

2.1 The Natural Numbers and Well-Ordering

Logic and Proof, Chapter 4 took one fact about the natural numbers on trust: the principle of induction (Logic and Proof, Axiom 4.2.1), which says that a property holding at 0 and passing from each n to $n + 1$ holds for every $n \in \mathbb{N}$. From it, *Logic and Proof*, Chapter 4 proved strong induction (Logic and Proof, Theorem 4.2.2), whose step may use the property at **every** smaller number. Everything else we have said about $\mathbb{N}$ was school knowledge: that $7 - 3$ is a natural number, that none lies strictly between 3 and 4, that every non-empty set of natural numbers has a least member. This section derives those facts from induction, extends them to the integers, and then proves that the least-member property, **well-ordering**, is induction in another form.

2.1.1 What we assume about the natural numbers

The principle of induction is usually used with a property written as a sentence. It has an equivalent form about sets, which is the one *Analysis on the Real Line*, Chapter 1 uses.

Remark. Let $S \subseteq \mathbb{N}$ contain 0, and suppose $n + 1 \in S$ whenever $n \in S$. Apply Logic and Proof, Axiom 4.2.1 to the property “ $n \in S$ ”: its base case is $0 \in S$, and its step is the closure of S . So every $n \in \mathbb{N}$ lies in S , that is, $\mathbb{N} \subseteq S$, and with $S \subseteq \mathbb{N}$ this gives $S = \mathbb{N}$ (Proposition 1.1.1). In words: the only subset of $\mathbb{N}$ that contains 0 and is closed under $n \mapsto n + 1$ is $\mathbb{N}$ itself. *Analysis on the Real Line*, Chapter 1 states this as “ $\mathbb{N}$ is contained in every inductive set”, where an inductive set contains 0, as here.

Here is everything the section assumes about $\mathbb{N}$. The natural numbers form a subset $\mathbb{N} \subseteq \mathbb{R}$ of the familiar real numbers such that

- (($\mathbb{N}$)0) $0 \in \mathbb{N}$;
- (NS) for every $n \in \mathbb{N}$, also $n + 1 \in \mathbb{N}$;

and Logic and Proof, Axiom 4.2.1 holds. The arithmetic and the order of the real numbers (the laws of $+$, $-$, $\cdot$ and $\leq$, trichotomy, multiplying an inequality by a positive number) are school facts in this volume and in *Logic and Proof*; *Analysis on the Real Line*, Chapter 1 states them as axioms of an ordered field. These three items are a description of $\mathbb{N}$, not new axioms: *Logic and Proof*, Chapter 4 already used all of them.

The rule for this section. From here to the end of the section, a fact about $\mathbb{N}$ is used only if it is (($\mathbb{N}$)0), (NS), Logic and Proof, Axiom 4.2.1, a statement proved earlier in the section, or Logic and Proof, Theorem 4.2.2 once the paragraph after [Lemma 2.1.1](#) has shown that its *Logic and Proof*, Chapter 4 proof rests only on these. The real-number arithmetic is used freely. In particular “ $n \geq 0$ ” for a natural number n , which looks too obvious to mention, is not available until it is proved below, in [Lemma 2.1.1](#) (a).

The integers and the rationals are then **defined** from $\mathbb{N}$, as subsets of $\mathbb{R}$:

$$\begin{aligned}\mathbb{Z} &:= \mathbb{N} \cup \{-n : n \in \mathbb{N}\}, \\ \mathbb{Z}_{>0} &:= \{n \in \mathbb{N} : n \neq 0\}, \\ \mathbb{Q} &:= \{m/n : m \in \mathbb{Z}, n \in \mathbb{Z}_{>0}\}.\end{aligned}$$

In words: an integer is a natural number or the negative of one; a positive integer is a natural number other than 0; a rational number is a quotient of an integer by a positive integer. These

are word for word the definitions of *Analysis on the Real Line*, Section 1.5, so the two chapters speak of the same sets. Examples: $-3 \in \mathbb{Z}$ because $3 \in \mathbb{N}$; 0 lies in $\mathbb{Z}$ twice over, as $0 \in \mathbb{N}$ and as -0 , which a union does not mind; $-\frac{1}{2} = (-1)/2 \in \mathbb{Q}$. The definitions do not yet tell us that $\frac{1}{2} \notin \mathbb{Z}$, or that $\mathbb{Z}_{>0}$ is the set of natural numbers ≥ 1 . Both need the lemma below.

Two pieces of notation will save words later. For $n \in \mathbb{N}$,

$$\{1, \dots, n\} := \{k \in \mathbb{N} : 1 \leq k \leq n\}, \quad \{0, \dots, n\} := \{k \in \mathbb{N} : k \leq n\}.$$

So $\{1, \dots, 0\} = \emptyset$, since no k has $1 \leq k \leq 0$. We do not write $[n]$ for these sets: square brackets will mean an equivalence class in Section 2.5.

2.1.2 The arithmetic of the natural numbers

The facts below are the ones *Logic and Proof*, Chapter 4 and *Analysis on the Real Line*, Chapter 1 used without proof. Each of (a)–(d) is one ordinary induction, and the only work is to choose the property to induct on; (e) follows from (a) and (d).

Lemma 2.1.1. Arithmetic of the Natural Numbers

For all $m, n \in \mathbb{N}$:

- (a) $n \geq 0$; and if $n \neq 0$, then $n \geq 1$;
- (b) $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$;
- (c) if $n \neq 0$ (equivalently, by (a), $n \geq 1$), then $n - 1 \in \mathbb{N}$;
- (d) if $m \leq n$, then $n - m \in \mathbb{N}$;
- (e) there is **no** $k \in \mathbb{N}$ with $n < k < n + 1$; equivalently, if $m < n$, then $m + 1 \leq n$.

In words: (a) says that 0 is the smallest natural number and that nothing in $\mathbb{N}$ lies between 0 and 1. (b) says $\mathbb{N}$ is closed under sums and products, (c) that every natural number except 0 has a predecessor in $\mathbb{N}$, and (d) that a difference “larger minus smaller” stays in $\mathbb{N}$. (e) says the natural numbers come one unit apart, with no gaps to hide in.

Idea. Each induction needs a property that is true at 0 and survives the step, and the statement as written does not always qualify. “If $n \neq 0$, then $n \geq 1$ ” says nothing useful at 0, so for (a) we induct on the disjunction “ $n = 0$ or $n \geq 1$ ”. For (b) we fix one of the two numbers and induct on the other. For (d) we induct on m . The step from m to $m + 1$ uses the hypothesis only at the same n , with the weaker bound $m \leq n$, and then subtracts 1 using (c). So n could be fixed first, as m is in (b); the proof below puts “for every n ” inside the property instead, which is harmless.

Proof. (a) Let $P(n)$ be “ $n = 0$ or $n \geq 1$ ”. *Base case:* $P(0)$ holds by its first disjunct. *Step:* let $n \in \mathbb{N}$ with $P(n)$. If $n = 0$, then $n + 1 = 1 \geq 1$; if $n \geq 1$, then $n + 1 \geq 2 \geq 1$. In both cases $n + 1 \geq 1$, so $P(n + 1)$ holds by its second disjunct. By Logic and Proof, Axiom 4.2.1, every $n \in \mathbb{N}$ satisfies $n = 0$ or $n \geq 1$. In both cases $n \geq 0$; and if $n \neq 0$, the first disjunct is excluded, so $n \geq 1$.

(b) Fix $m \in \mathbb{N}$. *Sums:* let $P(n)$ be “ $m + n \in \mathbb{N}$ ”. Then $P(0)$ holds, since $m + 0 = m \in \mathbb{N}$. If $m + n \in \mathbb{N}$, then $m + (n + 1) = (m + n) + 1 \in \mathbb{N}$ by (NS). By Logic and Proof, Axiom 4.2.1, $m + n \in \mathbb{N}$ for every $n \in \mathbb{N}$; as m was arbitrary, this holds for all $m, n \in \mathbb{N}$. *Products:* let

$Q(n)$ be “ $mn \in \mathbb{N}$ ”. Then $m \cdot 0 = 0 \in \mathbb{N}$ by $((\mathbb{N})0)$. If $mn \in \mathbb{N}$, then $m(n+1) = mn + m$, a sum of the two natural numbers mn and m , so it lies in $\mathbb{N}$ by the half just proved. By Logic and Proof, Axiom 4.2.1, $mn \in \mathbb{N}$ for every n .

(c) Let $P(n)$ be “ $n = 0$ or $n - 1 \in \mathbb{N}$ ”. $P(0)$ holds by its first disjunct. Let $n \in \mathbb{N}$; then $(n+1) - 1 = n \in \mathbb{N}$, so $P(n+1)$ holds by its second disjunct. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every $n \in \mathbb{N}$, and for $n \neq 0$ its second disjunct is the claim.

(d) Let $P(m)$ be “for every $n \in \mathbb{N}$, if $m \leq n$, then $n - m \in \mathbb{N}$ ”. *Base case:* $n - 0 = n \in \mathbb{N}$. *Step:* let $m \in \mathbb{N}$ with $P(m)$, and let $n \in \mathbb{N}$ with $m + 1 \leq n$. Then $m < m + 1 \leq n$, so $n - m \in \mathbb{N}$ by $P(m)$. Moreover $n - m \geq 1 > 0$, so $n - m \neq 0$, and (c) gives $(n - m) - 1 \in \mathbb{N}$. Since $(n - m) - 1 = n - (m + 1)$, this is $P(m + 1)$. By Logic and Proof, Axiom 4.2.1, $P(m)$ holds for every $m \in \mathbb{N}$.

(e) Let $m < n$. By (d), $n - m \in \mathbb{N}$, and $n - m > 0$, so $n - m \neq 0$ and (a) gives $n - m \geq 1$, that is, $m + 1 \leq n$. Now suppose $k \in \mathbb{N}$ with $n < k < n + 1$. Applying what we just proved to $n < k$ gives $n + 1 \leq k$, which contradicts $k < n + 1$. So no such k exists. This proves the lemma. ■

Read the proof of (c) again. Its inductive step never mentions $P(n)$.

Example. An induction that ignores its hypothesis

Logic and Proof, Chapter 4, after its first worked induction (Logic and Proof, Example (A sum of products of neighbors)), said: “A proof by induction that never uses its induction hypothesis is either not an induction or is hiding a gap.” The proof of [Lemma 2.1.1](#) (c) never uses its induction hypothesis. Is it an induction, and is it hiding a gap?

Solution. It is an induction, and it hides no gap. Its base case $P(0)$ is proved, and its step “ $P(n) \Rightarrow P(n + 1)$ ” is a valid implication for every $n \in \mathbb{N}$: the conclusion $P(n + 1)$ is proved outright, so the implication holds whatever $P(n)$ says. Then Logic and Proof, Axiom 4.2.1 delivers $P(n)$ for every n . The hypothesis $n \in \mathbb{N}$ of the step is used, through $(n + 1) - 1 = n \in \mathbb{N}$; only $P(n)$ is not.

Nor can a case analysis replace the axiom here. A direct proof would have to say which numbers lie in $\mathbb{N}$, and the only thing that says so is induction: the step shows that every number of the form $n + 1$ with $n \in \mathbb{N}$ has the property, and it is Logic and Proof, Axiom 4.2.1 that tells us every natural number other than 0 is of this form. *Logic and Proof*, Chapter 4’s sentence is a rule of thumb, and a good one: an unused hypothesis is a reason to check the proof line by line. Here the check passes. The exception is a step whose conclusion is reached without the hypothesis, and the axiom is still what carries the property from 0 to every n .

The lemma also closes a gap in *Logic and Proof*, Chapter 4. The proof of Logic and Proof, Theorem 4.2.2 used two facts about $\mathbb{N}$ as school knowledge. In its base case it said “No natural number is less than 0, so $P(k)$ holds for every $k \in \mathbb{N}$ with $k < 0$, vacuously” and “The only $k \in \mathbb{N}$ with $k \leq 0$ is 0”: both are (a), the second with trichotomy. In its inductive step it said “The natural numbers $k < n + 1$ are exactly those with $k \leq n$, since no natural number

lies strictly between n and $n + 1$ ”, and then “A natural number $k \leq n + 1$ satisfies $k \leq n$ or $k = n + 1$ ”: both are (e), with trichotomy. The proofs of (a), (d) and (e) above use only Logic and Proof, Axiom 4.2.1, $((\mathbb{N})0)$, (NS), part (c) and the arithmetic of $\mathbb{R}$, and none of them uses strong induction. So strong induction rests on those items alone, and from now on we may cite Logic and Proof, Theorem 4.2.2 with no school fact behind it.

Quick check. Where in the proof of Lemma 2.1.1 (d) is part (c) used, and could n have been fixed before the induction on m , as m was in (b)?

Solution. Part (c) is used to pass from $n - m \in \mathbb{N}$ to $n - (m + 1) = (n - m) - 1 \in \mathbb{N}$, after checking $n - m \neq 0$. The step from m to $m + 1$ is about one n with $m + 1 \leq n$, and it uses $P(m)$ at that same n , with the weaker bound $m \leq n$. So yes: fixing $n \in \mathbb{N}$ and inducting on “if $m \leq n$, then $n - m \in \mathbb{N}$ ” proves the same thing, and then n was arbitrary. Putting “for every n ” inside $P(m)$ is harmless but not needed. It would be needed only if the step used the hypothesis at a different n , such as $n - 1$.

2.1.3 The integers

Analysis on the Real Line, Chapter 1 uses that sums, differences and products of integers are integers, and that an integer greater than 3 is at least 4. Both now follow from the lemma, by sorting integers into natural numbers and their negatives.

Proposition 2.1.2. Arithmetic of the Integers

Let $m, n \in \mathbb{Z}$.

- (a) $m + n$, $m - n$ and mn are integers.
- (b) If $n \geq 0$, then $n \in \mathbb{N}$; if $n > 0$, then $n \in \mathbb{Z}_{>0}$. Hence

$$\mathbb{N} = \{n \in \mathbb{Z} : n \geq 0\}, \quad \mathbb{Z}_{>0} = \{n \in \mathbb{Z} : n > 0\} = \{n \in \mathbb{N} : n \geq 1\}.$$

- (c) (**Discreteness.**) If $m < n$, then $m + 1 \leq n$.

Idea. Every integer is a or $-a$ with $a \in \mathbb{N}$, so each claim splits into cases by signs. Only one case has content: $a + (-b) = a - b$ with $a, b \in \mathbb{N}$, which is in $\mathbb{N}$ when $b \leq a$, by Lemma 2.1.1 (d), and is the negative of a natural number when $a < b$. Discreteness then follows from (b) applied to the difference $n - m$: it is a positive integer, hence a natural number with $n - m \geq 1$, by (a) of the lemma.

Proof. (a) First, $\mathbb{Z}$ is closed under $x \mapsto -x$: if $x \in \mathbb{N}$, then $-x \in \mathbb{Z}$ by the definition of $\mathbb{Z}$; if $x = -k$ with $k \in \mathbb{N}$, then $-x = k \in \mathbb{N} \subseteq \mathbb{Z}$.

Next let $a, b \in \mathbb{N}$; we show $a - b \in \mathbb{Z}$. By trichotomy there are three cases. If $a > b$ or $a = b$, then $b \leq a$, and $a - b \in \mathbb{N}$ by Lemma 2.1.1 (d). If $a < b$, then $b - a \in \mathbb{N}$ by (d), and $a - b = -(b - a) \in \mathbb{Z}$.

Now write $m = \pm a$ and $n = \pm b$ with $a, b \in \mathbb{N}$. The table lists the four sign patterns; in each, $a + b$ and ab lie in $\mathbb{N}$ by [Lemma 2.1.1](#) (b), and $a - b$, $b - a$ lie in $\mathbb{Z}$ by the previous paragraph.

m	n	$m + n$	mn
a	b	$a + b \in \mathbb{N}$	$ab \in \mathbb{N}$
a	$-b$	$a - b \in \mathbb{Z}$	$-(ab) \in \mathbb{Z}$
$-a$	b	$b - a \in \mathbb{Z}$	$-(ab) \in \mathbb{Z}$
$-a$	$-b$	$-(a + b) \in \mathbb{Z}$	$ab \in \mathbb{N}$

So $m + n$ and mn are integers. Finally $m - n = m + (-n)$, a sum of two integers, since $-n \in \mathbb{Z}$ by the first paragraph.

(b) Let $n \geq 0$. By the definition of $\mathbb{Z}$, either $n \in \mathbb{N}$, and we are done, or $n = -k$ with $k \in \mathbb{N}$. In the second case $k = -n \leq 0$, and $k \geq 0$ by [Lemma 2.1.1](#) (a), so $k = 0$ and $n = 0 \in \mathbb{N}$ by $((\mathbb{N})0)$. If moreover $n > 0$, then n is a natural number with $n \neq 0$, so $n \in \mathbb{Z}_{>0}$.

For the set equalities: $\mathbb{N} \subseteq \mathbb{Z}$, and every $n \in \mathbb{N}$ has $n \geq 0$ by (a) of the lemma; with the first sentence of (b) this gives $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 0\}$. Every element of $\mathbb{Z}_{>0}$ is a natural number $n \neq 0$, so $n \geq 1 > 0$ by (a) of the lemma; with the second sentence of (b) this gives $\mathbb{Z}_{>0} = \{n \in \mathbb{Z} : n > 0\}$. Finally, for $n \in \mathbb{N}$, $n \neq 0$ implies $n \geq 1$ by (a), and $n \geq 1$ implies $n \neq 0$; so $\mathbb{Z}_{>0} = \{n \in \mathbb{N} : n \geq 1\}$.

(c) Let $m < n$. By (a), $n - m \in \mathbb{Z}$, and $n - m > 0$, so $n - m \in \mathbb{Z}_{>0}$ by (b), that is, $n - m \geq 1$. Hence $m + 1 \leq n$. This proves the proposition. ■

Discreteness is the fact behind “an integer greater than 3 is at least 4” (take $m = 3$), and behind “the integers x with $-2 \leq x \leq 2$ are $-2, -1, 0, 1, 2$ ”: an integer x with $-2 \leq x$ is -2 or at least -1 , and so on up to 2. It also settles the question left open above: $\frac{1}{2} \notin \mathbb{Z}$, since $0 < \frac{1}{2}$ would force $1 \leq \frac{1}{2}$.

2.1.4 Well-ordering

A fraction with even numerator and denominator can be halved, and halved again, and *Logic and Proof*, Chapter 2 claimed that this cannot go on for ever (the fact (L) in the proof of Logic and Proof, Theorem 2.2.1). The reason is that the absolute values of the denominators form a strictly decreasing list of positive integers, and such a list must stop. The precise form of “must stop” is a statement about least elements.

A **least element** of a set $S \subseteq \mathbb{R}$ is an element $m \in S$ such that $m \leq s$ for **every** $s \in S$. Not every set has one: $(0, 1]$ has none, since for every $x \in (0, 1]$ the number $x/2$ lies in the set and is smaller. The empty set has none either, as a least element must be an element. Reversing the inequality, a **greatest element** of S is an element $m \in S$ with $s \leq m$ for every $s \in S$; this is the maximum of *Logic and Proof*, Section 5.8.

Every non-empty set of natural numbers has a least element.

Theorem 2.1.3. Well-Ordering of the Natural Numbers

Every **non-empty** subset of $\mathbb{N}$ has a least element.

Try it first (ten minutes): suppose that $S \subseteq \mathbb{N}$ has no least element. Which property of n would you prove for every $n \in \mathbb{N}$ by strong induction, and why does it finish the proof?

Idea. A least element cannot be found by inspecting S , since we know nothing about S . So we suppose there is none and show S is empty, which contradicts “non-empty”. The property to carry is “ $n \notin S$ ”. If no number below n is in S and n were in S , then n would be a least element; so n is not in S . The hypothesis must speak about **every** number below n , which is why the induction is strong. *Before reading on: at which line is trichotomy used, and what would go wrong without it?*

Proof. Let $S \subseteq \mathbb{N}$ be non-empty, and suppose, for a contradiction, that S has no least element. For $n \in \mathbb{N}$, let $P(n)$ be “ $n \notin S$ ”.

Let $n \in \mathbb{N}$, and suppose $P(k)$ holds for every $k \in \mathbb{N}$ with $k < n$, that is, no natural number less than n lies in S . Suppose $n \in S$. Let $s \in S$. By trichotomy, $s < n$, $s = n$ or $s > n$. The first is impossible: s is a natural number less than n , so $s \notin S$ by the hypothesis. So $s \geq n$. As $s \in S$ was arbitrary, n is a least element of S , which contradicts our supposition. Hence $n \notin S$, that is, $P(n)$ holds.

By Logic and Proof, Theorem 4.2.2, $n \notin S$ for every $n \in \mathbb{N}$. Since $S \subseteq \mathbb{N}$, the set S has no elements, which contradicts S being non-empty. So S has a least element. This proves the theorem. ■

The outer frame is an RAA on the statement “ S has a least element”. The proof shows that a least element **exists**; it does not say how to find it. *Logic and Proof*, Section 8.7 explained why mathematicians have argued over proofs of this kind. Here the debate has a quiet ending: if S is given by a property that can be checked number by number, testing $0, 1, 2, \dots$ in turn finds the least element, and the theorem says the search stops. Nothing in the proof above depends on such a test.

Quick check. In the proof of [Theorem 2.1.3](#), to which property is strong induction applied, and what is the induction hypothesis at n ?

Solution. To $P(n)$: “ $n \notin S$ ”. At n , the induction hypothesis is that $k \notin S$ for every natural number $k < n$: no element of S lies below n . Together with “ $n \in S$ ” it would make n a least element, which is why $n \in S$ leads to a contradiction.

Warning. Well-ordering is a property of subsets of $\mathbb{N}$, not of every set of numbers. The set of positive rationals is non-empty and has no least element: for every positive rational q ,

the number $q/2$ is a smaller positive rational. Neither has $\mathbb{Z}$: $n - 1 < n$ is again an integer. A proof that takes “the least element” of a set must first show that the set is a non-empty subset of $\mathbb{N}$, or a non-empty set of integers with an integer lower bound, as in [Corollary 2.1.5](#) below.

Quick check. Does $\{n \in \mathbb{N} : n^2 > 50\}$ have a least element? If so, which?

Solution. Yes. The set is non-empty, since $10^2 = 100 > 50$, and it is a subset of $\mathbb{N}$, so [Theorem 2.1.3](#) applies. The least element is 8: $8^2 = 64 > 50$, while $7^2 = 49 \leq 50$, and for $n \leq 7$ we have $n^2 \leq 49$. The theorem promised a least element; finding it took a search from below.

2.1.5 Induction and well-ordering are the same principle

The proof of [Theorem 2.1.3](#) derived well-ordering from induction. The derivation also runs the other way, and the cleanest way to say so is to ask which sets of numbers satisfy which principle. For a set $X \subseteq \mathbb{R}$, consider three structural properties:

- $0 \in X$;
- **closure:** for every $n \in X$, $n + 1 \in X$;
- the **predecessor property:** for every $n \in X$ with $n \neq 0$, $n - 1 \in X$.

The set $\mathbb{N}$ has all three, by $((\mathbb{N})0)$, $(\mathbb{N}S)$ and [Lemma 2.1.1](#) (c). Say that X has the **induction property** if every $S \subseteq X$ with $0 \in S$ and $n + 1 \in S$ for every $n \in S$ equals X ; and the **least-element property** if every non-empty subset of X has a least element. The closure of S in the induction property is plain closure under $n \mapsto n + 1$, not “closure as long as one stays in X ”; the witnesses below show why that matters.

Theorem 2.1.4. Induction Is Equivalent to Well-Ordering

Let $X \subseteq \mathbb{R}$ contain 0, be closed under $n \mapsto n + 1$, and have the predecessor property. Then X has the induction property **if and only if** X has the least-element property.

Idea. $(\Rightarrow)$ A set X with the induction property and the first two properties must be $\mathbb{N}$ itself: $\mathbb{N}$ sits inside X by Logic and Proof, Axiom 4.2.1, and the induction property of X , applied to the subset $\mathbb{N}$, forces equality. Then [Theorem 2.1.3](#) applies. $(\Leftarrow)$ Take S as in the induction property and suppose $S \neq X$; the least element m of $X \setminus S$ is then a smallest failure; the number $m - 1$ just below it is not a failure, so it lies in S , and closure passes that success up to $m = (m - 1) + 1$, a contradiction. *Before reading on: in $(\Leftarrow)$, which of the three hypotheses on X gives $m - 1 \in X$, and which two are not used at all?*

Proof. $(\Rightarrow)$ Suppose X has the induction property. Apply Logic and Proof, Axiom 4.2.1 to the property “ $n \in X$ ”: its base case is $0 \in X$, and its step is the closure of X . So $\mathbb{N} \subseteq X$.

Now $\mathbb{N}$ is a subset of X that contains 0 and is closed under $n \mapsto n + 1$, by $((\mathbb{N})0)$ and (NS) ; the induction property of X gives $\mathbb{N} = X$. By [Theorem 2.1.3](#), every non-empty subset of $X = \mathbb{N}$ has a least element.

$(\Leftarrow)$ Suppose X has the least-element property. Let $S \subseteq X$ contain 0 and be closed under $n \mapsto n + 1$. Suppose $S \neq X$. Then $X \setminus S$ is non-empty: if it were empty, every element of X would lie in S , so $X \subseteq S$, and with $S \subseteq X$ this would give $S = X$ by Proposition 1.1.1. So $X \setminus S$ has a least element m . We have $m \neq 0$, since $0 \in S$. So $m - 1 \in X$, by the predecessor property. Since $m - 1 < m$ and m is least in $X \setminus S$, $m - 1 \notin X \setminus S$, that is, $m - 1 \in S$. Hence $m = (m - 1) + 1 \in S$ by the closure of S , which contradicts $m \in X \setminus S$. So $S = X$, and X has the induction property. This proves the theorem. ■

Each hypothesis on X has a job, and dropping any one of them breaks the theorem. Each witness below names the direction that fails and the step of the proof it blocks.

- **Drop the predecessor property; $(\Leftarrow)$ fails.** Let $X := \mathbb{N} \cup \{n + \frac{1}{2} : n \in \mathbb{N}\}$. It contains 0 and is closed, since $(n + \frac{1}{2}) + 1 = (n + 1) + \frac{1}{2}$. It has the least-element property: for non-empty $T \subseteq X$, compare a least element of $T \cap \mathbb{N}$ with $\frac{1}{2}$ plus a least element of $\{t - \frac{1}{2} : t \in T \setminus \mathbb{N}\}$, each of the two sets, when non-empty, being a subset of $\mathbb{N}$; the smaller of the candidates is least in T (Exercise C2 asks for the details). But $S := \mathbb{N}$ contains 0, is closed, and is not X , since $\frac{1}{2} \notin \mathbb{N}$ by [Lemma 2.1.1](#) (e). The proof of $(\Leftarrow)$ breaks at “ $m - 1 \in X$ ”: here $m = \frac{1}{2}$ is least in $X \setminus S$, and $m \neq 0$, but $m - 1 = -\frac{1}{2} \notin X$.
- **Drop closure; $(\Rightarrow)$ fails.** Let $X := \{-n : n \in \mathbb{N}\} = \{0, -1, -2, \dots\}$. It contains 0, and it has the predecessor property, since $(-n) - 1 = -(n + 1)$. Its induction property holds **vacuously**: a subset $S \subseteq X$ containing 0 and closed under $n \mapsto n + 1$ would contain 1, and $1 \notin X$, since $1 = -n$ would give $n = -1 < 0$, against [Lemma 2.1.1](#) (a); so no such S exists, and every one of them (there are none) equals X . But X itself has no least element, since $-(n + 1) < -n$. The proof of $(\Rightarrow)$ breaks at “ $\mathbb{N} \subseteq X$ by Logic and Proof, Axiom 4.2.1”: the property “ $n \in X$ ” has no inductive step.
- **Drop $0 \in X$; $(\Rightarrow)$ fails.** Let $X := \{k + \frac{1}{2} : k \in \mathbb{Z}\}$. It is closed, and it has the predecessor property, since $(k + \frac{1}{2}) \pm 1 = (k \pm 1) + \frac{1}{2}$ with $k \pm 1 \in \mathbb{Z}$ by [Proposition 2.1.2](#) (a). Its induction property holds vacuously, because $0 \notin X$, so no subset of X contains 0. (Indeed $0 = k + \frac{1}{2}$ would need $k = -\frac{1}{2} \in \mathbb{Z}$, and then $\frac{1}{2} = -k \in \mathbb{Z}$ by [Proposition 2.1.2](#) (a), which discreteness rules out, as shown above.) And X has no least element, since $(k - 1) + \frac{1}{2} < k + \frac{1}{2}$. The proof of $(\Rightarrow)$ breaks at “ $\mathbb{N} \subseteq X$ by Logic and Proof, Axiom 4.2.1”: the property “ $n \in X$ ” has no base case, since $0 \notin X$.

In the last two witnesses the induction property is not false but vacuous. That is why the theorem uses plain closure of S . Under a “closure relative to X ” reading ($n + 1 \in S$ only when $n + 1 \in X$), the set $S = \{0\}$ would qualify in the closure witness, the induction property would fail there, and the witness would no longer separate the two properties.

So the slogan “induction and well-ordering are the same principle” means exactly [Theorem 2.1.4](#): for a set of numbers with 0, closure and predecessors, either principle implies the other. So *Logic and Proof*, Chapter 4 could have taken, alongside $((\mathbb{N})0)$ and (NS) , the predecessor property and well-ordering as its axioms, and proved induction from them by the $(\Leftarrow)$ half of [Theorem 2.1.4](#). The first witness above shows that the predecessor property cannot be left out, and with induction gone it could no longer be proved as [Lemma 2.1.1](#) (c) was. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 1 builds $\mathbb{N}$ from sets and proves the Peano axioms, induction among them, there.

2.1.6 Sets of integers

Well-ordering moves to sets of integers by a shift, provided the bound that makes the shift work is itself an integer.

Corollary 2.1.5. Well-Ordering of Sets of Integers

Let $S \subseteq \mathbb{Z}$ be non-empty. If S has a lower bound $b \in \mathbb{Z}$, then S has a least element. If S has an upper bound $b \in \mathbb{Z}$, then S has a greatest element.

Idea. Slide S to the right by $-b$, so that its lower bound lands on 0; the shifted set lies in $\mathbb{N}$, where [Theorem 2.1.3](#) applies, and sliding back preserves order. For an upper bound, reflect: $-S$ is bounded below by $-b$.

Proof. Lower bound. Let $T := \{s - b : s \in S\}$. Each $s - b$ is an integer by [Proposition 2.1.2](#) (a), and $s - b \geq 0$ since $b \leq s$; so $s - b \in \mathbb{N}$ by [Proposition 2.1.2](#) (b). Thus T is a non-empty subset of $\mathbb{N}$, and by [Theorem 2.1.3](#) it has a least element $m_0 - b$ with $m_0 \in S$. For every $s \in S$, $m_0 - b \leq s - b$, so $m_0 \leq s$. Hence m_0 is a least element of S .

Upper bound. Let $-S := \{-s : s \in S\}$. It is a non-empty set of integers (negatives of integers are integers, by the definition of $\mathbb{Z}$ and [Proposition 2.1.2](#) (a)), and $-b$ is an integer lower bound for it, since $s \leq b$ gives $-b \leq -s$. By the first half, $-S$ has a least element $-m$ with $m \in S$. For every $s \in S$, $-m \leq -s$, so $s \leq m$: m is a greatest element of S . This proves the corollary. ■

The bound must be an integer, or at least have an integer below it. Given a set of integers bounded below by the real number $-\frac{7}{2}$, we would first replace $-\frac{7}{2}$ by the integer -4 , and that step, for an arbitrary real bound, is the Archimedean property of *Analysis on the Real Line*, Chapter 1, whose integer-part lemma in Section 1.6 does exactly this. In an ordered field without the Archimedean property, a set of integers can be bounded below and have no least element (in the field $\mathbb{R}(x)$ of *Analysis on the Real Line*, Chapter 1's example of a non-Archimedean field, every $n \in \mathbb{N}$ has $n < x$, so the set $\{-n : n \in \mathbb{N}\}$ is bounded below by $-x$, and it has no least element, since $-(n+1) < -n$), so this chapter, which has no Archimedean property, proves the corollary with an integer bound, and *Analysis on the Real Line*, Chapter 1 supplies the rest.

2.1.7 Exercises

2.1.7.1 A. Check your understanding

Exercise. A1

Parts (a)–(d) are about the proof of [Theorem 2.1.3](#).

- (a) Where is trichotomy used?
- (b) Why would ordinary induction (Logic and Proof, Axiom 4.2.1) on the same property “ $n \notin S$ ” not do?

- (c) Run the proof on $S = \{4, 7, 9\}$: at which n does the argument meet an element of S , and what does it conclude there?
- (d) State the idea of the proof in two sentences.
- (e) Let $X = \mathbb{N} \cup \{n + \frac{1}{2} : n \in \mathbb{N}\}$. Which statements of [Lemma 2.1.1](#) remain true when every “ $\mathbb{N}$ ” in them is replaced by “ X ”? Decide each clause of (a), each half of (b), and (c), (d), (e) separately, with a witness for each failure.

Solution. (a) In the inductive step, to split an arbitrary $s \in S$ into $s < n$, $s = n$ or $s > n$. The first case is excluded by the hypothesis, so $s \geq n$. Without trichotomy, “ s is not less than n ” would not give “ $s \geq n$ ”, and n would not be shown to be least.

(b) Ordinary induction gives only $P(n-1)$, that is, $n-1 \notin S$, as hypothesis for $P(n)$. That does not exclude a smaller element of S , such as $n-5$, so “ $n \in S$ ” would not make n least, and no contradiction would follow. The proof needs **all** numbers below n to be outside S .

(c) $S = \{4, 7, 9\}$ has a least element, so the supposition of the proof is false, and the argument meets its contradiction. For $n = 0, 1, 2, 3$, no smaller number is in S , and indeed $n \notin S$. At $n = 4$, no natural number below 4 is in S , and $4 \in S$; the argument shows that every $s \in S$ has $s \geq 4$, so 4 is a least element of S . That contradicts the supposition “ S has no least element”, and the proof concludes that S has a least element, namely 4.

(d) If S had no least element, then no n could be in S , because the first one would be least; strong induction makes “the first one” precise. So S would be empty, against the hypothesis.

(e) Holding: the first clause of (a) (every element is ≥ 0); the sum half of (b), since a sum of two halves $(m + \frac{1}{2}) + (n + \frac{1}{2}) = m + n + 1$ is a natural number and a half plus a natural number is a half; and (d): if $x \leq y$ in X , then $y - x \in X$. For (d) there are four cases. Two natural numbers, or two halves, have a difference in $\mathbb{N}$ by [Lemma 2.1.1](#) (d). For $x = m \leq y = n + \frac{1}{2}$, we have $m \leq n$ (else $m \geq n + 1 > y$ by (e) of the lemma), so $y - x = (n - m) + \frac{1}{2} \in X$. For $x = m + \frac{1}{2} \leq y = n$, we have $m < n$, so $m + 1 \leq n$ and $y - x = (n - m - 1) + \frac{1}{2} \in X$.

Failing: the second clause of (a), since $\frac{1}{2} \neq 0$ and $\frac{1}{2} < 1$; the product half of (b), since $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin X$ (it is not a natural number, as $0 < \frac{1}{4} < 1$, and not a half, as $\frac{1}{4} - \frac{1}{2} < 0$); (c), since $\frac{1}{2} \neq 0$ and $\frac{1}{2} - 1 = -\frac{1}{2} \notin X$; (e), since $0 < \frac{1}{2} < 1$ with $\frac{1}{2} \in X$.

Each clause had to be decided by its own witness. The proofs of (a)–(d) were inductions over $\mathbb{N}$, and X does not have the induction property ($\mathbb{N} \subseteq X$ contains 0 and is closed), so none of those proofs carries over; some conclusions survive anyway. (c) fails because the predecessor property fails at $\frac{1}{2}$. (e) fails through the second clause of (a), not through (d), which still holds. The set $\mathbb{Z} \cup \{k + \frac{1}{2} : k \in \mathbb{Z}\}$ has the predecessor property and still has $\frac{1}{2}$ between 0 and 1, so the predecessor property alone (with 0 and closure) does not give (e); together with the least-element property it does: the set then has the induction property by [Theorem 2.1.4](#), and, as in the proof of its ($\Rightarrow$) half, it equals $\mathbb{N}$.

2.1.7.2 B. Practice

Exercise. B1

Use only [Lemma 2.1.1](#) and the arithmetic of $\mathbb{R}$.

- (a) Prove that if $m, n \in \mathbb{N}$ and $mn = 1$, then $m = n = 1$.

(b) Prove that $n^2 \geq n$ for every $n \in \mathbb{N}$.

Solution. (a) Since $0 \cdot n = 0 \neq 1$, we have $m \neq 0$, and likewise $n \neq 0$. By the second clause of Lemma 2.1.1 (a), $m \geq 1$ and $n \geq 1$. Suppose $m > 1$. Multiplying by $n > 0$ gives $mn > n \geq 1$, which contradicts $mn = 1$. So $m = 1$, and then $n = mn = 1$.

(b) Let $n \in \mathbb{N}$. By Lemma 2.1.1 (a), $n = 0$ or $n \geq 1$. If $n = 0$, then $n^2 = 0 = n$. If $n \geq 1$, multiplying $n \geq 1$ by $n > 0$ gives $n^2 \geq n$. In both cases $n^2 \geq n$.

Exercise. B2: Putting a proof in order

The lines below, (i)–(ix), include the seven lines of a proof of $(\Leftarrow)$ in Theorem 2.1.4, shuffled, and two lines that do not belong. Here X has $0 \in X$, closure and the predecessor property, and the least-element property. Write the seven lines in an order that makes a correct proof, and say why each of the other two lines fails.

- (i) So $m - 1 \in X$, by the predecessor property.
- (ii) Let m be the least element of S .
- (iii) Then $X \setminus S$ is non-empty, so it has a least element m .
- (iv) Hence $m = (m - 1) + 1 \in S$, a contradiction; so $S = X$.
- (v) Let $S \subseteq X$ contain 0 and be closed under $n \mapsto n + 1$.
- (vi) $m - 1 < m$, so $m - 1 \notin X \setminus S$, that is, $m - 1 \in S$.
- (vii) Since m is least and $m - 1 < m$, $m - 1 \in X \setminus S$.
- (viii) Suppose $S \neq X$.
- (ix) $m \neq 0$, since $0 \in S$.

Solution. The order is (v), (viii), (iii), (ix), (i), (vi), (iv). It is the only admissible one. (v) introduces S , (viii) is the supposition the rest contradicts, and (iii) introduces m from it. (ix) must sit between (iii) and (i): it needs the m of (iii), and (i) applies the predecessor property, which needs $m \neq 0$. (vi) uses the $m - 1 \in X$ of (i): only an element of X can be sorted into S or $X \setminus S$. (iv) uses (vi) and closure.

Line (ii) takes the least element of the wrong set. The set whose least element locates a failure is $X \setminus S$: its least element is the first number of X missing from S . A least element of S says nothing about where S and X differ; in the case $X = \mathbb{N}$ it is 0, which lies in S by (v) and is no failure at all. Line (vii) reads leastness backwards: “ m is least in $X \setminus S$ ” says that nothing **below** m lies in $X \setminus S$, so a smaller number of X is in S , not outside it.

Exercise. B3

Prove the second half of Corollary 2.1.5 directly from Theorem 2.1.3, without using the first half: if $S \subseteq \mathbb{Z}$ is non-empty and $b \in \mathbb{Z}$ is an upper bound of S , then S has a greatest element.

Hint: shift by $s \mapsto b - s$.

Solution. Let $T := \{b - s : s \in S\}$. For $s \in S$, $b - s$ is an integer by [Proposition 2.1.2](#) (a), and $b - s \geq 0$ because $s \leq b$; so $b - s \in \mathbb{N}$ by [Proposition 2.1.2](#) (b). Thus T is a non-empty subset of $\mathbb{N}$, and by [Theorem 2.1.3](#) it has a least element, of the form $b - s_0$ with $s_0 \in S$. For every $s \in S$, $b - s_0 \leq b - s$, so $s \leq s_0$. Hence s_0 is a greatest element of S .

2.1.7.3 C. Going deeper

Exercise. C1: A greatest element from a least upper bound

Let $S \subseteq \mathbb{N}$ be non-empty, and suppose some $M \in \mathbb{N}$ satisfies $s \leq M$ for every $s \in S$.

- (a) Prove that S has a greatest element by applying [Theorem 2.1.3](#) to the set U of upper bounds of S that lie in $\mathbb{N}$, not by citing [Corollary 2.1.5](#): show that the least element of U lies in S .
- (b) Show that the hypothesis “some $M \in \mathbb{N}$ bounds S above” cannot be dropped.

Solution (Hint 1). Consider $U := \{u \in \mathbb{N} : s \leq u \text{ for every } s \in S\}$.

Solution (Hint 2). U is non-empty because $M \in U$; let u be its least element, which exists by [Theorem 2.1.3](#).

Solution. (a) Let $U := \{u \in \mathbb{N} : s \leq u \text{ for every } s \in S\}$. Then $M \in U$, so U is a non-empty subset of $\mathbb{N}$, and [Theorem 2.1.3](#) gives a least element u of U . We show $u \in S$.

Suppose $u \notin S$. Then every $s \in S$ satisfies $s \leq u$ and $s \neq u$, so $s < u$, and $s + 1 \leq u$ by [Lemma 2.1.1](#) (e); that is, $s \leq u - 1$. Since S is non-empty, it has an element s_0 , and $0 \leq s_0 < u$ by [Lemma 2.1.1](#) (a), so $u \neq 0$. By [Lemma 2.1.1](#) (c), $u - 1 \in \mathbb{N}$. So $u - 1$ is an upper bound of S in $\mathbb{N}$, that is, $u - 1 \in U$, and $u - 1 < u$, which contradicts the choice of u . Hence $u \in S$.

Since $u \in S$ and $s \leq u$ for every $s \in S$, u is a greatest element of S .

(b) $S = \mathbb{N}$ is non-empty and has no greatest element: for every $n \in \mathbb{N}$, also $n + 1 \in \mathbb{N}$ by (NS), and $n + 1 > n$. In the proof, U is then empty, and [Theorem 2.1.3](#) has nothing to apply to.

The number u of (a) is the **least upper bound** of S among natural numbers, and the proof shows that it lies in S . Section 2.6 defines least upper bounds in any partially ordered set, and *Analysis on the Real Line*, Chapter 1 is about sets of real numbers whose least upper bound, when it exists, need **not** lie in the set.

Marking scheme. (10 points) - 2: defines the set of upper bounds in $\mathbb{N}$, shows it is non-empty, and takes its least element by [Theorem 2.1.3](#). - 2: handles $u = 0$ separately, or shows $u \neq 0$ using that S is non-empty, before using $u - 1 \in \mathbb{N}$ ([Lemma 2.1.1](#) (c)). - 3: uses the minimality of u : either shows directly that $u - 1 \notin U$, so some $s \in S$ has $s > u - 1$, or, supposing $u \notin S$, derives $u - 1 \in U$ and contradicts minimality. - 1: uses discreteness ([Lemma 2.1.1](#) (e)) to show that an element of S greater than $u - 1$ equals u , or to get

$s \leq u - 1$ in the contradiction route, and concludes that $u \in S$ is a greatest element. - 2: (b) the witness $S = \mathbb{N}$, with the reason it has no greatest element. Fatal errors (0 for the step): using $u - 1 \in \mathbb{N}$ without checking $u \neq 0$; taking a least element of U without showing U non-empty.

A second route, through the least element $M - s_0$ of $\{M - s : s \in S\} \subseteq \mathbb{N}$ (as in [Exercise \(B3\)](#)), proves the conclusion of (a) but not by the method the task names, so it earns at most 4 points for (a): 2 for showing that this set is a non-empty subset of $\mathbb{N}$ and taking its least element, and 2 for deducing $s \leq s_0$ for every $s \in S$ from $M - s_0 \leq M - s$, with $s_0 \in S$; and (b) as above.

Exercise. C2: A well-ordered set with gaps

Let $X := \mathbb{N} \cup \{n + \frac{1}{2} : n \in \mathbb{N}\}$. Prove that every non-empty subset of X has a least element.

Solution. Let $T \subseteq X$ be non-empty, and put

$$A := T \cap \mathbb{N}, \quad B := \{t - \frac{1}{2} : t \in T \setminus \mathbb{N}\}.$$

Every $t \in T \setminus \mathbb{N}$ is $n + \frac{1}{2}$ for some $n \in \mathbb{N}$, since $t \in X$; so $t - \frac{1}{2} = n \in \mathbb{N}$, and $B \subseteq \mathbb{N}$. Since $T = A \cup (T \setminus \mathbb{N})$ is non-empty, A or B is non-empty. By [Theorem 2.1.3](#), A , if non-empty, has a least element a , and B , if non-empty, has a least element b . Define

$$c := \begin{cases} a & \text{if } B = \emptyset, \\ b + \frac{1}{2} & \text{if } A = \emptyset, \\ \min\{a, b + \frac{1}{2}\} & \text{otherwise.} \end{cases}$$

In each case $c \in T$: $a \in A \subseteq T$, and $b = t - \frac{1}{2}$ for some $t \in T \setminus \mathbb{N}$, so $b + \frac{1}{2} = t \in T$.

Let $t \in T$. If $t \in \mathbb{N}$, then $t \in A$, so $A \neq \emptyset$ and $t \geq a \geq c$. If $t \notin \mathbb{N}$, then $t - \frac{1}{2} \in B$, so $B \neq \emptyset$ and $t - \frac{1}{2} \geq b$, that is, $t \geq b + \frac{1}{2} \geq c$. (In both chains, the last inequality holds in every case of the definition of c that can occur.) So c is a least element of T .

The set X has the least-element property, contains 0 and is closed under $n \mapsto n + 1$, but it does not have the induction property ($\mathbb{N} \subseteq X$ contains 0 and is closed, and $\mathbb{N} \neq X$). That is the first witness after [Theorem 2.1.4](#): without the predecessor property, well-ordering does not give induction.

Marking scheme. (10 points) - 2: splits T into its natural-number part and its half part, and shows the shifted half part lies in $\mathbb{N}$. - 2: applies [Theorem 2.1.3](#) to each non-empty part, saying that at least one part is non-empty. - 2: defines the candidate in all cases, including those where one part is empty, and checks it lies in T . - 3: checks the candidate is $\leq t$ for every $t \in T$, by cases on $t \in \mathbb{N}$ or not. - 1: concludes, with the quantifiers right: one least element for the given T . Fatal errors (0 for the step): applying [Theorem 2.1.3](#) to T itself (it need not be a subset of $\mathbb{N}$); taking a least element of an empty part.

A second route, through the least element of $\{2t : t \in T\} \subseteq \mathbb{N}$, earns the same points. It earns 4 for showing that this set lies in $\mathbb{N}$, checking both $2n$ and $2n + 1$ by [Lemma 2.1.1](#) (b), and that it is non-empty, and for taking its least element $2t_0$ with $t_0 \in T$ by [Theorem 2.1.3](#).

It earns 4 for deducing $t_0 \leq t$ from $2t_0 \leq 2t$ for every $t \in T$, and 2 for the conclusion. The same fatal errors apply.