# Chapter 3

# Relations and functions

In this chapter we study how to relate, possibly different, sets through the set-theoretic definitions of relation and function. We will rely on the product of sets as the central construction for connecting sets. We are led to consider sets with extra structure, and the cardinality of sets, in particular the important notion of countability.

## 3.1 Ordered pairs and products

Given two elements $a, b$ we can form their ordered pair $(a, b)$. Two ordered pairs are equal iff their first components are equal and their second components are equal too, *i.e.*

$$(a, b) = (a', b') \iff a = a' \ \& \ b = b' \ .$$

There is also the concept of *unordered* pair of elements $a, b$—this is just the set $\{a, b\}$. We'll only rarely use unordered pairs so "pair" alone will mean ordered pair.

Often you'll see the ordered pair $(a, b)$ defined to be the set $\{\{a\}, \{a, b\}\}$—this is one particular way of coding the idea of ordered pair as a *set.* (See Exercise 3.2 below. Apart from this exercise we'll never again consider how ordered pairs are implemented.)

For sets $X$ and $Y$, their *product* is the set

$$X \times Y = \{(a, b) \mid a \in X \ \& \ b \in Y\},$$

the set of all ordered pairs of elements with the first from $X$ and the second from $Y$.

We can use the product construction on sets several times. A ternary product of sets $X \times Y \times Z$, consisting of triples $(x, y, z)$, can be understood as $X \times (Y \times Z)$, and so on. In the case where all the sets in a product are the same, as in $X \times X$ we often write the product as $X^2$, with $X \times X \times X$ written as $X^3$, and generally a product $X \times \cdots \times X$, the product of $n$ copies of $X$, as $X^n$. Such products are familiar from coordinate geometry: a point on a line can be identified with a real number in $\mathbb{R}$, the set of real numbers; the points on the plane can be identified with elements of the product $\mathbb{R} \times \mathbb{R}$, which we can also write as $\mathbb{R}^2$; three-dimensional space with $\mathbb{R}^3$, and so on.

**Exercise 3.1** Prove

(i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(ii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

(iii) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

(iv) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$ [Show the converse inclusion does not hold in general.]

□

**Exercise 3.2** Show that a set $\{\{a\}, \{a, b\}\}$ behaves as an ordered pair should, *i.e.*

$$\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\} \iff a = a' \ \& \ b = b' \ .$$

[This is trickier than you might at first think. Consider the two cases $a = b$ and $a \neq b$.] □

## 3.2 Relations and functions

A *binary relation* between $X$ and $Y$ is a subset $R \subseteq X \times Y$—so a subset of pairs in the relation. We shall often write $xRy$ for $(x, y) \in R$.

Let $R \subseteq X \times Y$. Write $R^{-1}$ for the *converse*, or *inverse*, relation $R^{-1} = \{(y, x) \mid (x, y) \in R\}$; so $R^{-1} \subseteq Y \times X$ with $yR^{-1}x$ iff $xRy$.

A *partial function* from $X$ to $Y$ is a relation $f \subseteq X \times Y$ for which

$$\forall x, y, y'.\ (x, y) \in f \ \&\ (x, y') \in f \Rightarrow y = y'.$$

We use the notation $f(x) = y$ when there is a $y$ such that $(x, y) \in f$ and then say $f(x)$ is *defined*, and otherwise say $f(x)$ is *undefined*; the set

$$\{x \in X \mid f(x) \text{ is defined}\}$$

is called the *domain of definition* of the partial function $f$. Sometimes we write $f : x \mapsto y$, or just $x \mapsto y$ when $f$ is understood, for $y = f(x)$. Occasionally one sees just $fx$, without the brackets, for $f(x)$.

A *(total) function* from $X$ to $Y$ is a partial function from $X$ to $Y$ such that for all $x \in X$ there is some $y \in Y$ such that $f(x) = y$. Although total functions are a special kind of partial function it is traditional to understand something described as simply a function to be a total function, so we always say explicitly when a function is partial.

To stress the fact that we are thinking of a function $f$ from $X$ to $Y$ as taking an element of $X$ and yielding an element of $Y$ we generally write it as $f : X \to Y$. To indicate a partial function $f$ from $X$ to $Y$ we write $f : X \rightharpoonup Y$. For both functions and partial functions from $X$ to $Y$, the set $X$ is called the *domain* of the function and $Y$ the *codomain* of the function.

Note that individual relations and functions are also sets. This fact determines equality between relations, and equality between functions; they are equal iff they consist of the same set of pairs. We can reword this fact in the case of functions and partial functions.

**Proposition 3.3**

*(i) Let $R, R' \subseteq X \times Y$. Then,*

$$R = R' \text{ iff } \forall x \in X, y \in Y.\ xRy \iff xR'y\ .$$

*(ii) Let $f, f' : X \to Y$. Then,*

$$f = f' \text{ iff } \forall x \in X.\ f(x) = f'(x)\ .$$

*(iii) Let $f, f' : X \rightharpoonup Y$. Then,*

$$\begin{aligned} f = f' \text{ iff } \forall x \in X.\ &(f(x) \text{ is defined } \Rightarrow f'(x) \text{ is defined } \ \&\ f(x) = f'(x))\ \&\\ &(f'(x) \text{ is defined } \Rightarrow f(x) \text{ is defined } \ \&\ f(x) = f'(x))\ . \end{aligned}$$

So, to investigate whether two functions with the same domain and codomain are equal it suffices to show that they give the same results when applied to an arbitrary common argument.

**Exercise 3.4** If $A$ has $k$ elements and $B$ has $m$ elements, how many relations are there between $A$ and $B$? □

**Exercise 3.5** Let $R$ and $S$ be relations between $A$ and $B$. Show that, if $R \subseteq S$, then $R^{-1} \subseteq S^{-1}$. Prove that $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ and $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$. □

**Exercise 3.6** If $A$ and $B$ are finite sets with $m$ and $n$ elements respectively, how many functions and how many partial functions are there from $A$ to $B$? □

### 3.2.1 Composing relations and functions

We compose relations, and so partial and total functions, $R$ between $X$ and $Y$ and $S$ between $Y$ and $Z$ by defining their *composition*, a relation between $X$ and $Z$, by

$$S \circ R =_{def} \{(x,z) \in X \times Z \mid \exists y \in Y.\ (x,y) \in R \ \&\ (y,z) \in S\}\ .$$

Let $R \subseteq X \times Y$, $S \subseteq Y \times Z$ and $T \subseteq Z \times W$. It should not be hard to convince yourself that

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

*i.e.* composition is associative.

**Exercise 3.7** Let $A = \{1,2,3,4\}$, $B = \{a,b,c,d\}$ and $C = \{x,y,z\}$. Let $R = \{(1,a),(2,d),(3,a),(3,b),(3,d)\}$ and $S = \{(b,x),(b,z),(c,y),(d,z)\}$. What is their composition $S \circ R$? □

**Exercise 3.8** Show that the composition of relations is associative. □

Each set $X$ is associated with an identity relation $\mathsf{id}_X$ where $\mathsf{id}_X = \{(x,x) \mid x \in X\}$. It is easy to see that for any relation $R$ between $X$ and $Y$

$$R \circ \mathsf{id}_X = \mathsf{id}_Y \circ R = R$$

—so the identity relation does indeed behave like an identity with respect to composition. Note that the identity relation is a function.

For functions $f : X \to Y$ and $g : Y \to Z$ their composition is also a function $g \circ f : X \to Z$ (check!). Similarly, the composition of partial functions $f : X \rightharpoonup Y$ and $g : Y \rightharpoonup Z$ is a partial function $g \circ f : X \rightharpoonup Z$ (check!).

We say a function $f : X \to Y$ is *injective* (or 1-1) iff

$$\forall x, x' \in X.\ f(x) = f(x') \Rightarrow x = x'\ .$$

In other words, taking the contrapositive of this implication, distinct elements of $X$ go to distinct elements of $Y$. An injective function is often called an *injection*.

We say a function $f : X \to Y$ is *surjective* (or onto) iff

$$\forall y \in Y \exists x \in X.\ y = f(x)\ .$$

A surjective function is often called an *surjection*.

A function $f : X \to Y$ is *bijective* iff it is both injective and surjective. Bijective functions $f : X \to Y$ are called *bijections*; the sets $X$ and $Y$ are said to be in *1-1 correspondence*, or *bijective correspondence*.

A function $f : X \to Y$ has an *inverse* function $g : Y \to X$ iff $g(f(x)) = x$ for all $x \in X$, and $f(g(y)) = y$ for all $y \in Y$. Notice the symmetry: $f$ has inverse $g$ means $g$ has inverse $f$, and *vice versa*.

**Lemma 3.9** *A function $f : X \to Y$ is bijective iff it has an inverse function.*

*Proof.*
*'if"*: Suppose $f : X \to Y$ has an inverse $g : Y \to X$. Let $x, x' \in X$ and suppose $f(x) = f(x')$. Then

$$x = g(f(x)) = g(f(x')) = x'\ .$$

Hence $f$ is injective. Let $y \in Y$. Then $f(g(y)) = y$. Hence $f$ is surjective. It follows that $f$ is bijective.
*"only if"*: Assume $f : X \to Y$ is bijective. Define the relation $g \subseteq Y \times X$ by $g = f^{-1}$, the converse relation of $f$, so $(y,x) \in g \iff f(x) = y$.

Suppose $(y,x),(y,x') \in g$. Then, $f(x) = y$ and $f(x') = y$, so $x = x'$ as $f$ is injective. Given $y \in Y$ there is $x \in X$ such that $f(x) = y$ as $f$ is surjective, making $(y,x) \in g$. This shows that $g$ is a function $g : Y \to X$ which moreover satisfies

$$g(y) = x \iff f(x) = y\ . \qquad (\dagger)$$

We now deduce that $g$ is injective. Suppose $g(y) = g(y')$, where $y, y' \in Y$. Letting $x = g(y) = g(y')$ we see from (†) that both $f(x) = y$ and $f(x) = y'$, whence $y = y'$.

If $g(f(x)) = x'$ then $f(x') = f(x)$ by (†), so $x = x'$, as $f$ is injective. If $f(g(y)) = y'$ then $g(y') = g(y)$ by (†), so $y = y'$, as $g$ is injective. This shows that $g$ is an inverse to $f$. □

Suppose $f : X \to Y$ has an inverse $g : Y \to X$. Then $g$ has $f$ as its inverse. So by Lemma 3.9, both $f$ and $g$ are bijective. It is traditional to write $f^{-1}$ for the inverse of a function $f$.

**Exercise 3.10** Show that the composition of injective/surjective/bijective functions is respectively injective/surjective/bijective. □

**Exercise 3.11** Let $D$ be the set $\{x \in \mathbb{R} \mid x > 1\}$. Define a binary relation $g \subseteq D \times D$ by taking

$$(u, v) \in g \text{ iff } \frac{1}{u} + \frac{1}{v} = 1 \ .$$

(i) Express $v$ as a formula in $u$ for $(u, v) \in g$. Deduce that $g$ is a function $g : D \to D$.

(ii) Define an inverse function to $g$ and prove that it has the desired properties. Deduce that $g : D \to D$ is a bijection.

[The formula $\frac{1}{u} + \frac{1}{v} = 1$ expresses the relation between the distance of an object $u$ and the distance of its image $v$ from a lens with focal length 1.] □

### 3.2.2 Direct and inverse image under a relation

We extend relations, and thus partial and total functions, $R \subseteq X \times Y$ to an operation acting on subsets by taking

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

for $A \subseteq X$. The set $R\,A$ is called the *direct image* of $A$ under $R$. We define

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

for $B \subseteq Y$. The set $R^{-1}B$ is called the *inverse image* of $B$ under $R$; note that it is the same set as the direct image of the set $B$ under the converse, or inverse, relation $R^{-1}$. Of course, the same notions of direct and inverse image also apply in the special cases where the relation is a partial function or function.

**Exercise 3.12** Suppose $f : X \to Y$ is a function. Show $f^{-1}$ preserves the Boolean operations of union, intersection and complement, *i.e.* for all $B, C \subseteq Y$,

$$\begin{aligned} &f^{-1}(B \cup C) = (f^{-1}B) \cup (f^{-1}C)\ , \qquad && f^{-1}\emptyset = \emptyset\ ,\\ &f^{-1}(B \cap C) = (f^{-1}B) \cap (f^{-1}C)\ , && f^{-1}Y = X\ ,\\ &f^{-1}(B^c) = (f^{-1}B)^c\ . \end{aligned}$$

What analogous properties hold of the direct image under $f$? Suppose now $f : X \rightharpoonup Y$ is a partial function. Describe how to modify the above identities to make them hold in this case. Which identities will hold if $f$ is assumed only to be a relation? □

## 3.3 Relations as structure

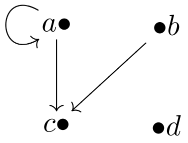
Often in mathematics and computer science we are not so much concerned with bare sets, but rather with sets that possess some extra structure. We consider three important examples, directed graphs, equivalence relations and partial orders. These all arise as a special kind of relation $R \subseteq X \times Y$, where in particular the sets $X$ and $Y$ are the same; then, we often describe $R$ as being a relation *on* the set $X$.

### 3.3.1 Directed graphs

One of the simplest examples of sets with structure is that of directed graphs.

**Definition:** A *directed graph* (or digraph) is a set $X$ on which there is a relation $R \subseteq X \times X$ and so is described by $(X, R)$. The elements of $X$ are called vertices (or nodes) and the elements of $R$ directed edges (or arcs).

Finite directed graphs (*i.e.* those with a finite set of vertices) have a natural diagrammatic representation in which vertices are drawn as nodes and directed edges as arcs between them. Here, for example, is the diagram of the directed graph with vertices $\{a, b, c, d\}$ and directed edges $\{(a, c), (b, c), (a, a)\}$:



Directed graphs are ubiquitous in computer science. They appear both as representations of data-types, expressing relations between objects, and of processes, expressing the possible transitions between states.

### 3.3.2 Equivalence relations

One often encounters relations that behave like a form of equality or equivalence, captured in the definition of equivalence relation.

An *equivalence relation* is a relation $R \subseteq X \times X$ on a set $X$ which is

- reflexive: $\forall x \in X.\ xRx$,
- symmetric: $\forall x, y \in X.\ xRy \Rightarrow yRx$ and
- transitive: $\forall x, y, z \in X.\ xRy\ \&\ yRz \Rightarrow xRz$.

If $R$ is an equivalence relation on $X$ then the *(R-)equivalence class* of an element $x \in X$ is the subset $\{x\}_R =_{def} \{y \in X \mid yRx\}$.

An equivalence relation on a set $X$ determines a partition of $X$. A *partition* of a set $X$ is a set $P$ of non-empty subsets of $X$ for which each element $x$ of $X$ belongs to one and only one member of $P$. In other words, a partition $P$ of $X$ is a collection of nonempty, disjoint subsets of $X$ such that each element $x$ of $X$ belongs to a member of $P$.

**Theorem 3.13** *Let $R$ be an equivalence relation on a set $X$. The set $X/R =_{def} \{\{x\}_R \mid x \in X\}$ of equivalence classes with respect to $R$ is a partition of the set $X$. Moreover, $\{x\}_R = \{y\}_R$ iff $xRy$ for all $x, y \in X$.*

*Proof.* Let $x \in X$. Then as $R$ is reflexive, $x \in \{x\}_R$. So every member of $X/R$ is nonempty and each element of $X$ belongs to a member of $X/R$. For $X/R$ to be a partition we also require that its members are disjoint. However, we will show

$$\begin{array}{ll} (1) & \{x\}_R \cap \{y\}_R \neq \emptyset \Rightarrow xRy\ , \text{ and} \\ (2) & xRy \Rightarrow \{x\}_R = \{y\}_R\ , \end{array}$$

from which $\{x\}_R \cap \{y\}_R \neq \emptyset \Rightarrow \{x\}_R = \{y\}_R$ follows, for any elements $x, y \in X$.

(1) Suppose $\{x\}_R \cap \{y\}_R \neq \emptyset$. Then there is some $z \in \{x\}_R \cap \{y\}_R$. Hence $zRx$ and $zRy$. Then $xRz$ and $zRy$, as $R$ is symmetric. As $R$ is transitive we obtain $xRy$.

(2) Suppose $xRy$. Let $w \in \{x\}_R$. Then $wRx$ and $xRy$, so $wRy$ by transitivity of $R$. Thus $w \in \{y\}_R$. This shows $\{x\}_R \subseteq \{y\}_R$. Because $R$ is symmetric we have $yRx$ and so by a similar argument we also obtain $\{y\}_R \subseteq \{x\}_R$. Hence $\{x\}_R = \{y\}_R$.

If $\{x\}_R = \{y\}_R$, then certainly $x \in \{x\}_R \cap \{y\}_R$, so $xRy$ by (1). Combining with (2) we see that $\{x\}_R = \{y\}_R$ iff $xRy$ for all $x, y \in X$. □

There is a simple converse to Theorem 3.13:

**Proposition 3.14** *Let $P$ be a partition of a set $X$. The relation $R$ on $X$, defined by*

$$xRy \iff \exists p \in P.\ x \in p\ \&\ y \in p\ ,$$

*is an equivalence relation on the set $X$ with $X/R = P$.*

**Exercise 3.15** Provide the proof to Proposition 3.14. □

### Modular arithmetic

Modular arithmetic is central to number theory in mathematics and very important in computer science, for example in cryptography. It furnishes an example of an equivalence relation.

Let $k \in \mathbb{N}$. There are many situations in which it is useful to regard integers as essentially the same if they give the same remainder when divided by $k$. Integers $a$ and $b$ give the same remainder when divided by $k$ iff their difference $a - b$ is divisible by $k$. For integers $a, b \in \mathbb{Z}$ define

$$\begin{aligned} a \equiv b \pmod{k} \text{ iff } \ & a - b \text{ is divisible by } k \\ & \textit{i.e. } (a-b) = n.k \ \text{ for some } n \in \mathbb{Z}\,. \end{aligned}$$

Then we say "$a$ is congruent to $b$ modulo $k$."

It is easy to show that congruence modulo $k$ is an equivalence relation on $\mathbb{Z}$, that it is:
*Reflexive:* $a \equiv a \pmod{k}$ as $(a - a) = 0 = 0.k$
*Symmetric:* If $a \equiv b \pmod{k}$ then $k$ divides $(a-b)$. Hence $k$ divides $-(a-b) = (b-a)$ giving $b \equiv a \pmod{k}$.
*Transitive:* Suppose $a \equiv b \pmod{k}$ and $b \equiv c \pmod{k}$. Then $k$ divides both $a-b$ and $b-c$. Hence $k$ divides their sum $(a-b)+(b-c) = (a-c)$. Thus $a \equiv c \pmod{k}$.

It is common to write $[a]$, called a congruence class, for the equivalence class of $a$ w.r.t. congruence modulo $k$. The congruence classes correspond to the possible remainders on dividing by $k$, *viz.* 0, 1, ..., $(k-1)$.

Assume $a \equiv b \pmod{k}$ and $a' \equiv b' \pmod{k}$. Then

$$\begin{aligned} & a + a' \equiv b + b' \pmod{k} \qquad a - a' \equiv b - b' \pmod{k} \\ & a \times a' \equiv b \times b' \pmod{k}\,. \end{aligned}$$

Consequently we can define these operations on congruence classes by taking

$$\begin{aligned} & [a] + [a'] = [a + a'] \qquad [a] - [a'] = [a - a'] \\ & [a] \times [a'] = [a \times a']\,. \end{aligned}$$

The operations are well-defined because independently of how we choose representatives for the congruence classes we obtain the same result.

**Exercise 3.16** Show that if $a \equiv b \pmod{k}$ and $a' \equiv b' \pmod{k}$, then $a + a' \equiv b + b' \pmod{k}$, $a - a' \equiv b - b' \pmod{k}$ and $a \times a' \equiv b \times b' \pmod{k}$. □

**Exercise 3.17** Let $A = \{1, 2, 3\}$. List all the partitions of $A$. How many equivalence relations are there on $A$? How many relations are there on $A$? □

**Exercise 3.18** Let $\cong$ be a relation on a set of sets $S$ such that $A \cong B$ iff the sets $A$ and $B$ in $S$ are in bijective correspondence. Show that $\cong$ is an equivalence relation. □

**Exercise 3.19** Let $R$ and $S$ be equivalence relations on sets $A$ and $B$ respectively. Let $p : A \to A/R$ and $q : B \to B/S$ be the obvious functions from elements to their equivalence classes. Suppose $f : A \to B$ is a function. Show that the following two statements are equivalent:

(i) $\exists g : A/R \to B/S.\ g \circ p = q \circ f$ ;

(ii) $\forall a, a' \in A.\ aRa' \Rightarrow f(a)Sf(a')$ . □

**Exercise 3.20** Suppose $(P, \longrightarrow)$ is a directed graph. A *bisimulation* on $P$ is a relation $R \subseteq P \times P$ such that whenever $p\,R\,q$ then

- $\forall p' \in P.\ p \longrightarrow p' \Rightarrow \exists q' \in P.\ q \longrightarrow q' \ \&\ p'\,R\,q'$, and
- $\forall q' \in P.\ q \longrightarrow q' \Rightarrow \exists p' \in P.\ p \longrightarrow p' \ \&\ p'\,R\,q'$.

Define the *bisimilarity* relation $\sim$ on $P$ by taking $p \sim q$ iff $p\,R\,q$, for some bisimulation $R$ on $P$.

Show the following:

(i) the identity relation $\mathsf{id}_P$ is a bisimulation on $P$;

(ii) if $R$ is a bisimulation on $P$ then its converse relation $R^{-1}$ is a bisimulation on $P$;

(iii) if relations $R$ and $S$ are bisimulations on $P$, then their composition $S \circ R$ is a bisimulation on $P$.

Deduce that the bisimilarity relation $\sim$ is an equivalence relation on $P$. Show that $\sim$ is itself a bisimulation on $P$. □

## 3.4 Size of sets

A useful way to compare sets is through an idea of their size. Write $A \cong B$ to mean there is bijective correspondence between sets $A$ and $B$. The relation $A \cong B$ satisfies the properties of an equivalence relation on sets. Two sets in the relation $\cong$ are said to have the same *size* or *cardinality.*[1]

### 3.4.1 Countability

In computation we are particularly concerned with sets whose size does not exceed that of the set of natural numbers $\mathbb{N}$, sets which are said to be countable because they can be paired off, in the manner of counting, with initial segments of the natural numbers, or possibly even the whole of the natural numbers. Here's the definition.

A set $A$ is *finite* iff there is a bijection from the set $\{m \in \mathbb{N} \mid m \leq n\}$ to $A$ for some $n \in \mathbb{N}_0$; in other words, $A$ is empty or in 1-1 correspondence with a set $\{1, 2, \cdots, n\}$. We say a set is *infinite* iff it is not finite. A set $A$ is *countable* iff it is finite or there is a bijection

$$f : \mathbb{N} \to A\ .$$

For example, the sets of natural numbers $\mathbb{N}$, of integers $\mathbb{Z}$, of rational numbers $\mathbb{Q}$ and real numbers $\mathbb{R}$ are all infinite. The set $\mathbb{N}$ is countable, as are $\mathbb{Z}$ and $\mathbb{Q}$, while $\mathbb{R}$ is not countable—we'll see this shortly.

**Lemma 3.21** *Any subset of natural numbers is countable.*

*Proof.* Let $A$ be a subset of $\mathbb{N}$. Define a partial function $f : \mathbb{N} \rightharpoonup A$ by taking

- $f(1)$ to be the least number in $A$ if $A$ is nonempty and undefined otherwise, and
- $f(n+1)$, where $n \in \mathbb{N}$, to be the least number in $A$ which is larger than $f(n)$ if $f(n)$ is defined and there is a member of $A$ larger that $f(n)$; and to be undefined otherwise.

This definition of $f$ is an example of *definition by mathematical induction*: we first define the basis of the definition by induction, $f(1)$, and then the induction step of the definition by induction, defining $f(n+1)$ in terms of $f(n)$.

From the definition of $f$ it is clear that if $f(n+1)$ is defined, then so is $f(n)$ and $f(n) < f(n+1)$, for all $n \in \mathbb{N}$. It follows that if $n < n'$ and $f(n')$ is defined, then $f(n)$ is defined and $f(n) < f(n')$. Hence

$$D = \{n \in \mathbb{N} \mid f(n) \text{ is defined}\}$$

is either $\mathbb{N}$, or of the form $\{n \in \mathbb{N} \mid n \leq m\}$, a finite initial segment of the natural numbers. Furthermore $f : D \to A$ is injective as two distinct elements of $D$ will be strictly ordered so have distinct images under $f$.

To show $f$ is also surjective, suppose otherwise. Then there would be a *least* $a \in A$ not in the image $fD$. The element $a$ cannot be the least element of $A$ because this least element is $f(1)$, clearly in $fD$. So there must be a largest element $a'$ of $A$ such that $a' < a$. Because $a' < a$ there is $n \in D$ such that $f(n) = a'$. But then $f(n+1) = a$—contradiction. □

[1] In fact Russell and Whitehead's definition of the cardinal numbers, including the natural numbers, was as $\cong$-equivalence classes.

**Corollary 3.22** *A set $B$ is countable iff there is a bijection $g : A \to B$ from $A \subseteq \mathbb{N}$.*

*Proof.* *"only if":* follows directly from the definition of countability. *"if":* By Lemma 3.21 a subset $A \subseteq \mathbb{N}$ is countable so there is a bijection $f : D \to A$ where $D$ is a finite initial segment or the whole of $\mathbb{N}$. The composition $g \circ f : D \to B$ is a bijection establishing the countability of $B$. □

In establishing countability of a set we do not need to be so demanding as Corollary 3.22; an injection from the set into the natural numbers suffices:

**Lemma 3.23** *A set $B$ is countable iff there is an injection $f : B \to \mathbb{N}$.*

*Proof.* *"only if":* Assuming $B$ is countable there is a bijection $g : A \to B$ from $A \subseteq \mathbb{N}$ by Corollary 3.22. The function $g$ has an inverse function $g^{-1} : B \to A$, by Lemma 3.9. Let $j; A \to \mathbb{N}$ be the inclusion function. Then $f = j \circ g^{-1} : B \to \mathbb{N}$ is an injection, being the composition of two injections. *"if":* An injection $f : B \to \mathbb{N}$ becomes a bijection $f : B \to f\,B$ because $f$ regarded as a function from $B$ to the direct image $f\,B$ is clearly both injective and surjective. Now its inverse $f^{-1} : f\,B \to B$ is a bijection from $f\,B \subseteq \mathbb{N}$. Hence by Corollary 3.22 the set $B$ is countable. □

So, a set is countable iff there is an injection from it into the natural numbers. We could instead have taken this as our definition of countability. Though our current definition has the advantage of being more customary and directly related to our intuitions about counting. As we will see, the following fact, a slight relaxation of Lemma 3.23, is often useful in establishing that a set is countable.

**Lemma 3.24** *A set $B$ is countable iff there is an injection $f : B \to A$ into a set $A$ which is countable.*

*Proof.* *"only if":* If $B$ is countable, then there is an injection $f : B \to \mathbb{N}$ by Lemma 3.23, and $\mathbb{N}$ is countable. *"if":* Suppose $f : B \to A$ is an injection and the set $A$ is countable. Then, by Lemma 3.23, there is an injection $h : A \to \mathbb{N}$. It follows that the composition $g = h \circ f : B \to \mathbb{N}$ is an injection. So, again by Lemma 3.23, the set $B$ is countable. □

Notice that if $B \subseteq A$ then there is an *inclusion* function from $B$ to $A$ taking $b \in B$ to $b \in A$—the inclusion function is clearly injective. So Lemma 3.24 specialises to say a set $B$ is countable iff it is included in a countable set $A$.

**Lemma 3.25** *The set $\mathbb{N} \times \mathbb{N}$ is countable.*

*Proof.* The function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$f(m, n) = 2^m \times 3^n$$

is an injection into a countable set. By Lemma 3.24, $\mathbb{N} \times \mathbb{N}$ is countable. □

**Corollary 3.26** *The set of positive rational numbers $\mathbb{Q}^+$ is countable.*

*Proof.* Any positive rational $q$ can be written uniquely as a fraction $m_q/n_q$ where $m_q$ and $n_q$ are natural numbers with no common factor. Define a function $f : \mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$ by taking $f(q) = (m_q, n_q)$. Then $f$ is an injection—two different rationals determine different fractions. So $\mathbb{Q}^+$ is countable by Lemma 3.24. □

**Corollary 3.27** *If $A$ and $B$ are countable sets, then so is their product $A \times B$.*

*Proof.* Assume sets $A$ and $B$ are countable. Then there are injections $f_A : A \to \mathbb{N}$ and $f_B : B \to \mathbb{N}$, by Lemma 3.24. We can combine them into an lnjection $f : A \times B \to \mathbb{N} \times \mathbb{N}$ by defining $f(a, b) = (f_A(a), f_B(b))$. We spell out the easy check that $f$ is an injection, which uses standard properties of pairs and that $f_A$ and $f_B$ are injections. Let $(a, b)$ and $(a', b')$ be pairs in $A \times B$ for which $f(a, b) = f(a', b')$. We obtain $(f_A(a), f_B(b)) = (f_A(a'), f_B(b'))$. Whence, $f_A(a) = f_A(a')$ and $f_B(b) = f_B(b')$. So $a = a'$ and $b = b'$ by the injectivity of $f_A$ and $f_B$. Thus $(a, b) = (a', b')$. □

We have seen unions, like $A_1 \cup A_2 \cup \cdots \cup A_k$, of finitely sets $A_1, \cdots, A_k$. Imagine now that we are given an infinite sequence of sets $A_1, A_2, A_3, \cdots, A_n, \cdots$ indexed by the natural numbers. We can also form their union; we might write that union as

$$A_1 \cup A_2 \cup A_3 \cup \cdots A_n \cup \cdots$$

though this perhaps makes the union seem more mysterious than it is, because it suggests wrongly a form of limiting process like those in real or complex analysis. A better way to write the union of the sequence of sets is as

$$\bigcup_{n \in \mathbb{N}} A_n =_{def} \{x \mid \exists n \in \mathbb{N}.\ x \in A_n\} \ ,$$

which exposes how innocent this union of countably many sets really is. The next lemma shows that if each of the sets $A_n$ is countable then so is their union. The lemma is often expressed as: a countable union of countable sets is countable.

**Lemma 3.28** *Suppose $A_1, A_2, \cdots, A_n, \cdots$ are all countable sets. Their union $\bigcup_{n \in \mathbb{N}} A_n$ is countable.*

*Proof.* Write $A$ for the set $\bigcup_{n \in \mathbb{N}} A_n$. By Lemma 3.23, for each $n$ there is an injection $f_n : A_n \to \mathbb{N}$. Define an injection $h : A \to \mathbb{N} \times \mathbb{N}$ as follows. For $x \in A$, let $n_x$ be the least number for which $x \in A_{n_x}$, and take

$$h(x) = (n_x, f_{n_x}(x)) \ .$$

We check that $h$ is an injection: Suppose $h(x) = h(y)$ for $x, y \in A$. Then $n_x = n_y$ so $x, y \in A_{n_x}$ and $f_{n_x}(x) = f_{n_x}(y)$. But $f_{n_x}$ is injective, so $x = y$. Hence $A$ is countable by Lemmas 3.24 and 3.25. □

Notice thay the above lemma also applies to finite unions, because the $A_n$'s could all be the empty set from some point on.

**Exercise 3.29** Prove that the set $\mathbb{Z}$ of integers and the set $\mathbb{Q}$ of all rational numbers are countable. [Both proofs involve the same idea.] □

**Exercise 3.30** Show that the set of all *finite* subsets of $\mathbb{N}$ is countable. □

**Exercise 3.31** Show that $\mathbb{Q} \times \mathbb{Q}$ is countable. Deduce that any set of disjoint discs (*i.e.* circular areas which may or may not include their perimeter) in the plane $\mathbb{R} \times \mathbb{R}$ is countable. Is the same true if "discs" is replaced by "circles" (*i.e.* just the perimeters of the circles)? □

**Exercise 3.32** Show that a nonempty set $A$ is countable iff there is a surjection $f : \mathbb{N} \to A$. □

### 3.4.2 Uncountability

Not all sets are countable. One of the notable mathematical accomplishments of the 19th century was Georg Cantor's proof that the set of real numbers $\mathbb{R}$ is uncountable, *i.e.* not countable. This opened up new ways to prove the existence of certain kinds of real numbers. His second, simpler proof of the uncountability of $\mathbb{R}$ used a *diagonal argument*, a style of argument which reappears in showing the undecidability of the halting problem, is implicit in the proof of Gödel's incompleteness theorem, and can sometimes be used in establishing the hierarchies of complexity theory.

**Theorem 3.33** *The set of real numbers $\mathbb{R}$ is uncountable.*

*Proof.* The proof is by contradiction. Assume that $\mathbb{R}$ is countable. Then by Lemma 3.24, the interval $(0, 1] = \{r \in \mathbb{R} \mid 0 < r \leq 1\} \subseteq \mathbb{R}$ will also be a countable set. Each number in $(0, 1]$ is represented uniquely by a non-terminating decimal expansion; for example 0.13 is represented by the non-terminating decimal $0.12999\cdots$. The set $(0, 1]$ is clearly infinite (any finite set of reals would contain a least element, which $(0, 1]$ clearly does not). So $(0, 1]$ being countable implies there is a bijection $f : \mathbb{N} \to (0, 1]$. Write

$$f(n) = 0.d_1^n d_2^n d_3^n \cdots d_i^n \cdots$$

to describe the non-terminating decimal expansion of the $n$th real in the enumeration given by $f$. We'll produce a number $r$ in $(0, 1]$ which can't be in the enumeration, so yielding a contradiction. Define the number's decimal expansion to be

$$0.r_1 r_2 r_3 \cdots r_i \cdots$$

where

$$r_i = \begin{cases} 1 & \text{if } d_i^i \neq 1, \\ 2 & \text{if } d_i^i = 1\ . \end{cases}$$

Clearly $r \in (0, 1]$. Thus there is some natural number $k$ such that $f(k) = r$. Hence by the uniqueness of the decimal expansions $r_i = d_i^k$ for all $i$. In particular,

$$r_k = d_k^k\ .$$

But, from the definition of $r_k$, we have that $r_k = 1$ if $d_k^k \neq 1$, and $r_k = 2$ if $d_k^k = 1$. In either case, $r_k \neq d_k^k$—a contradiction.

We conclude that the original assumption, that $\mathbb{R}$ is countable, is false. □

To see why it is called a diagonal argument, imagine writing the enumerations as an array:

$$\begin{array}{rcccccccc}
f(1) = & 0. & d_1^1 & d_2^1 & d_3^1 & \cdots & d_i^1 & \cdots \\
\\
f(2) = & 0. & d_1^2 & d_2^2 & d_3^2 & \cdots & d_i^2 & \cdots \\
\\
f(3) = & 0. & d_1^3 & d_2^3 & d_3^3 & \cdots & d_i^3 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
f(n) = & 0. & d_1^n & d_2^n & d_3^n & \cdots & d_i^n & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

The decimal expansion of the real $r$ which plays a key role in Cantor's argument is defined by running down the diagonal of the array changing 1's to 2's and non-1's to 1's. In this way the decimal expansion can never be in the enumeration; no matter which row one considers, the decimal expansion of $r$ will differ on the diagonal.

Notice that Cantor's theorem establishes the existence of irrational numbers, in fact shows that the set of irrational numbers is uncountable, without exhibiting a single irrational number explicitly.

**Exercise 3.34** Prove that the set of irrational numbers is uncountable. □

An analogous proof that there are uncountably many transcendental numbers is even more dramatic in that it is very hard to prove a number is transcendental. An *algebraic* number is a real number $x$ that is the solution of a polynomial equation

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

where $a_0, a_1, a_2, \cdots, a_n$ are integer coefficients. A real number which is not algebraic is called *transcendental.* There are only countably many such polynomial equations[2] and each has only finitely many solutions, so there are only countably many algebraic numbers. But there are uncountably many reals. It follows that there must be transcendental numbers, and indeed that the set of transcendental numbers is uncountable. (Do you now know a single transcendental number? Well, $\pi$ and $e$ are. But could you prove it? Probably not.)

**Exercise 3.35** Prove that the set of transcendental numbers is uncountable. (This uses essentially the same idea as Exercise 3.34.) □

[2] A polynomial is determined by its coefficients. So polynomials with integer coefficients are in 1-1 correspondence with tuples of integers in the set $\bigcup_{n \in N} \mathbb{Z}^n$, a countable union of countable sets, so countable.

### Investigating cardinality

By Lemma 3.24, if $f : B \to A$ is an injection and $A$ is countable, then so is $B$. So, when investigating cardinality,

- to show a set $B$ is countable it suffices to exhibit an injection from $B$ set into a set $A$ known to be countable; while
- to show a set $A$ is uncountable it suffices to exhibit an injection from a set $B$ known to be uncountable into $A$. Because then, if $A$ were countable, so would $B$ be countable—a contradiction.

Sometimes (though rarely in undergraduate courses) we need to investigate cardinality beyond countability or its failure. Then the key tool is the Schröder-Bernstein theorem.This says that two sets $A$ and $B$ have the same cardinality iff there are injections $f : A \to B$ and $g : B \to A$. The hard part of its proof shows how to construct a bijection between $A$ and $B$ out of the two injections—see Exercise 3.38.

**Exercise 3.36** By using a variation on the diagonal argument above, show that the powerset, $\mathcal{P}(\mathbb{N}) =_{def} \{S \mid S \subseteq \mathbb{N}\}$, is uncountable. (See Section 4.3.2 for a proof.) □

**Exercise 3.37** Which of the following sets are finite, which are infinite but countable, and which are uncountable?

- $\{f : \mathbb{N} \to \{0,1\} \mid \forall n \in \mathbb{N}.\ f(n) \le f(n+1)\}$
- $\{f : \mathbb{N} \to \{0,1\} \mid \forall n \in \mathbb{N}.\ f(2n) \ne f(2n+1)\}$
- $\{f : \mathbb{N} \to \{0,1\} \mid \forall n \in \mathbb{N}.\ f(n) \ne f(n+1)\}$
- $\{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N}.\ f(n) \le f(n+1)\}$
- $\{f : \mathbb{N} \to \mathbb{N} \mid \forall n \in \mathbb{N}.\ f(n) \ge f(n+1)\}$

□

**Exercise 3.38** (Schröder-Bernstein theorem) Let $f : A \to B$ and $g : B \to A$ be injections between two sets $A$ and $B$. Note that the function $g : B \to g\,B$ is a bijection, with inverse function $g^{-1} : g\,B \to B$. Define subsets $C_1, C_2, \cdots, C_n, \cdots$ of $A$ by the following induction:

$$\begin{array}{l} C_1 = A \setminus (g\,B) \\ C_{n+1} = (g \circ f)\,C_n \end{array} .$$

Define $C = \bigcup_{n \in \mathbb{N}} C_n$. Now define a function $h : A \to B$ by

$$\begin{array}{ll} h(a) = f(a) & \text{if } a \in C, \\ h(a) = g^{-1}(a) & \text{if } a \notin C \end{array}$$

—if $a \notin C$ then $a \in g\,B$, so it makes sense to apply $g^{-1}$ to $a \notin C$.

Prove $h$ is a bijection from $A$ to $B$ by showing:
(i) $h$ is injective: Show if $a \in C$ and $a' \notin C$, then $h(a) \ne h(a')$. Deduce that $h$ is injective.
(ii) $h$ is surjective: Show $(g \circ f)\,C = C \setminus C_1$. Deduce if $b \notin f\,C$, then $g(b) \notin C$, and hence that $h$ is surjective.
□