

1.5 The Recursion Theorem; Addition and Multiplication

The set ω now has a zero, a successor map and an induction theorem, and Theorem 1.4.2 shows that together they satisfy Peano's axioms. It has no addition yet. In *Sets, Relations, and Cardinality*, Chapter 2 the sum $m + n$ of two natural numbers came for free, from the real numbers; in ω a natural number is a set, and nothing we know about sets adds two of them. This section defines addition and multiplication by recursion, as school does (" $m + (n + 1)$ is one more than $m + n$ "), after first proving, from the axioms, that recursion defines something. Then it proves the laws of arithmetic one by one, most of them by an induction.

1.5.1 Recursion on ω

Sets, Relations, and Cardinality, Section 2.3 proved Sets, Relations, and Cardinality, Theorem 2.3.1: a starting value and a rule for the next value determine exactly one function on $\mathbb{N}$. That proof ran inside the familiar real numbers, where $\mathbb{N}$ is given. Its ingredients, though, were few: induction, and some facts about the sets $\{0, \dots, n\}$ on which the partial solutions live. On ω there is a natural replacement for $\{0, \dots, n\}$, namely the set $S(n) = n \cup \{n\}$ itself. (The next section proves that $S(n)$ is exactly the set of $k \in \omega$ with $k \leq n$; here we need no order, only $S(n)$ as a set.) So the proof can be repeated on ω , with one change, which we point out when we reach it.

A starting value and a rule for the next value determine exactly one function on ω .

Theorem 1.5.1. Recursion Theorem on ω

Let X be a set, let $a \in X$, and let $g: \omega \times X \rightarrow X$ be a function. Then there is **exactly one** function $f: \omega \rightarrow X$ such that

$$f(0) = a \quad \text{and} \quad f(S(n)) = g(n, f(n)) \quad \text{for every } n \in \omega.$$

This is the statement of Sets, Relations, and Cardinality, Theorem 2.3.1 word for word, with ω in place of $\mathbb{N}$ and $S(n)$ in place of $n + 1$. The set $\omega \times X$ exists by Proposition 1.2.2. As before, a is the starting value and g turns the stage n and the current value into the next value; the conclusion has an existence half and a uniqueness half.

Idea. Uniqueness is an induction. For existence, induction cannot build f , so we prove by induction that the finite pieces of f exist and are unique, and then glue them. The roadmap is that of *Sets, Relations, and Cardinality*, Section 2.3:

- ① **Uniqueness**, by Theorem 1.3.3.
- ② **Partial solutions.** A partial solution up to n is a function on $S(n)$ obeying the two equations wherever they make sense. A restriction of a partial solution is again one.
- ③ **Claim:** for every n there is exactly one partial solution up to n ; the next one adds a single pair at the new input $S(n)$.
- ④ **Glue:** the union of all their graphs is the graph of f .

The glue step of *Sets, Relations, and Cardinality*, Section 2.3 compared two indices: if $m \leq n$,

the piece up to m lies inside the piece up to n . We have no order on ω yet, so at each point k where both pieces are defined we cut both down to $S(k)$: by ② and ③, each restriction is the unique partial solution up to k .

Before reading on: where is $S(n) \notin S(n)$ used?

Proof. Step 0 (facts about $S(n)$). Let $n, k, m \in \omega$. Each of $S(n), S(m)$ is an element of ω by (P2) of Theorem 1.4.2. We use five facts.

- (i) $0 \in S(n)$, by Lemma 1.4.1 (e), since $S(n) \neq 0$ by (P3) of Theorem 1.4.2.
- (ii) If $S(k) \in S(n)$, then $k \in S(n)$: we have $k \in k \cup \{k\} = S(k)$, and $S(k) \subseteq S(n)$ because $S(n)$ is a transitive set (Lemma 1.4.1 (a), Definition 1.4.1).
- (iii) If $k \in S(m)$, then $S(k) \subseteq S(m)$: $k \subseteq S(m)$ because $S(m)$ is transitive, and $\{k\} \subseteq S(m)$, so $k \cup \{k\} \subseteq S(m)$.
- (iv) $S(n) \notin S(n)$, by Lemma 1.4.1 (c) applied to $S(n) \in \omega$.
- (v) The elements of $S(S(n)) = S(n) \cup \{S(n)\}$ are the elements of $S(n)$ and $S(n)$ itself (Definition 1.3.1). Every element of $S(n)$ lies in ω , by Lemma 1.4.1 (b).

Step 1 (uniqueness). Let $f, f': \omega \rightarrow X$ both satisfy the two equations, and let $P(n)$ be “ $f(n) = f'(n)$ ”. $P(0)$ holds, since $f(0) = a = f'(0)$. If $P(n)$ holds, then

$$f(S(n)) = g(n, f(n)) = g(n, f'(n)) = f'(S(n)),$$

so $P(S(n))$ holds. By Theorem 1.3.3 (b), $P(n)$ holds for every $n \in \omega$. The two functions have the same domain and codomain, so $f = f'$ by Sets, Relations, and Cardinality, Proposition 1.4.1.

Step 2 (partial solutions and their restrictions). For $n \in \omega$, a **partial solution up to n** is a function $h: S(n) \rightarrow X$ with $h(0) = a$ and $h(S(k)) = g(k, h(k))$ for every $k \in \omega$ with $S(k) \in S(n)$. The equations make sense: $0 \in S(n)$ by (i), and for such k , also $k \in S(n)$ by (ii).

Claim. If h is a partial solution up to m and $j \in S(m)$, then the restriction $h|_{S(j)}$ is a partial solution up to j .

Proof of Claim. Here $j \in \omega$ by (v), and $S(j) \subseteq S(m)$ by (iii), so the restriction (Sets, Relations, and Cardinality, Section 1.4) is a function $S(j) \rightarrow X$ with the same values as h . Its value at 0 is $h(0) = a$, since $0 \in S(j)$ by (i). Let $i \in \omega$ with $S(i) \in S(j)$. Then $S(i) \in S(m)$, because $S(j) \subseteq S(m)$, and $i \in S(j)$ by (ii). So the equation at $S(i)$ is one of the equations of h , and both of its sides are values at points of $S(j)$:

$$h|_{S(j)}(S(i)) = g(i, h(i)) = g(i, h|_{S(j)}(i)).$$

■

Step 3.

Claim. For every $n \in \omega$ there is exactly one partial solution up to n .

Proof of Claim. We use Theorem 1.3.3 (b) on n .

Base case. $S(0) = \emptyset \cup \{0\} = \{0\}$. The graph $\{(0, a)\}$ with codomain X is a function on $\{0\}$, since $a \in X$. It is a partial solution up to 0: its value at 0 is a , and the second condition is vacuous, because $S(k) \in \{0\}$ would mean $S(k) = 0$, which (P3) of Theorem 1.4.2 excludes. Any partial solution up to 0 has the value a at 0, so it equals this one by Sets, Relations, and Cardinality, Proposition 1.4.1.

Inductive step. Let $n \in \omega$, and suppose there is exactly one partial solution up to n ; call it f_n , with graph $G_n \subseteq S(n) \times X$. Since $n \in S(n)$, the value $f_n(n)$ is defined. Let

$$G' := G_n \cup \{(S(n), g(n, f_n(n)))\}.$$

We check Sets, Relations, and Cardinality, Definition 1.4.1 for G' on $S(S(n))$ with codomain X . By (v) and because g takes values in X , every pair of G' lies in $S(S(n)) \times X$. (Fn1): by (v), an input is an element of $S(n)$, which has an output in G_n , or is $S(n)$, which has the added output. (Fn2): every first coordinate in G_n lies in $S(n)$, while $S(n) \notin S(n)$ by (iv). So the added pair is the only pair of G' with first coordinate $S(n)$, and for an input in $S(n)$ all pairs of G' lie in G_n , which satisfies (Fn2). Hence $f' := (G', X)$ is a function $S(S(n)) \rightarrow X$ that agrees with f_n on $S(n)$.

It is a partial solution up to $S(n)$. Its value at 0 is $f_n(0) = a$, since $0 \in S(n)$. Let $k \in \omega$ with $S(k) \in S(S(n))$. By (v), there are two cases.

Case 1: $S(k) \in S(n)$. Then $k \in S(n)$ by (ii), and since f_n is a partial solution,

$$f'(S(k)) = f_n(S(k)) = g(k, f_n(k)) = g(k, f'(k)).$$

Case 2: $S(k) = S(n)$. Then $k = n$ by (P4) of Theorem 1.4.2, so the equation at the new input asks for $g(n, f'(n))$ and for nothing else; and $f'(S(n)) = g(n, f_n(n)) = g(n, f'(n))$ by the choice of the added pair.

It is the only one. Let h be a partial solution up to $S(n)$. Since $n \in S(S(n))$ by (v), the claim of Step 2 (with $m = S(n)$ and $j = n$) makes $h|_{S(n)}$ a partial solution up to n , so it is f_n by the induction hypothesis. Thus $h(k) = f_n(k) = f'(k)$ for every $k \in S(n)$, and, by the equation of h at $S(n) \in S(S(n))$,

$$h(S(n)) = g(n, h(n)) = g(n, f_n(n)) = f'(S(n)).$$

By (v) these are all the inputs, so $h = f'$ by Sets, Relations, and Cardinality, Proposition 1.4.1. This proves the claim. ■

For each $n \in \omega$, let f_n be the partial solution up to n , and G_n its graph. One consequence of the two claims is used below. If $k \in S(m)$, then $f_m|_{S(k)}$ is a partial solution up to k (Step 2), hence equals f_k (Step 3), and since $k \in S(k)$,

$$f_m(k) = f_k(k) \quad \text{whenever } k \in S(m). \quad (*)$$

Step 4 (glue). Each G_n is a subset of $S(n) \times X \subseteq \omega \times X$ (by (v)). Let

$$\mathcal{S} := \{G \in \mathcal{P}(\omega \times X) : (G, X) \text{ is a partial solution up to some } n \in \omega\},$$

a set by (Z5) and (Z6) of Axiom 1.1.1. By Step 3, the elements of $\mathcal{S}$ are exactly the graphs G_n . Let $F := \bigcup \mathcal{S}$, a set by (Z4); a pair lies in F if and only if it lies in some G_n , and $F \subseteq \omega \times X$. We check Sets, Relations, and Cardinality, Definition 1.4.1 for F .

(Fn1): for $k \in \omega$, the pair $(k, f_k(k))$ lies in $G_k \in \mathcal{S}$, hence in F .

(Fn2): let $(k, y) \in F$ and $(k, y') \in F$, say $(k, y) \in G_m$ and $(k, y') \in G_n$. Then k lies in the domains of both, $k \in S(m)$ and $k \in S(n)$, and by (*),

$$y = f_m(k) = f_k(k) = f_n(k) = y'.$$

No comparison of m with n was needed: both pieces were cut down to $S(k)$, where each is the unique partial solution up to k .

So $f := (F, X)$ is a function $\omega \rightarrow X$. If $k \in S(m)$, then $(k, f_m(k)) \in G_m \subseteq F$, so $f(k) = f_m(k)$. Hence $f(0) = f_0(0) = a$. For $n \in \omega$, both n and $S(n)$ lie in $S(S(n))$ by (v), and $f_{S(n)}$ is a partial solution up to $S(n)$, so

$$f(S(n)) = f_{S(n)}(S(n)) = g(n, f_{S(n)}(n)) = g(n, f(n)).$$

This proves existence, and with Step 1, the theorem. ■

The proof is that of *Sets, Relations, and Cardinality*, Section 2.3 with $\{0, \dots, n\}$ replaced by $S(n)$, and with one departure, in (Fn2) of Step 4. There, *Sets, Relations, and Cardinality*, Section 2.3 used that two indices m, n satisfy $m \leq n$ or $n < m$, and that $\{0, \dots, m\} \subseteq \{0, \dots, n\}$ when $m \leq n$. On ω those are facts about order, which the next section proves. Cutting both pieces down to $S(k)$ avoids the comparison altogether, so the recursion theorem does not have to wait for the order. In Step 3, (P4) did a quiet job: the new input $S(n)$ is the successor of n and of nothing else, so the added pair had to satisfy exactly one equation.

As in *Sets, Relations, and Cardinality*, Section 2.3, no choice is made: each partial solution is the only one, and $\mathcal{S}$ is cut out of a power set by a condition, so no family $n \mapsto f_n$ had to be formed first. From now on a definition “ $f(0) := a$, $f(S(n)) := g(n, f(n))$ ” on ω is legitimate whenever $a \in X$ and $g: \omega \times X \rightarrow X$ is a function, and f is **defined by recursion**.

Remark. The functions g that we feed to the theorem are usually given by a formula, such as $g(n, x) = S(x)$. Such a g is a function as soon as each pair (n, x) gets exactly one value in X : its graph, the set of pairs $((n, x), y) \in (\omega \times X) \times X$ such that y is the value the formula assigns to (n, x) , is a set by (Z6) of Axiom 1.1.1 inside a product (Proposition 1.2.2), and (Fn1), (Fn2) say exactly that the formula gives one value in X for each pair.

Warning. The hypothesis that g takes its values in X cannot be dropped. Let $X = \{0\}$, $a = 0$, and $g(n, x) := S(0)$ for $n \in \omega$, $x \in X$, so that g maps $\omega \times X$ into ω but not into X . Any $f: \omega \rightarrow X$ with the two equations would need $f(S(0)) = g(0, f(0)) = S(0)$, and $S(0) \notin X$ since $S(0) \neq 0$ by (P3) of Theorem 1.4.2; so no such f exists. The proof breaks in Step 3, where the added pair $(S(n), g(n, f_n(n)))$ must lie in $S(S(n)) \times X$.

1.5.2 Addition and multiplication

With the theorem, addition is the old school definition made official. To add n to m , start at m and take n successor steps: $m + 0$ is m , and $m + S(n)$ is one step further than $m + n$. Multiplication is repeated addition in the same way.

Adding n to m is taking n successor steps from m .

Definition 1.5.1. Addition and Multiplication on ω

- (a) For each $m \in \omega$, let $A_m: \omega \rightarrow \omega$ be the function given by Theorem 1.5.1 with $X = \omega$, $a = m$ and $g(n, x) = S(x)$. The **sum** of m and n is $m + n := A_m(n)$. Thus, for all $m, n \in \omega$,

$$m + 0 = m, \quad m + S(n) = S(m + n).$$

- (b) For each $m \in \omega$, let $M_m: \omega \rightarrow \omega$ be the function given by Theorem 1.5.1 with $X = \omega$, $a = 0$ and $g(n, x) = x + m$. The **product** of m and n is $m \cdot n := M_m(n)$, also written mn . Thus, for all $m, n \in \omega$,

$$m \cdot 0 = 0, \quad m \cdot S(n) = m \cdot n + m.$$

- (c) The **numerals** are $0 := \emptyset$ and $1 := S(0)$, $2 := S(1)$, $3 := S(2)$, and so on, as in Example (The first natural numbers as sets). For every $n \in \omega$, $n + 1 = S(n)$; in particular $1 + 1 = 2$ and $k + 2 = (k + 1) + 1$ for every $k \in \omega$.

In words: (a) and (b) are the two clauses we would write for a school definition, and the theorem guarantees that they define exactly one function A_m , respectively M_m , for each m . Multiplication binds more tightly than addition, so $m \cdot n + m$ is $(m \cdot n) + m$.

Well-definedness. Three things need checking. First, each g is a function $\omega \times \omega \rightarrow \omega$ (the remark above): $S(x) \in \omega$ for $x \in \omega$ by (P2) of Theorem 1.4.2, and $x + m \in \omega$ because A_x maps into ω . So (b) uses (a), and (a) uses nothing but the successor. Second, $+$ is a function $\omega \times \omega \rightarrow \omega$: its graph is the set of $((m, n), k) \in (\omega \times \omega) \times \omega$ such that $k = A(n)$ for some function $A: \omega \rightarrow \omega$ with $A(0) = m$ and $A(S(j)) = S(A(j))$ for every $j \in \omega$; this is a set by (Z6) of Axiom 1.1.1, and each (m, n) gets exactly one k because A_m exists and is unique. The same holds for $\cdot$. Third, nothing was chosen: each A_m and M_m is the only function with its property.

The successor is “plus one”. Proof of the last sentence of (c): for every $n \in \omega$,

$$n + 1 = n + S(0) = S(n + 0) = S(n),$$

by (c) and the two equations of (a). From now on we write $n + 1$ for $S(n)$ whenever $n \in \omega$; the defining equations then read as in school:

$$\begin{aligned} m + 0 &= m, & m + (n + 1) &= (m + n) + 1, \\ m \cdot 0 &= 0, & m \cdot (n + 1) &= m \cdot n + m. \end{aligned}$$

Two small computations are used repeatedly later: $1 + 1 = S(1) = 2$, and, for every $k \in \omega$,

$$k + 2 = k + S(1) = S(k + 1) = (k + 1) + 1.$$

A non-example by minimal change: keep $a = m$ in (a), but replace $g(n, x) = S(x)$ by $g(n, x) = S(n)$, which ignores the current value. This g is still a function $\omega \times \omega \rightarrow \omega$, so Theorem 1.5.1 gives exactly one $f: \omega \rightarrow \omega$ with $f(0) = m$ and $f(S(n)) = S(n)$. The first equation $m + 0 = m$ still

holds for this “sum”, but the second, $m + S(n) = S(m + n)$, fails: with $m = 2$, $f(1) = S(0) = 1$, while $S(f(0)) = S(2) = 3$. So it would give $2 + 1 = 1$, and it is not addition.

The defining equations immediately give the two Peano facts in the “plus one” notation.

Corollary 1.5.2. Successor Cancellation

For all $k, l \in \omega$: if $k + 1 = l + 1$, then $k = l$; and $k + 1 \neq 0$.

Proof. By (c) of Definition 1.5.1, $k + 1 = S(k)$ and $l + 1 = S(l)$. So the first claim is (P4) of Theorem 1.4.2, and the second is (P3). ■

Quick check. Compute $2 + 2$ and $2 \cdot 2$ from the defining equations alone.

Solution. By (a) of Definition 1.5.1, three times,

$$2 + 2 = S(2 + 1) = S(S(2 + 0)) = S(S(2)) = S(3) = 4.$$

By (b), twice and then at 0,

$$2 \cdot 2 = 2 \cdot 1 + 2 = (2 \cdot 0 + 2) + 2 = (0 + 2) + 2,$$

and $0 + 2 = S(0 + 1) = S(S(0 + 0)) = S(S(0)) = 2$. So $2 \cdot 2 = 2 + 2 = 4$.

1.5.3 The laws of arithmetic

Every law of arithmetic that *Sets, Relations, and Cardinality*, Chapter 2 took from the real numbers must now be proved, and the only tools are the four defining equations and induction. The equations are lopsided: they say what happens when the **second** argument goes up by one, and nothing about the first. So in every induction below we fix all variables but one and induct on the variable that the recursion runs on, the second argument of $+$ or $\cdot$.

Theorem 1.5.3. Laws of Arithmetic on ω

For all $k, m, n \in \omega$:

- (a) $0 + n = n$, and $(m + 1) + n = (m + n) + 1$;
- (b) $m + n = n + m$;
- (c) $(k + m) + n = k + (m + n)$;
- (d) $m(n + k) = mn + mk$ and $(n + k)m = nm + km$;
- (e) $0 \cdot n = 0$, $(m + 1) \cdot n = mn + n$, and $n \cdot 1 = 1 \cdot n = n$;
- (f) $mn = nm$;
- (g) $(km)n = k(mn)$.

Idea. The move is **fix the others, induct on the recursion variable**: in $m + n$ and $m \cdot n$ the recursion runs on n , so we fix m (and k) and induct on n . Then the base case is a defining equation at 0, and the step can open $m + (n + 1)$ or $m \cdot (n + 1)$ by the other defining equation, apply the induction hypothesis inside, and close up again. The order of the clauses matters: commutativity (b) needs the two facts (a) about the **first** argument, which no defining equation provides.

Proof. Each clause except the second half of (d) and the last part of (e), which the table derives from earlier clauses without induction, is proved by Theorem 1.3.3 (b), applied to the property of n stated in the clause, with the other variables fixed; for the first half of (d) the variable is k , the recursion variable of $m(n + k)$. “Def” refers to the equations of Definition 1.5.1, “IH” to the induction hypothesis.

We prove (c), associativity of addition, in full. Fix $k, m \in \omega$, and let $P(n)$ be “ $(k + m) + n = k + (m + n)$ ”. *Base case*: by the first equation of (a) of Definition 1.5.1, applied twice,

$$(k + m) + 0 = k + m = k + (m + 0).$$

Inductive step: suppose $P(n)$. Then

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

where the first equality is Def with first argument $k + m$, the second is $P(n)$, the third is Def with first argument k and second argument $m + n$, and the fourth is Def with first argument m . So $P(n + 1)$ holds, and by Theorem 1.3.3 (b), $P(n)$ holds for every $n \in \omega$.

The other clauses follow the same pattern; the table gives, for each, the property inducted on, the base case, the step, and the earlier clauses used. They are proved in the order of the table, so each row uses only rows above it.

Clause, variable	Base case	Inductive step (IH at the marked equality)	Uses
(a) $0 + n = n$; on n	$0 + 0 = 0$ (Def)	$0 + (n + 1) =$ $(0 + n) + 1 \stackrel{\text{IH}}{=} n + 1$	Def
(a) $(m + 1) + n =$ $(m + n) + 1$; m fixed, on n	both sides are $m + 1$ (Def)	$(m + 1) + (n + 1) =$ $((m + 1) + n) + 1 \stackrel{\text{IH}}{=}$ $((m + n) + 1) + 1 =$ $(m + (n + 1)) + 1$	Def
(b) $m + n = n + m$; m fixed, on n	$m + 0 = m = 0 + m$	$m + (n + 1) =$ $(m + n) + 1 \stackrel{\text{IH}}{=} (n +$ $m) + 1 = (n + 1) + m$	Def; (a), both halves
(c)	in full above		Def

(d)	$m(n+0) = mn =$	$m(n+(k+1)) =$	Def; (c)
$m(n+k) = mn+mk;$	$mn+0 = mn+m \cdot 0$	$m((n+k)+1) =$	
m, n fixed, on k		$m(n+k) + m \stackrel{\text{IH}}{=} (mn+mk) + m =$	
		$mn + (mk+m) =$	
		$mn + m(k+1)$	
(e) $0 \cdot n = 0;$ on n	$0 \cdot 0 = 0$ (Def)	$0 \cdot (n+1) =$	Def
		$0 \cdot n + 0 \stackrel{\text{IH}}{=} 0 + 0 = 0$	
(e)	$(m+1) \cdot 0 = 0 =$	$(m+1)(n+1) =$	Def; (b), (c)
$(m+1)n = mn+n;$	$0+0 = m \cdot 0 + 0$	$(m+1)n + (m+1) \stackrel{\text{IH}}{=} (mn+n) + (m+1) =$	
m fixed, on n		$mn + (n + (m+1)) =$	
		$mn + ((n+m)+1) =$	
		$mn + ((m+n)+1) =$	
		$mn + (m + (n+1)) =$	
		$(mn+m) + (n+1) =$	
		$m(n+1) + (n+1)$	
(e) $n \cdot 1 = n,$		$n \cdot 1 = n \cdot 0 + n =$	Def; (a); first two
$1 \cdot n = n;$ no		$0 + n = n;$	parts of (e)
induction		$1 \cdot n = (0+1) \cdot n =$	
		$0 \cdot n + n = 0 + n = n$	
(f) $mn = nm;$ m	$m \cdot 0 = 0 = 0 \cdot m$	$m(n+1) = mn+m \stackrel{\text{IH}}{=} nm+m = (n+1)m$	Def; (e)
fixed, on n		$(n+k)m =$	(d), first half; (f)
(d), second half; no		$m(n+k) =$	
induction		$mn+mk = nm+km$	
(g) $(km)n = k(mn);$	$(km) \cdot 0 = 0 =$	$(km)(n+1) =$	Def; (d)
k, m fixed, on n	$k \cdot 0 = k(m \cdot 0)$	$(km)n + km \stackrel{\text{IH}}{=} k(mn) + km =$	
		$k(mn+m) =$	
		$k(m(n+1))$	

In the step of (a), second half, the third equality is $(m+n)+1 = m+(n+1)$ (Def), read inside the outer $+1$; in the step of (b), the last equality is (a), second half, read from right to left. In the long step of (e), the equalities after IH use, in order, (c), Def, (b), Def, (c), Def. In the second half of (e), $1 = 0+1$ is the first half of (a), and $(0+1) \cdot n = 0 \cdot n + n$ is the second part of (e) with $m = 0$. In (g), $k(mn+m) = k(mn) + km$ is the first half of (d). This proves the theorem. ■

The laws (a)–(g) are the rules of school arithmetic for $+$ and $\cdot$ on the natural numbers, now proved from the seven axioms for sets. The next section defines the order of ω and ties it to them: $m \leq n$ exactly when $n = m + j$ for some $j \in \omega$.

Warning. Do not assume $0+n = n$. It is clause (a) of [Theorem 1.5.3](#), proved by induction; the defining equation is $n+0 = n$. For the same reason, inducting on m in $m+n = n+m$ gets stuck: the step would need $(m+1)+n$, and the definition says nothing about a sum

whose **first** argument is a successor until (a) is proved.

The order of the table is forced by the lopsided definition. Commutativity, which lets us move a successor from the second place to the first, comes only after the two facts in (a) that move it by hand; once it is available, (e) and (f) follow the same way for multiplication.

1.5.4 Exercises

1.5.4.1 A. Check your understanding

Exercise. A1

These questions are about the proof of [Theorem 1.5.1](#).

- (a) Where in the proof is $S(n) \notin S(n)$ used, and what would fail without it?
- (b) Run the construction for $X = \omega$, $a = 0$ and $g(n, x) = S(S(x))$: write the graphs of the partial solutions up to 0, 1 and 2.
- (c) Why does the uniqueness half need only an induction, while existence needs partial solutions?
- (d) State the idea of the proof in two sentences.

Solution.

- (a) In the inductive step of Step 3, in checking (Fn2) for the extended graph G' . The added pair has first coordinate $S(n)$, and every first coordinate in G_n lies in $S(n)$; because $S(n) \notin S(n)$, the input $S(n)$ is new, so adding the pair cannot give an old input a second output. If $S(n)$ were an element of $S(n)$, then G_n would already contain a pair $(S(n), y)$, and G' would contain both it and $(S(n), g(n, f_n(n)))$, so G' might fail to be a function.
- (b) Here $g(n, x) = S(S(x))$ adds two steps. The partial solution up to 0 has graph $\{(0, 0)\}$. The next adds the pair at $S(0) = 1$ with value $g(0, 0) = S(S(0)) = 2$: the graph up to 1 is $\{(0, 0), (1, 2)\}$. The next adds the pair at 2 with value $g(1, 2) = S(S(2)) = 4$: the graph up to 2 is $\{(0, 0), (1, 2), (2, 4)\}$. Each graph contains the previous one, as Step 3 says.
- (c) Uniqueness compares two functions that are **given**, value by value, and comparing values at $n + 1$ through the values at n is exactly an induction on n . Existence asks for a function that is not given; induction proves statements and builds nothing. So the proof proves by induction a statement (the claim of Step 3) about finite pieces, and builds f from them as a union, using (Z4).
- (d) For each n , induction shows that there is exactly one function on $S(n)$ obeying the equations, and any two of these agree at every point k where both are defined, because on $S(k)$ each restricts to the unique one up to k . Their union is the required function, and an induction shows there is no other.

1.5.4.2 B. Practice

Exercise. B1: Small products

Compute $3 \cdot 2$ and $2 \cdot 3$ from the defining equations of [Definition 1.5.1](#) alone, without using [Theorem 1.5.3](#). Here $5 := S(4)$ and $6 := S(5)$.

Solution. For $3 \cdot 2$, by (b) twice and then at 0:

$$3 \cdot 2 = 3 \cdot 1 + 3 = (3 \cdot 0 + 3) + 3 = (0 + 3) + 3.$$

By (a), $0 + 3 = S(0 + 2) = S(S(0 + 1)) = S(S(S(0 + 0))) = S(S(S(0))) = 3$. Then

$$3 + 3 = S(3 + 2) = S(S(3 + 1)) = S(S(S(3 + 0))) = S(S(S(3))) = 6.$$

So $3 \cdot 2 = 6$.

For $2 \cdot 3$, by (b), $2 \cdot 3 = 2 \cdot 2 + 2$, and $2 \cdot 2 = 4$ by the Quick check above. Then

$$4 + 2 = S(4 + 1) = S(S(4 + 0)) = S(S(4)) = 6.$$

So $2 \cdot 3 = 6 = 3 \cdot 2$, as (f) of [Theorem 1.5.3](#) predicts; but the two computations took different routes, and neither used a law.

Exercise. B2: Distributivity, last step blank

Here is the proof of $m(n + k) = mn + mk$ for all $m, n, k \in \omega$, with the last step left blank. Name the move, then complete it.

Fix $m, n \in \omega$ and induct on k . Base case: $m(n + 0) = mn = mn + 0 = mn + m \cdot 0$.

Inductive step: suppose $m(n + k) = mn + mk$. Then

$$m(n + (k + 1)) = m((n + k) + 1) = m(n + k) + m = (mn + mk) + m = \underline{\hspace{2cm}}.$$

Justify each equality you add.

Solution. The move is **fix the others, induct on the recursion variable**: in $m(n + k)$ the recursion of $+$ runs on k , so m and n are fixed and the induction is on k .

The completion is

$$(mn + mk) + m = mn + (mk + m) = mn + m(k + 1),$$

where the first equality is associativity, (c) of [Theorem 1.5.3](#), and the second is the defining equation $m(k + 1) = mk + m$ of [Definition 1.5.1](#) (b), read from right to left. This is the statement for $k + 1$, so by [Theorem 1.3.3](#) (b) it holds for every $k \in \omega$. (This is clause (d) of [Theorem 1.5.3](#), already proved; the exercise practices the move.)

1.5.4.3 C. Going deeper

Exercise. C1: Exit check: addition is commutative

From the two defining equations of addition, $m + 0 = m$ and $m + (n + 1) = (m + n) + 1$, and

Theorem 1.3.3 alone, prove that $m + n = n + m$ for all $m, n \in \omega$. Prove every auxiliary fact you need.

Solution (Hint 1). The definition says what happens when the second argument is 0 or a successor. To use it on $n + m$, you need to know the same for the first argument: prove two lemmas first.

Solution (Hint 2). The lemmas are $0 + n = n$ and $(m + 1) + n = (m + n) + 1$, each by induction on n .

Solution. All inductions are by Theorem 1.3.3 (b).

Lemma 1: $0 + n = n$ for every n . Induct on n . Base: $0 + 0 = 0$, by the first equation. Step: if $0 + n = n$, then $0 + (n + 1) = (0 + n) + 1 = n + 1$, by the second equation and the hypothesis.

Lemma 2: $(m + 1) + n = (m + n) + 1$ for all m, n . Fix m and induct on n . Base: $(m + 1) + 0 = m + 1 = (m + 0) + 1$, by the first equation twice. Step: if $(m + 1) + n = (m + n) + 1$, then

$$(m + 1) + (n + 1) = ((m + 1) + n) + 1 = ((m + n) + 1) + 1 = (m + (n + 1)) + 1,$$

by the second equation, the hypothesis, and the second equation read from right to left inside the outer $+1$.

Main induction. Fix m and induct on n for “ $m + n = n + m$ ”. Base: $m + 0 = m = 0 + m$, by the first equation and Lemma 1. Step: if $m + n = n + m$, then

$$m + (n + 1) = (m + n) + 1 = (n + m) + 1 = (n + 1) + m,$$

by the second equation, the hypothesis, and Lemma 2 (with n in the role of m and m in the role of n), read from right to left. Hence $m + n = n + m$ for all $m, n \in \omega$.

Marking scheme. (10 points) - 2: proves $0 + n = n$ by induction on n , from the first equation (base) and the second (step). - 3: proves, by an induction with the other variable fixed, a lemma that moves a successor out of the first argument (the book’s $(m + 1) + n = (m + n) + 1$, or $1 + n = n + 1$ together with associativity of addition), base and step both justified. - 2: in the main induction, the base case $m + 0 = 0 + m$, using the first lemma. - 2: in the main induction, the step, using the second equation, the hypothesis and that lemma. - 1: names the variable inducted on in each induction and fixes the other. Fatal errors (0 for the step): citing commutativity, or any law of [Theorem 1.5.3](#), without proving it from the two equations; treating $0 + n = n$ as if it were a defining equation. A second route inducts on m in the main induction with n fixed; it needs the same two lemmas, and its base and step map to the same 2 + 2 points. A third route proves associativity and $1 + n = n + 1$ (each by induction on n , from the equations and $0 + n = n$) and then closes the step as $m + (n + 1) = (m + n) + 1 = (n + m) + 1 = n + (m + 1) = n + (1 + m) = (n + 1) + m$; those two lemmas together earn the 3 points.

Exercise. C2: Associativity of multiplication, last half blank

Prove that $(km)n = k(mn)$ for all $k, m, n \in \omega$. The first half is given; *name the move, then complete it.*

Fix $k, m \in \omega$ and induct on n . Base case: $(km) \cdot 0 = 0 = k \cdot 0 = k(m \cdot 0)$. Inductive step: _____

You may use (a)–(f) of [Theorem 1.5.3](#).

Solution. The move is **fix the others, induct on the recursion variable**: in $(km)n$ and $k(mn)$ the variable n is the second argument of the outer and the inner product, where the recursion runs, so k and m are fixed.

Inductive step. Suppose $(km)n = k(mn)$. Then

$$\begin{aligned} (km)(n+1) &= (km)n + km = k(mn) + km \\ &= k(mn + m) = k(m(n+1)), \end{aligned}$$

where the first equality is the defining equation of [Definition 1.5.1](#) (b) with first factor km , the second is the induction hypothesis, the third is (d) of [Theorem 1.5.3](#) read from right to left ($k(x+y) = kx + ky$ with $x = mn$, $y = m$), and the fourth is the defining equation with first factor m . By [Theorem 1.3.3](#) (b), $(km)n = k(mn)$ for every n , and k, m were arbitrary.

The base case used the defining equation $x \cdot 0 = 0$ three times, with $x = km$, $x = k$ and $x = m$. Commutativity (f) is not needed for this route; a proof that first rewrites km as mk would need it.

Exercise. C3: Doubling

Show that there is exactly one function $D: \omega \rightarrow \omega$ with $D(0) = 0$ and $D(n+1) = (D(n)+1)+1$ for every $n \in \omega$, and prove that $D(n) = n + n$ for every $n \in \omega$.

Solution. Existence and uniqueness. The function $g: \omega \times \omega \rightarrow \omega$, $g(n, x) := S(S(x)) = (x+1)+1$, maps into ω by (P2) of [Theorem 1.4.2](#) applied twice. By [Theorem 1.5.1](#) with $X = \omega$ and $a = 0$, there is exactly one $D: \omega \rightarrow \omega$ with $D(0) = 0$ and $D(n+1) = g(n, D(n)) = (D(n)+1)+1$. (Its partial solutions up to 0, 1, 2 are those of [Exercise \(A1\)](#) (b), so $D(1) = 2$ and $D(2) = 4$.)

The formula. Induct on n by [Theorem 1.3.3](#) (b) for “ $D(n) = n + n$ ”. Base: $D(0) = 0 = 0 + 0$, by the defining equation $m + 0 = m$. Step: suppose $D(n) = n + n$. Then

$$\begin{aligned} (n+1) + (n+1) &= ((n+1) + n) + 1 = ((n+n) + 1) + 1 \\ &= (D(n) + 1) + 1 = D(n+1), \end{aligned}$$

where the first equality is the defining equation of [Definition 1.5.1](#) (a), the second is (a) of [Theorem 1.5.3](#), $(m+1) + n = (m+n) + 1$ with $m = n$, the third is the hypothesis, and the last is the equation of D . Hence $D(n) = n + n$ for every $n \in \omega$.

Alternatively, $n \mapsto n + n$ satisfies the two equations that define D (the computation above,

read without the hypothesis, shows $(n + 1) + (n + 1) = ((n + n) + 1) + 1$, so it is D by the uniqueness half of [Theorem 1.5.1](#). Either way the double $n + n$ is $2n$ too: $2n = n \cdot 2 = n \cdot 1 + n = n + n$ by (f), the defining equation of $\cdot$, and (e) of [Theorem 1.5.3](#).