

2.5 Equinumerous Sets and Finite Sets

Section 1.1 left a puzzle half solved: among any five lattice points, two have a lattice point as midpoint, provided that five objects in four boxes always put two in one box. That principle sounds too obvious to need proof, but it is a statement about every finite collection, and “finite” has no definition yet. Section 1.6 supplied the tool: a bijection pairs the elements of two sets one for one. This section makes “the same size” mean “there is a bijection”, defines finite sets by pairing with $\{1, \dots, n\}$, proves the pigeonhole principle and comes back to the five points, and then proves the facts about finite sets on which counting rests. Whether $\mathbb{Q}$ is larger than $\mathbb{N}$ is the question of Chapter 3.

2.5.1 Same size without counting

So far we have compared functions; now we compare sets. The everyday word is “as many as”, and we can check it without knowing any numbers. Put two piles of coins on a table, and take one coin from each pile at a time, setting the two aside as a pair. If both piles run out at the same moment, they had the same number of coins. We know this before counting either pile, and a child who cannot count past ten can do it with piles of a thousand. Section 1.6 proved that the bijections are exactly the maps with a two-sided inverse (Theorem 1.6.4), and said that such a pairing is how this book says “the same size”.

The pairing is a function from the first pile to the second. Different coins are paired with different coins, so it is injective; every coin of the second pile is used, so it is surjective. Pairing makes sense for any two sets, finite or not, and that is the definition.

Same size means there is a pairing.

Definition 2.5.1. Equinumerous Sets

Let A and B be sets. We say that A and B are **equinumerous**, and write $|A| = |B|$, if **there exists** a bijection $f: A \rightarrow B$. In symbols,

$$|A| = |B| \iff \exists f \in B^A \ (f \text{ is injective} \wedge f \text{ is surjective}).$$

In words: the definition asks for **one** bijection, and it does not care which. Injectivity says that no two elements of A are paired with the same element of B ; surjectivity says that no element of B is left over. The statement $|A| = |B|$ is read as a whole, “ A and B are equinumerous”. It is a relation between two sets. We do not define an object $|A|$, “the size of A ”, standing alone, and a second-reading fold below explains why the obvious candidate is not available. For finite sets, the definition of a finite set below gives $|A|$ a meaning as a natural number, and the two uses agree.

Here are four examples, the degenerate one first.

- *The empty set.* The empty function $\emptyset \rightarrow \emptyset$ of Proposition 1.5.2 (a) is injective and surjective, vacuously: there are no two inputs to compare and no output to reach. So $|\emptyset| = |\emptyset|$. Conversely, if $|A| = |\emptyset|$, there is a function $A \rightarrow \emptyset$, so $A = \emptyset$ by Proposition 1.5.2 (b). The empty set is equinumerous with itself and with nothing else. This case is the test case for every statement below about sets “with n elements”, at $n = 0$.
- *Three letters and three numbers.* Let a, b, c be three different letters. The function $\{a, b, c\} \rightarrow \{1, 2, 3\}$ with $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 3$ sends different letters to different numbers and reaches each of 1, 2, 3. So $|\{a, b, c\}| = |\{1, 2, 3\}|$.

- *Two intervals of different lengths.* The function $f: [0, 1] \rightarrow [0, 2]$, $f(x) = 2x$, has the inverse $y \mapsto y/2$, since $y/2 \in [0, 1]$ for $y \in [0, 2]$, $f(y/2) = y$ and $f(x)/2 = x$. By Theorem 1.6.4 it is a bijection, so $|[0, 1]| = |[0, 2]|$. Length and size are different things.
- *The natural numbers and the positive integers.* The function $\mathbb{N} \rightarrow \mathbb{Z}_{>0}$, $n \mapsto n + 1$, is a bijection. It is the Quick check near the end of this section, where it shows that $\mathbb{N}$ is infinite.

Quick check. Decide, from Definition 2.5.1: (a) $|\emptyset| = |\{\emptyset\}|$? (b) $|\{1, 2\}| = |\{\{1, 2\}\}|$? (c) $|\{x \in \mathbb{R} : x^2 = -1\}| = |\emptyset|$?

Solution.

- (a) No. The set $\{\emptyset\}$ has the element $\emptyset$, and a function $\emptyset \rightarrow \{\emptyset\}$ has no values, so it is not surjective. (b) No. The set $\{\{1, 2\}\}$ has one element, so every function $\{1, 2\} \rightarrow \{\{1, 2\}\}$ sends 1 and 2 to it and is not injective. (c) Yes. The set $\{x \in \mathbb{R} : x^2 = -1\}$ is empty, and the empty function $\emptyset \rightarrow \emptyset$ is a bijection.

A non-example by a minimal change. Shrink $\{1, 2, 3\}$ to $\{1, 2\}$. There is no bijection $\{a, b, c\} \rightarrow \{1, 2\}$. Let g be any function $\{a, b, c\} \rightarrow \{1, 2\}$. If $g(a) = g(b)$, then g is not injective. Otherwise $g(a)$ and $g(b)$ are 1 and 2 in some order, and $g(c)$, which is 1 or 2, equals one of them. In every case two different letters share a value. So the clause that fails is injectivity, and it fails for **every** function, which is what “not equinumerous” requires. Surjectivity can hold: $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 2$ reaches both numbers.

Warning. To show that two sets are **not** equinumerous, one map is never enough. The map $x \mapsto x$ from $[0, 1]$ to $[0, 2]$ is not surjective, since 2 is not a value, and yet $|[0, 1]| = |[0, 2]|$ by the map $x \mapsto 2x$ above. “Not equinumerous” is a statement about **all** functions, $\forall f \in B^A \neg(f \text{ bijective})$, and a proof of it must deal with an arbitrary f , as the non-example did.

Why this definition. To count a set is to pair it with $\{1, \dots, n\}$: saying “one, two, three” while pointing at the coins is a bijection from $\{1, 2, 3\}$ onto the pile. So the definition does not replace counting; it isolates the part of counting that still makes sense when the set is infinite. Each clause has a job. Without injectivity, the surjection $\{1, 2, 3\} \rightarrow \{1\}$ would make a three-element set as large as a one-element set. Without surjectivity, the inclusion $\{1\} \rightarrow \{1, 2, 3\}$ would do the same in the other direction.

The first result says that equinumerosity behaves like equality: reflexive, symmetric and transitive.

Proposition 2.5.1. Equinumerosity Is Reflexive, Symmetric and Transitive

For all sets A , B and C :

- (a) $|A| = |A|$;
- (b) if $|A| = |B|$, then $|B| = |A|$;
- (c) if $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.

Proof. (a) The identity id_A is injective, since $\text{id}_A(x) = \text{id}_A(y)$ says $x = y$, and surjective, since every $x \in A$ is $\text{id}_A(x)$.

(b) Let $f: A \rightarrow B$ be a bijection. By Theorem 1.6.4 it has a two-sided inverse $f^{-1}: B \rightarrow A$, with $f^{-1} \circ f = \text{id}_A$ and $f \circ f^{-1} = \text{id}_B$. Read with the roles exchanged, these two equations say that f is a two-sided inverse of f^{-1} (Definition 1.6.2). So f^{-1} is a bijection $B \rightarrow A$, by Theorem 1.6.4 again.

(c) If $f: A \rightarrow B$ and $g: B \rightarrow C$ are bijections, then $g \circ f: A \rightarrow C$ is a bijection by Theorem 1.5.4 (c). This proves the proposition. ■

Clauses (a)–(c) say that equinumerosity behaves like an equivalence relation: reflexive, symmetric and transitive, as equality is. We do not call it one. Chapter 4 makes “equivalence relation” precise for relations **on a set** X , subsets of $X \times X$; equinumerosity relates any two sets whatever, and there is no set of all sets for it to live on (Theorem 1.2.4). That is also why the book writes $|A| = |B|$ here and keeps the symbol $\sim$ for later.

🕒 **Second reading** · Why $|A|$ is not an object

Remark. Why not define $|A|$ as “the collection of all sets equinumerous with A ”? Because that collection is in general not a set. The next paragraph proves this for $A = \{0\}$.

Take $A = \{0\}$. Every singleton $\{x\}$ is equinumerous with $\{0\}$, by $0 \mapsto x$. If the singletons formed a set $\mathcal{S}$, its union $\bigcup \mathcal{S}$ would be a set by (W3) of Section 1.2, and every object x would be an element of it, since $x \in \{x\} \in \mathcal{S}$. That is a set of which every set is an element, which Theorem 1.2.4 rules out.

2.5.2 Finite sets

Counting is pairing with $\{1, \dots, n\}$, so “finite” is defined by such a pairing. Recall from Section 2.1 that for $n \in \mathbb{N}$,

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

so that $\{1, \dots, 0\} = \emptyset$, since no k has $1 \leq k \leq 0$.

Definition 2.5.2. Finite Set, Number of Elements

Let A be a set and $n \in \mathbb{N}$. We say that A **has n elements** if $|\{1, \dots, n\}| = |A|$, that is, if **there exists** a bijection $\varphi: \{1, \dots, n\} \rightarrow A$. The set A is **finite** if it has n elements for **some** $n \in \mathbb{N}$. In that case we write $|A| = n$.

In words: φ numbers the elements of A as $\varphi(1), \varphi(2), \dots, \varphi(n)$. Injectivity says that no element gets two numbers; surjectivity says that every element gets one. So a non-empty finite set is $A = \{\varphi(1), \dots, \varphi(n)\}$, a list without repetitions. By Proposition 2.5.1 (b), “ A has n elements”

is the same as $|A| = |\{1, \dots, n\}|$, so the notation $|A| = n$ is consistent with the relation of [Definition 2.5.1](#).

There is a gap in the notation $|A| = n$. It presents n as **the** number of elements, but the definition only says that **some** n works. Could a set have 3 elements and also 4? It cannot, and a corollary of the pigeonhole principle below proves it. That corollary is the well-definedness step this definition needs. Until it is proved, read $|A| = n$ as “ A has n elements”.

Examples:

- The empty set has 0 elements: $\{1, \dots, 0\} = \emptyset$, and the empty function $\emptyset \rightarrow \emptyset$ is a bijection. Conversely, a set with 0 elements is empty, since a bijection $\emptyset \rightarrow A$ is surjective and has no values.
- $\{1, \dots, n\}$ has n elements, by $\text{id}_{\{1, \dots, n\}}$.
- For $n \in \mathbb{N}$, $\{0, \dots, n\}$ has $n + 1$ elements: $k \mapsto k - 1$ maps $\{1, \dots, n + 1\}$ to $\{0, \dots, n\}$, because $k - 1 \in \mathbb{N}$ for $k \neq 0$ (Lemma 2.1.1 (c)) and $k - 1 \leq n$. It has the inverse $j \mapsto j + 1$, so it is a bijection (Theorem 1.6.4).
- The three-letter set $\{a, b, c\}$ has 3 elements, by the inverse of the bijection of the second example after [Definition 2.5.1](#).

Quick check. How many elements does $\{n \in \mathbb{N} : 3 \leq n \leq 7\}$ have? Give the bijection.

Solution. Five, by $k \mapsto k + 2$ from $\{1, \dots, 5\}$: for $1 \leq k \leq 5$, $3 \leq k + 2 \leq 7$. Its inverse is $m \mapsto m - 2$, which lies in $\{1, \dots, 5\}$ for $3 \leq m \leq 7$, since $m - 2 \in \mathbb{N}$ by Lemma 2.1.1 (d). The two maps undo each other, so the first is a bijection (Theorem 1.6.4).

Definition 2.5.3. Infinite Set

A set A is **infinite** if it is not finite: **for every** $n \in \mathbb{N}$ there is **no** bijection $\{1, \dots, n\} \rightarrow A$.

To prove a set infinite we must rule out every n at once, and for every n every candidate bijection. Nothing so far does that, not even for $\mathbb{N}$. The tool is the pigeonhole principle, and the last theorem of this section turns it into a usable test.

Shrinking the codomain. One small device is used in the rest of this section and in Chapter 3. Let $f: X \rightarrow Y$ be a function, and let $C \subseteq Y$ contain every value $f(x)$. The graph of f is then a subset of $X \times C$, and with the codomain C it is a function $X \rightarrow C$ with the same values (Definition 1.5.1). We call it “ f with codomain C ”. It is injective if and only if f is, since injectivity speaks only of values. In particular, f with codomain $f(X)$ is surjective (Definition 1.7.1). So an **injective** $f: X \rightarrow Y$ is a bijection $X \rightarrow f(X)$ once its codomain is shrunk, and $|X| = |f(X)|$.

2.5.3 Back to the pigeons

Section 1.1 reduced its question (Q1) to one step: five points, each with one of four parity patterns, put two points on one pattern. In the language of functions, sending each point to its pattern is a map from a five-element set to a four-element set, and the step says that it is not injective. Chapter 1 also found one function from a three-element set to a two-element set that is not injective (Example (Deciding injective and surjective) (c)), and observed without proof

that none can be. Here is the general fact, for the standard sets $\{1, \dots, m\}$ and $\{1, \dots, n\}$.

Theorem 2.5.2. Pigeonhole Principle

Let $m, n \in \mathbb{N}$ with $m > n$. Then there is **no** injection $\{1, \dots, m\} \rightarrow \{1, \dots, n\}$.

Idea (Scratch work). Induct on the number n of holes. In the step there are $n + 1$ holes, and we look at the last one. If no pigeon sits in hole $n + 1$, all the pigeons sit in n holes, and the hypothesis applies at once. If pigeon j sits there, there is only one, by injectivity. Move pigeon j to the hole of pigeon m , and send pigeon m away. That leaves $m - 1$ pigeons in n holes, still one to a hole, and $m - 1 > n$. The hypothesis is used at $m - 1$, not at m , so the property we induct on must say “for every m ”.

On scrap paper, with $n = 1$ and $m = 3$: three pigeons in two holes; if hole 2 is empty, all three sit in hole 1; if pigeon 2 sits in hole 2, move it to pigeon 3’s place and send pigeon 3 away. As givens and goal, inside the step:

Givens	Goal
$P(n)$; $m > n + 1$; $f: \{1, \dots, m\} \rightarrow \{1, \dots, n + 1\}$ injective Case 1: $n + 1$ is no value of f	a contradiction f with codomain $\{1, \dots, n\}$ is injective, $m > n$: against $P(n)$
Case 2: $f(j) = n + 1$	an injection $\{1, \dots, m - 1\} \rightarrow \{1, \dots, n\}$, with $m - 1 > n$: $g := f \circ \sigma$

Before reading on: self-explain the construction of the injection g in Case 2: why are its values in $\{1, \dots, n\}$, and why is it injective?

Proof. For $n \in \mathbb{N}$ let $P(n)$ be the statement

for every $m \in \mathbb{N}$ with $m > n$, there is no injection $\{1, \dots, m\} \rightarrow \{1, \dots, n\}$.

We prove $P(n)$ for every $n \in \mathbb{N}$ by Logic and Proof, Axiom 4.2.1.

Base case $P(0)$. Let $m \in \mathbb{N}$ with $m > 0$. Then $m \geq 1$ (Lemma 2.1.1 (a)), so $1 \in \{1, \dots, m\}$ and the domain is non-empty, while $\{1, \dots, 0\} = \emptyset$. By Proposition 1.5.2 (b) there is no function $\{1, \dots, m\} \rightarrow \emptyset$ at all, so there is no injection.

Inductive step. Let $n \in \mathbb{N}$ and suppose $P(n)$. Let $m \in \mathbb{N}$ with $m > n + 1$, and suppose, for a contradiction, that $f: \{1, \dots, m\} \rightarrow \{1, \dots, n + 1\}$ is injective. There are two cases.

Case 1: $n + 1$ is not a value of f . For every i , $f(i) \leq n + 1$ and $f(i) \neq n + 1$, so $f(i) < n + 1$, and $f(i) \leq n$ by Lemma 2.1.1 (e). So f with codomain $\{1, \dots, n\}$ is an injection $\{1, \dots, m\} \rightarrow \{1, \dots, n\}$, with $m > n + 1 > n$. This contradicts $P(n)$.

Case 2: $f(j) = n + 1$ for some $j \in \{1, \dots, m\}$. Since $m > n + 1 \geq 1$, we have $m \neq 0$, so $m - 1 \in \mathbb{N}$ by Lemma 2.1.1 (c); and $m - 1 > n$, by subtracting 1 from $m > n + 1$. Define

$\sigma: \{1, \dots, m-1\} \rightarrow \{1, \dots, m\}$ by

$$\sigma(i) := \begin{cases} i & \text{if } i \neq j, \\ m & \text{if } i = j. \end{cases}$$

(The second line applies only when $j \leq m-1$; if $j = m$, then $\sigma(i) = i$ for every i .) The map σ is injective: two different inputs other than j keep their different values, and if one input is j , its value is m , while the other has value $i \leq m-1 < m$. Moreover $\sigma(i) \neq j$ for every i : either $\sigma(i) = i \neq j$, or $\sigma(i) = m$, which happens only when $j \leq m-1 < m$.

Let $g := f \circ \sigma$. It is injective by Theorem 1.5.4 (a). For every i , $\sigma(i) \neq j$, and f is injective with $f(j) = n+1$, so $g(i) = f(\sigma(i)) \neq n+1$; as in Case 1, $g(i) \in \{1, \dots, n\}$. So g with codomain $\{1, \dots, n\}$ is an injection $\{1, \dots, m-1\} \rightarrow \{1, \dots, n\}$, with $m-1 > n$. This contradicts $P(n)$, applied to the number $m-1$.

In both cases the injection f cannot exist, so $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every $n \in \mathbb{N}$. This proves the theorem. ■

The theorem is about the standard sets only, but bijections carry it to any finite sets. Part (b) below is its mirror image for surjections.

Corollary 2.5.3. Pigeonhole for Finite Sets

Let $m, n \in \mathbb{N}$, let A have m elements, and let B have n elements.

- (a) If $m > n$, there is no injection $A \rightarrow B$.
- (b) If $m < n$, there is no surjection $A \rightarrow B$.

Idea. For (a), the bijections of Definition 2.5.2 turn an injection $A \rightarrow B$ into an injection $\{1, \dots, m\} \rightarrow \{1, \dots, n\}$, which Theorem 2.5.2 forbids. For (b), a surjection $g: A \rightarrow B$ has a right inverse h , and h is an injection $B \rightarrow A$, forbidden by (a). The right inverse is built by a rule: send b to the element of A with the **smallest** number among those that g sends to b (a least element, Example (Method: the least element)).

Proof. Let $\varphi: \{1, \dots, m\} \rightarrow A$ and $\psi: \{1, \dots, n\} \rightarrow B$ be bijections (Definition 2.5.2). By Theorem 1.6.4, ψ has an inverse $\psi^{-1}: B \rightarrow \{1, \dots, n\}$, which is a bijection: the equations $\psi^{-1} \circ \psi = \text{id}$ and $\psi \circ \psi^{-1} = \text{id}$ say that ψ is a two-sided inverse of ψ^{-1} (Definition 1.6.2), so Theorem 1.6.4 applies.

(a) Suppose $m > n$ and $f: A \rightarrow B$ is injective. Then $\psi^{-1} \circ f \circ \varphi: \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ is injective by Theorem 1.5.4 (a), which contradicts Theorem 2.5.2.

(b) Suppose $m < n$ and $g: A \rightarrow B$ is surjective. For $b \in B$ let

$$S_b := \{i \in \{1, \dots, m\} : g(\varphi(i)) = b\}.$$

It is non-empty: since g is onto, $b = g(a)$ for some $a \in A$, and $a = \varphi(i)$ for some i , since φ is onto. By Theorem 2.1.3, S_b has a least element. Define $h: B \rightarrow A$ by $h(b) := \varphi(\min S_b)$.

Then $g(h(b)) = b$ for every $b \in B$, because $\min S_b \in S_b$. So $g \circ h = \text{id}_B$: the function g is a left inverse of h , and h is injective by Theorem 1.6.1 (a). Now h is an injection from the n -element set B to the m -element set A , with $n > m$, which contradicts (a). This proves the corollary. ■

The function h in (b) is defined by a **rule**, “the least element”, applied to each b at once, so its existence needs nothing beyond specification. Section 3.2 meets surjections for which no such rule is available, and there the book adds a new principle.

🕒 **Second reading** · Two loose ends from Chapter 1 and Logic and Proof

Two special cases settle earlier loose ends. With $m = n + 1$, part (a) says that a set with n elements has no $n + 1$ different elements: there is no injection $\{1, \dots, n + 1\} \rightarrow A$. That is the second school fact that Logic and Proof, Exercise (C2: A sentence with no finite model, used later) took on trust. With $m = 3$, $n = 2$ in (a) and $m = 2$, $n = 3$ in (b), the corollary gives the two observations after Example (Deciding injective and surjective) in general.

Here is a typical use of (a). Among any three different integers, two have an even sum. Let A be a set of three different integers, and let $p: A \rightarrow \{0, 1\}$ send each a to its remainder r on division by 2 (Theorem 2.2.3), an integer with $0 \leq r < 2$; then $r \in \mathbb{N}$ by Proposition 2.1.2 (b), and $r \leq 1$ by Lemma 2.1.1 (e), so $r \in \{0, 1\}$. The set $\{0, 1\}$ has 2 elements, so by (a), p is not injective: there are $a \neq b$ in A with the same remainder r . Writing $a = 2q + r$ and $b = 2q' + r$,

$$a + b = 2(q + q' + r),$$

which is even, since $q + q' + r \in \mathbb{Z}$ (Proposition 2.1.2 (a)). The pigeons are the integers and the holes are the remainders; the whole skill is choosing the holes.

Example. Method: the pigeonhole principle

Template. (1) Choose the pigeons, a set A whose number of elements you know, and the holes, a set B with fewer. (2) Define $p: A \rightarrow B$, “the hole of a pigeon”, and check that its values lie in B . (3) By [Corollary 2.5.3](#) (a), p is not injective: two different pigeons $a \neq a'$ share a hole. (4) Translate “same hole” back into the property you want.

When to use it. The claim says “among any N objects, two have ...”, or “some value is taken twice”, and N exceeds the number of possible values.

The usual failure. Holes for which sharing a hole does not give the property: choose the holes by what two pigeons should share. Pigeons that need not be different: a list with repeats is not a set with N elements. Claiming to know which two pigeons share a hole.

Example. Back to the five lattice points

Show that among any five different lattice points, two have a lattice point as midpoint.

Idea. The pigeons are the points and the holes are the parity patterns (Example (Method: the pigeonhole principle)).

Solution. Let A be a set of five lattice points, so A has 5 elements. Let $B := \{0, 1\} \times \{0, 1\}$, which has the 4 elements $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ (number them 1 to 4). Send $(a, b) \in A$ to (r, s) , where r and s are the remainders of a and b on division by 2 (Theorem 2.2.3); $r, s \in \{0, 1\}$ as in the three-integers paragraph above, so the values lie in B . Since $5 > 4$, Corollary 2.5.3 (a) gives two different points $(a, b) \neq (c, d)$ in A with the same remainders. Then a and c have the same parity (Definition 1.1.1: remainder 0 means $a = 2q$, which is even, and remainder 1 means $a = 2q + 1$, which is odd), and so do b and d , so their midpoint is a lattice point by Example (Same pattern, lattice midpoint). This answers (Q1) of Section 1.1: yes.

The word “different” costs nothing, since a point and itself have that point as midpoint; and the four corners of a unit square (Section 1.1) show that five cannot be lowered to four.

Quick check. Choose pigeons and holes: among any 11 different integers, two differ by a multiple of 10.

Solution. The pigeons are the 11 different integers. The holes are the remainders $0, \dots, 9$ on division by 10 (Theorem 2.2.3), a set with 10 elements. By Corollary 2.5.3 (a) two of the integers, $a \neq b$, have the same remainder r : $a = 10q + r$ and $b = 10q' + r$, so $a - b = 10(q - q')$.

The next corollary is the well-definedness promised after Definition 2.5.2.

Corollary 2.5.4. The Number of Elements Is Unique

Let A be a set and $m, n \in \mathbb{N}$. If A has m elements and A has n elements, then $m = n$.

Proof. Let $\varphi: \{1, \dots, m\} \rightarrow A$ and $\psi: \{1, \dots, n\} \rightarrow A$ be bijections. If $m > n$, then $\psi^{-1} \circ \varphi: \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ is injective (Theorem 1.6.4, Theorem 1.5.4 (a)), which contradicts Theorem 2.5.2. Exchanging the roles of φ and ψ rules out $m < n$ in the same way. By trichotomy, $m = n$. ■

So a finite set has exactly one number of elements, and from now on $|A| = n$ means “the number of elements of A is n ”.

2.5.4 Subsets and unions of finite sets

Three facts about finite sets are used everywhere below: the sizes of disjoint sets add, a subset is no larger than the whole, and removing one point lowers the size by one. The first uses nothing

else from this section, so it comes first.

Proposition 2.5.5. Disjoint Unions

Let $m, n \in \mathbb{N}$, let A have m elements, let B have n elements, and suppose $A \cap B = \emptyset$. Then $A \cup B$ has $m + n$ elements.

Idea. Number A with $1, \dots, m$ and then carry on numbering B with $m + 1, \dots, m + n$: shift the numbering of B up by m .

Proof. Let $\varphi: \{1, \dots, m\} \rightarrow A$ and $\psi: \{1, \dots, n\} \rightarrow B$ be bijections. Note $m + n \in \mathbb{N}$ by Lemma 2.1.1 (b). For $k \in \{1, \dots, m + n\}$ with $k > m$, we have $m + 1 \leq k$ by Lemma 2.1.1 (e), so $k - m \in \mathbb{N}$ with $1 \leq k - m \leq n$ (Lemma 2.1.1 (d)). So we may define $\chi: \{1, \dots, m + n\} \rightarrow A \cup B$ by

$$\chi(k) := \begin{cases} \varphi(k) & \text{if } k \leq m, \\ \psi(k - m) & \text{if } k > m. \end{cases}$$

Injective. Let $\chi(k) = \chi(k')$. If $k, k' \leq m$, then $\varphi(k) = \varphi(k')$ gives $k = k'$. If $k, k' > m$, then $\psi(k - m) = \psi(k' - m)$ gives $k - m = k' - m$, so $k = k'$. If $k \leq m < k'$, then $\chi(k) \in A$ and $\chi(k') \in B$, and $A \cap B = \emptyset$, so $\chi(k) \neq \chi(k')$: this case cannot occur, nor can its mirror image.

Surjective. Let $x \in A \cup B$. If $x \in A$, then $x = \varphi(i)$ with $1 \leq i \leq m$, and $\chi(i) = x$. If $x \in B$, then $x = \psi(j)$ with $1 \leq j \leq n$; put $k := m + j$, so $m < k \leq m + n$, and $\chi(k) = \psi(j) = x$.

So χ is a bijection, and $A \cup B$ has $m + n$ elements. ■

🕒 **Second reading** · Why the step does not remove a point

Now subsets. The proof is an induction on the size of the whole set, and it must be set up with care: the step peels off one element, and the obvious way to say “peel off one element” is the corollary after it, on removing a point. But that corollary is proved **from** this proposition. So the step peels off $\varphi(n + 1)$ by restricting the bijection φ directly, and cites nothing proved later.

Proposition 2.5.6. Subsets of Finite Sets

Let $n \in \mathbb{N}$, let A have n elements, and let $S \subseteq A$. Then S is finite and has k elements for some $k \leq n$. If $S \neq A$, then $k < n$.

Idea. Remove the last element $\varphi(n + 1)$ from A . Either it is outside S , and S sits inside the smaller set; or it is in S , and S is its part in the smaller set plus one point, which [Proposition 2.5.5](#) counts.

Proof. For $n \in \mathbb{N}$ let $P(n)$ be the statement

for every set A with n elements and every $S \subseteq A$, the set S has k elements for some $k \leq n$, and $k < n$ if $S \neq A$.

We prove $P(n)$ for every n by Logic and Proof, Axiom 4.2.1.

Base case $P(0)$. A set A with 0 elements is empty, so $S \subseteq \emptyset$ gives $S = \emptyset = A$, which has $0 \leq 0$ elements; the second clause is vacuous.

Inductive step. Let $n \in \mathbb{N}$ and suppose $P(n)$. Let A have $n + 1$ elements, with a bijection $\varphi: \{1, \dots, n + 1\} \rightarrow A$, and let $S \subseteq A$. Put

$$A' := \varphi(\{1, \dots, n\}), \quad a := \varphi(n + 1).$$

The restriction of φ to $\{1, \dots, n\}$, with codomain A' , is injective and surjective, so A' has n elements. Every element of A is $\varphi(i)$ with $i \leq n$ or $i = n + 1$ (Lemma 2.1.1 (e)), so $A = A' \cup \{a\}$. And $a \notin A'$: if $a = \varphi(i)$ with $i \leq n$, injectivity would give $i = n + 1$.

Case $a \notin S$. Then $S \subseteq A'$, and $P(n)$, applied to A' and S , shows that S has $k \leq n < n + 1$ elements. In this case $S \neq A$, since $a \in A \setminus S$, and indeed $k < n + 1$, as required.

Case $a \in S$. Then $S = (S \cap A') \cup \{a\}$, and the union is disjoint because $a \notin A'$. By $P(n)$, applied to A' and $S \cap A' \subseteq A'$, the set $S \cap A'$ has j elements for some $j \leq n$. The set $\{a\}$ has 1 element (by $1 \mapsto a$). By Proposition 2.5.5, S has $j + 1 \leq n + 1$ elements. If $S \neq A$, then $S \cap A' \neq A'$, since otherwise $S = A' \cup \{a\} = A$; so $j < n$ by $P(n)$, and $j + 1 < n + 1$.

In both cases $P(n + 1)$ holds. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every $n \in \mathbb{N}$. This proves the proposition. ■

Read contrapositively, with Corollary 2.5.4: a subset of an n -element set that itself has n elements is the whole set. (If $S \neq A$, its number of elements is $k < n$, and by uniqueness it is not n .) That is the first school fact that Logic and Proof, Exercise (C1: True in every finite model, used later) took on trust.

Quick check. A set $S \subseteq \{1, \dots, 7\}$ has 7 elements. What is S , and which results say so?

Solution. $S = \{1, \dots, 7\}$. If $S \neq \{1, \dots, 7\}$, then Proposition 2.5.6 gives S some number $k < 7$ of elements, and Corollary 2.5.4 forbids S to have both k and 7 elements.

Quick check. Choose parts and sizes: among any 5 different elements of $\{1, 2\} \times \{1, 2, 3\}$, three have the same first coordinate.

Solution. Let $A \subseteq \{1, 2\} \times \{1, 2, 3\}$ have 5 elements, and let A_i be its elements with first coordinate i , for $i = 1, 2$; these are disjoint with union A , and both are finite by Proposition 2.5.6. If both had at most 2 elements, then Proposition 2.5.5 would give A at most

4 elements, contradicting [Corollary 2.5.4](#). So some A_i has $k_i > 2$ elements, that is $k_i \geq 3$ (Lemma 2.1.1 (e)), and a bijection $\varphi: \{1, \dots, k_i\} \rightarrow A_i$ gives three different elements $\varphi(1)$, $\varphi(2)$, $\varphi(3)$ of A , all with first coordinate i .

Corollary 2.5.7. Removing a Point

Let $n \in \mathbb{N}$, let A have $n + 1$ elements, and let $a \in A$. Then $A \setminus \{a\}$ has n elements.

Proof. Since $a \in A$, the set $A \setminus \{a\}$ is a proper subset of A , so by [Proposition 2.5.6](#) it has k elements for some $k < n + 1$. Now $A = (A \setminus \{a\}) \cup \{a\}$ is a disjoint union, and $\{a\}$ has 1 element, so A has $k + 1$ elements by [Proposition 2.5.5](#). By [Corollary 2.5.4](#), $k + 1 = n + 1$, so $k = n$. ■

Every later induction on the number of elements uses this corollary in the same way: its step starts from an **arbitrary** set A with $n + 1$ elements, picks some $a \in A$ (there is one, since $n + 1 \geq 1$), and applies the hypothesis to $A \setminus \{a\}$, which has n elements. It never presents the set as “ X with one point added” from the outset, which would prove the claim only for sets that come in that form. Here is the first such induction. Chapter 1 promised the count of subsets of a finite set.

Proposition 2.5.8. Counting Subsets

Let $n \in \mathbb{N}$. A set with n elements has 2^n subsets: if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

Idea. Fix one element a . Every subset either leaves a out or contains it, and adding a pairs the subsets of the first kind with those of the second. So the count doubles with each new element.

Proof. We use Logic and Proof, Axiom 4.2.1 on n . *Base case.* A set with 0 elements is $\emptyset$, and $\mathcal{P}(\emptyset) = \{\emptyset\}$ has $1 = 2^0$ element (Definition 2.3.2).

Inductive step. Let $n \in \mathbb{N}$, and suppose every set with n elements has 2^n subsets. Let A have $n + 1$ elements, pick $a \in A$, and put $X := A \setminus \{a\}$. By [Corollary 2.5.7](#), X has n elements, so $\mathcal{P}(X)$ has 2^n elements by the hypothesis (here $2^n \in \mathbb{N}$ by Proposition 2.3.4 (d), so the count makes sense; likewise $2^{n+1} \in \mathbb{N}$). Let

$$T := \{S \cup \{a\} : S \in \mathcal{P}(X)\},$$

the image of $\mathcal{P}(X)$ under $S \mapsto S \cup \{a\}$, a function $\mathcal{P}(X) \rightarrow \mathcal{P}(A)$.

$\mathcal{P}(A)$ is the disjoint union of $\mathcal{P}(X)$ and T . Every member of T contains a , and no member of $\mathcal{P}(X)$ does, since $a \notin X$; so the union is disjoint. Both sets consist of subsets of A . Conversely, let $U \subseteq A$. If $a \notin U$, then $U \subseteq X$. If $a \in U$, then $U = (U \setminus \{a\}) \cup \{a\}$ with $U \setminus \{a\} \subseteq X$, so $U \in T$.

T has 2^n elements. The map $S \mapsto S \cup \{a\}$, with codomain T , is surjective by the definition of T . It is injective: for $S \subseteq X$ we have $a \notin S$, so $(S \cup \{a\}) \setminus \{a\} = S$, and S can be read back from $S \cup \{a\}$. So it is a bijection $\mathcal{P}(X) \rightarrow T$, and composing a bijection $\{1, \dots, 2^n\} \rightarrow \mathcal{P}(X)$ with it (Theorem 1.5.4 (c)) shows that T has 2^n elements.

By Proposition 2.5.5, $\mathcal{P}(A)$ has $2^n + 2^n = 2^n \cdot 2 = 2^{n+1}$ elements (Definition 2.3.2). By Logic and Proof, Axiom 4.2.1, the claim holds for every $n \in \mathbb{N}$. ■

🕒 **Second reading** · Subsets and functions to $\{0, 1\}$

For any set Y , the map $S \mapsto \mathbf{1}_S$, with inverse $f \mapsto \{y \in Y : f(y) = 1\}$, is a bijection $\mathcal{P}(Y) \rightarrow \{0, 1\}^Y$ onto the set of functions $Y \rightarrow \{0, 1\}$ (the correspondence of Section 1.5 between subsets and indicator functions). Taking Y with n elements, a set with n elements also has exactly 2^n functions to $\{0, 1\}$, and the two counting problems of Chapter 1 are one. Exercise C2 counts all functions between finite sets.

2.5.5 No finite set is equinumerous with a proper subset

For finite sets, “a proper part is smaller” is a theorem.

Theorem 2.5.9. A Finite Set Has No Proper Copy

Let A be a finite set and $B \subsetneq A$. Then A and B are not equinumerous: there is no bijection $A \rightarrow B$.

Proof. Let A have n elements, with a bijection $\varphi: \{1, \dots, n\} \rightarrow A$. By Proposition 2.5.6, B has k elements for some $k < n$, since $B \neq A$. Suppose $g: A \rightarrow B$ were a bijection. Then $g \circ \varphi: \{1, \dots, n\} \rightarrow B$ is a bijection (Theorem 1.5.4 (c)), so B also has n elements, and Corollary 2.5.4 gives $k = n$. This contradicts $k < n$. ■

Contradiction at scale. The proof never computes with g . It supposes the bijection, hands it to two theorems already proved, and lets them disagree about the number of elements of B . The claim is a negation, “no bijection”, so this is face (i), chosen by Example (Method: choosing direct, contrapositive or contradiction); but the clash is between results, not between two lines. The proofs of Theorem 2.5.2 and Corollary 2.5.4 have the same shape inside them.

Turned around, the theorem is a test for infinity: **a set that is equinumerous with a proper subset of itself is infinite**. Here is its first use. For the even natural numbers we write

$$2\mathbb{N} := \{2n : n \in \mathbb{N}\},$$

the image of $\mathbb{N}$ under $n \mapsto 2n$.

Example. Hilbert's Hotel

A hotel has one room for every natural number, and every room is taken. A coach arrives with guests for the odd-numbered rooms: the guest in room n is asked to move to room $2n$. Show that this is a bijection $\mathbb{N} \rightarrow 2\mathbb{N}$, that $2\mathbb{N}$ is a proper subset of $\mathbb{N}$, and deduce that $\mathbb{N}$ is infinite.

Solution. Let $d: \mathbb{N} \rightarrow 2\mathbb{N}$, $d(n) := 2n$. Its values lie in $2\mathbb{N}$ by definition, and $2\mathbb{N} \subseteq \mathbb{N}$ by Lemma 2.1.1 (b). It is injective, since $2n = 2n'$ gives $n = n'$, and surjective, since every element of $2\mathbb{N}$ is $2n = d(n)$ for some $n \in \mathbb{N}$. So $|\mathbb{N}| = |2\mathbb{N}|$.

The inclusion is proper because $1 \notin 2\mathbb{N}$: if $n = 0$, then $2n = 0$; if $n \neq 0$, then $n \geq 1$ (Lemma 2.1.1 (a)) and $2n \geq 2$. So $2n \neq 1$ for every $n \in \mathbb{N}$.

If $\mathbb{N}$ were finite, Theorem 2.5.9 would forbid a bijection from $\mathbb{N}$ onto its proper subset $2\mathbb{N}$. So $\mathbb{N}$ is infinite. Every guest still has a room, and the odd rooms are now free.

The finite intuition “a proper part is smaller” fails for $\mathbb{N}$, and it fails exactly because $\mathbb{N}$ is infinite. Section 3.5 proves that it fails for **every** infinite set.

Warning. $A \subsetneq B$ does not make A smaller than B when B is infinite: $2\mathbb{N} \subsetneq \mathbb{N}$ and $|2\mathbb{N}| = |\mathbb{N}|$. Equinumerous is not “one is a subset of the other”, in either direction.

Warning. “Finite” does not mean “bounded”. The set $E := \{1/n : n \in \mathbb{Z}_{>0}\}$ lies in $[0, 1]$, and it is infinite: $x \mapsto x/(1+x)$ sends $1/n$ to $1/(n+1)$, and it is a bijection from E onto $\{1/n : n \geq 2\}$, with inverse $y \mapsto y/(1-y)$. That set is a proper subset of E , since $1 \in E$ and $1/n \leq 1/2$ for $n \geq 2$.

Quick check. Is $n \mapsto n+1$ a bijection $\mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$? What does that show?

Solution. Yes. Its values lie in $\mathbb{N} \setminus \{0\}$, since $n+1 \geq 1$. Its inverse is $m \mapsto m-1$, which is defined on $\mathbb{N} \setminus \{0\}$ because $m-1 \in \mathbb{N}$ for $m \neq 0$ (Lemma 2.1.1 (c)); the two maps undo each other, so it is a bijection by Theorem 1.6.4. So $\mathbb{N}$ is equinumerous with its proper subset $\mathbb{N} \setminus \{0\} = \mathbb{Z}_{>0}$, and by Theorem 2.5.9, $\mathbb{N}$ is infinite, a second time. In the hotel, every guest moves up one room, and room 0 is free.

Remark. By Definition 2.5.2, a non-empty finite set A with n elements is $\{x_1, \dots, x_n\}$, with $x_k := \varphi(k)$. So when its elements are real numbers it has a maximum and a minimum, by Proposition 2.3.8. Section 2.3 announced this passage from a finite set to a list.

Quick check. Show that the set of primes is infinite.

Solution. Suppose it is finite. It is non-empty, since 2 is prime, so it is $\{p_1, \dots, p_n\}$ with $n \geq 1$ (Definition 2.5.2 and the remark above), and it has a maximum M (Proposition 2.3.8). By Theorem 2.4.1 there is a prime $p > M$. That prime lies in the set and exceeds its maximum, a contradiction.

Remark (Looking ahead). Chapter 4 defines equivalence relations on a set, and meets equinumerosity again as a relation that behaves like one without living on a set.

2.5.6 Exercises

2.5.6.1 A. Check your understanding

Exercise. A1

- (a) Define “ A is finite”, and write its negation in symbols, with every quantifier shown.
- (b) True or false, with a reason: a subset of an infinite set is infinite; a set that has an infinite subset is infinite.
- (c) How many injections $\{1, 2, 3\} \rightarrow \{1, 2\}$ are there?
- (d) Let $f: A \rightarrow B$, where A and B are finite and A has more elements than B . What does the pigeonhole principle guarantee about f ?

Solution.

- (a) A is finite if there are $n \in \mathbb{N}$ and a bijection $\varphi: \{1, \dots, n\} \rightarrow A$ (Definition 2.5.2): $\exists n \in \mathbb{N} \exists \varphi \in A^{\{1, \dots, n\}}$ (φ injective $\wedge$ φ surjective). By Logic and Proof, Proposition 6.2.3, applied to each quantifier, and De Morgan, its negation is

$$\forall n \in \mathbb{N} \forall \varphi \in A^{\{1, \dots, n\}} (\varphi \text{ not injective} \vee \varphi \text{ not surjective}),$$

which is Definition 2.5.3.

- (b) The first is false: $\emptyset \subseteq \mathbb{N}$, and $\emptyset$ is finite while $\mathbb{N}$ is infinite (Example (Hilbert’s Hotel)). The second is true: if B were finite, every subset of B would be finite by Proposition 2.5.6; so a set with an infinite subset is not finite.
- (c) None. By Theorem 2.5.2 with $m = 3 > 2 = n$, there is no injection $\{1, 2, 3\} \rightarrow \{1, 2\}$.
- (d) That f is not injective (Corollary 2.5.3 (a)): there are two **different** elements $a \neq a'$ of A with $f(a) = f(a')$. It does not say which two, and it says nothing when A has at most as many elements as B .

2.5.6.2 B. Practice

Exercise. B1: Moving the guests

Give explicit bijections $\mathbb{N} \rightarrow \mathbb{N} \setminus \{0, 1, 2\}$, $\mathbb{N} \rightarrow \{n \in \mathbb{N} : n \geq 5\}$ and $\mathbb{N} \rightarrow \{2n + 1 : n \in \mathbb{N}\}$, and prove that each is a bijection by writing down its inverse.

Solution. First. For $m \in \mathbb{N}$: if $m \notin \{0, 1, 2\}$, then $m \geq 3$. Indeed $m \neq 0$ gives $m \geq 1$ (Lemma 2.1.1 (a)); with $m \neq 1$, $m > 1$, so $m \geq 2$ (Lemma 2.1.1 (e)); with $m \neq 2$, $m \geq 3$ likewise. Conversely every $m \geq 3$ lies outside $\{0, 1, 2\}$. So $\mathbb{N} \setminus \{0, 1, 2\} = \{m \in \mathbb{N} : m \geq 3\}$. Let $f(n) := n + 3$; then $f(n) \in \mathbb{N}$ and $f(n) \geq 3$. Let $g(m) := m - 3$ for $m \geq 3$; then $g(m) \in \mathbb{N}$ by Lemma 2.1.1 (d). Since $g(f(n)) = n$ and $f(g(m)) = m$, the map f is a bijection by Theorem 1.6.4.

Second. The same with 5 in place of 3: $n \mapsto n + 5$, with inverse $m \mapsto m - 5$, which lies in $\mathbb{N}$ for $m \geq 5$ by Lemma 2.1.1 (d).

Third. Let $O := \{2n + 1 : n \in \mathbb{N}\}$, the odd natural numbers, and $f(n) := 2n + 1$, which lies in O by definition. Every $m \in O$ is $2n + 1$ for exactly one $n \in \mathbb{N}$: one by the definition of O , and only one since $2n + 1 = 2n' + 1$ gives $n = n'$. So $g(m) := (m - 1)/2$ is that n , a natural number. Then $g(f(n)) = n$ and $f(g(m)) = m$, so f is a bijection $\mathbb{N} \rightarrow O$. Each of the three sets is a proper subset of $\mathbb{N}$ equinumerous with $\mathbb{N}$, which shows again that $\mathbb{N}$ is infinite.

Exercise. B2: Choosing the holes

- (a) Prove that among any 6 different integers, two have the same remainder on division by 5.
- (b) Prove that among any 7 different points of $\{1, 2, 3\} \times \{1, 2, 3\}$, three lie in one row, that is, have the same first coordinate.

Hint: in (b), the rows are the holes; how many points can a row take if no row takes three?

Solution.

- (a) Let A be a set of 6 integers. By Theorem 2.2.3 with divisor 5, each $a \in A$ has a unique remainder $r(a)$, an integer with $0 \leq r(a) < 5$; then $r(a) \in \mathbb{N}$ by Proposition 2.1.2 (b), and $r(a) \leq 4$ by discreteness, Proposition 2.1.2 (c), so $r(a) \in \{0, \dots, 4\}$. This defines $r: A \rightarrow \{0, \dots, 4\}$. The set $\{0, \dots, 4\}$ has 5 elements (the third example after Definition 2.5.2). Since $6 > 5$, Corollary 2.5.3 (a) shows that r is not injective: there are $a \neq a'$ in A with $r(a) = r(a')$.
- (b) Let $A \subseteq \{1, 2, 3\} \times \{1, 2, 3\}$ have 7 elements, and for $i = 1, 2, 3$ let $A_i := \{(x, y) \in A : x = i\}$, the points of A in row i . These sets are pairwise disjoint and their union is A . Each is a subset of A , so it is finite by Proposition 2.5.6; say A_i has k_i elements. If every $k_i \leq 2$, then by Proposition 2.5.5, applied twice, $A = (A_1 \cup A_2) \cup A_3$ has $k_1 + k_2 + k_3 \leq 6$ elements, and Corollary 2.5.4 forbids A to have both that number and 7 elements. So some $k_i > 2$, that is $k_i \geq 3$ (Lemma 2.1.1 (e)); if $\varphi: \{1, \dots, k_i\} \rightarrow A_i$ is a bijection, then $\varphi(1), \varphi(2), \varphi(3)$ are three different points of A in row i . Seven is the least number that works: the six points with second coordinate 1 or 2 put exactly two in each row.

Exercise. B3: Finite unions

Let $n \in \mathbb{N}$, and let $A_1, \dots, A_n$ be finite sets, that is, a family $(A_i)_{i \in \{1, \dots, n\}}$ of finite sets. Prove that $\bigcup_{i \in \{1, \dots, n\}} A_i$ is finite.

Solution. For $n \in \mathbb{N}$ let $P(n)$ be “for every family $(A_i)_{i \in \{1, \dots, n\}}$ of finite sets, the union $U_n := \bigcup_{i \in \{1, \dots, n\}} A_i$ is finite”. We use Logic and Proof, Axiom 4.2.1.

Base case. For $n = 0$ the index set is $\{1, \dots, 0\} = \emptyset$, and the union of the empty family is $\emptyset$ (Definition 1.3.4: no x lies in some A_i), which has 0 elements.

Step. Suppose $P(n)$, and let $(A_i)_{i \in \{1, \dots, n+1\}}$ be a family of finite sets. Since $\{1, \dots, n+1\} = \{1, \dots, n\} \cup \{n+1\}$, we have $U_{n+1} = U_n \cup A_{n+1}$, and U_n is finite by $P(n)$, applied to the first n sets; say it has p elements. Write

$$U_{n+1} = U_n \cup (A_{n+1} \setminus U_n),$$

a disjoint union. The set $A_{n+1} \setminus U_n$ is a subset of the finite set A_{n+1} , so it is finite by Proposition 2.5.6; say it has q elements. By Proposition 2.5.5, U_{n+1} has $p + q$ elements. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every n .

The detour through $A_{n+1} \setminus U_n$ is needed because Proposition 2.5.5 is about **disjoint** sets, and U_n and A_{n+1} may overlap.

Exercise. B4: Prove or disprove

Prove each true statement and refute each false one with a counterexample.

- (a) Among any 12 different integers, two differ by a multiple of 12.
- (b) Among any 3 different integers, two have an even sum.
- (c) Among any 5 different lattice points of space (points of $\mathbb{Z}^3$), two have a lattice point as midpoint.
- (d) If A has 8 elements and $f: A \rightarrow \{1, 2, 3, 4\}$, then some value of f is taken at least 3 times.
- (e) No function from the set of subsets of $\{1, 2, 3\}$ to $\{1, \dots, 7\}$ is injective.
- (f) Every injection $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$ is surjective.

Solution.

- (a) **False.** Take $0, 1, \dots, 11$. Any two of them differ by an integer d with $1 \leq |d| \leq 11$, which is not a multiple of 12. Thirteen integers would do, by the argument of the Quick check on 11 integers.
- (b) **True.** The pigeons are the three integers and the holes are the two parities (Theorem 1.1.2), a set with 2 elements. Since $3 > 2$, two of the integers have the same parity (Corollary 2.5.3 (a)), and their sum is even (Example (The parity of a sum)).
- (c) **False.** Take five of the eight points with all coordinates in $\{0, 1\}$ (Exercise C3 of Section 1.1). Two different ones differ in some coordinate, where one has 0 and the other 1; the sum there is 1, so that coordinate of the midpoint is $\frac{1}{2}$.
- (d) **False.** Take $A = \{1, \dots, 8\}$ and $f(k) :=$ the integer part of $(k+1)/2$, with values 1, 1, 2, 2, 3, 3, 4, 4: each value is taken exactly twice. Nine elements would force some value three times, as in Exercise B2 (b).
- (e) **True.** The set of subsets of $\{1, 2, 3\}$ has $2^3 = 8$ elements (Proposition 2.5.8), and $8 > 7$, so Corollary 2.5.3 (a) applies.

- (f) **True.** Let f be such an injection. With its codomain shrunk to its image, f is a bijection, so $f(\{1, \dots, n\})$ has n elements. It is a subset of $\{1, \dots, n\}$, so it is all of it, by the remark after [Proposition 2.5.6](#); that is, f is surjective.

Three are true, (b), (e) and (f), and three are false. Each true item is the method of [Example \(Method: the pigeonhole principle\)](#) with the holes named; each false one either has too few pigeons or holes that do not give the property.

2.5.6.3 C. Going deeper

Exercise. C1: Infinite means arbitrarily large finite pieces

Prove that a set A is infinite if and only if for every $n \in \mathbb{N}$ there is an injection $\{1, \dots, n\} \rightarrow A$. In the direction $(\Rightarrow)$, say whether your proof makes infinitely many choices at once, and why.

Solution (Hint 1). For $(\Leftarrow)$, suppose A has m elements and use the hypothesis at one well-chosen n . For $(\Rightarrow)$, induct on n .

Solution (Hint 2). For $(\Rightarrow)$: let $P(n)$ be “there is an injection $\{1, \dots, n\} \rightarrow A$ ”; the base case is the empty function.

Solution. $(\Leftarrow)$ Suppose the condition holds and, for a contradiction, that A has m elements, with a bijection $\varphi: \{1, \dots, m\} \rightarrow A$. Take $n := m+1$ and an injection $f: \{1, \dots, m+1\} \rightarrow A$. By Theorem 1.6.4, φ has an inverse $\varphi^{-1}: A \rightarrow \{1, \dots, m\}$, which is a bijection, since φ is a two-sided inverse of it (Definition 1.6.2, Theorem 1.6.4). Then $\varphi^{-1} \circ f: \{1, \dots, m+1\} \rightarrow \{1, \dots, m\}$ is injective (Theorem 1.5.4 (a)), which contradicts [Theorem 2.5.2](#). So A is infinite.

$(\Rightarrow)$ Let A be infinite. For $n \in \mathbb{N}$ let $P(n)$ be “there is an injection $\{1, \dots, n\} \rightarrow A$ ”. We use Logic and Proof, Axiom 4.2.1.

Base case. $\{1, \dots, 0\} = \emptyset$, and the empty function $\emptyset \rightarrow A$ (Proposition 1.5.2 (a)) is injective, vacuously.

Step. Suppose $P(n)$, and let $f: \{1, \dots, n\} \rightarrow A$ be an injection. With its codomain shrunk to its image $F := f(\{1, \dots, n\})$, it is a bijection, so F has n elements. Since A is infinite, $F \neq A$; and $F \subseteq A$, so there is some $a \in A \setminus F$. Define $g: \{1, \dots, n+1\} \rightarrow A$ by $g(k) := f(k)$ for $k \leq n$ and $g(n+1) := a$; this is a function because $\{1, \dots, n+1\} = \{1, \dots, n\} \cup \{n+1\}$ and $n+1 \notin \{1, \dots, n\}$ (Lemma 2.1.1 (e)). It is injective: two inputs $\leq n$ are separated by f , and $g(n+1) = a \notin F$ differs from every $g(k)$ with $k \leq n$. So $P(n+1)$ holds. By Logic and Proof, Axiom 4.2.1, $P(n)$ holds for every n .

No infinitely many choices are made. The step uses two existence statements, $P(n)$ and “ $A \setminus F \neq \emptyset$ ”, and names one witness for each: one $\exists E$ each, inside the proof of the single implication $P(n) \Rightarrow P(n+1)$. Its conclusion, $P(n+1)$, is again an existence statement, so the witnesses never leave the step. Induction then gives $P(n)$ for each n **separately**: for each n **some** injection exists, and different n may use unrelated ones. Gluing the steps into one injection $\mathbb{N} \rightarrow A$, with a new point picked at every stage, would require all the picks at once, with no rule saying which point to pick. That is a different statement; Section 3.5

proves it with the principle of choice of Section 3.2.

Marking scheme. (10 points) - 2: ($\Leftarrow$) supposes A has m elements and uses the hypothesis at $n = m + 1$ to contradict the pigeonhole principle ([Theorem 2.5.2](#) or [Corollary 2.5.3](#) (a)). - 1: ($\Rightarrow$) sets up an induction on n with the base case $n = 0$ (the empty function); a base $n = 1$ earns the point only if $n = 0$ is also covered (by the empty function). - 3: in the step, shows that the image of the given injection has n elements and is therefore not A , and takes a point outside it. - 2: extends the injection by that point and checks injectivity, including the new value against the old ones. - 2: explains that each step makes finitely many choices inside one implication, so no principle of choice is used, and that building one injection on all of $\mathbb{N}$ would be a different statement. Fatal errors (0 for the step): picking “a new point for every n ” to define one function $\mathbb{N} \rightarrow A$ and calling it induction; taking a point outside the image without showing the image is not all of A .

Exercise. C2: Counting products and functions

Let $m, n \in \mathbb{N}$, let A have m elements, and let B have n elements.

- (a) Prove that $A \times B$ has mn elements.
- (b) Prove that the set B^A of functions $A \rightarrow B$ has n^m elements.
- (c) Check your formula in (b) against Proposition 1.5.2 in the cases $m = 0$ and $m \geq 1$, $n = 0$.

Solution (Hint 1). Induct on m , with B fixed, and remove one point a from A by [Corollary 2.5.7](#).

Solution (Hint 2). For (b), a function on A is the same as a function on $A \setminus \{a\}$ together with one value at a : consider $f \mapsto (f|_{A \setminus \{a\}}, f(a))$.

Solution.

- (a) Fix B with n elements. For $m \in \mathbb{N}$ let $P(m)$ be “for every set A with m elements, $A \times B$ has mn elements” ($mn \in \mathbb{N}$ by Lemma 2.1.1 (b)). *Base case.* If A has 0 elements, then $A = \emptyset$, and $A \times B = \emptyset$, since a pair in it would need a first coordinate in $\emptyset$. It has $0 = 0 \cdot n$ elements. *Step.* Suppose $P(m)$, let A have $m + 1$ elements, pick $a \in A$, and put $A' := A \setminus \{a\}$, which has m elements by [Corollary 2.5.7](#). Then

$$A \times B = (A' \times B) \cup (\{a\} \times B),$$

and the union is disjoint, since first coordinates in A' differ from a (Definition 1.4.1). The first set has mn elements by $P(m)$. The map $B \rightarrow \{a\} \times B$, $b \mapsto (a, b)$, is injective by Definition 1.4.1 and surjective by Definition 1.4.2, so $\{a\} \times B$ has n elements. By [Proposition 2.5.5](#), $A \times B$ has $mn + n = (m + 1)n$ elements. By Logic and Proof, Axiom 4.2.1, $P(m)$ holds for every m , and B was arbitrary.

- (b) Fix B with n elements, and let $Q(m)$ be “for every set A with m elements, B^A has n^m elements” ($n^m \in \mathbb{N}$ by Proposition 2.3.4 (d)). *Base case.* $A = \emptyset$, and by Proposition 1.5.2

(a), $B^\emptyset$ has exactly one element, the empty function; $n^0 = 1$ (Definition 2.3.2), also when $n = 0$. *Step.* Suppose $Q(m)$, let A have $m + 1$ elements, pick $a \in A$, and let $A' := A \setminus \{a\}$, with m elements. Define

$$R: B^A \rightarrow B^{A'} \times B, \quad R(f) := (f|_{A'}, f(a)).$$

Injective: if $R(f) = R(f')$, then f and f' agree on A' and at a , hence on $A = A' \cup \{a\}$, and they have the same domain and codomain, so $f = f'$ by Proposition 1.5.1.

Surjective: given $(h, b) \in B^{A'} \times B$, let f have graph $G \cup \{(a, b)\}$, where G is the graph of h , and codomain B . Each $x \in A'$ has exactly one partner, its h -value, because (a, b) has first coordinate $a \notin A'$; and a has exactly one, b , because every pair of G has first coordinate in A' . So $f \in B^A$, and $R(f) = (h, b)$. Hence R is a bijection. By $Q(m)$, $B^{A'}$ has n^m elements, so by (a), applied to the sets $B^{A'}$ and B , the product $B^{A'} \times B$ has $n^m \cdot n = n^{m+1}$ elements (Definition 2.3.2). Since R is a bijection, $|B^A| = |B^{A'} \times B|$ (Definition 2.5.1), and $|\{1, \dots, n^{m+1}\}| = |B^{A'} \times B|$. By Proposition 2.5.1 (b) and (c), $|\{1, \dots, n^{m+1}\}| = |B^A|$, that is, B^A has n^{m+1} elements. By Logic and Proof, Axiom 4.2.1, $Q(m)$ holds for every m .

- (c) For $m = 0$: $B^\emptyset$ has one element by Proposition 1.5.2 (a), and $n^0 = 1$, even for $n = 0$. For $m \geq 1$ and $n = 0$: $A \neq \emptyset$, so there is no function $A \rightarrow \emptyset$ by Proposition 1.5.2 (b), and $B^A = \emptyset$ has 0 elements; and $0^m = 0^{m-1} \cdot 0 = 0$. Both agree with (b). With $B = \{0, 1\}$, (b) recovers the count 2^m of the paragraph after Proposition 2.5.8.

Marking scheme. (10 points) - 2: sets up each induction on m with B fixed, and handles $m = 0$ (the empty product; the empty function). - 2: in each step, takes an **arbitrary** A with $m + 1$ elements, removes one point by Corollary 2.5.7, and applies the hypothesis to the rest. - 2: (a) splits $A \times B$ into two disjoint pieces and counts $\{a\} \times B$ by a bijection with B . - 3: (b) gives a bijection between B^A and $B^{A'} \times B$, checking injectivity (equality of functions) and surjectivity (the extended graph is a function). - 1: (c) checks both degenerate cases against Proposition 1.5.2. - Direct route for (a): composing the given bijections with a bijection $\{1, \dots, m\} \times \{1, \dots, n\} \rightarrow \{1, \dots, mn\}$, e.g. $(i, j) \mapsto (i-1)n + j$, with injectivity and surjectivity checked (for example by Theorem 2.2.3) and the case $m = 0$ or $n = 0$ handled, earns the 2 points of the (a) line and the (a) halves (1 point each) of the two induction lines. Fatal errors (0 for the step): “each of the m elements has n possible values, so n^m ” with no bijection or induction; a step that applies the hypothesis to a set not shown to have m elements.

2.5.6.4 R. Review

Exercise. R1

Decide whether each function is injective and whether it is surjective. Justify your answers.

- (a) $g: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, $g(a, b) := 4a + 6b$.
 (b) $k: \mathbb{Z} \rightarrow \mathbb{Z}$, $k(n) := 3n + 1$.

Solution. (a) g is neither injective nor surjective. Not surjective (Definition 1.5.4): 1 is not a value. Every value $g(a, b) = 2(2a + 3b)$ is even, with $2a + 3b \in \mathbb{Z}$ by Proposition 2.1.2 (a) (Definition 1.1.1), while $1 = 2 \cdot 0 + 1$ is odd, and no integer is both (Theorem 1.1.2). Not injective (Definition 1.5.3): $g(3, -2) = 12 - 12 = 0 = g(0, 0)$, and $(3, -2) \neq (0, 0)$, since

their first coordinates differ (Definition 1.4.1). The method of Example (Method: proving surjectivity) has nothing to work with here: a witness for the value 1 would be a pair with $4a + 6b = 1$, and the parity argument shows there is none.

(b) k is injective and not surjective. Injective, by the method of Example (Method: proving injectivity): if $3n + 1 = 3n' + 1$, then $3n = 3n'$ and $n = n'$. Not surjective (Definition 1.5.4): 0 is not a value. If $3n + 1 = 0$ for some $n \in \mathbb{Z}$, then $0 = 3n + 1$ and $0 = 3 \cdot 0 + 0$ are two divisions of 0 by 3, with remainders 1 and 0 in $\{0, 1, 2\}$, against the uniqueness in Theorem 2.2.3.

Exercise. R2

For a set X and a property $R(x, y)$ of two elements of X , consider the statements

$$(S1) \quad \exists x \in X \forall y \in X \ R(x, y), \quad (S2) \quad \forall y \in X \exists x \in X \ R(x, y).$$

- (a) Decide (S1) and (S2) for $R(x, y)$: “ $x \mid y$ ”, first with $X = \{1, \dots, 6\}$, then with $X = \{2, \dots, 6\}$.
- (b) Decide (S1) and (S2) for $X = \mathbb{Z}$ and $R(x, y)$: “ $x + y = 0$ ”.
- (c) Prove that (S1) implies (S2) for every X and R .

Solution. (a) For $X = \{1, \dots, 6\}$ both hold: $x = 1$ divides every y ($y = y \cdot 1$), which is (S1); and (S2) follows by (c). For $X = \{2, \dots, 6\}$, (S2) holds with $x := y$, since $y = 1 \cdot y$. (S1) fails: its negation is $\forall x \in X \exists y \in X \ x \nmid y$ (Logic and Proof, Proposition 6.2.3), and for $x = 2$ take $y = 3$, for $x \in \{3, \dots, 6\}$ take $y = 2$, since a positive divisor of 2 is at most 2.

(b) (S2) holds: for $y \in \mathbb{Z}$, $x := -y \in \mathbb{Z}$ has $x + y = 0$. (S1) fails: its negation is $\forall x \in \mathbb{Z} \exists y \in \mathbb{Z} \ x + y \neq 0$, and for $x \in \mathbb{Z}$ the choice $y := 1 - x$, an integer by Proposition 2.1.2 (a), gives $x + y = 1 \neq 0$.

(c) Suppose (S1), and let $x_0 \in X$ be a witness: $R(x_0, y)$ for every $y \in X$ ($\exists E$). Let $y \in X$. Then $R(x_0, y)$, so $\exists x \in X \ R(x, y)$, with witness x_0 ($\exists I$). As y was arbitrary, (S2) holds ($\forall I$). This is Logic and Proof, Proposition 5.6.2, with bounded quantifiers. The converse fails, by (a) for $X = \{2, \dots, 6\}$ and by (b): one x for all y is more than one x for each y .

Exercise. R3

Let v and w be valuations such that every atom true under v is true under w . Prove that every formula built from atoms with $\wedge$ and $\vee$ alone (no $\neg$, $\perp$, $\rightarrow$ or $\leftrightarrow$) that is true under v is true under w . Deduce that $\neg p$ is equivalent to no such formula.

Solution. By structural induction (Logic and Proof, Theorem 4.3.1), with $P(\varphi)$: “if φ contains none of $\neg$, $\perp$, $\rightarrow$, $\leftrightarrow$ and $v(\varphi) = T$, then $w(\varphi) = T$ ”. Truth values are those of Logic and Proof, Definition 4.4.2.

Atoms and $\perp$. For an atom p with $v(p) = T$, $w(p) = T$ by the hypothesis on v and w . The formula $\perp$ contains $\perp$, so $P(\perp)$ holds vacuously.

Step for $\neg$. $\neg\varphi$ contains $\neg$, so $P(\neg\varphi)$ holds vacuously.

Step for $(\varphi \circ \psi)$. If $\circ$ is $\rightarrow$ or $\leftrightarrow$, P holds vacuously. Otherwise, if $(\varphi \circ \psi)$ contains none of the four symbols, neither do φ and ψ , whose symbols are among its own, so $P(\varphi)$ and $P(\psi)$ apply to them. For $\circ = \wedge$: $v(\varphi \wedge \psi) = \text{T}$ gives $v(\varphi) = v(\psi) = \text{T}$, so $w(\varphi) = w(\psi) = \text{T}$, and $w(\varphi \wedge \psi) = \text{T}$. For $\circ = \vee$: $v(\varphi) = \text{T}$ or $v(\psi) = \text{T}$, so $w(\varphi) = \text{T}$ or $w(\psi) = \text{T}$, and $w(\varphi \vee \psi) = \text{T}$.

The consequence. Let v be the all-F valuation and w the all-T valuation; every atom true under v (there is none) is true under w . Then $v(\neg p) = \text{T}$ and $w(\neg p) = \text{F}$. If φ , built with $\wedge$ and $\vee$ alone, were equivalent to $\neg p$, it would have the same value as $\neg p$ under every valuation: $v(\varphi) = \text{T}$, hence $w(\varphi) = \text{T}$ by the first part, against $w(\varphi) = w(\neg p) = \text{F}$.

This consequence is a special case of Logic and Proof, Theorem 4.9.6 (b), which allows $\rightarrow$ as well and looks only at the all-T row; here the $\wedge/\vee$ case comes out of the stronger statement that such formulas are monotone in the valuation.