, $m + 1 \leq n$.

Idea. By Proposition 2.3.3 it is enough to check (P1) and (P2) for $P_{\mathbb{Z}}$, each a fact about $\mathbb{N}$. For products, write $a = b + k$, $c = d + l$: the product’s two coordinates differ by exactly $kl \neq 0$. (P2) is trichotomy in $\mathbb{N}$. Parts (a)–(c) follow from the positive classes being the $[(k, 0)]$ with $k \neq 0$.

Proof. By Theorem 2.3.1, $\mathbb{Z}$ is a commutative ring. We check (P1) and (P2) of Proposition 2.3.3 for $P = P_{\mathbb{Z}}$, using the criterion $[(a, b)] \in P_{\mathbb{Z}} \iff b < a$.

(P1), sums. Let $x = [(a, b)]$ and $y = [(c, d)]$ with $b < a$ and $d < c$. Then $x + y = [(a + c, b + d)]$, and

$$b + d < a + d < a + c$$

by Proposition 1.6.3 (c) twice (with commutativity), so $b + d < a + c$ by transitivity (Theo-

rem 1.6.1 (a)). Hence $x + y \in P_{\mathbb{Z}}$.

(P1), products. With the same x, y , write $a = b + k$ and $c = d + l$ with $k, l \neq 0$ (Proposition 1.6.3 (a)). Then $xy = [(ac + bd, ad + bc)]$, and expanding by Theorem 1.5.3,

$$\begin{aligned} ac + bd &= (b + k)(d + l) + bd = bd + bl + kd + kl + bd, \\ ad + bc &= (b + k)d + b(d + l) = bd + kd + bd + bl. \end{aligned}$$

So $ac + bd = (ad + bc) + kl$. Since $k \neq 0$ and $l \neq 0$, $kl \neq 0$ by Proposition 1.6.3 (d), and therefore $ad + bc < ac + bd$ by Proposition 1.6.3 (a). Hence $xy \in P_{\mathbb{Z}}$.

(P2). Let $x = [(a, b)]$. Then $x \in P_{\mathbb{Z}}$ if and only if $b < a$. Next, $x = [(0, 0)]$ if and only if $(a, b) \sim (0, 0)$ (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)), that is, $a + 0 = b + 0$, that is, $a = b$. Finally, $-x = [(b, a)] \in P_{\mathbb{Z}}$ if and only if $a < b$. By trichotomy in $\mathbb{N}$ (Theorem 1.6.1 (a)), exactly one of $b < a$, $a = b$, $a < b$ holds. So exactly one of $x \in P_{\mathbb{Z}}$, $x = 0$, $-x \in P_{\mathbb{Z}}$ holds.

By Proposition 2.3.3, $(\mathbb{Z}, <)$ is an ordered commutative ring with positive set $P_{\mathbb{Z}}$.

- (a) By Definition 2.2.1, $\iota(n) - \iota(m) = [(n, 0)] + [(0, m)] = [(n, m)]$, which lies in $P_{\mathbb{Z}}$ if and only if $m < n$.
- (b) If $x = [(a, b)] > 0$, then $a = b + k$ with $k \neq 0$ (Proposition 1.6.3 (a)), and $x = [(k, 0)] = \iota(k)$ by Proposition 2.1.2 (a). Conversely, for $k \neq 0$, $\iota(k) = [(k, 0)]$ is positive since $0 < k$ (Theorem 1.6.1 (d)). So the positive integers are the $\iota(k)$ with $k \in \mathbb{Z}_{>0}$; adding $0 = \iota(0)$ gives the first equation.
- (c) If $0 < k$, then $k = \iota(m)$ with $m \neq 0$ by (b), so $1 \leq m$ (Theorem 1.6.1 (d)) and $1 \leq k$ by (a); then $k < 1$ would give $1 < 1$ by (O2), or contradict (O1) directly. Now let $m < n$. Then $n - m > 0$ (Proposition 2.3.3), so $n - m \geq 1$, and adding m by (O3) gives $n \geq 1 + m$. This proves the theorem. ■

With the identification of Section 2.2, (a) says that the order of $\mathbb{Z}$ **extends** the order of $\mathbb{N}$.

Two non-examples by minimal change, each breaking exactly one order axiom:

- Replace $<$ by $\leq$. (O2)–(O4) still hold, by the axioms for $<$ and the cases of equality (for (O4), $ab = 0$ when a factor is 0, by Proposition 2.3.2 (b)). But (O1) fails at $a = b = 0$: both “ $0 \leq 0$ ” and “ $0 = 0$ ” hold. The axioms describe a **strict** order.
- Reverse the order: $a \prec b$ means $b < a$. (O1)–(O3) hold, by the same axioms for $<$. But (O4) fails: $0 \prec -1$, since $0 - (-1) = 1 = [(1, 0)] \in P_{\mathbb{Z}}$ (Proposition 2.3.2 (a)), and $(-1)(-1) = 1$ (Proposition 2.3.2 (c)), yet $0 \prec 1$ is false, since $0 - 1 = [(0, 1)] \notin P_{\mathbb{Z}}$. So (O4) fixes which way round the order goes.

2.3.5 Rules for inequalities

The rules below hold in every ordered commutative ring: in $\mathbb{Z}$ now, and in $\mathbb{Q}$ once Section 2.5 orders it. One of them needs multiples first.

Multiples. Let R be a commutative ring and $a \in R$. By Sets, Relations, and Cardinality, Theorem 2.3.1, read on $\mathbb{N} = \omega$ through Corollary 1.7.3 (b), with $X = R$, starting value 0 and step $(n, y) \mapsto y + a$, there is exactly one function $\mathbb{N} \rightarrow R$, written $n \mapsto n \cdot a$, with

$$0 \cdot a = 0, \quad (n + 1) \cdot a = n \cdot a + a \quad \text{for every } n \in \mathbb{N}.$$

So $1 \cdot a = a$ and $2 \cdot a = a + a$. From here to the end of the section, a dot with a natural number on its left means this multiple, and the product of two elements of R is written by juxtaposition, ab . When $R = \mathbb{Z}$, the two readings agree, by Logic and Proof, Axiom 4.2.1 (through Corollary 1.7.3 (b)): $0 \cdot a = 0 = 0a$ by Proposition 2.3.2 (b) and (F6), and $n \cdot a = na$ gives $(n+1) \cdot a = na + a = (n+1)a$, since $(n+1)a = a(n+1) = an + a = na + a$ by (F6), then (F9) with (F7), then (F6) (the sum $n+1$ is the same in $\mathbb{N}$ and $\mathbb{Z}$ by Proposition 2.2.3 (a)).

Proposition 2.3.5. Rules for Inequalities in an Ordered Ring

Let R be an ordered commutative ring, and let $a, b, c, d \in R$.

- (a) $a < b$ if and only if $b - a > 0$, if and only if $-b < -a$.
- (b) If $a \leq b$ and $c \leq d$, then $a + c \leq b + d$, and the conclusion is strict if one of the hypotheses is strict.
- (c) If $a < b$ and $c > 0$, then $ac < bc$.
- (d) If $a < b$ and $c < 0$, then $ac > bc$.
- (e) If $a \neq 0$, then $a^2 > 0$. If $1 \neq 0$, then $1 > 0$.
- (f) If $ab = 0$, then $a = 0$ or $b = 0$.
- (g) If $a \geq 0$ and $b \geq 0$, then $a < b$ if and only if $a^2 < b^2$.
- (h) For every $m, k \in \mathbb{N}$, $(m+k) \cdot a = m \cdot a + k \cdot a$. If $1 \neq 0$, then $n \cdot 1 > 0$ for every $n \in \mathbb{N}$ with $n \geq 1$, and $m \cdot 1 < n \cdot 1$ whenever $m, n \in \mathbb{N}$ and $m < n$.
- (i) $\leq$ is a total order on R (Sets, Relations, and Cardinality, Definition 2.6.1), and its strict part is $<$.

Idea. The method is **turn the comparison into one positive element**: by Proposition 2.3.3, $a < b$ says that $b - a$ is positive, and positive elements are closed under $+$ and $\cdot$. For instance (c) says: if $b - a$ and c are positive, so is $bc - ac = (b - a)c$. We prove (i) first, since (b) and (g) use it.

Proof.

- (i) Reflexivity is $a = a$. Antisymmetry: $a \leq b$, $b \leq a$ and $a \neq b$ give $a < b < a$, so $a < a$ by (O2), against (O1). Transitivity: if $a \leq b \leq c$, either an equality holds and we substitute, or $a < c$ by (O2); and $a < c$ whenever one step is strict. Totality is (O1). Strict part: $a < b$ implies $a \neq b$ by (O1), and $a \leq b$, $a \neq b$ give $a < b$.
- (a) The first equivalence is the last claim of Proposition 2.3.3. For the second, $(-a) - (-b) = (-a) + b = b - a$ by Proposition 2.3.2 (a) and (F1), so $-b < -a$ also says $b - a > 0$.
- (b) By (O3) (or equality) and (F1), $a + c \leq b + c \leq b + d$; conclude by (i).
- (c) By (a), $b - a > 0$. By (O4), $(b - a)c > 0$. By (F9), (F6) and Proposition 2.3.2 (c), $(b - a)c = bc + (-a)c = bc - ac$. So $bc - ac > 0$, and $ac < bc$ by (a).
- (d) By (a), $c < 0$ gives $0 - c = -c > 0$. By (c) applied with $-c$, $a(-c) < b(-c)$, that is, $-(ac) < -(bc)$ by Proposition 2.3.2 (c), and then $bc < ac$ by (a) together with $-(-x) = x$.
- (e) If $a > 0$, then $a^2 = aa > 0$ by (O4). If $a < 0$, then $-a > 0$ as in (d), and $a^2 = (-a)(-a) > 0$ by Proposition 2.3.2 (c) and (O4). By (O1) one of the two cases occurs when $a \neq 0$. If $1 \neq 0$, then $1 = 1^2 > 0$.

- (f) Contrapositive: let $a, b \neq 0$. By (O1) and (a), some $a' \in \{a, -a\}$ and $b' \in \{b, -b\}$ are positive, so $a'b' > 0$ by (O4). By Proposition 2.3.2 (c), $a'b'$ is ab or $-(ab)$; if $ab = 0$, both are 0, against (O1). So $ab \neq 0$.
- (g) Let $a, b \geq 0$. $(\Rightarrow)$ If $a < b$, then $b > 0$ by (i), and (c) gives $ab < b^2$. Also $a^2 \leq ab$: by (c) if $a > 0$, and by Proposition 2.3.2 (b) if $a = 0$. So $a^2 < b^2$ by (i). $(\Leftarrow)$ If $a^2 < b^2$ but not $a < b$, then $b = a$ or $b < a$ by (O1), giving $a^2 = b^2$ or, by $(\Rightarrow)$, $b^2 < a^2$; both contradict (O1).
- (h) Fix $m \in \mathbb{N}$. We prove the sum law by Logic and Proof, Axiom 4.2.1 on k (through Corollary 1.7.3 (b)), for $P(k)$: “ $(m+k) \cdot a = m \cdot a + k \cdot a$ ”. The base case is $(m+0) \cdot a = m \cdot a + 0 \cdot a$, by Definition 1.5.1 (a), (F3) and $0 \cdot a = 0$. For the step, $P(k)$ gives $(m + (k+1)) \cdot a = (m+k) \cdot a + a = (m \cdot a + k \cdot a) + a = m \cdot a + (k+1) \cdot a$, by associativity in $\mathbb{N}$ (Theorem 1.5.3 (c)) with the definition of multiples, $P(k)$, and (F2) with the definition of multiples again.

Now let $1 \neq 0$. By Logic and Proof, Axiom 4.2.1 on n , for $Q(n)$: “ $(n+1) \cdot 1 > 0$ ”: the base is $1 \cdot 1 = 0 + 1 = 1 > 0$ by (e), and the step is $(n+2) \cdot 1 = (n+1) \cdot 1 + 1 > 0$ by (b) and (e). Every $n \geq 1$ in $\mathbb{N}$ is $j+1$ for some j (Proposition 1.6.3 (a)), so $n \cdot 1 > 0$. Finally, if $m < n$, then $n = m+k$ with $k \neq 0$ (Proposition 1.6.3 (a)), so $k \geq 1$ (Theorem 1.6.1 (d)), and by the sum law and (b),

$$n \cdot 1 = m \cdot 1 + k \cdot 1 > m \cdot 1 + 0 = m \cdot 1.$$

This proves the proposition. ■

The school rules for inequalities between integers are now theorems about $\mathbb{Z}$. The hypothesis $1 \neq 0$ in (e) and (h) cannot be dropped: in the zero ring with the empty order, neither $1 > 0$ nor $1 \cdot 1 > 0$ holds.

Warning. (O4) and (c) are about multiplying by something **positive**. The tempting rule “if $a < b$ and $c < d$, then $ac < bd$ ” is false in $\mathbb{Z}$: $-3 < -1$ and $-3 < -1$, yet $(-3)(-3) = 9$ and $(-1)(-1) = 1$, and $9 > 1$. What is true is the version with $0 \leq a$ and $0 \leq c$: then $b > 0$ by (i), so $ac \leq bc < bd$, the first step by (c) if $c > 0$ and by Proposition 2.3.2 (b) if $c = 0$, the second by (c) and (F6); conclude by (i).

Quick check. Is $\mathbb{Z}$ a field?

Solution. No: $1+1$ is non-zero (it is $> 1 > 0$) and has no inverse. Suppose $(1+1)x = 1$. Since $(1+1)x = x(1+1) = x+x$ by (F6), (F9) and (F7), this says $x+x = 1$. If $x \leq 0$, then $x+x \leq 0 < 1$ by Proposition 2.3.5 (b), (e). If $x > 0$, then $x \geq 1$ by discreteness (Theorem 2.3.4 (c)), so $x+x \geq 1+1 > 1$ by Proposition 2.3.5 (b), (e). Both contradict $x+x = 1$ by (O1).

2.3.6 Least elements, and a ring that cannot be ordered

The natural numbers are well ordered (Theorem 1.6.2); the integers are not, since $x - 1 < x$ for every x . But a set of integers bounded below can be shifted into $\mathbb{N}$.

Proposition 2.3.6. Least and Greatest Elements of Sets of Integers

Let $S \subseteq \mathbb{Z}$ be **non-empty**. If S has a lower bound $b \in \mathbb{Z}$ (that is, $b \leq s$ for every $s \in S$), then S has a least element. If S has an upper bound $c \in \mathbb{Z}$, then S has a greatest element.

Proof. Let b be a lower bound and $T := \{s - b : s \in S\}$, a non-empty set. For $s \in S$, $s \geq b$ gives $s - b \geq 0$ by (O3), so $T \subseteq \{x \in \mathbb{Z} : x \geq 0\} = \mathbb{N}$ by Theorem 2.3.4 (b). By Theorem 1.6.2, T has an element m with $m \leq t$ for every $t \in T$, in the order of $\mathbb{N}$ and so in that of $\mathbb{Z}$ (Theorem 2.3.4 (a)). Then $m = s_0 - b$ for some $s_0 \in S$, so $m + b = s_0 \in S$; and for $s \in S$, $s - b \geq m$ gives $s \geq m + b$ by (O3). So $m + b$ is least in S .

If c is an upper bound, then $-S := \{-s : s \in S\}$ has the lower bound $-c$ (Proposition 2.3.5 (a)), so by the first part it has a least element, which is $-s_1$ for some $s_1 \in S$, by the definition of $-S$. For $s \in S$, $-s_1 \leq -s$ gives $s \leq s_1$, by Proposition 2.3.5 (a), or by $-(-s) = s$ (Proposition 2.3.2 (a)) when $-s_1 = -s$. So s_1 is greatest in S . This proves the proposition. ■

Both hypotheses are needed: $\mathbb{Z}$ has no least element, and neither has $\emptyset$, which every integer bounds. The rules of Proposition 2.3.5 also show that some rings carry no order at all.

Example. A field with two elements that cannot be ordered

Let $R := \{0, 1\}$, two distinct elements, with addition and multiplication given by the tables

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Check that R satisfies (F1)–(F9), so that it is a field, and show that no relation $<$ on R makes it an ordered commutative ring.

Solution. The axioms. (F1), (F6): both tables are symmetric. (F3), (F7): the row of 0 in the first table and of 1 in the second repeat the headings. (F4): $-0 = 0$ and $-1 = 1$, since $1 + 1 = 0$. (F8): 1 has inverse 1, since the second table gives the product of 1 and 1 as 1. And $1 \neq 0$.

The three laws with three variables can be checked over the eight triples (a, b, c) , or by cases. From the tables, $0x = 0$ and $1x = x$, and $x + y = 1$ exactly when exactly one of x, y is 1. (F2): both sides are 1 exactly when an odd number of a, b, c (one or three) are 1. (F5): both sides are 1 exactly when $a = b = c = 1$. (F9): if $a = 0$, both sides are 0; if $a = 1$, both sides are $b + c$. So R is a field.

No order. If $<$ made R an ordered commutative ring, then, as $1 \neq 0$, [Proposition 2.3.5](#) (h) would give $2 \cdot 1 > 0$. But $2 \cdot 1 = 1 \cdot 1 + 1 = (0 + 1) + 1 = 0$ by the definition of multiples, and $0 > 0$ is forbidden by (O1).

The argument uses only $1 \neq 0$ and $n \cdot 1 = 0$ for some $n \geq 1$. So **no commutative ring with $1 \neq 0$ in which $n \cdot 1 = 0$ for some $n \in \mathbb{N}$, $n \geq 1$, can be ordered.** The integers modulo $n \geq 2$ of *Sets, Relations, and Cardinality*, Section 2.5 are such rings (their ring laws taken for granted, as in the warning after [Definition 2.3.1](#)), since $n \cdot [1] = [n] = [0]$; a later chapter of this volume rebuilds them on the constructed $\mathbb{Z}$.

2.3.7 Exercises

2.3.7.1 A. Check your understanding

Exercise. A1

Let R be an ordered commutative ring.

- Here is a proof that if $a < 0 < b$, then $ab < a^2 + b^2$. Name the axiom, rule or result that justifies each of the five steps. (1) $ab < 0b$. (2) $0b = 0$. (3) $a^2 > 0$ and $b^2 > 0$. (4) $a^2 + b^2 > 0 + 0 = 0$. (5) $ab < a^2 + b^2$.
- True or false: “ R has no zero divisors.” Give a reason.
- True or false: “ $1 > 0$ in every ordered commutative ring.” Give a reason.
- Name the move by which [Theorem 2.3.1](#) was proved, and say which row of its table needed the relation $\sim$ rather than equality of pairs.

Solution.

- (a) [Proposition 2.3.5](#) (c), with $a < 0$ and $b > 0$. (2) [Proposition 2.3.2](#) (b) and (F6). (3) [Proposition 2.3.5](#) (e), as $a, b \neq 0$ by (O1). (4) [Proposition 2.3.5](#) (b), strict, and (F3). (5) (O2).
- True, by [Proposition 2.3.5](#) (f); a general commutative ring may have zero divisors (the warning after [Definition 2.3.1](#)).
- False: in the zero ring with the empty relation, $1 = 0$. It is true when $1 \neq 0$ ([Proposition 2.3.5](#) (e)).
- Reduce to the level below:** on representatives, each axiom becomes an identity in $\mathbb{N}$. Only (F4) needed $\sim$: $(a + b, b + a)$ is related to $(0, 0)$ but is not that pair.

2.3.7.2 B. Practice

Exercise. B1: Three rows in detail

Let $x = [(a, b)]$, $y = [(c, d)]$, $z = [(e, f)]$ be integers. Verify in detail, naming the law of $\mathbb{N}$ used at each step, the rows (F9), (F4) and (F6) of the table in the proof of [Theorem 2.3.1](#).

Solution. All operations are those of Definition 2.2.1, and “Law” refers to Theorem 1.5.3.

(F9). Since $y + z = [(c + e, d + f)]$, $x(y + z) = [(a(c + e) + b(d + f), a(d + f) + b(c + e))]$, whose coordinates are $ac + ae + bd + bf$ and $ad + af + bc + be$ by Law (d). And $xy + xz = [((ac + bd) + (ae + bf), (ad + bc) + (af + be))]$, whose coordinates are the same sums by Laws (b), (c). So both sides are the class of one pair.

(F4). $x + (-x) = [(a + b, b + a)]$, and $(a + b, b + a) \sim (0, 0)$ means $(a + b) + 0 = (b + a) + 0$ (Definition 2.1.1), true by Definition 1.5.1 (a) and Law (b). So $x + (-x) = [(0, 0)]$ by Sets, Relations, and Cardinality, Theorem 2.5.1 (b).

(F6). $yx = [(ca + db, cb + da)]$. By Law (f), $ca = ac$, $db = bd$, $cb = bc$, $da = ad$, and by Law (b), $bc + ad = ad + bc$; so the pair is $(ac + bd, ad + bc)$, the pair of xy .

Exercise. B2: The wrong positive set

Let $P' := \{[(a, b)] : a < b\} \subseteq \mathbb{Z}$. Show that membership in P' does not depend on the representative, that P' satisfies (P2) of Proposition 2.3.3, and that it does not satisfy (P1). Which part of (P1) fails?

Solution. Independence of representatives. If $(a, b) \sim (a', b')$ and $b = a + k$ with $k \neq 0$, then $b' + a = a + b' = b + a' = (a + k) + a' = (a' + k) + a$ (Theorem 1.5.3 (b), (c)), so $b' = a' + k$ by cancellation (Proposition 1.6.3 (b)), and $a' < b'$ by Proposition 1.6.3 (a). By Theorem 2.2.1 (c), $[(a, b)] \in P'$ if and only if $a < b$.

(P2). For $x = [(a, b)]$: $x \in P'$ iff $a < b$; $x = 0$ iff $a = b$ (as in the proof of Theorem 2.3.4); $-x \in P'$ iff $b < a$. By trichotomy in $\mathbb{N}$ (Theorem 1.6.1 (a)), exactly one holds.

(P1) fails for products. $[(0, 1)] \in P'$, but, by Definition 2.2.1 with $a = c = 0$ and $b = d = 1$ in $[(ac + bd, ad + bc)]$,

$$[(0, 1)][(0, 1)] = [(1, 0)],$$

and $[(1, 0)] \notin P'$, since $1 < 0$ is false. The sum half of (P1) holds, as in the proof of Theorem 2.3.4. So P' , the negative integers, fails only closure under products; it would define the reversed order, which breaks exactly (O4).

2.3.7.3 C. Going deeper

Exercise. C1: Ordered rings with $1 \neq 0$ are infinite

- Prove the sum law of Proposition 2.3.5 (h) in full: for every ordered commutative ring R , every $a \in R$ and all $m, k \in \mathbb{N}$, $(m + k) \cdot a = m \cdot a + k \cdot a$. State the property you induct on and justify every equality.
- Deduce that every ordered commutative ring with $1 \neq 0$ is infinite (Sets, Relations, and Cardinality, Definition 3.1.3).
- The set $\{0, 1, 2\}$ with addition and multiplication “modulo 3”, given by the tables below, is a commutative ring with $1 \neq 0$ (you may take this for granted). Show that it cannot be ordered.

+	0	1	2		·	0	1	2
0	0	1	2		0	0	0	0
1	1	2	0		1	0	1	2
2	2	0	1		2	0	2	1

Solution (Hint 1). For (b): what does (h) say about $k \mapsto k \cdot 1$?

Solution (Hint 2). Suppose R has m elements; consider $k \mapsto k \cdot 1$ on $\{1, \dots, m+1\}$.

Solution.

- (a) Fix R , $a \in R$, $m \in \mathbb{N}$, and use Logic and Proof, Axiom 4.2.1 (through Corollary 1.7.3 (b)) on k , for $P(k)$: “ $(m+k) \cdot a = m \cdot a + k \cdot a$ ”. *Base*: $(m+0) \cdot a = m \cdot a = m \cdot a + 0 = m \cdot a + 0 \cdot a$, by Definition 1.5.1 (a), (F3) and $0 \cdot a = 0$. *Step*: assume $P(k)$. Then

$$\begin{aligned}
 (m + (k + 1)) \cdot a &= ((m + k) + 1) \cdot a = (m + k) \cdot a + a \\
 &= (m \cdot a + k \cdot a) + a = m \cdot a + (k \cdot a + a) \\
 &= m \cdot a + (k + 1) \cdot a,
 \end{aligned}$$

by associativity in $\mathbb{N}$ (Theorem 1.5.3 (c)), the recursion for multiples, $P(k)$, (F2), and the recursion again. So $P(k+1)$ holds, and $P(k)$ holds for every k .

- (b) Let $1 \neq 0$ in R , and suppose R has m elements for some $m \in \mathbb{N}$ (Sets, Relations, and Cardinality, Definition 3.1.2). Let $f: \{1, \dots, m+1\} \rightarrow R$, $f(k) := k \cdot 1$. If $k < l$, then $k \cdot 1 < l \cdot 1$ by Proposition 2.3.5 (h), so $k \cdot 1 \neq l \cdot 1$ by (O1): f is injective. But $\{1, \dots, m+1\}$ has $m+1 > m$ elements (by its identity map), so Sets, Relations, and Cardinality, Corollary 3.1.3 (a) forbids an injection into R . This contradiction shows that R is infinite (Sets, Relations, and Cardinality, Definition 3.1.3).
- (c) By the definition of multiples and the tables, $1 \cdot 1 = 0 + 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ and $3 \cdot 1 = 2 + 1 = 0$. An order would give $3 \cdot 1 > 0$ by Proposition 2.3.5 (h), since $1 \neq 0$, that is, $0 > 0$, against (O1). (Alternatively, (b) applies to this finite ring.)

Marking scheme. (10 points) - 1: (a) states the induction property with m and a fixed and k the induction variable. - 2: (a) base case, citing $m+0 = m$, $0 \cdot a = 0$ and (F3). - 2: (a) inductive step, with associativity in $\mathbb{N}$, the recursion, the hypothesis and (F2) each named. - 2: (b) shows that $k \mapsto k \cdot 1$ is injective, citing (h) and (O1). - 2: (b) derives the contradiction from Sets, Relations, and Cardinality, Corollary 3.1.3 (a) with $m+1 > m$ elements (or any correct count). - 1: (c) computes $3 \cdot 1 = 0$ and concludes. Fatal errors (0 for the step): inducting on m and k at once without fixing one; using $1 > 0$ without $1 \neq 0$; in (b), “the multiples are all different, so there are infinitely many” with no finiteness result cited (Sets, Relations, and Cardinality, Corollary 3.1.3, Sets, Relations, and Cardinality, Proposition 3.1.6 with $\mathbb{N}$ infinite, or equivalent). A route for (b) composing the inverse of a bijection $\{1, \dots, m\} \rightarrow R$ with f earns the same 4 points. So does a route that shows $k \mapsto k \cdot 1$ is an injection $\mathbb{N} \rightarrow R$ (2 points, as above), so that its image is an infinite subset of R , and concludes with Sets, Relations, and Cardinality, Proposition 3.1.6 (2 points).