Chapter 2
Relations, Functions, Partial Functions

2.1 What is a Function?

We use functions all the time in mathematics and in computer science. But, what exactly is a function?

Roughly speaking, a function f is a rule or mechanism that takes input values in some *input domain*, say X, and produces output values in some *output domain*, say Y, in such a way that to each input $x \in X$ corresponds a *unique* output value $y \in Y$, denoted $f(x)$. We usually write $y = f(x)$, or better, $x \mapsto f(x)$.

Often, functions are defined by some sort of closed expression (a formula), but not always. For example, the formula

$$y = 2x$$

defines a function. Here, we can take both the input and output domain to be $\mathbb{R}$, the set of real numbers. Instead, we could have taken $\mathbb{N}$, the set of natural numbers; this gives us a different function. In the above example, $2x$ makes sense for all input x, whether the input domain is $\mathbb{N}$ or $\mathbb{R}$, so our formula yields a function defined for all of its input values.

Now, look at the function defined by the formula

$$y = \frac{x}{2}.$$

If the input and output domains are both $\mathbb{R}$, again this function is well defined. However, what if we assume that the input and output domains are both $\mathbb{N}$? This time, we have a problem when x is odd. For example, $3/2$ is not an integer, so our function is not defined for all of its input values. It is actually a *partial function*, a concept that subsumes the notion of a function but is more general. Observe that this partial function is defined for the set of even natural numbers (sometimes denoted $2\mathbb{N}$) and this set is called the *domain* (of definition) of f. If we enlarge the output domain to be $\mathbb{Q}$, the set of rational numbers, then our partial function is defined for all inputs.

Another example of a partial function is given by

$$y = \frac{x+1}{x^2 - 3x + 2},$$

assuming that both the input and output domains are $\mathbb{R}$. Observe that for $x = 1$ and $x = 2$, the denominator vanishes, so we get the undefined fractions $2/0$ and $3/0$. This partial function "blows up" for $x = 1$ and $x = 2$, its value is "infinity" $(= \infty)$, which is not an element of $\mathbb{R}$. So, the domain of f is $\mathbb{R} - \{1, 2\}$.

In summary, partial functions need not be defined for all of their input values and we need to pay close attention to both the input and the output domain of our partial functions.

The following example illustrates another difficulty: consider the partial function given by

$$y = \sqrt{x}.$$

If we assume that the input domain is $\mathbb{R}$ and that the output domain is $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x \geq 0\}$, then this partial function is not defined for negative values of x. To fix this problem, we can extend the output domain to be $\mathbb{C}$, the complex numbers. Then we can make sense of $\sqrt{x}$ when $x < 0$. However, a new problem comes up: every negative number x has two complex square roots, $-i\sqrt{-x}$ and $+i\sqrt{-x}$ (where i is "the" square root of -1). Which of the two should we pick?

In this case, we could systematically pick $+i\sqrt{-x}$ but what if we extend the input domain to be $\mathbb{C}$? Then, it is not clear which of the two complex roots should be picked, as there is no obvious total order on $\mathbb{C}$. We can treat f as a *multivalued function*, that is, a function that may return several possible outputs for a given input value.

Experience shows that it is awkward to deal with multivalued functions and that it is best to treat them as relations (or to change the output domain to be a power set, which is equivalent to viewing the function as a relation).

Let us give one more example showing that it is not always easy to make sure that a formula is a proper definition of a function. Consider the function from $\mathbb{R}$ to $\mathbb{R}$ given by

$$f(x) = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}.$$

Here, $n!$ is the function *factorial*, defined by

$$n! = n \cdot (n-1) \cdots 2 \cdot 1.$$

How do we make sense of this infinite expression? Well, that's where analysis comes in, with the notion of limit of a series, and so on. It turns out that $f(x)$ is the exponential function $f(x) = e^x$. Actually, e^x is even defined when x is a complex number or even a square matrix (with real or complex entries). Don't panic, we do not use such functions in this course.

Another issue comes up, that is, the notion of *computability*. In all of our examples, and for most (partial) functions we will ever need to compute, it is clear

that it is possible to give a mechanical procedure, that is, a computer program that computes our functions (even if it hard to write such a program or if such a program takes a very long time to compute the output from the input).

Unfortunately, there are functions that, although well defined mathematically, are not computable.[1] For an example, let us go back to first-order logic and the notion of provable proposition. Given a finite (or countably infinite) alphabet of function, predicate, constant symbols, and a countable supply of variables, it is quite clear that the set $\mathscr{F}$ of all propositions built up from these symbols and variables can be enumerated systematically. We can define the function Prov with input domain $\mathscr{F}$ and output domain $\{0,1\}$, so that, for every proposition $P \in \mathscr{F}$,

$$\mathrm{Prov}(P) = \begin{cases} 1 & \text{if } P \text{ is provable (classically)} \\ 0 & \text{if } P \text{ is not provable (classically).} \end{cases}$$

Mathematically, for every proposition, $P \in \mathscr{F}$, either P is provable or it is not, so this function makes sense. However, by Church's theorem (see Section 1.11), we know that there is **no** computer program that will terminate for all input propositions and give an answer in a finite number of steps. So, although the function Prov makes sense as an abstract function, it is not computable.

Is this a paradox? No, if we are careful when defining a function not to incorporate in the definition any notion of computability and instead to take a more abstract and, in some some sense, naive view of a function as some kind of input/output process given by pairs $\langle$input value, output value$\rangle$ (without worrying about the way the output is "computed" from the input).

A rigorous way to proceed is to use the notion of ordered pair and of graph of a function. Before we do so, let us point out some facts about "functions" that were revealed by our examples:

1. In order to define a "function," in addition to defining its input/output behavior, it is also important to specify what is its *input domain* and its *output domain*.
2. Some "functions" may not be defined for all of their input values; a function can be a *partial function*.
3. The input/output behavior of a "function" can be defined by a set of ordered pairs. As we show next, this is the *graph* of the function.

We are now going to formalize the notion of function (possibly partial) using the concept of ordered pair.

---

[1] This can be proved quickly using the notion of *countable set* defined later in this chapter. The set of functions from $\mathbb{N}$ to itself is not countable but computer programs are finite strings over a finite alphabet, so the set of computer programs is countable.

2.2 Ordered Pairs, Cartesian Products, Relations, Functions, Partial Functions

Given two sets A and B, one of the basic constructions of set theory is the formation of an *ordered pair*, $\langle a,b \rangle$, where $a \in A$ and $b \in B$. Sometimes, we also write (a,b) for an ordered pair. The main property of ordered pairs is that if $\langle a_1,b_1 \rangle$ and $\langle a_2,b_2 \rangle$ are ordered pairs, where $a_1,a_2 \in A$ and $b_1,b_2 \in B$, then

$$\langle a_1,b_1 \rangle = \langle a_2,b_2 \rangle \text{ iff } a_1 = a_2 \text{ and } b_1 = b_2.$$

Observe that this property implies that

$$\langle a,b \rangle \neq \langle b,a \rangle,$$

unless $a = b$. Thus, the ordered pair $\langle a,b \rangle$ is not a notational variant for the set $\{a,b\}$; implicit to the notion of ordered pair is the fact that there is an order (even though we have not yet defined this notion) among the elements of the pair. Indeed, in $\langle a,b \rangle$, the element a comes first and b comes second. Accordingly, given an ordered pair $p = \langle a,b \rangle$, we denote a by $pr_1(p)$ and b by $pr_2(p)$ (*first and second projection* or *first and second coordinate*).

Remark: Readers who like set theory will be happy to hear that an ordered pair $\langle a,b \rangle$ can be defined as the set $\{\{a\},\{a,b\}\}$. This definition is due to K. Kuratowski, 1921. An earlier (more complicated) definition given by N. Wiener in 1914 is $\{\{\{a\},\emptyset\},\{\{b\}\}\}$.

Fig. 2.1 Kazimierz Kuratowski, 1896–1980

Now, from set theory, it can be shown that given two sets A and B, the set of all ordered pairs $\langle a,b \rangle$, with $a \in A$ and $b \in B$, is a set denoted $A \times B$ and called the *Cartesian product of A and B* (in that order). The set $A \times B$ is also called the *cross-product* of A and B.

By convention, we agree that $\emptyset \times B = A \times \emptyset = \emptyset$. To simplify the terminology, we often say *pair* for *ordered pair*, with the understanding that pairs are always ordered (otherwise, we should say set).

Of course, given three sets, A, B, C, we can form $(A \times B) \times C$ and we call its elements (ordered) *triples* (or *triplets*). To simplify the notation, we write $\langle a, b, c \rangle$ instead of $\langle \langle a, b \rangle, c \rangle$ and $A \times B \times C$ instead of $(A \times B) \times C$.

More generally, given n sets $A_1, \ldots, A_n$ ($n \geq 2$), we define the set of *n-tuples*, $A_1 \times A_2 \times \cdots \times A_n$, as $(\cdots ((A_1 \times A_2) \times A_3) \times \cdots) \times A_n$. An element of $A_1 \times A_2 \times \cdots \times A_n$ is denoted by $\langle a_1, \ldots, a_n \rangle$ (an *n*-tuple). We agree that when $n = 1$, we just have A_1 and a 1-tuple is just an element of A_1.

We now have all we need to define relations.

Definition 2.1. Given two sets A and B, a (binary) *relation between A and B* is any triple $\langle A, R, B \rangle$, where $R \subseteq A \times B$ is any set of ordered pairs from $A \times B$. When $\langle a, b \rangle \in R$, we also write aRb and we say that *a and b are related by R*. The set

$$dom(R) = \{a \in A \mid \exists b \in B, \ \langle a, b \rangle \in R\}$$

is called the *domain of R* and the set

$$range(R) = \{b \in B \mid \exists a \in A, \ \langle a, b \rangle \in R\}$$

is called the *range of R*. Note that $dom(R) \subseteq A$ and $range(R) \subseteq B$. When $A = B$, we often say that *R is a (binary) relation over A*.

Sometimes, the term *correspondence between A and B* is used instead of the term relation between A and B and the word *relation* is reserved for the case where $A = B$.

It is worth emphasizing that two relations $\langle A, R, B \rangle$ and $\langle A', R', B' \rangle$ are equal iff $A = A'$, $B = B'$, and $R = R'$. In particular, if $R = R'$ but either $A \neq A'$ or $B \neq B'$, then the relations $\langle A, R, B \rangle$ and $\langle A', R', B' \rangle$ *are considered to be different*. For simplicity, we usually refer to a relation $\langle A, R, B \rangle$ as a relation $R \subseteq A \times B$.

Among all relations between A and B, we mention three relations that play a special role:

1. $R = \emptyset$, the *empty relation*. Note that $dom(\emptyset) = range(\emptyset) = \emptyset$. This is not a very exciting relation.
2. When $A = B$, we have the *identity relation*,

$$\mathrm{id}_A = \{\langle a, a \rangle \mid a \in A\}.$$

   The identity relation relates every element to itself, and that's it. Note that $dom(\mathrm{id}_A) = range(\mathrm{id}_A) = A$.
3. The relation $A \times B$ itself. This relation relates every element of A to every element of B. Note that $dom(A \times B) = A$ and $range(A \times B) = B$.

Relations can be represented graphically by pictures often called graphs. (Beware, the term "graph" is very much overloaded. Later on, we define what a graph is.) We depict the elements of both sets A and B as points (perhaps with different colors) and we indicate that $a \in A$ and $b \in B$ are related (i.e., $\langle a, b \rangle \in R$) by drawing

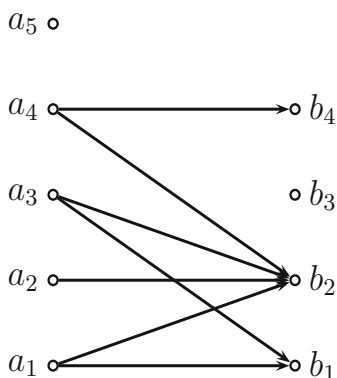an oriented edge (an arrow) starting from a (its source) and ending in b (its target). Here is an example:

$$a_5 \circ$$

Fig. 2.2 A binary relation, R

In Figure 2.2, $A = \{a_1, a_2, a_3, a_4, a_5\}$ and $B = \{b_1, b_2, b_3, b_4\}$. Observe that a_5 is not related to any element of B, b_3 is not related to any element of A, and that some elements of A, namely, a_1, a_3, a_4, are related to several elements of B.

Now, given a relation $R \subseteq A \times B$, some element $a \in A$ may be related to several distinct elements $b \in B$. If so, R does not correspond to our notion of a function, because we want our functions to be single-valued. So, we impose a natural condition on relations to get relations that correspond to functions.

Definition 2.2. We say that a relation R between two sets A and B is *functional* if for every $a \in A$, there is *at most one* $b \in B$ so that $\langle a, b \rangle \in R$. Equivalently, R is functional if for all $a \in A$ and all $b_1, b_2 \in B$, if $\langle a, b_1 \rangle \in R$ and $\langle a, b_2 \rangle \in R$, then $b_1 = b_2$.

The picture in Figure 2.3 shows an example of a functional relation.

Using Definition 2.2, we can give a rigorous definition of a function (partial or not).

Definition 2.3. A *partial function* f is a triple $f = \langle A, G, B \rangle$, where A is a set called the *input domain of f*, B is a set called the *output domain of f* (sometimes *codomain of f*), and $G \subseteq A \times B$ is a functional relation called the *graph of f* (see Figure 2.4); we let $graph(f) = G$. We write $f : A \to B$ to indicate that A is the input domain of f and that B is the codomain of f and we let $dom(f) = dom(G)$ and $range(f) = range(G)$. For every $a \in dom(f)$, the unique element $b \in B$, so that $\langle a, b \rangle \in graph(f)$ is denoted by $f(a)$ (so, $b = f(a)$). Often we say that $b = f(a)$ is the *image of a by f*. The range of f is also called the *image of f* and is denoted $\mathrm{Im}(f)$. If $dom(f) = A$, we say that f is a *total function*, for short, a *function with domain A*.
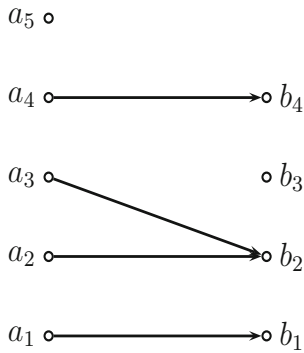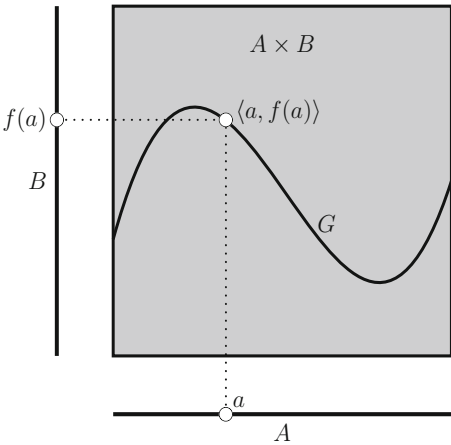
Fig. 2.3 A functional relation G

Fig. 2.4 A (partial) function $\langle A, G, B \rangle$

As in the case of relations, it is worth emphasizing that two functions (partial or total) $f = \langle A, G, B \rangle$ and $f' = \langle A', G', B' \rangle$ are equal iff $A = A'$, $B = B'$, and $G = G'$. In particular, if $G = G'$ but either $A \neq A'$ or $B \neq B'$, then the functions (partial or total) f and f' *are considered to be different.*

Observe that most computer programs are not defined for all inputs. For example, programs designed to run on numerical inputs will typically crash when given strings as input. Thus, most computer programs compute partial functions that are not total and it may be very hard to figure out what is the domain of these functions.

This is a strong motivation for considering the notion of a partial function and not just the notion of a (total) function.

Remarks:

1. If $f = \langle A, G, B \rangle$ is a partial function and $b = f(a)$ for some $a \in dom(f)$, we say that f *maps* a *to* b; we may write $f: a \mapsto b$. For any $b \in B$, the set

$$\{a \in A \mid f(a) = b\}$$

is denoted $f^{-1}(b)$ and called the *inverse image* or *preimage of b by f*. (It is also called the *fibre of f above b*. We explain this peculiar language later on.) Note that $f^{-1}(b) \neq \emptyset$ iff b is in the image (range) of f. Often, a function, partial or not, is called a *map*.

2. Note that Definition 2.3 allows $A = \emptyset$. In this case, we must have $G = \emptyset$ and, technically, $\langle \emptyset, \emptyset, B \rangle$ is a total function. It is the *empty function from $\emptyset$ to B*.

3. When a partial function is a total function, we don't call it a "partial total function," but simply a "function." The usual practice is that the term "function" refers to a total function. However, sometimes we say "total function" to stress that a function is indeed defined on all of its input domain.

4. Note that if a partial function $f = \langle A, G, B \rangle$ is not a total function, then $dom(f) \neq A$ and for all $a \in A - dom(f)$, there is **no** $b \in B$ so that $\langle a, b \rangle \in graph(f)$. This corresponds to the intuitive fact that f does not produce any output for any value not in its domain of definition. We can imagine that f "blows up" for this input (as in the situation where the denominator of a fraction is 0) or that the program computing f loops indefinitely for that input.

5. If $f = \langle A, G, B \rangle$ is a total function and $A \neq \emptyset$, then $B \neq \emptyset$.

6. For any set A, the identity relation id_A, is actually a function $id_A: A \to A$.

7. Given any two sets A and B, the rules $\langle a, b \rangle \mapsto a = pr_1(\langle a, b \rangle)$ and $\langle a, b \rangle \mapsto b = pr_2(\langle a, b \rangle)$ make pr_1 and pr_2 into functions $pr_1: A \times B \to A$ and $pr_2: A \times B \to B$ called the *first and second projections*.

8. A function $f: A \to B$ is sometimes denoted $A \xrightarrow{f} B$. Some authors use a different kind of arrow to indicate that f is partial, for example, a dotted or dashed arrow. We do not go that far.

9. The set of all functions, $f: A \to B$, is denoted by B^A. If A and B are finite, A has m elements and B has n elements, it is easy to prove that B^A has n^m elements.

The reader might wonder why, in the definition of a (total) function, $f: A \to B$, we do not require $B = \text{Im} f$, inasmuch as we require that $\text{dom}(f) = A$.

The reason has to do with experience and convenience. It turns out that in most cases, we know what the domain of a function is, but it may be very hard to determine exactly what its image is. Thus, it is more convenient to be flexible about the codomain. As long as we know that f maps into B, we are satisfied.

For example, consider functions $f: \mathbb{R} \to \mathbb{R}^2$ from the real line into the plane. The image of such a function is a *curve* in the plane $\mathbb{R}^2$. Actually, to really get "decent" curves we need to impose some reasonable conditions on f, for example, to be differentiable. Even continuity may yield very strange curves (see Section 2.10).

But even for a very well-behaved function, f, it may be very hard to figure out what the image of f is. Consider the function $t \mapsto (x(t), y(t))$ given by

$$x(t) = \frac{t(1+t^2)}{1+t^4}$$
$$y(t) = \frac{t(1-t^2)}{1+t^4}.$$

The curve that is the image of this function, shown in Figure 2.5, is called the "lemniscate of Bernoulli."
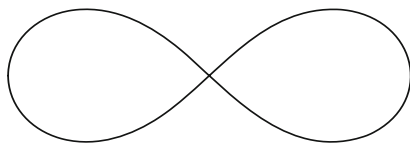

Fig. 2.5 Lemniscate of Bernoulli

Observe that this curve has a self-intersection at the origin, which is not so obvious at first glance.

2.3 Induction Principles on $\mathbb{N}$

Now that we have the notion of function, we can restate the induction principle (Version 2) stated at the end of Section 1.12 to make it more flexible. We define a *property of the natural numbers* as any function, $P: \mathbb{N} \to \{\textbf{true}, \textbf{false}\}$. The idea is that $P(n)$ holds iff $P(n) = \textbf{true}$, else $P(n) = \textbf{false}$. Then, we have the following principle.

Principle of Induction for $\mathbb{N}$ (Version 3).
Let P be any property of the natural numbers. In order to prove that $P(n)$ holds for all $n \in \mathbb{N}$, it is enough to prove that

(1) $P(0)$ holds.
(2) For every $n \in \mathbb{N}$, the implication $P(n) \Rightarrow P(n+1)$ holds.

As a formula, (1) and (2) can be written

$$[P(0) \wedge (\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))] \Rightarrow (\forall n \in \mathbb{N})P(n).$$

Step (1) is usually called the *basis* or *base step* of the induction and step (2) is called the *induction step*. In step (2), $P(n)$ is called the *induction hypothesis*. That the above induction principle is valid is given by the following.

Proposition 2.1. *The principle of induction stated above is valid.*

Proof. Let

$$S = \{n \in \mathbb{N} \mid P(n) = \textbf{true}\}.$$

By the induction principle (Version 2) stated at the end of Section 1.12, it is enough to prove that S is inductive, because then $S = \mathbb{N}$ and we are done.

Because $P(0)$ hold, we have $0 \in S$. Now, if $n \in S$ (i.e., if $P(n)$ holds), because $P(n) \Rightarrow P(n+1)$ holds for every n we deduce that $P(n+1)$ holds; that is, $n+1 \in S$. Therefore, S is inductive as claimed and this finishes the proof. $\square$

Induction is a very valuable tool for proving properties of the natural numbers and we make extensive use of it. We also show other more powerful induction principles. Let us give some examples illustrating how it is used.

We begin by finding a formula for the sum

$$1+2+3+\cdots+n,$$

where $n \in \mathbb{N}$. If we compute this sum for small values of n, say $n = 0,1,2,3,4,5,6$ we get

$$
\begin{aligned}
0 &= 0 \\
1 &= 1 \\
1+2 &= 3 \\
1+2+3 &= 6 \\
1+2+3+4 &= 10 \\
1+2+3+4+5 &= 15 \\
1+2+3+4+5+6 &= 21.
\end{aligned}
$$

What is the pattern?

After a moment of reflection, we see that

$$
\begin{aligned}
0 &= (0 \times 1)/2 \\
1 &= (1 \times 2)/2 \\
3 &= (2 \times 3)/2 \\
6 &= (3 \times 4)/2 \\
10 &= (4 \times 5)/2 \\
15 &= (5 \times 6)/2 \\
21 &= (6 \times 7)/2,
\end{aligned}
$$

so we conjecture

Claim 1:

$$1+2+3+\cdots+n = \frac{n(n+1)}{2},$$

where $n \in \mathbb{N}$.

For the basis of the induction, where $n = 0$, we get $0 = 0$, so the base step holds.

For the induction step, for any $n \in \mathbb{N}$, assume that

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

Consider $1+2+3+\cdots+n+(n+1)$. Then, using the induction hypothesis, we have

$$1+2+3+\cdots+n+(n+1) = \frac{n(n+1)}{2}+n+1$$
$$= \frac{n(n+1)+2(n+1)}{2}$$
$$= \frac{(n+1)(n+2)}{2},$$

establishing the induction hypothesis and therefore proving our formula. □

Next, let us find a formula for the sum of the first $n+1$ odd numbers:

$$1+3+5+\cdots+2n+1,$$

where $n \in \mathbb{N}$. If we compute this sum for small values of n, say $n = 0,1,2,3,4,5,6$ we get

$$1 = 1$$
$$1+3 = 4$$
$$1+3+5 = 9$$
$$1+3+5+7 = 16$$
$$1+3+5+7+9 = 25$$
$$1+3+5+7+9+11 = 36$$
$$1+3+5+7+9+11+13 = 49.$$

This time, it is clear what the pattern is: we get perfect squares. Thus, we conjecture

Claim 2:

$$1+3+5+\cdots+2n+1 = (n+1)^2,$$

where $n \in \mathbb{N}$.

For the basis of the induction, where $n = 0$, we get $1 = 1^2$, so the base step holds.

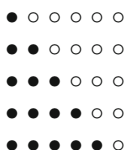For the induction step, for any $n \in \mathbb{N}$, assume that

$$1+3+5+\cdots+2n+1 = (n+1)^2.$$

Consider $1+3+5+\cdots+2n+1+2(n+1)+1 = 1+3+5+\cdots+2n+1+2n+3$. Then, using the induction hypothesis, we have

$$1+3+5+\cdots+2n+1+2n+3 = (n+1)^2+2n+3$$
$$= n^2+2n+1+2n+3 = n^2+4n+4$$
$$= (n+2)^2.$$

Therefore, the induction step holds and this completes the proof by induction. □

The two formulae that we just discussed are subject to a nice geometric interpetation that suggests a closed-form expression for each sum and this is often the case for sums of special kinds of numbers. For the first formula, if we represent n as a sequence of n "bullets," then we can form a rectangular array with n rows and $n+1$ columns showing that the desired sum is half of the number of bullets in the array, which is indeed $n(n+1)/2$, as shown below for $n=5$:

$$
\begin{array}{cccccc}
\bullet & \circ & \circ & \circ & \circ & \circ \\
\bullet & \bullet & \circ & \circ & \circ & \circ \\
\bullet & \bullet & \bullet & \circ & \circ & \circ \\
\bullet & \bullet & \bullet & \bullet & \circ & \circ \\
\bullet & \bullet & \bullet & \bullet & \bullet & \circ \\
\end{array}
$$

Thus, we see that the numbers

$$\Delta_n = \frac{n(n+1)}{2},$$

have a simple geometric interpretation in terms of triangles of bullets; for example, $\Delta_4 = 10$ is represented by the triangle

$$
\begin{array}{ccccccc}
 & & & \bullet & & & \\
 & & \bullet & & \bullet & & \\
 & \bullet & & \bullet & & \bullet & \\
\bullet & & \bullet & & \bullet & & \bullet \\
\end{array}
$$

For this reason, the numbers Δ_n are often called *triangular numbers*. A natural question then arises; what is the sum

$$\Delta_1+\Delta_2+\Delta_3+\cdots+\Delta_n?$$

The reader should compute these sums for small values of n and try to guess a formula that should then be proved correct by induction. It is not too hard to find a nice formula for these sums. The reader may also want to find a geometric interpretation for the above sums (stacks of cannon balls).

In order to get a geometric interpretation for the sum

$$1+3+5+\cdots+2n+1,$$

we represent $2n+1$ using $2n+1$ bullets displayed in a V-shape; for example, $7 = 2 \times 3 + 1$ is represented by

Then, the sum $1 + 3 + 5 + \cdots + 2n + 1$ corresponds to the square

which clearly reveals that

$$1 + 3 + 5 + \cdots + 2n + 1 = (n+1)^2.$$

A natural question is then; what is the sum

$$1^2 + 2^2 + 3^2 + \cdots + n^2?$$

Again, the reader should compute these sums for small values of n, then guess a formula and check its correctness by induction. It is not too difficult to find such a formula. For a fascinating discussion of all sorts of numbers and their geometric interpretations (including the numbers we just introduced), the reader is urged to read Chapter 2 of Conway and Guy [1].

Sometimes, it is necessary to prove a property $P(n)$ for all natural numbers $n \geq m$, where $m > 0$. Our induction principle does not seem to apply because the base case is not $n = 0$. However, we can define the property $Q(n)$ given by

$$Q(n) = P(m+n), \ n \in \mathbb{N},$$

and because $Q(n)$ holds for all $n \in \mathbb{N}$ iff $P(k)$ holds for all $k \geq m$, we can apply our induction principle to prove $Q(n)$ for all $n \in \mathbb{N}$ and thus, $P(k)$, for all $k \geq m$ (note, $k = m+n$). Of course, this amounts to considering that the base case is $n = m$ and this is what we always do without any further justification. Here is an example.

Let us prove that

$$(3n)^2 \leq 2^n, \ \text{for all } n \geq 10.$$

The base case is $n = 10$. For $n = 10$, we get

$$(3 \times 10)^2 = 30^2 = 900 \leq 1024 = 2^{10},$$

which is indeed true. Let us now prove the induction step. Assuming that $(3n)^2 \leq 2^n$ holds for all $n \geq 10$, we want to prove that $(3(n+1))^2 \leq 2^{n+1}$. As

$$(3(n+1))^2 = (3n+3)^2 = (3n)^2 + 18n + 9,$$

if we can prove that $18n + 9 \leq (3n)^2$ when $n \geq 10$, using the induction hypothesis, $(3n)^2 \leq 2^n$, we have

$$(3(n+1))^2 = (3n)^2 + 18n + 9 \leq (3n)^2 + (3n)^2 \leq 2^n + 2^n = 2^{n+1},$$

establishing the induction step. However,

$$(3n)^2 - (18n + 9) = (3n - 3)^2 - 18$$

and $(3n - 3)^2 \geq 18$ as soon as $n \geq 3$, so $18n + 9 \leq (3n)^2$ when $n \geq 10$, as required.

Observe that the formula $(3n)^2 \leq 2^n$ fails for $n = 9$, because $(3 \times 9)^2 = 27^2 = 729$ and $2^9 = 512$, but $729 > 512$. Thus, the base has to be $n = 10$.

There is another induction principle which is often more flexible than our original induction principle. This principle, called *complete induction* (or sometimes *strong induction*), is stated below.

Complete Induction Principle for $\mathbb{N}$.

In order to prove that a predicate $P(n)$ holds for all $n \in \mathbb{N}$ it is enough to prove that

(1) $P(0)$ holds (the base case).
(2) For every $m \in \mathbb{N}$, if $(\forall k \in \mathbb{N})(k \leq m \Rightarrow P(k))$ then $P(m+1)$.

The difference between ordinary induction and complete induction is that in complete induction, the induction hypothesis $(\forall k \in \mathbb{N})(k \leq m \Rightarrow P(k))$ assumes that $P(k)$ holds for all $k \leq m$ and not just for m (as in ordinary induction), in order to deduce $P(m+1)$. This gives us more proving power as we have more knowledge in order to prove $P(m+1)$. Complete induction is discussed more extensively in Section 5.3 and its validity is proved as a consequence of the fact that every nonempty subset of $\mathbb{N}$ has a smallest element but we can also justify its validity as follows. Define $Q(m)$ by

$$Q(m) = (\forall k \in \mathbb{N})(k \leq m \Rightarrow P(k)).$$

Then, it is an easy exercise to show that if we apply our (ordinary) induction principle to $Q(m)$ (induction principle, Version 3), then we get the principle of complete induction. Here is an example of a proof using complete induction.

Define the sequence of natural numbers F_n (*Fibonacci sequence*) by

$$F_0 = 1, \; F_1 = 1, \; F_{n+2} = F_{n+1} + F_n, \; n \geq 0.$$

We claim that

$$F_n \geq \frac{3^{n-2}}{2^{n-3}}, \; n \geq 3.$$

Fig. 2.6 Leonardo P. Fibonacci, 1170–1250

The base case corresponds to $n = 3$, where

$$F_3 = 3 \geq \frac{3^1}{2^0} = 3,$$

which is true. Note that we also need to consider the case $n = 4$ by itself before we do the induction step because even though $F_4 = F_3 + F_2$, the induction hypothesis only applies to F_3 ($n \geq 3$ in the inequality above). We have

$$F_4 = 5 \geq \frac{3^2}{2^1} = \frac{9}{2},$$

which is true because $10 > 9$. Now for the induction step where $n \geq 3$, we have

$$
\begin{aligned}
F_{n+2} &= F_{n+1} + F_n \\
&\geq \frac{3^{n-1}}{2^{n-2}} + \frac{3^{n-2}}{2^{n-3}} \\
&\geq \frac{3^{n-2}}{2^{n-3}}\left(1 + \frac{3}{2}\right) = \frac{3^{n-2}}{2^{n-3}}\frac{5}{2} \geq \frac{3^{n-2}}{2^{n-3}}\frac{9}{4} = \frac{3^n}{2^{n-1}},
\end{aligned}
$$

since $5/2 > 9/4$, which concludes the proof of the induction step. Observe that we used the induction hypothesis for both F_{n+1} and F_n in order to deduce that it holds for F_{n+2}. This is where we needed the extra power of complete induction.

Remark: The Fibonacci sequence F_n is really a function from $\mathbb{N}$ to $\mathbb{N}$ defined recursively but we haven't proved yet that recursive definitions are legitimate methods for defining functions. In fact, certain restrictions are needed on the kind of recursion used to define functions. This topic is explored further in Section 2.5. Using results from Section 2.5, it can be shown that the Fibonacci sequence is a well-defined function (but this does not follow immediately from Theorem 2.1).

Induction proofs can be subtle and it might be instructive to see some examples of *faulty* induction proofs.

Assertion 1: For every natural numbers $n \geq 1$, the number $n^2 - n + 11$ is an odd prime (recall that a prime number is a natural number $p \geq 2$, which is only divisible by 1 and itself).

Proof. We use induction on $n \geq 1$. For the base case $n = 1$, we have $1^2 - 1 + 11 = 11$, which is an odd prime, so the induction step holds.

Assume inductively that $n^2 - n + 11$ is prime. Then, as

$$(n+1)^2 - (n+1) + 11 = n^2 + 2n + 1 - n - 1 + 11 = n^2 + n + 11,$$

we see that

$$(n+1)^2 - (n+1) + 11 = n^2 - n + 11 + 2n.$$

By the induction hypothesis, $n^2 - n + 11$ is an odd prime p, and because $2n$ is even, $p + 2n$ is odd and therefore prime, establishing the induction hypothesis.   □

If we compute $n^2 - n + 11$ for $n = 1, 2, \ldots, 10$, we find that these numbers are indeed all prime, but for $n = 11$, we get

$$121 = 11^2 - 11 + 11 = 11 \times 11,$$

which is not prime.

Where is the mistake?

What is wrong is the induction step: the fact that $n^2 - n + 11$ is prime does not imply that $(n+1)^2 - (n+1) + 11 = n^2 + n + 11$ is prime, as illustrated by $n = 10$. Our "proof" of the induction step is nonsense.

The lesson is: the fact that a statement holds for many values of $n \in \mathbb{N}$ does not imply that it holds for all $n \in \mathbb{N}$ (or all $n \geq k$, for some fixed $k \in \mathbb{N}$).

Interestingly, the prime numbers k, so that $n^2 - n + k$ is prime for $n = 1, 2, \ldots, k - 1$, are all known (there are only six of them). It can be shown that these are the prime numbers k such that $1 - 4k$ is a *Heegner number*, where the Heegner numbers are the nine integers:

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

The above results are hard to prove and require some deep theorems of number theory. What can also be shown (and you should prove it) is that no nonconstant polynomial takes prime numbers as values for all natural numbers.

Assertion 2: Every Fibonacci number F_n is even.

Proof.   For the base case, $F_2 = 2$, which is even, so the base case holds.

Assume inductively that F_n is even for all $n \geq 2$. Then, as

$$F_{n+2} = F_{n+1} + F_n$$

and as both F_n and F_{n+1} are even by the induction hypothesis, we conclude that F_{n+2} is even.   □

However, Assertion 2 is clearly false, because the Fibonacci sequence begins with

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots.$$

This time, the mistake is that we did not check the two base cases, $F_0 = 1$ and $F_1 = 1$.

Our experience is that if an induction proof is wrong, then, in many cases, the base step is faulty. So, pay attention to the base step(s).

A useful way to produce new relations or functions is to compose them.

2.4 Composition of Relations and Functions

We begin with the definition of the composition of relations.

Definition 2.4. Given two relations $R \subseteq A \times B$ and $S \subseteq B \times C$, the *composition of R and S*, denoted $R \circ S$, is the relation between A and C defined by

$$R \circ S = \{\langle a,c \rangle \in A \times C \mid \exists b \in B, \langle a,b \rangle \in R \text{ and } \langle b,c \rangle \in S\}.$$

One should check that for any relation $R \subseteq A \times B$, we have $\mathrm{id}_A \circ R = R$ and $R \circ \mathrm{id}_B = R$. If R and S are the graphs of functions, possibly partial, is $R \circ S$ the graph of some function? The answer is yes, as shown in the following.

Proposition 2.2. *Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be two relations.*

(a) *If R and S are both functional relations, then $R \circ S$ is also a functional relation. Consequently, $R \circ S$ is the graph of some partial function.*
(b) *If $dom(R) = A$ and $dom(S) = B$, then $dom(R \circ S) = A$.*
(c) *If R is the graph of a (total) function from A to B and S is the graph of a (total) function from B to C, then $R \circ S$ is the graph of a (total) function from A to C.*

Proof.   (a) Assume that $\langle a,c_1 \rangle \in R \circ S$ and $\langle a,c_2 \rangle \in R \circ S$. By definition of $R \circ S$, there exist $b_1, b_2 \in B$ so that

$$\langle a,b_1 \rangle \in R, \ \langle b_1,c_1 \rangle \in S,$$
$$\langle a,b_2 \rangle \in R, \ \langle b_2,c_2 \rangle \in S.$$

As R is functional, $\langle a,b_1 \rangle \in R$ and $\langle a,b_2 \rangle \in R$ implies $b_1 = b_2$. Let $b = b_1 = b_2$, so that $\langle b_1,c_1 \rangle = \langle b,c_1 \rangle$ and $\langle b_2,c_2 \rangle = \langle b,c_2 \rangle$. But, S is also functional, so $\langle b,c_1 \rangle \in S$ and $\langle b,c_2 \rangle \in S$ implies that $c_1 = c_2$, which proves that $R \circ S$ is functional.

(b) If $A = \emptyset$ then $R = \emptyset$ and so $R \circ S = \emptyset$, which implies that $dom(R \circ S) = \emptyset = A$. If $A \neq \emptyset$, pick any $a \in A$. The fact that $dom(R) = A \neq \emptyset$ means that there is some $b \in B$ so that $\langle a,b \rangle \in R$ and so, $B \neq \emptyset$. As $dom(S) = B \neq \emptyset$, there is some $c \in C$ so that $\langle b,c \rangle \in S$. Then, by the definition of $R \circ S$, we see that $\langle a,c \rangle \in R \circ S$. The argument holds for any $a \in A$, therefore we deduce that $dom(R \circ S) = A$.

(c) If R and S are the graphs of partial functions, then this means that they are functional and (a) implies that $R \circ S$ is also functional. This shows that $R \circ S$ is the graph of the partial function $\langle A, R \circ S, C \rangle$. If R and S are the graphs of total functions, then $dom(R) = A$ and $dom(S) = B$. By (b), we deduce that $dom(R \circ S) = A$. By the

first part of (c), $R \circ S$ is the graph of the partial function $\langle A, R \circ S, C \rangle$, which is a total function, inasmuch as $dom(R \circ S) = A$. $\square$

Proposition 2.2 shows that it is legitimate to define the composition of functions, possibly partial. Thus, we make the following definition.

Definition 2.5. Given two functions $f: A \to B$ and $g: B \to C$, possibly partial, the *composition of f and g*, denoted $g \circ f$, is the function (possibly partial)

$$g \circ f = \langle A, graph(f) \circ graph(g), C \rangle.$$

The reader must have noticed that the composition of two functions $f: A \to B$ and $g: B \to C$ is denoted $g \circ f$, whereas the graph of $g \circ f$ is denoted $graph(f) \circ graph(g)$. This "reversal" of the order in which function composition and relation composition are written is unfortunate and somewhat confusing.

Once again, we are the victims of tradition. The main reason for writing function composition as $g \circ f$ is that traditionally the result of applying a function f to an argument x is written $f(x)$. Then, $(g \circ f)(x) = g(f(x))$, because $z = (g \circ f)(x)$ iff there is some y so that $y = f(x)$ and $z = g(y)$; that is, $z = g(f(x))$. Some people, in particular algebraists, write function composition as $f \circ g$, but then, they write the result of applying a function f to an argument x as xf. With this convention, $x(f \circ g) = (xf)g$, which also makes sense.

We prefer to stick to the convention where we write $f(x)$ for the result of applying a function f to an argument x and, consequently, we use the notation $g \circ f$ for the composition of f with g, even though it is the opposite of the convention for writing the composition of relations.

Given any three relations, $R \subseteq A \times B$, $S \subseteq B \times C$, and $T \subseteq C \times D$, the reader should verify that

$$(R \circ S) \circ T = R \circ (S \circ T).$$

We say that composition is *associative*. Similarly, for any three functions (possibly partial), $f: A \to B$, $g: B \to C$, and $h: C \to D$, we have (associativity of function composition)

$$(h \circ g) \circ f = h \circ (g \circ f).$$

2.5 Recursion on $\mathbb{N}$

The following situation often occurs. We have some set A, some fixed element $a \in A$, some function $g: A \to A$, and we wish to define a new function $h: \mathbb{N} \to A$, so that

$$h(0) = a,$$
$$h(n+1) = g(h(n)) \text{ for all } n \in \mathbb{N}.$$

This way of defining h is called a *recursive definition* (or a definition by *primitive recursion*). I would be surprised if any computer scientist had any trouble with this "definition" of h but how can we justify rigorously that such a function exists and is unique?

Indeed, the existence (and uniqueness) of h requires proof. The proof, although not really hard, is surprisingly involved and in fact quite subtle. For those reasons, we do not give a proof of the following theorem but instead the main idea of the proof. The reader will find a complete proof in Enderton [2] (Chapter 4).

Theorem 2.1. *(Recursion theorem on $\mathbb{N}$) Given any set A, any fixed element $a \in A$, and any function $g\colon A \to A$, there is a unique function $h\colon \mathbb{N} \to A$, so that*

$$h(0) = a,$$
$$h(n+1) = g(h(n)) \text{ for all } n \in \mathbb{N}.$$

Proof. The idea is to approximate h. To do this, define a function f to be *acceptable* iff

1. $dom(f) \subseteq \mathbb{N}$ and $range(f) \subseteq A$.
2. If $0 \in dom(f)$, then $f(0) = a$.
3. If $n+1 \in dom(f)$, then $n \in dom(f)$ and $f(n+1) = g(f(n))$.

Let $\mathscr{F}$ be the collection of all acceptable functions and set

$$h = \bigcup \mathscr{F}.$$

All we can say, so far, is that h is a relation. We claim that h is the desired function. For this, four things need to be proved:

1. The relation h is a function.
2. The function h is acceptable.
3. The function h has domain $\mathbb{N}$.
4. The function h is unique.

As expected, we make heavy use of induction in proving (1)–(4). For complete details, see Enderton [2] (Chapter 4). $\square$

Theorem 2.1 is very important. Indeed, experience shows that it is used almost as much as induction. As an example, we show how to define addition on $\mathbb{N}$. Indeed, at the moment, we know what the natural numbers are but we don't know what are the arithmetic operations such as $+$ or $*$ (at least, not in our axiomatic treatment; of course, nobody needs an axiomatic treatment to know how to add or multiply).

How do we define $m+n$, where $m, n \in \mathbb{N}$?

If we try to use Theorem 2.1 directly, we seem to have a problem, because addition is a function of two arguments, but h and g in the theorem only take one argument. We can overcome this problem in two ways:

(1) We prove a generalization of Theorem 2.1 involving functions of several argu-
ments, but with recursion only in a *single* argument. This can be done quite
easily but we have to be a little careful.
(2) For any fixed m, we define $add_m(n)$ as $add_m(n) = m + n$; that is, we define
addition of a *fixed* m to any n. Then, we let $m + n = add_m(n)$.

Solution (2) involves much less work, thus we follow it. Let S denote the succes-
sor function on $\mathbb{N}$, that is, the function given by

$$S(n) = n^+ = n + 1.$$

Then, using Theorem 2.1 with $a = m$ and $g = S$, we get a function, add_m, such that

$$add_m(0) = m,$$
$$add_m(n+1) = S(add_m(n)) = add_m(n) + 1 \qquad \text{for all} \quad n \in \mathbb{N}.$$

Finally, for all $m, n \in \mathbb{N}$, we define $m + n$ by

$$m + n = add_m(n).$$

Now, we have our addition function on $\mathbb{N}$. But this is not the end of the story be-
cause we don't know yet that the above definition yields a function having the usual
properties of addition, such as

$$m + 0 = m$$
$$m + n = n + m$$
$$(m + n) + p = m + (n + p).$$

To prove these properties, of course, we use induction.
     We can also define multiplication. Mimicking what we did for addition, define
$mult_m(n)$ by recursion as follows.

$$mult_m(0) = 0,$$
$$mult_m(n+1) = mult_m(n) + m \text{ for all } n \in \mathbb{N}.$$

Then, we set

$$m \cdot n = mult_m(n).$$

Note how the recursive definition of $mult_m$ uses the adddition function $+$, previ-
ously defined. Again, to prove the usual properties of multiplication as well as the
distributivity of $\cdot$ over $+$, we use induction. Using recursion, we can define many
more arithmetic functions. For example, the reader should try defining exponentia-
tion m^n.

We still haven't defined the usual ordering on the natural numbers but we do so later. Of course, we all know what it is and we do not refrain from using it. Still, it is interesting to give such a definition in our axiomatic framework.

2.6 Inverses of Functions and Relations

Given a function $f\colon A \to B$ (possibly partial), with $A \neq \emptyset$, suppose there is some function $g\colon B \to A$ (possibly partial), called a *left inverse of f*, such that

$$g \circ f = \mathrm{id}_A.$$

If such a g exists, we see that f must be total but more is true. Indeed, assume that $f(a) = f(b)$. Then, by applying g, we get

$$(g \circ f)(a) = g(f(a)) = g(f(b)) = (g \circ f)(b).$$

However, because $g \circ f = \mathrm{id}_A$, we have $(g \circ f)(a) = \mathrm{id}_A(a) = a$ and $(g \circ f)(b) = \mathrm{id}_A(b) = b$, so we deduce that
$$a = b.$$

Therefore, we showed that if a function f with nonempty domain has a left inverse, then f is total and has the property that for all $a, b \in A$, $f(a) = f(b)$ implies that $a = b$, or equivalently $a \neq b$ implies that $f(a) \neq f(b)$. We say that f is *injective*. As we show later, injectivity is a very desirable property of functions.

Remark: If $A = \emptyset$, then f is still considered to be injective. In this case, g is the empty partial function (and when $B = \emptyset$, both f and g are the empty function from $\emptyset$ to itself).

Now, suppose there is some function $h\colon B \to A$ (possibly partial) with $B \neq \emptyset$ called a *right inverse of f*, but this time, we have

$$f \circ h = \mathrm{id}_B.$$

If such an h exists, we see that it must be total but more is true. Indeed, for any $b \in B$, as $f \circ h = \mathrm{id}_B$, we have

$$f(h(b)) = (f \circ h)(b) = \mathrm{id}_B(b) = b.$$

Therefore, we showed that if a function f with nonempty codomain has a right inverse h then h is total and f has the property that for all $b \in B$, there is some $a \in A$, namely, $a = h(b)$, so that $f(a) = b$. In other words, $\mathrm{Im}\,(f) = B$ or equivalently, every element in B is the image by f of some element of A. We say that f is *surjective*. Again, surjectivity is a very desirable property of functions.

Remark: If $B = \emptyset$, then f is still considered to be surjective but h is not total unless $A = \emptyset$, in which case f is the empty function from $\emptyset$ to itself.

If a function has a left inverse (respectively, a right inverse), then it may have more than one left inverse (respectively, right inverse).

If a function (possibly partial) $f: A \to B$ with $A, B \neq \emptyset$ happens to have both a left inverse $g: B \to A$ and a right inverse $h: B \to A$, then we know that f and h are total. We claim that $g = h$, so that g is total and moreover g is uniquely determined by f.

Lemma 2.1. *Let $f: A \to B$ be any function and suppose that f has a left inverse $g: B \to A$ and a right inverse $h: B \to A$. Then, $g = h$ and, moreover, g is unique, which means that if $g': B \to A$ is any function that is both a left and a right inverse of f, then $g' = g$.*

Proof. Assume that

$$g \circ f = \mathrm{id}_A \text{ and } f \circ h = \mathrm{id}_B.$$

Then, we have

$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h.$$

Therefore, $g = h$. Now, if g' is any other left inverse of f and h' is any other right inverse of f, the above reasoning applied to g and h' shows that $g = h'$ and the same reasoning applied to g' and h' shows that $g' = h'$. Therefore, $g' = h' = g = h$, that is, g is uniquely determined by f.   □

This leads to the following definition.

Definition 2.6. A function $f: A \to B$ is said to be *invertible* iff there is a function $g: B \to A$ which is both a left inverse and a right inverse; that is,

$$g \circ f = \mathrm{id}_A \text{ and } f \circ g = \mathrm{id}_B.$$

In this case, we know that g is unique and it is denoted f^{-1}.

From the above discussion, if a function is invertible, then it is both injective and surjective. This shows that a function *generally does not have an inverse*. In order to have an inverse a function needs to be injective and surjective, but this fails to be true for many functions. It turns out that if a function is injective and surjective then it has an inverse. We prove this in the next section.

The notion of inverse can also be defined for relations, but it is a somewhat weaker notion.

Definition 2.7. Given any relation $R \subseteq A \times B$, the *converse* or *inverse* of R is the relation $R^{-1} \subseteq B \times A$, defined by

$$R^{-1} = \{\langle b, a \rangle \in B \times A \mid \langle a, b \rangle \in R\}.$$

In other words, R^{-1} is obtained by swapping A and B and reversing the orientation of the arrows. Figure 2.7 below shows the inverse of the relation of Figure 2.2:
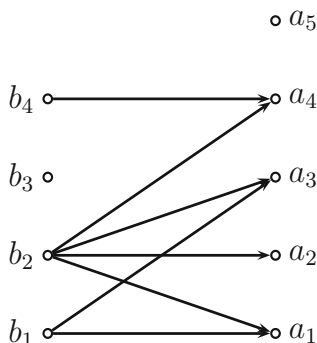
Fig. 2.7 The inverse of the relation R from Figure 2.2

Now, if R is the graph of a (partial) function f, beware that R^{-1} is generally *not* the graph of a function at all, because R^{-1} may not be functional. For example, the inverse of the graph G in Figure 2.3 is *not* functional; see below.
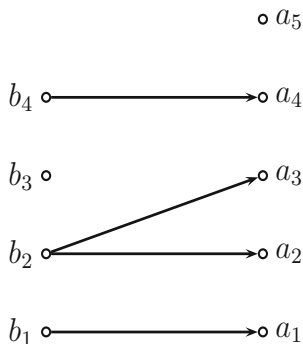
Fig. 2.8 The inverse, G^{-1}, of the graph of Figure 2.3

The above example shows that one has to be careful not to view a function as a relation in order to take its inverse. In general, this process does not produce a function. This only works if the function is invertible.

Given any two relations, $R \subseteq A \times B$ and $S \subseteq B \times C$, the reader should prove that

$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}.$$

(Note the switch in the order of composition on the right-hand side.) Similarly, if $f : A \to B$ and $g : B \to C$ are any two invertible functions, then $g \circ f$ is invertible and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

2.7 Injections, Surjections, Bijections, Permutations

We encountered injectivity and surjectivity in Section 2.6. For the record, let us give the following.

Definition 2.8. Given any function $f: A \to B$, we say that f *is injective* (or *one-to-one*) iff for all $a, b \in A$, if $f(a) = f(b)$, then $a = b$, or equivalently, if $a \neq b$, then $f(a) \neq f(b)$. We say that f *is surjective* (or *onto*) iff for every $b \in B$, there is some $a \in A$ so that $b = f(a)$, or equivalently if $\mathrm{Im}(f) = B$. The function f is *bijective* iff it is both injective and surjective. When $A = B$, a bijection $f: A \to A$ is called a *permutation of A*.
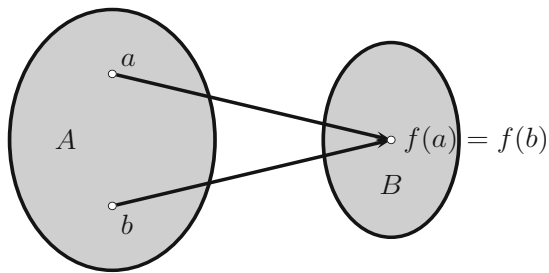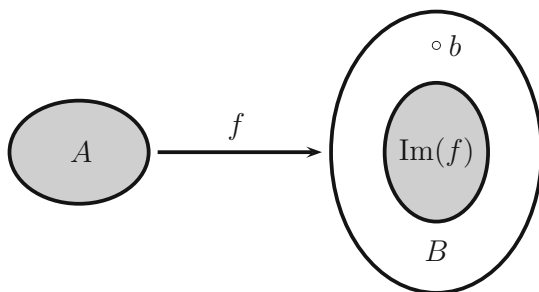
Remarks:

1. If $A = \emptyset$, then any function, $f: \emptyset \to B$ is (trivially) injective.
2. If $B = \emptyset$, then f is the empty function from $\emptyset$ to itself and it is (trivially) surjective.
3. A function, $f: A \to B$, is **not injective** iff **there exist** $a, b \in A$ with $a \neq b$ and **yet** $f(a) = f(b)$; see Figure 2.9.
4. A function, $f: A \to B$, is **not surjective** iff **for some** $b \in B$, **there is no** $a \in A$ with $b = f(a)$; see Figure 2.10.
5. We have $\mathrm{Im} f = \{b \in B \mid (\exists a \in A)(b = f(a))\}$, thus a function $f: A \to B$ is always surjective onto its image.
6. The notation $f: A \hookrightarrow B$ is often used to indicate that a function $f: A \to B$ is an injection.
7. If $A \neq \emptyset$, a function $f: A \to B$ is injective iff for every $b \in B$, there *at most one* $a \in A$ such that $b = f(a)$.
8. If $A \neq \emptyset$, a function $f: A \to B$ is surjective iff for every $b \in B$, there *at least one* $a \in A$ such that $b = f(a)$ iff $f^{-1}(b) \neq \emptyset$ for all $b \in B$.
9. If $A \neq \emptyset$, a function $f: A \to B$ is bijective iff for every $b \in B$, there is *a unique* $a \in A$ such that $b = f(a)$.
10. When A is the finite set $A = \{1, \ldots, n\}$, also denoted $[n]$, it is not hard to show that there are $n!$ permutations of $[n]$.

The function $f_1: \mathbb{Z} \to \mathbb{Z}$ given by $f_1(x) = x + 1$ is injective and surjective. However, the function $f_2: \mathbb{Z} \to \mathbb{Z}$ given by $f_2(x) = x^2$ is neither injective nor surjective (why?). The function $f_3: \mathbb{Z} \to \mathbb{Z}$ given by $f_3(x) = 2x$ is injective but not surjective. The function $f_4: \mathbb{Z} \to \mathbb{Z}$ given by

$$f_4(x) = \begin{cases} k & \text{if } x = 2k \\ k & \text{if } x = 2k+1 \end{cases}$$

is surjective but not injective.

Fig. 2.9 A noninjective function

Fig. 2.10 A nonsurjective function

Remark: The reader should prove that if A and B are finite sets, A has m elements and B has n elements ($m \leq n$) then the set of injections from A to B has

$$\frac{n!}{(n-m)!}$$

elements. The following theorem relates the notions of injectivity and surjectivity to the existence of left and right inverses.

Theorem 2.2. *Let $f \colon A \to B$ be any function and assume $A \neq \emptyset$.*

(a) The function f is injective iff it has a left inverse g (i.e., a function $g \colon B \to A$ so that $g \circ f = \mathrm{id}_A$).
(b) The function f is surjective iff it has a right inverse h (i.e., a function $h \colon B \to A$ so that $f \circ h = \mathrm{id}_B$).
(c) The function f is invertible iff it is injective and surjective.

Proof. (a) We already proved in Section 2.6 that the existence of a left inverse implies injectivity. Now, assume f is injective. Then, for every $b \in range(f)$, there

is a unique $a_b \in A$ so that $f(a_b) = b$. Because $A \neq \emptyset$, we may pick some a_0 in A. We define $g\colon B \to A$ by

$$g(b) = \begin{cases} a_b & \text{if } b \in range(f) \\ a_0 & \text{if } b \in B - range(f). \end{cases}$$

Then, $g(f(a)) = a$ for all $a \in A$, because $f(a) \in range(f)$ and a is the only element of A so that $f(a) = f(a)$. This shows that $g \circ f = \mathrm{id}_A$, as required.

(b) We already proved in Section 2.6 that the existence of a right inverse implies surjectivity. For the converse, assume that f is surjective. As $A \neq \emptyset$ and f is a function (i.e., f is total), $B \neq \emptyset$. So, for every $b \in B$, the preimage $f^{-1}(b) = \{a \in A \mid f(a) = b\}$ is nonempty. We make a function $h\colon B \to A$ as follows. For each $b \in B$, pick some element $a_b \in f^{-1}(b)$ (which is nonempty) and let $h(b) = a_b$. By definition of $f^{-1}(b)$, we have $f(a_b) = b$ and so,

$$f(h(b)) = f(a_b) = b, \quad \text{for all } b \in B.$$

This shows that $f \circ h = \mathrm{id}_B$, as required.

(c) If f is invertible, we proved in Section 2.6 that f is injective and surjective. Conversely, if f is both injective and surjective, by (a) the function f has a left inverse g and by (b) it has a right inverse h. However, by Lemma 2.1, $g = h$, which shows that f is invertible. $\square$

The alert reader may have noticed a "fast turn" in the proof of the converse in (b). Indeed, we constructed the function h by choosing, for each $b \in B$, some element in $f^{-1}(b)$. How do we justify this procedure from the axioms of set theory?

Well, we can't. For this we need another (historically somewhat controversial) axiom, the *axiom of choice*. This axiom has many equivalent forms. We state the following form which is intuitively quite plausible.

Axiom of Choice (Graph Version).
For every relation $R \subseteq A \times B$, there is a partial function $f\colon A \to B$, with $graph(f) \subseteq R$ and $dom(f) = dom(R)$.

We see immediately that the axiom of choice justifies the existence of the function h in part (b) of Theorem 2.2.

Remarks:

1. Let $f\colon A \to B$ and $g\colon B \to A$ be any two functions and assume that

$$g \circ f = \mathrm{id}_A.$$

Thus, f is a right inverse of g and g is a left inverse of f. So, by Theorem 2.2 (a) and (b), we deduce that f is injective and g is surjective. In particular, this shows that any left inverse of an injection is a surjection and that any right inverse of a surjection is an injection.

2. Any right inverse h of a surjection $f \colon A \to B$ is called a *section* of f (which is an abbreviation for *cross-section*). This terminology can be better understood as follows: Because f is surjective, the preimage, $f^{-1}(b) = \{a \in A \mid f(a) = b\}$ of any element $b \in B$ is nonempty. Moreover, $f^{-1}(b_1) \cap f^{-1}(b_2) = \emptyset$ whenever $b_1 \neq b_2$. Therefore, the pairwise disjoint and nonempty subsets $f^{-1}(b)$, where $b \in B$, partition A. We can think of A as a big "blob" consisting of the union of the sets $f^{-1}(b)$ (called fibres) and lying over B. The function f maps each fibre, $f^{-1}(b)$ onto the element, $b \in B$. Then, any right inverse $h \colon B \to A$ of f picks out some element in each fibre, $f^{-1}(b)$, forming a sort of horizontal section of A shown as a curve in Figure 2.11.
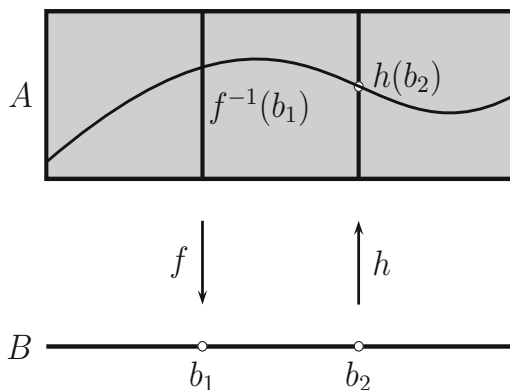
Fig. 2.11 A section h of a surjective function f.

3. Any left inverse g of an injection $f \colon A \to B$ is called a *retraction* of f. The terminology reflects the fact that intuitively, as f is injective (thus, g is surjective), B is bigger than A and because $g \circ f = \mathrm{id}_A$, the function g "squeezes" B onto A in such a way that each point $b = f(a)$ in $\mathrm{Im}\, f$ is mapped back to its ancestor $a \in A$. So, B is "retracted" onto A by g.

Before discussing direct and inverse images, we define the notion of restriction and extension of functions.

Definition 2.9. Given two functions, $f \colon A \to C$ and $g \colon B \to C$, with $A \subseteq B$, we say that f *is the restriction of* g *to* A if $graph(f) \subseteq graph(g)$; we write $f = g \upharpoonright A$. In this case, we also say that g *is an extension of* f *to* B.

2.8 Direct Image and Inverse Image

A function $f\colon X \to Y$ induces a function from 2^X to 2^Y also denoted f and a function from 2^Y to 2^X, as shown in the following definition.

Definition 2.10. Given any function $f\colon X \to Y$, we define the function $f\colon 2^X \to 2^Y$ so that, for every subset A of X,

$$f(A) = \{y \in Y \mid \exists x \in A, \, y = f(x)\}.$$

The subset $f(A)$ of Y is called the *direct image of A under f*, for short, the *image of A under f*. We also define the function $f^{-1}\colon 2^Y \to 2^X$ so that, for every subset B of Y,

$$f^{-1}(B) = \{x \in X \mid \exists y \in B, \, y = f(x)\}.$$

The subset $f^{-1}(B)$ of X is called the *inverse image of B under f* or the *preimage of B under f*.

Remarks:

1. The overloading of notation where f is used both for denoting the original function $f\colon X \to Y$ and the new function $f\colon 2^X \to 2^Y$ may be slightly confusing. If we observe that $f(\{x\}) = \{f(x)\}$, for all $x \in X$, we see that the new f is a natural extension of the old f to the subsets of X and so, using the same symbol f for both functions is quite natural after all. To avoid any confusion, some authors (including Enderton) use a different notation for $f(A)$, for example, $f[\![A]\!]$. We prefer not to introduce more notation and we hope that which f we are dealing with is made clear by the context.
2. The use of the notation f^{-1} for the function $f^{-1}\colon 2^Y \to 2^X$ may even be more confusing, because we know that f^{-1} is generally not a function from Y to X. However, it *is* a function from 2^Y to 2^X. Again, some authors use a different notation for $f^{-1}(B)$, for example, $f^{-1}[\![A]\!]$. We stick to $f^{-1}(B)$.
3. The set $f(A)$ is sometimes called the *push-forward of A along f* and $f^{-1}(B)$ is sometimes called the *pullback of B along f*.
4. Observe that $f^{-1}(y) = f^{-1}(\{y\})$, where $f^{-1}(y)$ is the preimage defined just after Definition 2.3.
5. Although this may seem counterintuitive, the function f^{-1} has a better behavior than f with respect to union, intersection, and complementation.

Some useful properties of $f\colon 2^X \to 2^Y$ and $f^{-1}\colon 2^Y \to 2^X$ are now stated without proof. The proofs are easy and left as exercises.

Proposition 2.3. *Given any function $f\colon X \to Y$, the following properties hold.*

(1) For any $B \subseteq Y$, we have

$$f(f^{-1}(B)) \subseteq B.$$

(2) If $f: X \to Y$ is surjective, then

$$f(f^{-1}(B)) = B.$$

(3) For any $A \subseteq X$, we have

$$A \subseteq f^{-1}(f(A)).$$

(4) If $f: X \to Y$ is injective, then

$$A = f^{-1}(f(A)).$$

The next proposition deals with the behavior of $f: 2^X \to 2^Y$ and $f^{-1}: 2^Y \to 2^X$ with respect to union, intersection, and complementation.

Proposition 2.4. *Given any function $f: X \to Y$ the following properties hold.*

(1) For all $A, B \subseteq X$, we have

$$f(A \cup B) = f(A) \cup f(B).$$

(2)

$$f(A \cap B) \subseteq f(A) \cap f(B).$$

Equality holds if $f: X \to Y$ is injective.
(3)

$$f(A) - f(B) \subseteq f(A - B).$$

Equality holds if $f: X \to Y$ is injective.
(4) For all $C, D \subseteq Y$, we have

$$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D).$$

(5)

$$f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D).$$

(6)

$$f^{-1}(C - D) = f^{-1}(C) - f^{-1}(D).$$

As we can see from Proposition 2.4, the function $f^{-1}: 2^Y \to 2^X$ has better behavior than $f: 2^X \to 2^Y$ with respect to union, intersection, and complementation.

2.9 Equinumerosity; The Pigeonhole Principle and the Schröder–Bernstein Theorem

The notion of size of a set is fairly intuitive for finite sets but what does it mean for infinite sets? How do we give a precise meaning to the questions:

(a) Do X and Y have the same size?
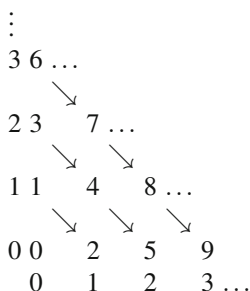
(b) Does X have more elements than Y?

For finite sets, we can rely on the natural numbers. We count the elements in the two sets and compare the resulting numbers. If one of the two sets is finite and the other is infinite, it seems fair to say that the infinite set has more elements than the finite one.

But what if both sets are infinite?

Remark: A critical reader should object that we have not yet defined what a finite set is (or what an infinite set is). Indeed, we have not. This can be done in terms of the natural numbers but, for the time being, we rely on intuition. We should also point out that when it comes to infinite sets, experience shows that our intuition fails us miserably. So, we should be very careful.

Let us return to the case where we have two infinite sets. For example, consider $\mathbb{N}$ and the set of even natural numbers, $2\mathbb{N} = \{0, 2, 4, 6, \ldots\}$. Clearly, the second set is properly contained in the first. Does that make $\mathbb{N}$ bigger? On the other hand, the function $n \mapsto 2n$ is a bijection between the two sets, which seems to indicate that they have the same number of elements. Similarly, the set of squares of natural numbers, $\text{Squares} = \{0, 1, 4, 9, 16, 25, \ldots\}$ is properly contained in $\mathbb{N}$ and many natural numbers are missing from Squares. But, the map $n \mapsto n^2$ is a bijection between $\mathbb{N}$ and Squares, which seems to indicate that they have the same number of elements.

A more extreme example is provided by $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$. Intuitively, $\mathbb{N} \times \mathbb{N}$ is two-dimensional and $\mathbb{N}$ is one-dimensional, so $\mathbb{N}$ seems much smaller than $\mathbb{N} \times \mathbb{N}$. However, it is possible to construct bijections between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ (try to find one). In fact, such a function J has the graph partially shown below:

$$
\begin{array}{llllll}
\vdots & & & & & \\
3 & 6 & \ldots & & & \\
 & & \searrow & & & \\
2 & 3 & & 7 & \ldots & \\
 & & \searrow & & \searrow & \\
1 & 1 & & 4 & & 8 & \ldots \\
 & & \searrow & & \searrow & & \searrow \\
0 & 0 & & 2 & & 5 & & 9 \\
 & 0 & & 1 & & 2 & & 3 & \ldots
\end{array}
$$

The function J corresponds to a certain way of enumerating pairs of integers. Note that the value of $m + n$ is constant along each diagonal, and consequently, we have

$$
\begin{aligned}
J(m, n) &= 1 + 2 + \cdots + (m + n) + m, \\
&= ((m + n)(m + n + 1) + 2m)/2, \\
&= ((m + n)^2 + 3m + n)/2.
\end{aligned}
$$

For example, $J(2, 1) = ((2 + 1)^2 + 3 \cdot 2 + 1)/2 = (9 + 6 + 1)/2 = 16/2 = 8$. The function

$$J(m,n) = \frac{1}{2}((m+n)^2 + 3m + n)$$

is a bijection but that's not so easy to prove.

Perhaps even more surprising, there are bijections between $\mathbb{N}$ and $\mathbb{Q}$. What about between $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R}$? Again, the answer is yes, but that's harder to prove.

These examples suggest that the notion of bijection can be used to define rigorously when two sets have the same size. This leads to the concept of equinumerosity.

Definition 2.11. A set A is *equinumerous* to a set B, written $A \approx B$, iff there is a bijection $f \colon A \to B$. We say that A is *dominated* by B, written $A \preceq B$, iff there is an injection from A to B. Finally, we say that A is *strictly dominated* by B, written $A \prec B$, iff $A \preceq B$ and $A \not\approx B$.

Using the above concepts, we can give a precise definition of finiteness. First, recall that for any $n \in \mathbb{N}$, we defined $[n]$ as the set $[n] = \{1, 2, \ldots, n\}$, with $[0] = \emptyset$.

Definition 2.12. A set A is *finite* if it is equinumerous to a set of the form $[n]$, for some $n \in \mathbb{N}$. A set A is *infinite* iff it is not finite. We say that A is *countable* (or *denumerable*) iff A is dominated by $\mathbb{N}$.

Two pretty results due to Cantor (1873) are given in the next theorem. These are among the earliest results of set theory. We assume that the reader is familiar with the fact that every number, $x \in \mathbb{R}$, can be expressed in decimal expansion (possibly infinite). For example,

$$\pi = 3.14159265358979\cdots$$

Theorem 2.3. *(Cantor's Theorem)* *(a) The set $\mathbb{N}$ is not equinumerous to the set $\mathbb{R}$ of real numbers.*

(b) For every set A there is no surjection from A onto 2^A. Consequently, no set A is equinumerous to its power set 2^A.

Proof. (a) We use a famous proof method due to Cantor and known as a *diagonal argument*. We prove that if we assume there is a bijection $f \colon \mathbb{N} \to \mathbb{R}$, then there is a real number z not belonging to the image of f, contradicting the surjectivity of f. Now, if f exists, we can form a bi-infinite array

$$f(0) = k_0.d_{01}d_{02}d_{03}d_{04}\cdots,$$
$$f(1) = k_1.d_{11}d_{12}d_{13}d_{14}\cdots,$$
$$f(2) = k_2.d_{21}d_{22}d_{23}d_{24}\cdots,$$
$$\vdots$$
$$f(n) = k_n.d_{n1}d_{n2}\cdots d_{nn+1}\cdots,$$
$$\vdots$$

where k_n is the integer part of $f(n)$ and the d_{ni} are the decimals of $f(n)$, with $i \geq 1$.

The number

$$z = 0.d_1 d_2 d_3 \cdots d_{n+1} \cdots$$

is defined so that $d_{n+1} = 1$ if $d_{nn+1} \neq 1$, else $d_{n+1} = 2$ if $d_{nn+1} = 1$, for every $n \geq 0$, The definition of z shows that

$$d_{n+1} \neq d_{nn+1}, \text{ for all } n \geq 0,$$

which implies that z is not in the above array; that is, $z \notin \text{Im } f$.

(b) The proof is a variant of Russell's paradox. Assume that there is a surjection, $g : A \to 2^A$; we construct a set $B \subseteq A$ that is not in the image of g, a contradiction. Consider the set

$$B = \{a \in A \mid a \notin g(a)\}.$$

Obviously, $B \subseteq A$. However, for every $a \in A$,

$$a \in B \text{ iff } a \notin g(a),$$

which shows that $B \neq g(a)$ for all $a \in A$; that is, B is not in the image of g. $\square$

As there is an obvious injection of $\mathbb{N}$ into $\mathbb{R}$, Theorem 2.3 shows that $\mathbb{N}$ is strictly dominated by $\mathbb{R}$. Also, as we have the injection $a \mapsto \{a\}$ from A into 2^A, we see that every set is strictly dominated by its power set. So, we can form sets as big as we want by repeatedly using the power set operation.

Remark: In fact, $\mathbb{R}$ is equinumerous to $2^{\mathbb{N}}$; see Problem 2.39

The following proposition shows an interesting connection between the notion of power set and certain sets of functions. To state this proposition, we need the concept of characteristic function of a subset.

Given any set X for any subset A of X, define the *characteristic function of A*, denoted χ_A, as the function $\chi_A : X \to \{0,1\}$ given by

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

In other words, χ_A tests membership in A. For any $x \in X$, $\chi_A(x) = 1$ iff $x \in A$. Observe that we obtain a function $\chi : 2^X \to \{0,1\}^X$ from the power set of X to the set of characteristic functions from X to $\{0,1\}$, given by

$$\chi(A) = \chi_A.$$

We also have the function, $\mathscr{S} : \{0,1\}^X \to 2^X$, mapping any characteristic function to the set that it defines and given by

$$\mathscr{S}(f) = \{x \in X \mid f(x) = 1\},$$

for every characteristic function, $f \in \{0,1\}^X$.

Proposition 2.5. *For any set X the function* $\chi\colon 2^X \to \{0,1\}^X$ *from the power set of X to the set of characteristic functions on X is a bijection whose inverse is* $\mathscr{S}\colon \{0,1\}^X \to 2^X$.

Proof. Simply check that $\chi \circ \mathscr{S} = \mathrm{id}$ and $\mathscr{S} \circ \chi = \mathrm{id}$, which is straightforward. □

In view of Proposition 2.5, there is a bijection between the power set 2^X and the set of functions in $\{0,1\}^X$. If we write $2 = \{0,1\}$, then we see that the two sets look the same. This is the reason why the notation 2^X is often used for the power set (but others prefer $\mathscr{P}(X)$).

There are many other interesting results about equinumerosity. We only mention four more, all very important.

Theorem 2.4. *(Pigeonhole Principle) No set of the form* $[n]$ *is equinumerous to a proper subset of itself, where* $n \in \mathbb{N}$,

Proof. Although the pigeonhole principle seems obvious, the proof is not. In fact, the proof requires induction. We advise the reader to skip this proof and come back to it later after we have given more examples of proof by induction.

Suppose we can prove the following claim.

Claim. Whenever a function $f\colon [n] \to [n]$ is an injection, then it is a surjection onto $[n]$ (and thus, a bijection).

Observe that the above claim implies the pigeonhole principle. This is proved by contradiction. So, assume there is a function $f\colon [n] \to [n]$, such that f is injective and $\mathrm{Im}\, f = A \subseteq [n]$ with $A \neq [n]$; that is, f is a bijection between $[n]$ and A, a proper subset of $[n]$. Because $f\colon [n] \to [n]$ is injective, by the claim, we deduce that $f\colon [n] \to [n]$ is surjective, that is, $\mathrm{Im}\, f = [n]$, contradicting the fact that $\mathrm{Im}\, f = A \neq [n]$.

It remains to prove by induction on $n \in \mathbb{N}$ that if $f\colon [n] \to [n]$ is an injection, then it is a surjection (and thus, a bijection). For $n = 0$, f must be the empty function, which is a bijection.

Assume that the induction hypothesis holds for any $n \geq 0$ and consider any injection, $f\colon [n+1] \to [n+1]$. Observe that the restriction of f to $[n]$ is injective.

Case 1. The subset $[n]$ is closed under f; that is, $f([n]) \subseteq [n]$. Then, we know that $f \upharpoonright [n]$ is injective and by the induction hypothesis, $f([n]) = [n]$. Because f is injective, we must have $f(n+1) = n+1$. Hence, f is surjective, as claimed.

Case 2. The subset $[n]$ is not closed under f; that is, there is some $p \leq n$ such that $f(p) = n+1$. We can create a new injection $\widehat{f}$ from $[n+1]$ to itself with the same image as f by interchanging two values of f so that $[n]$ closed under $\widehat{f}$. Define $\widehat{f}$ by

$$\widehat{f}(p) = f(n+1)$$
$$\widehat{f}(n+1) = f(p) = n+1$$
$$\widehat{f}(i) = f(i), \qquad 1 \leq i \leq n, i \neq p.$$

Then, $\widehat{f}$ is an injection from $[n+1]$ to itself and $[n]$ is closed under $\widehat{f}$. By Case 1, $\widehat{f}$ is surjective, and as $\mathrm{Im}\, f = \mathrm{Im}\,\widehat{f}$, we conclude that f is also surjective. □

Corollary 2.1. *(Pigeonhole Principle for Finite Sets) No finite set is equinumerous to a proper subset of itself.*

Proof. To say that a set A is finite is to say that there is a bijection $g\colon A \to [n]$ for some $n \in \mathbb{N}$. Assume that there is a bijection f between A and some proper subset of A. Then, consider the function $g \circ f \circ g^{-1}$, from $[n]$ to itself, as shown in the diagram below:

$$
\begin{array}{ccc}
A & \xleftarrow{\;g^{-1}\;} & [n] \\
{\scriptstyle f}\Big\downarrow & & \Big\downarrow{\scriptstyle g \circ f \circ g^{-1}} \\
A & \xrightarrow[\;g\;]{} & [n]
\end{array}
$$
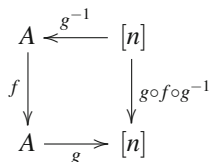
The rest of the proof consists in showing that $[n]$ would be equinumerous to a proper subset of itself, contradicting Theorem 2.4. We leave the details as an exercise. □

The pigeonhole principle is often used in the following way. If we have m distinct slots and $n > m$ distinct objects (the pigeons), then when we put all n objects into the m slots, two objects must end up in the same slot. This fact was apparently first stated explicitly by Dirichlet in 1834. As such, it is also known as *Dirichlet's box principle*.

Fig. 2.12 Johan Peter Gutav Lejeune Dirichlet, 1805–1859

Let A be a finite set. Then, by definition, there is a bijection $f\colon A \to [n]$ for some $n \in \mathbb{N}$. We claim that such an n is unique. Otherwise, there would be another bijection $g\colon A \to [p]$ for some $p \in \mathbb{N}$ with $n \neq p$. But now, we would have a bijection $g \circ f^{-1}$ between $[n]$ and $[p]$ with $n \neq p$. This would imply that there is either an injection from $[n]$ to a proper subset of itself or an injection from $[p]$ to a proper subset of itself,[2] contradicting the pigeonhole principle.

---

[2] Recall that $n+1 = \{0, 1, \ldots, n\} = [n] \cup \{0\}$. Here in our argument, we are using the fact that for any two natural numbers n, p, either $n \subseteq p$ or $p \subseteq n$. This fact is indeed true but requires a proof. The proof uses induction and some special properties of the natural numbers implied by the definition of a natural number as a set that belongs to every inductive set. For details, see Enderton [2], Chapter 4.

If A is a finite set, the unique natural number, $n \in \mathbb{N}$, such that $A \approx [n]$ is called the *cardinality of A* and we write $|A| = n$ (or sometimes, $\mathrm{card}(A) = n$).

Remark: The notion of cardinality also makes sense for infinite sets. What happens is that every set is equinumerous to a special kind of set (an initial ordinal) called a *cardinal* (or *cardinal number*). Let us simply mention that the cardinal number of $\mathbb{N}$ is denoted $\aleph_0$ (say "aleph" 0). A naive way to define the cardinality of a set X would be to define it as the equivalence class $\{Y \mid Y \approx X\}$ of all sets equinumerous to X. However, this does not work because the collection of sets Y such that $Y \approx X$, is not a set! In order to avoid this logical difficulty, one has to define the notion of a cardinal in a more subtle manner. One way to proceed is to first define *ordinals*, certain kinds of well-ordered sets. Then, assuming the axiom of choice, every set X is equinumerous to some ordinal and the cardinal $|X|$ of the set X is defined as the least ordinal equinumerous to X (an initial ordinal). The theory of ordinals and cardinals is thoroughly developed in Enderton [2] and Suppes [3] but it is beyond the scope of this book.

Corollary 2.2. *(a) Any set equinumerous to a proper subset of itself is infinite.*
    (b) The set $\mathbb{N}$ is infinite.

Proof. Left as an exercise to the reader. $\square$

The image of a finite set by a function is also a finite set. In order to prove this important property we need the next two propositions. The first of these two propositions may appear trivial but again, a rigorous proof requires induction.

Proposition 2.6. *Let n be any positive natural number, let A be any nonempty set, and pick any element $a_0 \in A$. Then there exists a bijection $f \colon A \to [n+1]$ iff there exists a bijection $g \colon (A - \{a_0\}) \to [n]$.*

Proof. We proceed by induction on $n \geq 1$. The proof of the induction step is very similar to the proof of the induction step in Proposition 2.4. The details of the proof are left as an exercise to the reader. $\square$

Proposition 2.7. *For any function $f \colon A \to B$ if f is surjective and if A is a finite nonempty set, then B is also a finite set and there is an injection $h \colon B \to A$ such that $f \circ h = \mathrm{id}_B$. Moreover, $|B| \leq |A|$.*

Proof. The existence of an injection $h \colon B \to A$, such that $f \circ h = \mathrm{id}_B$, follows immediately from Theorem 2.2 (b), but the proof uses the axiom of choice, which seems a bit of an overkill. However, we can give an alternate proof avoiding the use of the axiom of choice by proceeding by induction on the cardinality of A.

If A has a single element, say a, because f is surjective, B is the one-element set (obviously finite), $B = \{f(a)\}$, and the function, $h \colon B \to A$, given by $g(f(a)) = a$ is obviously a bijection such that $f \circ h = \mathrm{id}_B$.

For the induction step, assume that A has $n+1$ elements. If f is a bijection, then $h = f^{-1}$ does the job and B is a finite set with $n+1$ elements.

If f is surjective but not injective, then there exist two distinct elements, $a', a'' \in A$, such that $f(a') = f(a'')$. If we let $A' = A - \{a''\}$ then, by Proposition 2.6, the set A' has n elements and the restriction f' of f to A' is surjective because for every $b \in B$, if $b \neq f(a')$, then by the surjectivity of f there is some $a \in A - \{a', a''\}$ such that $f'(a) = f(a) = b$ and if $b = f(a')$, then $f'(a') = f(a')$. By the induction hypothesis, B is a finite set and there is an injection $h' : B \to A'$ such that $f' \circ h' = \mathrm{id}_B$. However, our injection $h' : B \to A'$ can be viewed as an injection $h : B \to A$, which satisfies the identity $f \circ h = \mathrm{id}_B$, and this concludes the induction step.

Inasmuch as we have an injection $h : B \to A$ and A and B are finite sets, as every finite set has a uniquely defined cardinality, we deduce that $|B| \leq |A|$. $\square$

Corollary 2.3. *For any function* $f : A \to B$, *if* A *is a finite set, then the image* $f(A)$ *of* f *is also finite and* $|f(A)| \leq |A|$.

Proof. Any function $f : A \to B$ is surjective on its image $f(A)$, so the result is an immediate consequence of Proposition 2.7. $\square$

Corollary 2.4. *For any two sets* A *and* B, *if* B *is a finite set of cardinality* n *and is* A *is a proper subset of* B, *then* A *is also finite and* A *has cardinality* $m < n$.

Proof. Corollary 2.4 can be proved by induction on n using Proposition 2.6. Another proof goes as follows: Because $A \subseteq B$, the inclusion function $j : A \to B$ given by $j(a) = a$ for all $a \in A$, is obviously an injection. By Theorem 2.2(a), there is a surjection, $g : B \to A$. Because B is finite, by Proposition 2.7, the set A is also finite and because there is an injection $j : A \to B$, we have $m = |A| \leq |B| = n$. However, inasmuch as B is a proper subset of A, by the pigeonhole principle, we must have $m \neq n$, that is, $m < n$. $\square$

If A is an infinite set, then the image $f(A)$ is not finite in general but we still have the following fact.

Proposition 2.8. *For any function* $f : A \to B$ *we have* $f(A) \preceq A$; *that is, there is an injection from the image of* f *to* A.

Proof. Any function $f : A \to B$ is surjective on its image $f(A)$. By Theorem 2.2(b), there is an injection $h : f(B) \to A$, such that $f \circ h = \mathrm{id}_B$, which means that $f(A) \preceq A$. $\square$

Here are two more important facts that follow from the pigeonhole principle for finite sets and Proposition 2.7.

Proposition 2.9. *Let* A *be any finite set. For any function* $f : A \to A$ *the following properties hold.*

(a) If f *is injective, then* f *is a bijection.*
(b) If f *is surjective, then* f *is a bijection.*

The proof of Proposition 2.9 is left as an exercise (use Corollary 2.1 and Proposition 2.7).

Proposition 2.9 *only holds for finite sets*. Indeed, just after the remarks following Definition 2.8 we gave examples of functions defined on an infinite set for which Proposition 2.9 fails.

A convenient characterization of countable sets is stated below.

Proposition 2.10. *A nonempty set A is countable iff there is a surjection $g\colon \mathbb{N} \to A$ from $\mathbb{N}$ onto A.*

Proof. Recall that by definition, A is countable iff there is an injection $f\colon A \to \mathbb{N}$. The existence of a surjection $g\colon \mathbb{N} \to A$ follows from Theorem 2.2(a). Conversely, if there is a surjection $g\colon \mathbb{N} \to A$, then by Theorem 2.2(b), there is an injection $f\colon A \to \mathbb{N}$. However, the proof of Theorem 2.2(b) requires the axiom of choice. It is possible to avoid the axiom of choice by using the fact that every nonempty subset of $\mathbb{N}$ has a smallest element (see Theorem 5.3). $\square$

The following fact about infinite sets is also useful to know.

Theorem 2.5. *For every infinite set A, there is an injection from $\mathbb{N}$ into A.*

Proof. The proof of Theorem 2.5 is actually quite tricky. It requires a version of the axiom of choice and a subtle use of the recursion theorem (Theorem 2.1). Let us give a sketch of the proof.

The version of the axiom of choice that we need says that for every nonempty set A there is a function F (a *choice function*) such that the domain of F is $2^A - \{\emptyset\}$ (all nonempty subsets of A) and such that $F(B) \in B$ for every nonempty subset B of A.

We use the recursion theorem to define a function h from $\mathbb{N}$ to the set of finite subsets of A. The function h is defined by

$$h(0) = \emptyset$$
$$h(n+1) = h(n) \cup \{F(A - h(n))\}.$$

Because A is infinite and $h(n)$ is finite, $A - h(n)$ is nonempty and we use F to pick some element in $A - h(n)$, which we then add to the set $h(n)$, creating a new finite set $h(n+1)$. Now, we define $g\colon \mathbb{N} \to A$ by

$$g(n) = F(A - h(n))$$

for all $n \in \mathbb{N}$. Because $h(n)$ is finite and A is infinite, g is well defined. It remains to check that g is an injection. For this, we observe that $g(n) \notin h(n)$ because $F(A - h(n)) \in A - h(n)$; the details are left as an exercise. $\square$

The intuitive content of Theorem 2.5 is that $\mathbb{N}$ is the "smallest" infinite set.

An immediate consequence of Theorem 2.5 is that every infinite subset of $\mathbb{N}$ is equinumerous to $\mathbb{N}$.

Here is a characterization of infinite sets originally proposed by Dedekind in 1888.

Proposition 2.11. *A set A is infinite iff it is equinumerous to a proper subset of itself.*

Proof. If A is equinumerous to a proper subset of itself, then it must be infinite because otherwise the pigeonhole principle would be contradicted.

Conversely, assume A is infinite. By Theorem 2.5, there is an injection $f\colon \mathbb{N} \to A$. Define the function $g\colon A \to A$ as follows.

$$g(f(n)) = f(n+1) \quad \text{if} \quad n \in \mathbb{N}$$
$$g(a) = a \qquad\quad \text{if} \quad a \notin \mathrm{Im}(f).$$

It is easy to check that g is a bijection of A onto $A - \{f(0)\}$, a proper subset of A. $\square$

Let us give another application of the pigeonhole principle involving sequences of integers. Given a finite sequence S of integers $a_1, \ldots, a_n$, a *subsequence of S* is a sequence $b_1, \ldots, b_m$, obtained by deleting elements from the original sequence and keeping the remaining elements in the same order as they originally appeared. More precisely, $b_1, \ldots, b_m$ is a subsequence of $a_1, \ldots, a_n$ if there is an injection $g\colon \{1, \ldots, m\} \to \{1, \ldots, n\}$ such that $b_i = a_{g(i)}$ for all $i \in \{1, \ldots, m\}$ and $i \leq j$ implies $g(i) \leq g(j)$ for all $i, j \in \{1, \ldots, m\}$. For example, the sequence

$$1 \quad \mathbf{9} \quad 10 \quad \mathbf{8} \quad 3 \quad 7 \quad 5 \quad 2 \quad \mathbf{6} \quad \mathbf{4}$$

contains the subsequence

$$9 \quad 8 \quad 6 \quad 4.$$

An *increasing subsequence* is a subsequence whose elements are in strictly increasing order and a *decreasing subsequence* is a subsequence whose elements are in strictly decreasing order. For example, $9\,8\,6\,4$ is a decreasing subsequence of our original sequence. We now prove the following beautiful result due to Erdös and Szekeres.

Theorem 2.6. *(Erdös and Szekeres) Let n be any nonzero natural number. Every sequence of $n^2 + 1$ pairwise distinct natural numbers must contain either an increasing subsequence or a decreasing subsequence of length $n + 1$.*

Proof. The proof proceeds by contradiction. So, assume there is a sequence S of $n^2 + 1$ pairwise distinct natural numbers so that all increasing or decreasing subsequences of S have length at most n. We assign to every element s of the sequence S a pair of natural numbers (u_s, d_s), called a *label*, where u_s, is the length of a longest increasing subsequence of S that starts at s and where d_s is the length of a longest decreasing subsequence of S that starts at s.

There are no increasing or descreasing subsequences of length $n + 1$ in S, thus observe that $1 \leq u_s, d_s \leq n$ for all $s \in S$. Therefore,

Claim 1: There are at most n^2 distinct labels (u_s, d_s), where $s \in S$.

We also assert the following.

Claim 2: If s and t are any two distinct elements of S, then $(u_s, d_s) \neq (u_t, d_t)$.

We may assume that s precedes t in S because otherwise we interchange s and t in the following argument. Inasmuch as $s \neq t$, there are two cases:

(a) $s < t$. In this case, we know that there is an increasing subsequence of length u_t starting with t. If we insert s in front of this subsequence, we get an increasing subsequence of $u_t + 1$ elements starting at s. Then, as u_s is the maximal length of all increasing subsequences starting with s, we must have $u_t + 1 \leq u_s$; that is,

$$u_s > u_t,$$

which implies $(u_s, d_s) \neq (u_t, d_t)$.

(b) $s > t$. This case is similar to case (a), except that we consider a decreasing subsequence of length d_t starting with t. We conclude that

$$d_s > d_t,$$

which implies $(u_s, d_s) \neq (u_t, d_t)$.

Therefore, in all cases, we proved that s and t have distinct labels.

Now, by Claim 1, there are only n^2 distinct labels and S has $n^2 + 1$ elements so, by the pigeonhole principle, two elements of S must have the same label. But, this contradicts Claim 2, which says that distinct elements of S have distinct labels. Therefore, S must have either an increasing subsequence or a decreasing subsequence of length $n + 1$, as originally claimed. $\quad \square$

Remark: Note that this proof is not constructive in the sense that it does not produce the desired subsequence; it merely asserts that such a sequence exists.

Our next theorem is the historically famous Schröder–Bernstein theorem, sometimes called the "Cantor–Bernstein theorem." Cantor proved the theorem in 1897 but his proof used a principle equivalent to the axiom of choice. Schröder announced the theorem in an 1896 abstract. His proof, published in 1898, had problems and he published a correction in 1911. The first fully satisfactory proof was given by Felix Bernstein and was published in 1898 in a book by Emile Borel. A shorter proof was given later by Tarski (1955) as a consequence of his fixed point theorem. We postpone giving this proof until the section on lattices (see Section 5.2).

Theorem 2.7. *(Schröder–Bernstein Theorem) Given any two sets A and B, if there is an injection from A to B and an injection from B to A, then there is a bijection between A and B. Equivalently, if $A \preceq B$ and $B \preceq A$, then $A \approx B$.*

The Schröder–Bernstein theorem is quite a remarkable result and it is a main tool to develop cardinal arithmetic, a subject beyond the scope of this course.

Our third theorem is perhaps the one that is the more surprising from an intuitive point of view. If nothing else, it shows that our intuition about infinity is rather poor.

Theorem 2.8. *If A is any infinite set, then $A \times A$ is equinumerous to A.*

Fig. 2.13 Georg Cantor, 1845–1918 (left), Ernst Schröder, 1841–1902 (middle left), Felix Bernstein, 1878–1956 (middle right) and Emile Borel, 1871–1956 (right)

Proof. The proof is more involved than any of the proofs given so far and it makes use of the axiom of choice in the form known as *Zorn's lemma* (see Theorem 5.1). For these reasons, we omit the proof and instead refer the reader to Enderton [2] (Chapter 6). □

Fig. 2.14 Max August Zorn, 1906–1993

In particular, Theorem 2.8 implies that $\mathbb{R} \times \mathbb{R}$ is in bijection with $\mathbb{R}$. But, geometrically, $\mathbb{R} \times \mathbb{R}$ is a plane and $\mathbb{R}$ is a line and, intuitively, it is surprising that a plane and a line would have "the same number of points." Nevertheless, that's what mathematics tells us.

Remark: It is possible to give a bijection between $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R}$ without using Theorem 2.8; see Problem 2.40.

Our fourth theorem also plays an important role in the theory of cardinal numbers.

Theorem 2.9. *(Cardinal Comparability) Given any two sets, A and B, either there is an injection from A to B or there is an injection from B to A (i.e., either $A \preceq B$ or $B \preceq A$).*

Proof. The proof requires the axiom of choice in a form known as the *well-ordering theorem*, which is also equivalent to Zorn's lemma. For details, see Enderton [2] (Chapters 6 and 7). □

Theorem 2.8 implies that there is a bijection between the closed line segment

$$[0,1] = \{x \in \mathbb{R} \mid 0 \le x \le 1\}$$

and the closed unit square

$$[0,1] \times [0,1] = \{(x,y) \in \mathbb{R}^2 \mid 0 \le x, y \le 1\}.$$

As an interlude, in the next section, we describe a famous space-filling function due to Hilbert. Such a function is obtained as the limit of a sequence of curves that can be defined recursively.

2.10 An Amazing Surjection: Hilbert's Space-Filling Curve

In the years 1890–1891, Giuseppe Peano and David Hilbert discovered examples of *space-filling functions* (also called *space-filling curves*). These are surjective functions from the line segment $[0,1]$ onto the unit square and thus their image is the whole unit square. Such functions defy intuition because they seem to contradict our intuition about the notion of dimension; a line segment is one-dimensional, yet the unit square is two-dimensional. They also seem to contradict our intuitive notion of area. Nevertheless, such functions do exist, even continuous ones, although to justify their existence rigorously requires some tools from mathematical analysis. Similar curves were found by others, among whom we mention Sierpinski, Moore, and Gosper.

Fig. 2.15 David Hilbert 1862–1943 and Waclaw Sierpinski, 1882–1969

We describe Hilbert's scheme for constructing such a square-filling curve. We define a sequence (h_n) of polygonal lines $h_n \colon [0,1] \to [0,1] \times [0,1]$, starting from the simple pattern h_0 (a "square cap" ⊓) shown on the left in Figure 2.16.

The curve h_{n+1} is obtained by scaling down h_n by a factor of $\frac{1}{2}$, and connecting the four copies of this scaled-down version of h_n obtained by rotating by $\pi/2$ (left lower part), rotating by $-\pi/2$, and translating right (right lower part), translating

up (left upper part), and translating diagonally (right upper part), as illustrated in Figure 2.16.
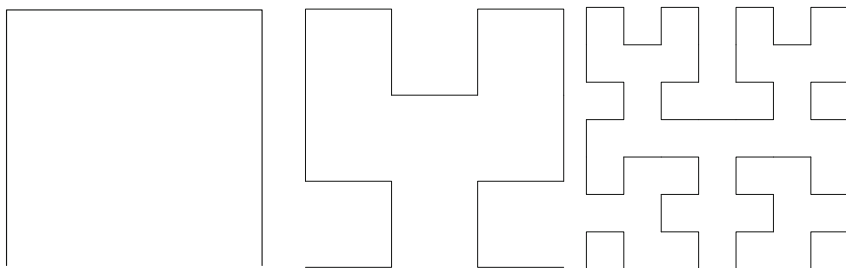

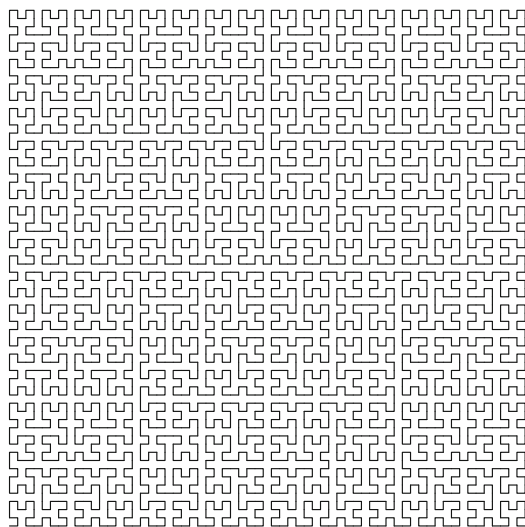**Fig. 2.16** A sequence of Hilbert curves h_0, h_1, h_2

Fig. 2.17 The Hilbert curve h_5

It can be shown that the sequence (h_n) converges (uniformly) to a continuous curve $h \colon [0,1] \to [0,1] \times [0,1]$ whose trace is the entire square $[0,1] \times [0,1]$. The Hilbert curve h is surjective, continuous, and nowhere differentiable. It also has infinite length.

The curve h_5 is shown in Figure 2.17. You should try writing a computer program to plot these curves. By the way, it can be shown that no continuous square-filling function can be injective. It is also possible to define cube-filling curves and even higher-dimensional cube-filling curves.

Before we close this chapter and move on to special kinds of relations, namely, partial orders and equivalence relations, we illustrate how the notion of function can be used to define strings, multisets, and indexed families rigorously.

2.11 Strings, Multisets, Indexed Families

Strings play an important role in computer science and linguistics because they are the basic tokens of which languages are made. In fact, formal language theory takes the (somewhat crude) view that a language is a set of strings. A string is a finite sequence of letters, for example, "Jean", "Val", "Mia", "math", "gaga", "abab". Usually, we have some alphabet in mind and we form strings using letters from this alphabet. Strings are not sets; the order of the letters matters: "abab" and "baba" are different strings. What matters is the position of every letter. In the string "aba", the leftmost "a" is in position 1, "b" is in position 2, and the rightmost "b" is in position 3. All this suggests defining strings as certain kinds of functions whose domains are the sets $[n] = \{1, 2, \ldots, n\}$ (with $[0] = \emptyset$) encountered earlier. Here is the very beginning of the theory of formal languages.

Definition 2.13. An *alphabet* Σ is any **finite** set.

We often write $\Sigma = \{a_1, \ldots, a_k\}$. The a_i are called the *symbols* of the alphabet.

Remark: There are a few occasions where we allow infinite alphabets but normally an alphabet is assumed to be finite.
   Examples:
   $\Sigma = \{a\}$
   $\Sigma = \{a, b, c\}$
   $\Sigma = \{0, 1\}$
   A string is a finite sequence of symbols. Technically, it is convenient to define strings as functions.

Definition 2.14. Given an alphabet Σ a *string over Σ (or simply a string) of length n* is any function

$$u \colon [n] \to \Sigma.$$

The integer n is the *length* of the string u, and it is denoted by $|u|$. When $n = 0$, the special string $u \colon [0] \to \Sigma$, of length 0 is called the *empty string, or null string*, and is denoted by ε.

Given a string $u \colon [n] \to \Sigma$ of length $n \geq 1$, $u(i)$ is the ith letter in the string u. For simplicity of notation, we denote the string u as

$$u = u_1 u_2 \ldots u_n,$$

with each $u_i \in \Sigma$.

For example, if $\Sigma = \{a, b\}$ and $u \colon [3] \to \Sigma$ is defined such that $u(1) = a$, $u(2) = b$, and $u(3) = a$, we write

$$u = aba.$$

Strings of length 1 are functions $u \colon [1] \to \Sigma$ simply picking some element $u(1) = a_i$ in Σ. Thus, we identify every symbol $a_i \in \Sigma$ with the corresponding string of length 1.

The set of all strings over an alphabet Σ, including the empty string, is denoted as Σ^*. Observe that when $\Sigma = \emptyset$, then

$$\emptyset^* = \{\varepsilon\}.$$

When $\Sigma \neq \emptyset$, the set Σ^* is countably infinite. Later on, we show ways of ordering and enumerating strings.

Strings can be juxtaposed, or concatenated.

Definition 2.15. Given an alphabet Σ, given two strings $u \colon [m] \to \Sigma$ and $v \colon [n] \to \Sigma$, the *concatenation, $u \cdot v$, (also written uv) of u and v* is the string $uv \colon [m+n] \to \Sigma$, defined such that

$$uv(i) = \begin{cases} u(i) & \text{if } 1 \leq i \leq m, \\ v(i-m) & \text{if } m+1 \leq i \leq m+n. \end{cases}$$

In particular, $u\varepsilon = \varepsilon u = u$.

It is immediately verified that

$$u(vw) = (uv)w.$$

Thus, concatenation is a binary operation on Σ^* that is associative and has ε as an identity. Note that generally, $uv \neq vu$, for example, for $u = a$ and $v = b$.

Definition 2.16. Given an alphabet Σ, given any two strings $u, v \in \Sigma^*$, we define the following notions as follows.

u *is a prefix of v* iff there is some $y \in \Sigma^*$ such that

$$v = uy.$$

u *is a suffix of v* iff there is some $x \in \Sigma^*$ such that

$$v = xu.$$

u *is a substring of v* iff there are some $x, y \in \Sigma^*$ such that

$$v = xuy.$$

We say that *u is a proper prefix (suffix, substring) of v* iff *u* is a prefix (suffix, substring) of *v* and $u \neq v$.

For example, *ga* is a prefix of *gallier*, the string *lier* is a suffix of *gallier*, and *all* is a substring of *gallier*.

Finally, languages are defined as follows.

Definition 2.17. Given an alphabet Σ, a *language over Σ (or simply a language)* is any subset L of Σ^*.

The next step would be to introduce various formalisms to define languages, such as automata or grammars but you'll have to take another course to learn about these things.

We now consider multisets. We already encountered multisets in Section 1.2 when we defined the axioms of propositional logic. As for sets, in a multiset, the order of elements does not matter, but as in strings, multiple occurrences of elements matter. For example,

$$\{a,a,b,c,c,c\}$$

is a multiset with two occurrences of a, one occurrence of b, and three occurrences of c. This suggests defining a multiset as a function with range $\mathbb{N}$, to specify the multiplicity of each element.

Definition 2.18. Given any set S a *multiset M over S* is any function $M \colon S \to \mathbb{N}$. A *finite multiset M over S* is any function $M \colon S \to \mathbb{N}$ such that $M(a) \neq 0$ only for finitely many $a \in S$. If $M(a) = k > 0$, we say that *a appears with mutiplicity k in M*.

For example, if $S = \{a,b,c\}$, we may use the notation $\{a,a,a,b,c,c\}$ for the multiset where a has multiplicity 3, b has multiplicity 1, and c has multiplicity 2.

The empty multiset is the function having the constant value 0. The *cardinality* $|M|$ of a (finite) multiset is the number

$$|M| = \sum_{a \in S} M(a).$$

Note that this is well defined because $M(a) = 0$ for all but finitely many $a \in S$. For example,

$$|\{a,a,a,b,c,c\}| = 6.$$

We can define the *union* of multisets as follows. If M_1 and M_2 are two multisets, then $M_1 \cup M_2$ is the multiset given by

$$(M_1 \cup M_2)(a) = M_1(a) + M_2(a), \text{ for all } a \in S.$$

A multiset M_1 is a *submultiset* of a multiset M_2 if $M_1(a) \leq M_2(a)$ for all $a \in S$. The *difference of M_1 and M_2* is the multiset $M_1 - M_2$ given by

$$(M_1 - M_2)(a) = \begin{cases} M_1(a) - M_2(a) & \text{if } M_1(a) \geq M_2(a) \\ 0 & \text{if } M_1(a) < M_2(a). \end{cases}$$

Intersection of multisets can also be defined but we leave this as an exercise.

Let us now discuss indexed families. The Cartesian product construct, $A_1 \times A_2 \times \cdots \times A_n$, allows us to form finite indexed sequences, $\langle a_1, \ldots, a_n \rangle$, but there are situations where we need to have infinite indexed sequences. Typically, we want to be able to consider families of elements indexed by some index set of our choice, say I. We can do this as follows.

Definition 2.19. Given any X and any other set I, called the *index set*, the set of *I-indexed families (or sequences) of elements from X* is the set of all functions $A: I \to X$; such functions are usually denoted $A = (A_i)_{i \in I}$. When X is a set of sets, each A_i is some set in X and we call $(A_i)_{i \in I}$ a *family of sets (indexed by I)*.

Observe that if $I = [n] = \{1, \ldots, n\}$, then an I-indexed family is just a string over X. When $I = \mathbb{N}$, an $\mathbb{N}$-indexed family is called an *infinite sequence* or often just a *sequence*. In this case, we usually write (x_n) for such a sequence $((x_n)_{n \in \mathbb{N}}$, if we want to be more precise). Also, note that although the notion of indexed family may seem less general than the notion of arbitrary collection of sets, this is an illusion. Indeed, given any collection of sets X, we may choose the index set I to be X itself, in which case X appears as the range of the identity function, id: $X \to X$.

The point of indexed families is that the operations of union and intersection can be generalized in an interesting way. We can also form infinite Cartesian products, which are very useful in algebra and geometry.

Given any indexed family of sets $(A_i)_{i \in I}$, the *union of the family* $(A_i)_{i \in I}$, denoted $\bigcup_{i \in I} A_i$, is simply the union of the range of A; that is,

$$\bigcup_{i \in I} A_i = \bigcup range(A) = \{a \mid (\exists i \in I),\, a \in A_i\}.$$

Observe that when $I = \emptyset$, the union of the family is the empty set. When $I \neq \emptyset$, we say that we have a *nonempty family* (even though some of the A_i may be empty).

Similarly, if $I \neq \emptyset$, then the *intersection of the family* $(A_i)_{i \in I}$, denoted $\bigcap_{i \in I} A_i$, is simply the intersection of the range of A; that is,

$$\bigcap_{i \in I} A_i = \bigcap range(A) = \{a \mid (\forall i \in I),\, a \in A_i\}.$$

Unlike the situation for union, when $I = \emptyset$, the intersection of the family does not exist. It would be the set of all sets, which does not exist.

It is easy to see that the laws for union, intersection, and complementation generalize to families but we leave this to the exercises.

An important construct generalizing the notion of finite Cartesian product is the product of families.

Definition 2.20. Given any family of sets $(A_i)_{i \in I}$, the *product of the family* $(A_i)_{i \in I}$, denoted $\prod_{i \in I} A_i$, is the set

$$\prod_{i \in I} A_i = \{a: I \to \bigcup_{i \in I} A_i \mid (\forall i \in I),\, a(i) \in A_i\}.$$

Definition 2.20 says that the elements of the product $\prod_{i \in I} A_i$ are the functions $a \colon I \to \bigcup_{i \in I} A_i$, such that $a(i) \in A_i$ for every $i \in I$. We denote the members of $\prod_{i \in I} A_i$ by $(a_i)_{i \in I}$ and we usually call them *I-tuples*. When $I = \{1, \ldots, n\} = [n]$, the members of $\prod_{i \in [n]} A_i$ are the functions whose graph consists of the sets of pairs

$$\{\langle 1, a_1 \rangle, \langle 2, a_2 \rangle, \ldots, \langle n, a_n \rangle\}, \ a_i \in A_i, \ 1 \leq i \leq n,$$

and we see that the function

$$\{\langle 1, a_1 \rangle, \langle 2, a_2 \rangle, \ldots, \langle n, a_n \rangle\} \mapsto \langle a_1, \ldots, a_n \rangle$$

yields a bijection between $\prod_{i \in [n]} A_i$ and the Cartesian product $A_1 \times \cdots \times A_n$. Thus, if each A_i is nonempty, the product $\prod_{i \in [n]} A_i$ is nonempty. But what if I is infinite?

If I is infinite, we smell choice functions. That is, an element of $\prod_{i \in I} A_i$ is obtained by choosing for every $i \in I$ some $a_i \in A_i$. Indeed, the axiom of choice is needed to ensure that $\prod_{i \in I} A_i \neq \emptyset$ if $A_i \neq \emptyset$ for all $i \in I$. For the record, we state this version (among many) of the axiom of choice.

Axiom of Choice (Product Version)
For any family of sets, $(A_i)_{i \in I}$, if $I \neq \emptyset$ and $A_i \neq \emptyset$ for all $i \in I$, then $\prod_{i \in I} A_i \neq \emptyset$.

Given the product of a family of sets, $\prod_{i \in I} A_i$, for each $i \in I$, we have the function $pr_i \colon \prod_{i \in I} A_i \to A_i$, called the *ith projection function*, defined by

$$pr_i((a_i)_{i \in I}) = a_i.$$

2.12 Summary

This chapter deals with the notions of relations, partial functions and functions, and their basic properties. The notion of a function is used to define the concept of a finite set and to compare the "size" of infinite sets. In particular, we prove that the power set 2^A of any set A is always "strictly bigger" than A itself (Cantor's theorem).

- We give some examples of functions, emphasizing that a function has a set of input values and a set of output values but that a function may not be defined for all of its input values (it may be a *partial function*). A function is given by a set of $\langle$ input, output $\rangle$ pairs.
- We define *ordered pairs* and the *Cartesian product* $A \times B$ of two sets A and B.
- We define the *first and second projection* of a pair.
- We define *binary relations* and their *domain* and *range*.
- We define the *identity relation*.
- We define *functional* relations.
- We define *partial functions*, *total functions*, the *graph* of a partial or total function, the *domain*, and the *range* of a (partial) function.
- We define the *preimage* or *inverse image* $f^{-1}(a)$ of an element a by a (partial) function f.

- The set of all functions from A to B is denoted B^A.
- We revisit the *induction principle for* $\mathbb{N}$ stated in terms of properties and give several examples of proofs by induction.
- We state the *complete induction principle for* $\mathbb{N}$ and prove its validity; we prove a property of the *Fibonacci numbers* by complete induction.
- We define the *composition* $R \circ S$ of two relations R and S.
- We prove some basic properties of the composition of functional relations.
- We define the *composition* $g \circ f$ of two (partial or total) functions, f and g.
- We describe the process of defining functions on $\mathbb{N}$ by *recursion* and state a basic result about the validity of such a process (The *recursion theorem on* $\mathbb{N}$).
- We define the *left inverse* and the *right inverse* of a function.
- We define *invertible* functions and prove the uniqueness of the inverse f^{-1} of a function f when it exists.
- We define the *inverse* or *converse* of a relation .
- We define, *injective*, *surjective*, and *bijective* functions.
- We characterize injectivity, surjectivity, and bijectivity in terms of left and right inverses.
- We observe that to prove that a surjective function has a right inverse, we need the *axiom of choice* (AC).
- We define *sections*, *retractions*, and the *restriction* of a function to a subset of its domain.
- We define *direct* and *inverse* images of a set under a function ($f(A)$, respectively, $f^{-1}(B)$).
- We prove some basic properties of direct and inverse images with respect to union, intersection, and relative complement.
- We define when two sets are *equinumerous* or when a set A *dominates* a set B.
- We give a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$.
- We define when a set if *finite* or *infinite*.
- We prove that $\mathbb{N}$ is not equinumerous to $\mathbb{R}$ (the real numbers), a result due to Cantor, and that there is no surjection from A to 2^A.
- We define the *characteristic function* χ_A of a subset A.
- We state and prove the *pigeonhole principle*.
- The set of natural numbers $\mathbb{N}$ is infinite.
- Every finite set A is equinumerous with a unique set $[n] = \{1, \ldots, n\}$ and the integer n is called the *cardinality of* A and is denoted $|A|$.
- If A is a finite set, then for every function $f \colon A \to B$ the image $f(A)$ of f is finite and $|f(A)| \le |A|$.
- Any subset A of a finite set B is also finite and $|A| \le |B|$.
- If A is a finite set, then every injection $f \colon A \to A$ is a bijection and every surjection $f \colon A \to A$ is a bijection.
- A set A is countable iff there is a surjection from $\mathbb{N}$ onto A.
- For every infinite set A there is an injection from $\mathbb{N}$ into A.
- A set A is infinite iff it is equinumerous to a proper subset of itself.
- We state the *Schröder–Bernstein theorem*.
- We state that every infinite set A is equinumerous to $A \times A$.

- We state the *cardinal comparability theorem*.
- We mention *Zorn's lemma*, one of the many versions of the axiom of choice.
- We describe *Hilbert's space-filling curve*.
- We define *strings* and *multisets*.
- We define the *product of a family of sets* and explain how the non-emptyness of such a product is equivalent to the axiom of choice.

Problems

2.1. Given any two sets A, B, prove that for all $a_1, a_2 \in A$ and all $b_1, b_2 \in B$,

$$\{\{a_1\}, \{a_1, b_1\}\} = \{\{a_2\}, \{a_2, b_2\}\}$$

iff

$$a_1 = a_2 \quad \text{and} \quad b_1 = b_2.$$

2.2. (a) Prove that the composition of two injective functions is injective. Prove that the composition of two surjective functions is surjective.

(b) Prove that a function $f\colon A \to B$ is injective iff for all functions $g, h\colon C \to A$,

$$\text{if } f \circ g = f \circ h, \text{ then } g = h.$$

(c) Prove that a function $f\colon A \to B$ is surjective iff for all functions $g, h\colon B \to C$,

$$\text{if } g \circ f = h \circ f, \text{ then } g = h.$$

2.3. (a) Prove that

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

(b) Prove that

$$\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2.$$

2.4. Given any finite set A, let $|A|$ denote the number of elements in A.

(a) If A and B are finite sets, prove that

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

(b) If A, B, and C are finite sets, prove that

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

2.5. Prove that there is no set X such that

$$2^X \subseteq X.$$

Hint. Given any two sets A, B, if there is an injection from A to B, then there is a surjection from B to A.

2.6. Let $f \colon X \to Y$ be any function. (a) Prove that for any two subsets $A, B \subseteq X$ we have

$$f(A \cup B) = f(A) \cup f(B)$$
$$f(A \cap B) \subseteq f(A) \cap f(B).$$

Give an example of a function f and of two subsets A, B such that

$$f(A \cap B) \neq f(A) \cap f(B).$$

Prove that if $f \colon X \to Y$ is injective, then

$$f(A \cap B) = f(A) \cap f(B).$$

(b) For any two subsets $C, D \subseteq Y$, prove that

$$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$$
$$f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D).$$

(c) Prove that for any two subsets $A \subseteq X$ and $C \subseteq Y$, we have

$$f(A) \subseteq C \quad \text{iff} \quad A \subseteq f^{-1}(C).$$

2.7. Prove that the set of natural numbers $\mathbb{N}$ is infinite. (Recall, a set X is finite iff there is a bijection from X to $[n] = \{1, \ldots, n\}$, where $n \in \mathbb{N}$ is a natural number with $[0] = \emptyset$. Thus, a set X is infinite iff there is no bijection from X to any $[n]$, with $n \in \mathbb{N}$.)

2.8. Let $R \subseteq A \times A$ be a relation. Prove that if $R \circ R = \mathrm{id}_A$, then R is the graph of a bijection whose inverse is equal to itself.

2.9. Given any three relations $R \subseteq A \times B$, $S \subseteq B \times C$, and $T \subseteq C \times D$, prove the associativity of composition:

$$(R \circ S) \circ T = R \circ (S \circ T).$$

2.10. Let $f \colon A \to A'$ and $g \colon B \to B'$ be two functions and define $h \colon A \times B \to A' \times B'$ by

$$h(\langle a, b \rangle) = \langle f(a), g(b) \rangle,$$

for all $a \in A$ and $b \in B$.
    (a) Prove that if f and g are injective, then so is h.

Hint. Use the definition of injectivity, not the existence of a left inverse and do not proceed by contradiction.

(b) Prove that if f and g are surjective, then so is h.

Hint. Use the definition of surjectivity, not the existence of a right inverse and do not proceed by contradiction.

2.11. Let $f\colon A \to A'$ and $g\colon B \to B'$ be two injections. Prove that if $\operatorname{Im} f \cap \operatorname{Im} g = \emptyset$, then there is an injection from $A \cup B$ to $A' \cup B'$.

Is the above still correct if $\operatorname{Im} f \cap \operatorname{Im} g \neq \emptyset$?

2.12. Let $[0,1]$ and $(0,1)$ denote the set of real numbers

$$[0,1] = \{x \in \mathbb{R} \mid 0 \le x \le 1\}$$
$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

(a) Give a bijection $f\colon [0,1] \to (0,1)$.

Hint. There are such functions that are the identity almost everywhere but for a countably infinite set of points in $[0,1]$.

(b) Consider the open square $(0,1) \times (0,1)$ and the closed square $[0,1] \times [0,1]$. Give a bijection $f\colon [0,1] \times [0,1] \to (0,1) \times (0,1)$.

2.13. Consider the function, $J\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, given by

$$J(m,n) = \frac{1}{2}[(m+n)^2 + 3m + n].$$

(a) Prove that for any $z \in \mathbb{N}$, if $J(m,n) = z$, then

$$8z + 1 = (2m + 2n + 1)^2 + 8m.$$

Deduce from the above that

$$2m + 2n + 1 \le \sqrt{8z+1} < 2m + 2n + 3.$$

(b) If $x \mapsto \lfloor x \rfloor$ is the function from $\mathbb{R}$ to $\mathbb{N}$ (the *floor function*), where $\lfloor x \rfloor$ is the largest integer $\le x$ (e.g., $\lfloor 2.3 \rfloor = 2$, $\lfloor \sqrt{2} \rfloor = 1$), prove that

$$\lfloor \sqrt{8z+1} \rfloor + 1 = 2m + 2n + 2 \text{ or } \lfloor \sqrt{8z+1} \rfloor + 1 = 2m + 2n + 3,$$

so that

$$\lfloor (\lfloor \sqrt{8z+1} \rfloor + 1)/2 \rfloor = m + n + 1.$$

(c) Because $J(m,n) = z$ means that

$$2z = (m+n)^2 + 3m + n,$$

prove that m and n are solutions of the system

$$m+n = \lfloor(\lfloor\sqrt{8z+1}\rfloor+1)/2\rfloor - 1$$
$$3m+n = 2z - (\lfloor(\lfloor\sqrt{8z+1}\rfloor+1)/2\rfloor - 1)^2.$$

If we let

$$Q_1(z) = \lfloor(\lfloor\sqrt{8z+1}\rfloor+1)/2\rfloor - 1$$
$$Q_2(z) = 2z - (\lfloor(\lfloor\sqrt{8z+1}\rfloor+1)/2\rfloor - 1)^2 = 2z - (Q_1(z))^2,$$

prove that $Q_2(z) - Q_1(z)$ is even and that

$$m = \frac{1}{2}(Q_2(z) - Q_1(z)) = K(z)$$

$$n = Q_1(z) - \frac{1}{2}(Q_2(z) - Q_1(z)) = L(z).$$

Conclude that J is a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$, with

$$m = K(J(m,n))$$
$$n = L(J(m,n)).$$

Remark: It can also be shown that $J(K(z), L(z)) = z$.

2.14. (i) In 3-dimensional space $\mathbb{R}^3$ the sphere S^2 is the set of points of coordinates (x,y,z) such that $x^2 + y^2 + z^2 = 1$. The point $N = (0,0,1)$ is called the *north pole*, and the point $S = (0,0,-1)$ is called the *south pole*. The *stereographic projection map* $\sigma_N \colon (S^2 - \{N\}) \to \mathbb{R}^2$ is defined as follows. For every point $M \neq N$ on S^2, the point $\sigma_N(M)$ is the intersection of the line through N and M and the equatorial plane of equation $z = 0$.

Prove that if M has coordinates (x,y,z) (with $x^2 + y^2 + z^2 = 1$), then

$$\sigma_N(M) = \left(\frac{x}{1-z}, \frac{y}{1-z}\right).$$

Hint. Recall that if $A = (a_1, a_2, a_3)$ and $B = (b_1, b_2, b_3)$ are any two distinct points in $\mathbb{R}^3$, then the unique line (AB) passing through A and B has parametric equations

$$x = (1-t)a_1 + tb_1$$
$$y = (1-t)a_2 + tb_2$$
$$z = (1-t)a_3 + tb_3,$$

which means that every point (x,y,z) on the line (AB) is of the above form, with $t \in \mathbb{R}$. Find the intersection of a line passing through the North pole and a point $M \neq N$ on the sphere S^2.

Prove that σ_N is bijective and that its inverse is given by the map $\tau_N \colon \mathbb{R}^2 \to (S^2 - \{N\})$ with

$$(x,y) \mapsto \left(\frac{2x}{x^2+y^2+1}, \frac{2y}{x^2+y^2+1}, \frac{x^2+y^2-1}{x^2+y^2+1} \right).$$

Hint. Find the intersection of a line passing through the North pole and some point P of the equatorial plane $z = 0$ with the sphere of equation

$$x^2 + y^2 + z^2 = 1.$$

Similarly, $\sigma_S \colon (S^2 - \{S\}) \to \mathbb{R}^2$ is defined as follows. For every point $M \neq S$ on S^2, the point $\sigma_S(M)$ is the intersection of the line through S and M and the plane of equation $z = 0$.

Prove that

$$\sigma_S(M) = \left(\frac{x}{1+z}, \frac{y}{1+z} \right).$$

Prove that σ_S is bijective and that its inverse is given by the map, $\tau_S \colon \mathbb{R}^2 \to (S^2 - \{S\})$, with

$$(x,y) \mapsto \left(\frac{2x}{x^2+y^2+1}, \frac{2y}{x^2+y^2+1}, \frac{1-x^2-y^2}{x^2+y^2+1} \right).$$

(ii) Give a bijection between the sphere S^2 and the equatorial plane of equation $z = 0$.

Hint. Use the stereographic projection and the method used in Problem 2.12, to define a bijection between $[0,1]$ and $(0,1)$.

2.15. (a) Give an example of a function $f \colon A \to A$ such that $f^2 = f \circ f = f$ and f is not the identity function.

(b) Prove that if a function $f \colon A \to A$ is not the identity function and $f^2 = f$, then f is not invertible.

(c) Give an example of an invertible function $f \colon A \to A$, such that $f^3 = f \circ f \circ f = f$, yet $f \circ f \neq f$.

(d) Give an example of a noninvertible function $f \colon A \to A$, such that $f^3 = f \circ f \circ f = f$, yet $f \circ f \neq f$.

2.16. Let X be any finite set.

(1) Prove that every injection $f \colon X \to X$ is actually a bijection.

(2) Prove that every surjection $f \colon X \to X$ is actually a bijection.

(3) Give counterexamples to both (1) and (2) when X is infinite.

2.17. (1) Let $(-1, 1)$ be the set of real numbers

$$(-1, 1) = \{x \in \mathbb{R} \mid -1 < x < 1\}.$$

Let $f \colon \mathbb{R} \to (-1, 1)$ be the function given by

$$f(x) = \frac{x}{\sqrt{1+x^2}}.$$

Prove that f is a bijection. Find the inverse of f.

(2) Let $(0,1)$ be the set of real numbers

$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

Give a bijection between $(-1,1)$ and $(0,1)$. Use (1) and (2) to give a bijection between $\mathbb{R}$ and $(0,1)$.

2.18. Let $D \subseteq \mathbb{R}^2$ be the subset of the real plane given by

$$D = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 < 1\},$$

that is, all points strictly inside of the unit circle $x^2 + y^2 = 1$. The set D is often called the *open unit disc*. Let $f : \mathbb{R}^2 \to D$ be the function given by

$$f(x,y) = \left(\frac{x}{\sqrt{1+x^2+y^2}}, \frac{y}{\sqrt{1+x^2+y^2}} \right).$$

(1) Prove that f is a bijection and find its inverse.

(2) Give a bijection between the sphere S^2 and the open unit disk D in the equatorial plane.

2.19. Prove by induction on n that

$$n^2 \leq 2^n \text{ for all } n \geq 4.$$

Hint. You need to show that $2n + 1 \leq n^2$ for all $n \geq 3$.

2.20. Let $f : A \to A$ be a function.

(a) Prove that if

$$f \circ f \circ f = f \circ f \text{ and } f \neq \text{id}_A, \tag{$*$}$$

then f is neither injective nor surjective.

Hint. Proceed by contradiction and use the characterization of injections and surjections in terms of left and right inverses.

(b) Give a simple example of a function $f : \{a,b,c\} \to \{a,b,c\}$, satisfying the conditions of $(*)$.

2.21. Recall that a set A is infinite iff there is no bijection from $\{1,\dots,n\}$ onto A, for any natural number $n \in \mathbb{N}$. Prove that the set of odd natural numbers is infinite.

2.22. Consider the sum

$$\frac{3}{1 \cdot 4} + \frac{5}{4 \cdot 9} + \dots + \frac{2n+1}{n^2 \cdot (n+1)^2},$$

with $n \geq 1$.

Which of the following expressions is the sum of the above:

$$(1) \ \frac{n+2}{(n+1)^2} \quad (2) \ \frac{n(n+2)}{(n+1)^2}.$$

Justify your answer.

Hint. Note that

$$n^4 + 6n^3 + 12n^2 + 10n + 3 = (n^3 + 3n^2 + 3n + 1)(n+3).$$

2.23. Consider the following version of the Fibonacci sequence starting from $F_0 = 0$ and defined by:

$$F_0 = 0$$
$$F_1 = 1$$
$$F_{n+2} = F_{n+1} + F_n, \ n \geq 0.$$

Prove the following identity, for any fixed $k \geq 1$ and all $n \geq 0$,

$$F_{n+k} = F_k F_{n+1} + F_{k-1} F_n.$$

2.24. Recall that the triangular numbers Δ_n are given by the formula

$$\Delta_n = \frac{n(n+1)}{2},$$

with $n \in \mathbb{N}$.

(a) Prove that

$$\Delta_n + \Delta_{n+1} = (n+1)^2$$

and

$$\Delta_1 + \Delta_2 + \Delta_3 + \cdots + \Delta_n = \frac{n(n+1)(n+2)}{6}.$$

(b) The numbers

$$T_n = \frac{n(n+1)(n+2)}{6}$$

are called *tetrahedral numbers*, due to their geometric interpretation as 3-D stacks of triangular numbers. Prove that

$$T_1 + T_2 + \cdots + T_n = \frac{n(n+1)(n+2)(n+3)}{24}.$$

Prove that

$$T_n + T_{n+1} = 1^2 + 2^2 + \cdots + (n+1)^2,$$

and from this, derive the formula

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

(c) The numbers

$$P_n = \frac{n(n+1)(n+2)(n+3)}{24}$$

are called *pentatope numbers*. The above numbers have a geometric interpretation in four dimensions as stacks of tetrahedral numbers. Prove that

$$P_1 + P_2 + \cdots + P_n = \frac{n(n+1)(n+2)(n+3)(n+4)}{120}.$$

Do you see a pattern? Can you formulate a conjecture and perhaps even prove it?

2.25. Consider the following table containing 11 copies of the triangular number, $\Delta_5 = 1 + 2 + 3 + 4 + 5$:

$$
\begin{array}{llll}
1 & & 1^2 \\
1\ 2\ 1 & & 2^2 \\
1\ 2\ 3\ 2\ 1 & & 3^2 \\
1\ 2\ 3\ 4\ 3\ 2\ 1 & & 4^2 \\
1\ 2\ 3\ 4\ 5\ 4\ 3\ 2\ 1 & & 5^2 \\
\hline
1\ 2\ 3\ 4\ 5 \quad 5\ 4\ 3\ 2\ 1 \\
1^2\ 2\ 3\ 4\ 5 \qquad 5\ 4\ 3\ 2\ 1^2 \\
2^2\ 3\ 4\ 5 \qquad\quad 5\ 4\ 3\ 2^2 \\
3^2\ 4\ 5 \qquad\qquad 5\ 4\ 3^2 \\
4^2\ 5 \qquad\qquad\quad 5\ 4^2 \\
5^2 \qquad\qquad\qquad 5^2
\end{array}
$$

Note that the above array splits into three triangles, one above the solid line and two below the solid line. Observe that the upward diagonals of the left lower triangle add up to 1^2, 2^2, 3^2, 4^2, 5^2; similarly the downward diagonals of the right lower triangle add up to 1^2, 2^2, 3^2, 4^2, 5^2, and the rows of the triangle above the solid line add up to 1^2, 2^2, 3^2, 4^2, 5^2. Therefore,

$$3 \times (1^2 + 2^2 + 3^2 + 4^2 + 5^2) = 11 \times \Delta_5.$$

In general, use a generalization of the above array to prove that

$$3 \times (1^2 + 2^2 + 3^2 + \cdots + n^2) = (2n+1)\Delta_n,$$

which yields the familiar formula:

$$1^2 + 2^2 + 3^2 \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

2.26. Consider the following table:

$$1 = 1^3$$
$$3 + 5 = 2^3$$
$$7 + 9 + 11 = 3^3$$
$$13 + 15 + 17 + 19 = 4^3$$
$$21 + 23 + 25 + 27 + 29 = 5^3$$
$$\cdots\cdots\cdots\cdots\cdots$$

(a) If we number the rows starting from $n = 1$, prove that the leftmost number on row n is $1 + (n-1)n$. Then, prove that the sum of the numbers on row n (the n consecutive odd numbers beginning with $1 + (n-1)n)$) is n^3.

(b) Use the triangular array in (a) to give a geometric proof of the identity

$$\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k \right)^2.$$

Hint. Recall that

$$1 + 3 + \cdots + 2n - 1 = n^2.$$

2.27. Let $f: A \to B$ be a function and define the function $g: B \to 2^A$ by

$$g(b) = f^{-1}(b) = \{a \in A \mid f(a) = b\},$$

for all $b \in B$. (a) Prove that if f is surjective, then g is injective.

(b) If g is injective, can we conclue that f is surjective?

2.28. Let X, Y, Z be any three nonempty sets and let $f: X \to Y$ be any function. Define the function $R_f: Z^Y \to Z^X$ (R_f, as a reminder that we compose with f on the right), by

$$R_f(h) = h \circ f,$$

for every function $h: Y \to Z$.

Let T be another nonempty set and let $g: Y \to T$ be any function.

(a) Prove that

$$R_{g \circ f} = R_f \circ R_g$$

and if $X = Y$ and $f = \mathrm{id}_X$, then

$$R_{\mathrm{id}_X}(h) = h,$$

for every function $h: X \to Z$.

(b) Use (a) to prove that if f is surjective, then R_f is injective and if f is injective, then R_f is surjective.

2.29. Let X, Y, Z be any three nonempty sets and let $g: Y \to Z$ be any function. Define the function $L_g: Y^X \to Z^X$ (L_g, as a reminder that we compose with g on the left), by

$$L_g(f) = g \circ f,$$

for every function $f \colon X \to Y$.

(a) Prove that if $Y = Z$ and $g = \mathrm{id}_Y$, then

$$L_{\mathrm{id}_Y}(f) = f,$$

for all $f \colon X \to Y$.

Let T be another nonempty set and let $h \colon Z \to T$ be any function. Prove that

$$L_{h \circ g} = L_h \circ L_g.$$

(b) Use (a) to prove that if g is injective, then $L_g \colon Y^X \to Z^X$ is also injective and if g is surjective, then $L_g \colon Y^X \to Z^X$ is also surjective.

2.30. Recall that given any two sets X, Y, every function $f \colon X \to Y$ induces a function $f \colon 2^X \to 2^Y$ such that for every subset $A \subseteq X$,

$$f(A) = \{f(a) \in Y \mid a \in A\}$$

and a function $f^{-1} \colon 2^Y \to 2^X$, such that, for every subset $B \subseteq Y$,

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

(a) Prove that if $f \colon X \to Y$ is injective, then so is $f \colon 2^X \to 2^Y$.

(b) Prove that if f is bijective then $f^{-1}(f(A)) = A$ and $f(f^{-1}(B)) = B$, for all $A \subseteq X$ and all $B \subseteq Y$. Deduce from this that $f \colon 2^X \to 2^Y$ is bijective.

(c) Prove that for any set A there is an injection from the set A^A of all functions from A to A to $2^{A \times A}$, the power set of $A \times A$. If A is infinite, prove that there is an injection from A^A to 2^A.

2.31. Recall that given any two sets X, Y, every function $f \colon X \to Y$ induces a function $f \colon 2^X \to 2^Y$ such that for every subset $A \subseteq X$,

$$f(A) = \{f(a) \in Y \mid a \in A\}$$

and a function $f^{-1} \colon 2^Y \to 2^X$, such that, for every subset $B \subseteq Y$,

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

(a) Prove that if $f \colon X \to Y$ is surjective, then so is $f \colon 2^X \to 2^Y$.

(b) If A is infinite, prove that there is a bijection from A^A to 2^A.

Hint. Prove that there is an injection from A^A to 2^A and an injection from 2^A to A^A.

2.32. (a) Finish the proof of Theorem 2.5, which states that for any infinite set X there is an injection from $\mathbb{N}$ into X. Use this to prove that there is a bijection between X and $X \times \mathbb{N}$.

(b) Prove that if a subset $A \subseteq \mathbb{N}$ of $\mathbb{N}$ is not finite, then there is a bijection between A and $\mathbb{N}$.

(c) Prove that every infinite set X can be written as a disjoint union $X = \bigcup_{i \in I} X_i$, where every X_i is in bijection with $\mathbb{N}$.

(d) If X is any set, finite or infinite, prove that if X has at least two elements then there is a bijection f of X leaving no element fixed (i.e., so that $f(x) \neq x$ for all $x \in X$).

2.33. Prove that if $(X_i)_{i \in I}$ is a family of sets and if I and all the X_i are countable, then $(X_i)_{i \in I}$ is also countable.
Hint. Define a surjection from $\mathbb{N} \times \mathbb{N}$ onto $(X_i)_{i \in I}$.

2.34. Consider the alphabet, $\Sigma = \{a, b\}$. We can enumerate all strings in $\{a, b\}^*$ as follows. Say that u precedes v if $|u| < |v|$ and if $|u| = |v|$, use the lexicographic (dictionary) order. The enumeration begins with

$$\varepsilon$$
$$a, b$$
$$aa, ab, ba, bb$$
$$aaa, aab, aba, abb, baa, bab, bba, bbb$$

We would like to define a function, $f: \{a, b\}^* \to \mathbb{N}$, such that $f(u)$ is the position of the string u in the above list, starting with $f(\varepsilon) = 0$. For example,

$$f(baa) = 11.$$

(a) Prove that if $u = u_1 \cdots u_n$ (with $u_j \in \{a, b\}$ and $n \geq 1$), then

$$f(u) = i_1 2^{n-1} + i_2 2^{n-2} + \cdots + i_{n-1} 2^1 + i_n$$
$$= 2^n - 1 + (i_1 - 1)2^{n-1} + (i_2 - 1)2^{n-2} + \cdots + (i_{n-1} - 1)2^1 + i_n - 1,$$

with $i_j = 1$ if $u_j = a$, else $i_j = 2$ if $u_j = b$.

(b) Prove that the above function is a bijection $f: \{a, b\}^* \to \mathbb{N}$.

(c) Consider any alphabet $\Sigma = \{a_1, \ldots, a_m\}$, with $m \geq 2$. We can also list all strings in Σ^* as in (a). Prove that the listing function $f: \Sigma^* \to \mathbb{N}$ is given by $f(\varepsilon) = 0$ and if $u = a_{i_1} \cdots a_{i_n}$ (with $a_{i_j} \in \Sigma$ and $n \geq 1$) by

$$f(u) = i_1 m^{n-1} + i_2 m^{n-2} + \cdots + i_{n-1} m^1 + i_n$$
$$= \frac{m^n - 1}{m - 1} + (i_1 - 1)m^{n-1} + (i_2 - 1)m^{n-2} + \cdots + (i_{n-1} - 1)m^1 + i_n - 1,$$

Prove that the above function $f: \Sigma^* \to \mathbb{N}$ is a bijection.

(d) Consider any infinite set A and pick two distinct elements, a_1, a_2, in A. We would like to define a surjection from A^A to 2^A by mapping any function $f: A \to A$ to its image,

$$\mathrm{Im} f = \{f(a) \mid a \in A\}.$$

The problem with the above definition is that the empty set is missed. To fix this problem, let f_0 be the function defined so that $f(a_0) = a_1$ and $f(a) = a_0$ for all

$a \in A - \{a_0\}$. Then, we define $S \colon A^A \to 2^A$ by

$$S(f) = \begin{cases} \emptyset & \text{if } f = f_0 \\ \text{Im}(f) & \text{if } f \neq f_0. \end{cases}$$

Prove that the function $S \colon A^A \to 2^A$ is indeed a surjection.

(e) Assume that Σ is an infinite set and consider the set of all *finite* strings Σ^*. If Σ^n denotes the set of all strings of length n, observe that

$$\Sigma^* = \bigcup_{n \geq 0} \Sigma^n.$$

Prove that there is a bijection between Σ^* and Σ.

2.35. Let $\text{Aut}(A)$ denote the set of all bijections from A to itself.

(a) Prove that there is a bijection between $\text{Aut}(\mathbb{N})$ and $2^{\mathbb{N}}$.

Hint. Consider the map, $S \colon \text{Aut}(\mathbb{N}) \to 2^{\mathbb{N} - \{0\}}$, given by

$$S(f) = \{n \in \mathbb{N} - \{0\} \mid f(n) = n\}$$

and prove that it is surjective. Also, there is a bijection between $\mathbb{N}$ and $\mathbb{N} - \{0\}$

(b) Prove that for any infinite set A there is a bijection between $\text{Aut}(A)$ and 2^A.

Hint. Use results from Problem 2.32 and adapt the method of Part (a).

2.36. Recall that a set A is infinite iff there is no bijection from $\{1, \ldots, n\}$ onto A, for any natural number $n \in \mathbb{N}$. Prove that the set of even natural numbers is infinite.

2.37. Consider the sum

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n \cdot (n+1)},$$

with $n \geq 1$.

Which of the following expressions is the sum of the above:

$$(1) \ \frac{1}{n+1} \quad (2) \ \frac{n}{n+1}.$$

Justify your answer.

2.38. Consider the triangular region T_1, defined by $0 \leq x \leq 1$ and $|y| \leq x$ and the subset D_1, of this triangular region inside the closed unit disk, that is, for which we also have $x^2 + y^2 \leq 1$. See Figure 2.18 where D_1 is shown shaded in gray.

(a) Prove that the map $f_1 \colon T_1 \to D_1$ defined so that

$$f_1(x, y) = \left(\frac{x^2}{\sqrt{x^2 + y^2}}, \frac{xy}{\sqrt{x^2 + y^2}} \right), \quad x \neq 0$$
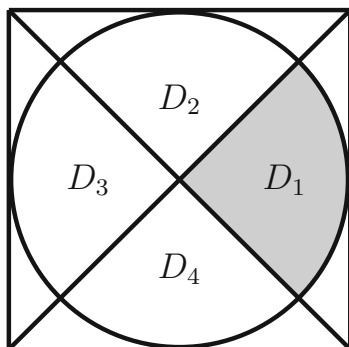
$$f_1(0, 0) = (0, 0),$$

Fig. 2.18 The regions D_i

is bijective and that its inverse is given by

$$g_1(x,y) = \left(\sqrt{x^2+y^2}, \frac{y}{x}\sqrt{x^2+y^2}\right), \; x \neq 0$$
$$g_1(0,0) = (0,0).$$

If T_3 and D_3 are the regions obtained from T_3 and D_1 by the reflection about the y axis, $x \mapsto -x$, show that the map, $f_3 \colon T_3 \to D_3$, defined so that

$$f_3(x,y) = \left(-\frac{x^2}{\sqrt{x^2+y^2}}, -\frac{xy}{\sqrt{x^2+y^2}}\right), \; x \neq 0$$
$$f_3(0,0) = (0,0),$$

is bijective and that its inverse is given by

$$g_3(x,y) = \left(-\sqrt{x^2+y^2}, \frac{y}{x}\sqrt{x^2+y^2}\right), \; x \neq 0$$
$$g_3(0,0) = (0,0).$$

(b) Now consider the triangular region T_2 defined by $0 \leq y \leq 1$ and $|x| \leq y$ and the subset D_2, of this triangular region inside the closed unit disk, that is, for which we also have $x^2+y^2 \leq 1$. The regions T_2 and D_2 are obtained from T_1 and D_1 by a counterclockwise rotation by the angle $\pi/2$.

Prove that the map $f_2 \colon T_2 \to D_2$ defined so that

$$f_2(x,y) = \left(\frac{xy}{\sqrt{x^2+y^2}}, \frac{y^2}{\sqrt{x^2+y^2}}\right), \; y \neq 0$$
$$f_2(0,0) = (0,0),$$

is bijective and that its inverse is given by

$$g_2(x,y) = \left(\frac{x}{y}\sqrt{x^2+y^2}, \sqrt{x^2+y^2}\right), \; y \neq 0$$
$$g_2(0,0) = (0,0).$$

If T_4 and D_4 are the regions obtained from T_2 and D_2 by the reflection about the x axis $y \mapsto -y$, show that the map $f_4 \colon T_4 \to D_4$, defined so that

$$f_4(x,y) = \left(-\frac{xy}{\sqrt{x^2+y^2}}, -\frac{y^2}{\sqrt{x^2+y^2}}\right), \; y \neq 0$$
$$f_4(0,0) = (0,0),$$

is bijective and that its inverse is given by

$$g_4(x,y) = \left(\frac{x}{y}\sqrt{x^2+y^2}, -\sqrt{x^2+y^2}\right), \; y \neq 0$$
$$g_4(0,0) = (0,0).$$

(c) Use the maps, f_1, f_2, f_3, f_4 to define a bijection between the closed square $[-1,1] \times [-1,1]$ and the closed unit disk $\overline{D} = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$, which maps the boundary square to the boundary circle. Check that this bijection is continuous. Use this bijection to define a bijection between the closed unit disk $\overline{D}$ and the open unit disk $D = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 < 1\}$.

2.39. The purpose of this problem is to prove that there is a bijection between $\mathbb{R}$ and $2^{\mathbb{N}}$. Using the results of Problem 2.17, it is sufficient to prove that there is a bijection betwen $(0,1)$ and $2^{\mathbb{N}}$. To do so, we represent the real numbers $r \in (0,1)$ in terms of their decimal expansions,

$$r = 0.r_1 r_2 \cdots r_n \cdots,$$

where $r_i \in \{0,1,\ldots,9\}$. However, some care must be exercised because this representation is ambiguous due to the possibility of having sequences containing the infinite suffix $9999\cdots$. For example,

$$0.1200000000\cdots = 0.1199999999\cdots$$

Therefore, we only use representations not containing the infinite suffix $9999\cdots$. Also recall that by Proposition 2.5, the power set $2^{\mathbb{N}}$ is in bijection with the set $\{0,1\}^{\mathbb{N}}$ of countably infinite binary sequences

$$b_0 b_1 \cdots b_n \cdots,$$

with $b_i \in \{0,1\}$.

(1) Prove that the function $f \colon \{0,1\}^{\mathbb{N}} \to (0,1)$ given by

$$f(b_0 b_1 \cdots b_n \cdots) = 0.1 b_0 b_1 \cdots b_n \cdots,$$

where $0.1b_0b_1\cdots b_n\cdots$ (with $b_n \in \{0,1\}$) is interpreted as a *decimal* (not binary) expansion, is an injection.

(2) Show that the image of the function f defined in (1) is the closed interval $[\frac{1}{10}, \frac{1}{9}]$ and thus, that f is not surjective.

(3) Every number, $k \in \{0,1,2,\ldots,9\}$ has a binary representation, bin(k), as a string of four bits; for example,

$$\text{bin}(1) = 0001, \ \text{bin}(2) = 0010, \ \text{bin}(5) = 0101, \ \text{bin}(6) = 0110, \ \text{bin}(9) = 1001.$$

Prove that the function $g: (0,1) \to \{0,1\}^{\mathbb{N}}$ defined so that

$$g(0.r_1r_2\cdots r_n\cdots) = .\text{bin}(r_1)\text{bin}(r_2)\text{bin}(r_1)\cdots\text{bin}(r_n)\cdots$$

is an injection (Recall that we are assuming that the sequence $r_1r_2\cdots r_n\cdots$ does not contain the infinite suffix $99999\cdots$). Prove that g is not surjective.

(4) Use (1) and (3) to prove that there is a bijection between $\mathbb{R}$ and $2^{\mathbb{N}}$.

2.40. The purpose of this problem is to show that there is a bijection between $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R}$. In view of the bijection between $\{0,1\}^{\mathbb{N}}$ and $\mathbb{R}$ given by Problem 2.39, it is enough to prove that there is a bijection between $\{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}}$ and $\{0,1\}^{\mathbb{N}}$, where $\{0,1\}^{\mathbb{N}}$ is the set of countably infinite sequences of 0 and 1.

(1) Prove that the function $f: \{0,1\}^{\mathbb{N}} \times \{0,1\}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$ given by

$$f(a_0a_1\cdots a_n\cdots, b_0b_1\cdots b_n\cdots) = a_0b_0a_1b_1\cdots a_nb_n\cdots$$

is a bijection (here, $a_i, b_i \in \{0,1\}$).

(2) Suppose, as in Problem 2.39, that we represent the reals in $(0,1)$ by their decimal expansions not containing the infinite suffix $99999\cdots$. Define the function $h: (0,1) \times (0,1) \to (0,1)$ by

$$h(0.r_0r_1\cdots r_n\cdots, 0.s_0s_1\cdots s_n\cdots) = 0.r_0s_0r_1s_1\cdots r_ns_n\cdots$$

with $r_i, s_i \in \{0,1,2,\ldots,9\}$. Prove that h is injective but not surjective.

If we pick the decimal representations ending with the infinite suffix $99999\cdots$ rather that an infinite string of 0s, prove that h is also injective but still not surjective.

(3) Prove that for every positive natural number $n \in \mathbb{N}$, there is a bijection between $\mathbb{R}^n$ and $\mathbb{R}$.

2.41. Let E, F, G, be any arbitrary sets.

(1) Prove that there is a bijection

$$E^G \times F^G \longrightarrow (E \times F)^G.$$

(2) Prove that there is a bijection

$$(E^F)^G \longrightarrow E^{F \times G}.$$

(3) If F and G are disjoint, then prove that there is a bijection

$$E^F \times E^G \longrightarrow E^{F \cup G}.$$

2.42. Let E, F, G, be any arbitrary sets.
  (1) Prove that if G is disjoint from both E and F and if $E \preceq F$, then $E \cup G \preceq F \cup G$.
  (2) Prove that if $E \preceq F$, then $E \times G \preceq F \times G$.
  (3) Prove that if $E \preceq F$, then $E^G \preceq F^G$.
  (4) Prove that if E and G are not both empty and if $E \preceq F$, then $G^E \preceq G^F$.

References

1. John H. Conway and K. Guy, Richard. *The Book of Numbers*. Copernicus. New York: Springer-Verlag, first edition, 1996.
2. Herbert B. Enderton. *Elements of Set Theory*. New York: Academic Press, first edition, 1977.
3. Patrick Suppes. *Axiomatic Set Theory*. New York: Dover, first edition, 1972.