Course 221: Michaelmas Term 2006
Section 1: Sets, Functions and Countability

David R. Wilkins

Contents

1 Sets, Functions and Countability

1.1 Sets

A *set* is a collection of objects; these objects are known as *elements* of the set. If an element x belongs to a set X then we denote this fact by writing $x \in X$. Sets with small numbers of elements can be specified by listing the elements of the set enclosed within braces. For example $\{a, b, c, d\}$ is the set consisting of the elements a, b, c and d. Two sets are equal if and only if they have the same elements.

The *empty set* $\emptyset$ is the set with no elements.

Standard notations $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are adopted for the following sets:

- the set $\mathbb{N}$ of positive integers;
- the set $\mathbb{Z}$ of integers;
- the set $\mathbb{Q}$ of rational numbers;
- the set $\mathbb{R}$ of real numbers;
- the set $\mathbb{C}$ of complex numbers.

A set A is said to be a *subset* of a set B if every element of A is also an element of B. If A is a subset of B but is not equal to B, then we say that A is a *proper subset* of B. If A is a subset of a set B then we denote this fact by writing $A \subset B$. Note that $A = B$ if and only if $A \subset B$ and $B \subset A$.

Given a set X and a *condition* that may or may not be satisfied by elements of X, the subset of X consisting of all elements of X that satisfy the stated *condition* is represented using the notation

$$\{x \in X : \textit{condition}\}.$$

Thus for example $\{n \in \mathbb{Z} : n > 0\}$ is the subset of the set $\mathbb{Z}$ of integers which consists of all strictly positive integers. (In certain contexts it is possible to simplify the above notation to $\{x : \textit{condition}\}$ if it is clear from the context what the set is to which the elements x in question belong.)

Let a and b be real numbers satisfying $a \leq b$. Then intervals in the set of real numbers are denoted using the following standard notation:

- $[a, b]$ denotes the set $\{x \in \mathbb{R} : a \leq x \leq b\}$;
- (a, b) denotes the set $\{x \in \mathbb{R} : a < x < b\}$;
- $[a, b)$ denotes the set $\{x \in \mathbb{R} : a \leq x < b\}$;

- $(a, b]$ denotes the set $\{x \in \mathbb{R} : a < x \leq b\}$;
- $[a, +\infty)$ denotes the set $\{x \in \mathbb{R} : x \geq a\}$;
- $(a, +\infty)$ denotes the set $\{x \in \mathbb{R} : x > a\}$;
- $(-\infty, a]$ denotes the set $\{x \in \mathbb{R} : x \leq a\}$;
- $(-\infty, a)$ denotes the set $\{x \in \mathbb{R} : x < a\}$.

The *union*, *intersection* and *difference* of two sets are defined as follows:—

- the *union* $X \cup Y$ of two sets X and Y is the set consisting of all elements that belong to X or to Y (or to both);
- the *intersection* $X \cap Y$ of two sets X and Y is the set consisting of all elements that belong to both X and Y;
- the *difference* $X \setminus Y$ of two sets X and Y is the set consisting of all elements that belong to X but not to Y.

The sets X and Y are said to be *disjoint* if no element belongs to both X and Y (i.e., $X \cap Y = \emptyset$.)

Note that $X \cup Y$ is the union of the three sets $X \cap Y$, $X \setminus Y$ and $Y \setminus X$. Moreover these three sets are pairwise disjoint (i.e., each pair is disjoint).

We can also consider unions and intersections of more than two sets. The *union* of a given collection of sets is the set consisting of all elements that belong to at least one of the given sets. The *intersection* of a given collection of sets is the set consisting of all elements that belong to every one of the given sets.

Let $X_1, X_2, X_3, \ldots, X_n$ be sets. We denote the union and intersection of these sets by $X_1 \cup X_2 \cup X_3 \cup \cdots \cup X_n$ and $X_1 \cap X_2 \cap X_3 \cap \cdots \cap X_n$ respectively.

The union and intersection of an infinite sequence $X_1, X_2, X_3, \ldots$ of sets are denoted by $\bigcup\limits_{i=1}^{\infty} X_i$ and by $\bigcap\limits_{i=1}^{\infty} X_i$ respectively. More generally, given any collection $\mathcal{C}$ of sets, the union and intersection of the sets in the collection are denoted by $\bigcup_{X \in \mathcal{C}} X$ and $\bigcap_{X \in \mathcal{C}} X$ respectively.

It is handy to introduce the notion of a collection $(X_i : i \in I)$ of sets indexed by some set I. This associates to each element i of the indexing set I a corresponding set X_i. We can form the union or intersection of the sets in such an indexed collection. The union $\bigcup_{i \in I} X_i$ consists of everything that belongs to at least one of the sets X_i in the indexed collection; the intersection $\bigcap_{i \in I} X_i$ consists of everything that belongs to every single set in the indexed collection. Thus for example if $I = \{1, 2, \ldots, n\}$ then a collection of sets indexed by I is just a finite collection of sets $X_1, X_2, \ldots, X_n$; and in this case

$$\bigcup_{i\in I} X_i = X_1 \cup X_2 \cup \cdots \cup X_n, \quad \bigcap_{i\in I} X_i = X_1 \cap X_2 \cap \cdots \cap X_n.$$

Similarly if $I = \mathbb{N}$ then a collection $(X_i : i \in I)$ of sets indexed by I is just an infinite sequence $X_1, X_2, X_3, \ldots$ of sets, and in this case $\bigcup_{i\in I} X_i = \bigcup_{i=1}^{\infty} X_i$ and $\bigcap_{i\in I} X_i = \bigcap_{i=1}^{\infty} X_i$.

Let X be a set, and let A be a subset of X. The *complement* of A (in X) is the set $X \setminus A$ of all elements of X that do not belong to A.

For each subset A of a given set X, let A^c denote the complement of A in X. Then $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$ for all subsets A and B of X. These identities generalize to situations where the number of subsets of X involved is greater than two. This basic result is stated formally in the following lemma.

Lemma 1.1 *Let X be a set, and let $\mathcal{C}$ be an indexed collection of sets. Then*

$$\bigcup_{Y\in\mathcal{C}} (X \setminus Y) = X \setminus \bigcap_{Y\in\mathcal{C}} Y \text{ and } \bigcap_{Y\in\mathcal{C}} (X \setminus Y) = X \setminus \bigcup_{Y\in\mathcal{C}} Y.$$

Proof Let x be an element of X. Then

$$\begin{aligned} x \in \bigcup_{Y\in\mathcal{C}} (X \setminus Y) &\iff \text{there exists } Y \in \mathcal{C} \text{ such that } x \in X \setminus Y \\ &\iff \text{there exists } Y \in \mathcal{C} \text{ such that } x \notin Y \\ &\iff x \notin \bigcap_{Y\in\mathcal{C}} Y, \\ &\iff x \in X \setminus \bigcap_{Y\in\mathcal{C}} Y. \end{aligned}$$

It follows from this that the subsets $\bigcup_{Y\in\mathcal{C}} (X \setminus Y)$ and $X \setminus \bigcap_{Y\in\mathcal{C}} Y$ of X have the same elements, and are therefore the same set.

Similarly

$$\begin{aligned} x \in \bigcap_{Y\in\mathcal{C}} (X \setminus Y) &\iff \text{for all } Y \in \mathcal{C},\ x \in X \setminus Y \\ &\iff \text{for all } Y \in \mathcal{C},\ x \notin Y \\ &\iff x \notin \bigcup_{Y\in\mathcal{C}} Y, \\ &\iff x \in X \setminus \bigcup_{Y\in\mathcal{C}} Y, \end{aligned}$$

and therefore $\bigcap_{Y\in\mathcal{C}} (X \setminus Y) = X \setminus \bigcup_{Y\in\mathcal{C}} Y$, as required. ∎

Lemma 1.1 thus ensures that the complement of the intersection of any collection of subsets of a given set is the union of the complements of those subsets; and the complement of the union of any collection of subsets of a given set is the intersection of the complements of those subsets. In particular, if X is a set, and if $(Y_i : i \in Y)$ is any indexed collection of sets, then

$$\bigcup_{i\in I}(X \setminus Y_i) = X \setminus \bigcap_{i\in I} Y_i \text{ and } \bigcap_{i\in I}(X \setminus Y_i) = X \setminus \bigcup_{i\in I} Y_i,$$

1.2 Cartesian Products of Sets

Let X and Y be sets. An element x of X and an element y of Y together specify an *ordered pair* (x, y). Ordered pairs (x, y) are characterized by the following property:

$$(x, y) = (u, v) \text{ if and only if } x = u \text{ and } y = v.$$

The set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$ is referred to as the *Cartesian product* of the sets X and Y, and is denoted by $X \times Y$.

Example The Cartesian product $\mathbb{R} \times \mathbb{R}$ consists of all ordered pairs (x, y) where x and y are real numbers. This set is denoted by $\mathbb{R}^2$.

Example Let $X = \{1, 2, 3\}$ and $Y = \{2, 4\}$. Then

$$X \times Y = \{(1, 2),\ (1, 4),\ (2, 2),\ (2, 4),\ (3, 2),\ (3, 4)\}.$$

The Cartesian product $X_1 \times X_2 \times X_3 \times \cdots \times X_n$ of n sets $X_1, X_2, X_3, \ldots, X_n$ is the set consisting of all ordered n-tuples $(x_1, x_2, \ldots, x_n)$, where $x_i \in X_i$ for $i = 1, 2, 3, \ldots, n$.

Example Points of 3-dimensional space are represented with respect to a Cartesian co-ordinate system as ordered triples (x, y, z), where x, y and z are real numbers. The set of all such ordered triples is the Cartesian product $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ (denoted by $\mathbb{R}^3$).

Note that if X_i is a finite set with m_i elements for $i = 1, 2, \ldots, n$, then the Cartesian product $X_1 \times X_2 \times X_3 \times \cdots \times X_n$ has $m_1 m_2 m_3 \cdots m_n$ elements.

1.3 Relations

Let X be a set. A *binary relation* on X determines, for elements u and v of X, whether or not u is related to v. For example, there is a binary relation on the set of real numbers, where two real numbers x and y are related if and only if x is less than y.

It is traditional to denote binary relations by inserting the symbol for the relation between any two elements that are related. Thus if $\sim$ is a relation on a set X then $u \sim v$ is true for elements u and v of X if and only if u and v are related. Familiar examples of this notation are provided by the relations $=$ ('equals'), $<$ ('less than') and $\leq$ ('less than or equal to') on sets of numbers.

Any binary relation $\sim$ on a set X determines a corresponding subset $\{(u, v) \in X \times X : u \sim v\}$ of the Cartesian product $X \times X$. Conversely any subset R of $X \times X$ determines a corresponding relation $\sim$ on X, where elements u and v of X satisfy $u \sim v$ if and only if $(u, v) \in R$. There is thus a one-to-one correspondence between binary relations on a set X and subsets of $X \times X$.

1.4 Equivalence Relations

Let $\sim$ be a binary relation on a set S.

- The relation $\sim$ is *reflexive* on S if the following is true: $x \sim x$ for all elements x of S.
- The relation $\sim$ is *symmetric* on S if the following is true: if x and y are elements of S and if $x \sim y$ then $y \sim x$.
- The relation $\sim$ is *transitive* on S if the following is true: if x, y and z are elements of S and if if $x \sim y$ and $y \sim z$ then $x \sim z$.

Example The relation $=$ (i.e., 'is equal to') is reflexive, symmetric and transitive on any set.

Example The relation $<$ (i.e., 'is less than') is transitive on the set of real numbers but is neither reflexive nor symmetric.

Example The relation $\leq$ (i.e., 'is less than of equal to') is reflexive and transitive on the set of real numbers but is not symmetric.

Example The relation $\neq$ (i.e., 'is not equal to') is symmetric on the set of real numbers but is neither reflexive nor transitive.

Example The relation 'has the same number of elements as' is reflexive, symmetric and transitive on any collection of finite sets.

Definition An *equivalence relation* on a given set is a binary relation on that set which is reflexive, symmetric and transitive.

The relation of equality is an equivalence relation on any set.

The relation $<$ (i.e., 'is less than') is not an equivalence relation on the set of real numbers because it is neither reflexive nor symmetric.

Definition Let $\sim$ be an equivalence relation on a set X. The *equivalence class* of x in X (with respect to the equivalence relation $\sim$) is the set C_x consisting of all elements of X that are related to x. Thus

$$C_x = \{y \in X : x \sim y\}.$$

Lemma 1.2 *Let $\sim$ be an equivalence relation on a set X, and, for each $x \in X$, let C_x denote equivalence class of x, defined by*

$$C_x = \{y \in X : x \sim y\}.$$

Then the following are true:

(i) *$x \in C_x$ for all $x \in X$;*

(ii) *$y \in C_x$ if and only if $C_x = C_y$;*

(iii) *if x and y are elements of X and if $C_x \cap C_y$ is non-empty, then $C_x = C_y$;*

(iv) *an element x of X belongs to exactly one equivalence class.*

Proof The fact that $x \in C_x$ for all $x \in X$ follows immediately from the fact that any equivalence relation is required to be reflexive. This proves (i).

Suppose that $y \in C_x$. Then $x \sim y$. Also $y \sim x$, since any equivalence relation is transitive. If $z \in C_y$ then $x \sim y$ and $y \sim z$, and hence $x \sim z$, since any equivalence relation is transitive. It follows that if $z \in C_y$ then $z \in C_x$, and thus $C_y \subset C_x$. Similarly $C_x \subset C_y$. Thus if $y \in C_x$ then $C_x = C_y$. Conversely if $C_x = C_y$ then $y \in C_x$, since $y \in C_y$. This proves (ii).

Next note that if x and y are elements of X and if $C_x \cap C_y$ is non-empty, then there exists some element z of X such that $z \in C_x$ and $z \in C_y$. It follows from (ii) that $C_x = C_z$ and $C_y = C_z$, and therefore $C_x = C_y$. This proves (iii).

Finally (iv) is a consequence of (i) and (iii). ∎

Definition Let X be a set. A *partition* of X is a collection of subsets of X with the property that every element of X belongs to exactly one of these subsets.

Let an equivalence relation be given on a set X. Then the collection of equivalence classes constitutes a partition of X. Conversely any partition of a set X determines an equivalence relation, where two elements of X are related if and only if they belong to the same subset in the partition.

1.5 Functions

Let X and Y be sets. A *function* $f\colon X \to Y$ from X to Y assigns to each element x of the set X exactly one element $f(x)$ of the set Y. The set X is the *domain* of the function, and the set Y is the *co-domain* of the function.

The notation $f\colon X \to Y$ is used to specify a function f whose domain is the set X and whose co-domain is the set Y.

A function is not fully specified unless its domain and co-domain are specified.

Example Let us consider 'the function that sends x to $1/x^2$'. Note that $1/x^2$ is is not defined when $x = 0$. Therefore we cannot view this 'function' as a function on the set of real numbers. We can however take as the domain of the function the set $\mathbb{R} \setminus \{0\}$ of all non-zero real numbers. We thus obtain a function $f\colon \mathbb{R} \setminus \{0\} \to \mathbb{R}$ from the set $\mathbb{R} \setminus \{0\}$ of non-zero real numbers to the set $\mathbb{R}$ of real numbers, where $f(x) = 1/x^2$ for all non-zero real numbers x.

There is also a function $g\colon \mathbb{C} \setminus \{0\} \to \mathbb{C}$ from the set $\mathbb{C} \setminus \{0\}$ of non-zero complex numbers to the set $\mathbb{C}$ of complex numbers, where $g(z) = 1/z^2$ for all non-zero complex numbers z. The functions f and g have different domains, and are therefore considered to be different functions.

Note that there is no element x of the domain $\mathbb{R} \setminus \{0\}$ of $f\colon \mathbb{R} \setminus \{0\} \to \mathbb{R}$ for which $f(x) = 0$. Also $f(x) = f(-x)$ for all non-zero real numbers x. Thus, given an element y of the co-domain $\mathbb{R}$ of the function f, there need not be exactly one element x of the domain satisfying $f(x) = y$. There may not be any such elements x, as is the case when $y < 0$, or there may be more than one such element x, as is the case when $y > 0$.

Let X be a set. There is a function $i\colon X \to X$ from X to itself, where $i(x) = x$ for all $x \in X$. This function is referred to as the *identity map* of X.

Let $f\colon X \to Y$ be a function from a set X to a set Y. The *range* $f(X)$ of the function is defined to be the set $\{f(x) : x \in X\}$ of all elements of the co-domain Y that are of the form $f(x)$ for some element x of the domain.

The *image* $f(A)$ of a subset A of X is defined to be the set $\{f(x) : x \in A\}$ of all elements of the co-domain Y that are of the form $f(x)$ for some element x of A.

Note that the range of a function $f: X \to Y$ is the image $f(X)$ of the domain X of the function. Also $f^{-1}(Y) = X$.

Example Let $f: \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x) = x^2$ for all $x \in \mathbb{R}$. The range of f is the set $[0, +\infty)$ of non-negative real numbers. The image $f([1, 2])$ of the interval $[1, 2]$ is the interval $[1, 4]$.

Let X, Y and Z be sets, and let $f: X \to Y$ and $g: Y \to Z$ be functions, where the domain Y of $g: Y \to Z$ is the co-domain of $f: X \to Y$. The composition function $g \circ f: X \to Z$ is defined by $(g \circ f)(x) = g(f(x))$ for all $x \in X$. Note that $g \circ f$ denotes the function 'f followed by g'.

1.6 The Graph of a Function

Let X and Y be sets. To every function $f: X \to Y$ from X to Y there corresponds a subset $\Gamma(f)$ of the Cartesian product $X \times Y$, where

$$\Gamma(f) = \{(x, y) \in X \times Y : y = f(x)\}.$$

Mathematicians often refer to the subset of $X \times Y$ corresponding to a function $f: X \to Y$ as the *graph* of the function. The following example suggests the reason for this terminology.

Example Let $q: \mathbb{R} \to \mathbb{R}$ be the function from the set $\mathbb{R}$ of real numbers to itself defined such that $q(x) = x^2$ for all real numbers x. The graph of this function is the subset of $\mathbb{R} \times \mathbb{R}$ given by

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2\}.$$

Note that this subset consists of the Cartesian coordinates of the points of the plane that lie on the curve that represents the graph of the given function.

Whilst every function from X to Y determines a corresponding subset $\Gamma(f)$ of $X \times Y$, it is not possible to obtain every subset of $X \times Y$ in this fashion. Indeed it is easy to see that a subset R of $X \times Y$ is the graph of some function $f: X \to Y$ if and only if, for every element x of X, there exists exactly one element y of Y for which $(x, y) \in R$. If the subset R of $X \times Y$ has this property, then the corresponding function $f: X \to Y$ is characterized by the property that, for each element x of X, $f(x)$ is the unique element of Y for which $(x, f(x)) \in R$.

Remark Some mathematicians choose to define a *function* from a set X to a set Y to be a subset G of the Cartesian product with the property that, to each element x of G there exists exactly one element y of Y for which the ordered pair (x, y) belongs to the subset G. This amounts to identifying the function with its graph.

1.7 Functions and the Empty Set

We shall adopt the convention that, given any any set Y, there exists exactly one function from the empty set $\emptyset$ to the set Y. This convention may at first seem a bit strange. Nevertheless experience shows it is in practice a natural convention to adopt, and it tends to simplify the statements and proofs of theorems (which would otherwise be hedged about with all sorts of qualifications and subsidiary arguments to cover the special cases where one of more of the sets involved happens to be the empty set).

This convention can also be justified on the grounds that functions from a set X to a set Y correspond to subsets G of the Cartesian product that have the property that, given any element x of X, the set $\{y \in Y : (x, y) \in G\}$ has exactly one element. (The subset G of $X \times Y$ is the graph of the function f.) In the case where X is the empty set, the Cartesian product $X \times Y$ is also the empty set. The empty set has exactly one subset. This subset is of course the empty set. Moreover it has, vacuously, the property required in order to be the graph of the function, for if the set X is empty, then it is not possible to find any element x of X for which the number of elements belonging to the subset $\{y \in Y : (x, y) \in G\}$ of Y differs from one. Thus, if X is the empty set, then the Cartesian product $X \times Y$ has exactly one subset which has the properties required of the graph of any function.

Note that if there exists a function $f: X \to Y$ from a set X to a set Y, and if the set Y is the empty set, then the set X must also be the empty set. (For if x were an element of X, then $f(x)$ would be an element of Y, and therefore the set Y would be non-empty.)

We see therefore that the number of functions from a set X to the empty set is zero if X is non-empty, but is one if X is the empty set.

When defining properties that sets may or may not have, it is sometimes necessary to decide whether or not the empty set has the given property. There are standard conventions and forms of reasoning that mathematicians regularly adopt to settle such questions.

In mathematics, one often meets definitions of properties, applicable to sets, where a set is said to have some property P if and only if all the elements of the set have some property Q. (For example suppose that P represents the property of being a subset of a given set Y. Then the corresponding property

Q is that of being an element of the set Y. For a set X is a subset of a given set Y if and only if all the elements of X are elements of Y.) In such cases the question arises as to whether or not the empty set has the property P. The standard convention adopted is that in such cases the empty set does indeed have the property P. Note that if a non-empty set X fails to have the property P, then there must exist at least one element of X which fails to have the property Q. It is natural to extend this basic logical principle to the case where the set X is empty. Clearly the empty set cannot have any elements that fail to have this property Q. So it makes sense to say that all elements of the empty set have the property Q, and therefore the empty set has property P.

In effect, we are saying that, if Q is some property that elements of sets may or may not have, then the empty set is considered to be an example of a set whose elements all have the property Q. As a result, given any set X, empty or non-empty, and given any property Q, the statement "all elements of X have the property Q" is the logical negation of the statement "there exists an element of X which does not have the property Q".

Example To give a concrete example, consider the definition of a subset of a given set Y. We say that a set X is a subset of Y if and only if every element of X is an element of Y. Thus if a set X fails to be a subset of Y, there must exist at least one element of X that is not an element of Y. According to the convention we have described, the empty set is to be regarded as a subset of Y, since the empty set clearly does not have any elements that are not elements of Y. (Of course, it does not have any elements at all.)

Example Let u be a real number. We say that a subset X of the set of real numbers is *bounded above* by u if every element x of X satisfies the inequality $x \leq u$. Accordingly the empty set is bounded above by u. Moreover if X is a subset of the set of real numbers (empty or non-empty), and if X is not bounded above by the real number u, then there exists at least one element x of the set X which satisfies the inequality $x > u$.

1.8 Injective, Surjective and Bijective Functions

We now define *injective*, *surjective* and *bijective* functions:—

- a function $f: X \to Y$ is said to be *injective* (or *one-to-one*) if $f(u) \neq f(v)$ whenever u and v are elements of the domain X with $u \neq v$;
- a function $f: X \to Y$ is said to be *surjective* (or *onto*) if each element of the codomain of the function is the image $f(x)$ of at least one element x of the domain X;

- a function $f: X \to Y$ is said to be *bijective* (or is said to be a *one-to-one correspondence*) if it is both injective and surjective.

Injective, surjective and bijective functions are also referred to as *injections*, *surjections* and *bijections* respectively.

Note that a function $f: X \to Y$ is bijective if and only if, given any element y of the co-domain Y of the function, there exists exactly one element x of the domain X satisfying $f(x) = y$.

Example Let $\mathbb{N}$ denote the set $\{1, 2, 3, 4, \ldots\}$ of positive integers. Let $f: \mathbb{N} \to \mathbb{N}$ be the function defined by $f(n) = n^2$ for all positive integers n. This function is injective, for if m and n are positive integers and if $m \neq n$ then $m^2 \neq n^2$. The function is not surjective, since there is no positive integer n satisfying $f(n) = 3$.

Example Let $g: \mathbb{R} \to [0, +\infty)$ be the function from the set $\mathbb{R}$ of real numbers to the set $[0, +\infty)$ of non-negative real numbers that sends each real number x to x^2. This function is not injective, since $g(2) = g(-2) = 4$. It is surjective: for any non-negative real number y, there is a real number $\sqrt{y}$ satisfying $g(\sqrt{y}) = y$.

Example Let $h: \mathbb{N} \to \mathbb{N}$ be the function from the set $\mathbb{N}$ of positive integers to itself defined by

$$h(n) = \begin{cases} n+1 & \text{if } n \text{ is odd;} \\ n-1 & \text{if } n \text{ is even.} \end{cases}$$

Thus $h(1) = 2$, $h(2) = 1$, $h(3) = 4$, $h(4) = 3$, etc. The function is injective. Indeed let m and n be positive integers with $m \neq n$. If m is odd and n is even then $h(m) \neq h(n)$, since $h(m)$ is even and $h(n)$ is odd. If m is even and n is odd then $h(m) \neq h(n)$, since $h(m)$ is odd and $h(n)$ is even. If m and n are both odd then $h(m) \neq h(n)$ since $h(m) = m + 1$, $h(n) = n + 1$ and $m + 1 \neq n + 1$. If m and n are both even then $h(m) \neq h(n)$ since $h(m) = m - 1$, $h(n) = n - 1$ and $m - 1 \neq n - 1$. We have thus verified that $h(m) \neq h(n)$ for all positive integers m and n satisfying $m \neq n$. Thus the function is injective.

Let n be a positive integer. If n is odd then $n = h(n + 1)$. If n is even then $n = h(n - 1)$. Thus the function is surjective.

The function $h: \mathbb{N} \to \mathbb{N}$ is therefore bijective.

Example Let Y be a set. We have adopted the convention that there is exactly one function $e: \emptyset \to Y$ from the empty set $\emptyset$ to the set Y. Clearly there do not exist distinct elements of the empty set that get mapped to the same element of Y. Therefore this function $e: \emptyset \to Y$ is an injective function. The function e is surjective if and only if $Y = \emptyset$.

Lemma 1.3 *Let X, Y and Z be sets, and let $f: X \to Y$ and $g: Y \to Z$ be functions.*

(i) *If $f: X \to Y$ and $g: Y \to Z$ are injective, then so is $g \circ f: X \to Z$.*

(ii) *If $f: X \to Y$ and $g: Y \to Z$ are surjective, then so is $g \circ f: X \to Z$.*

(iii) *If $f: X \to Y$ and $g: Y \to Z$ are bijective, then so is $g \circ f: X \to Z$.*

Proof First suppose that $f: X \to Y$ and $g: Y \to Z$ are injective. We must prove that $g \circ f: X \to Z$ is injective. Let u and v be elements of X with $u \neq v$. Then $f(u) \neq f(v)$, since $f: X \to Y$ is injective. But then $g(f(u)) \neq g(f(v))$, since $g: Y \to Z$ is injective. It follows that $g \circ f: X \to Z$ is injective. This proves (i).

Next suppose that $f: X \to Y$ and $g: Y \to Z$ are surjective. We must prove that $g \circ f: X \to Z$ is surjective. Let z be an element of Z. Then there exists $y \in Y$ satisfying $g(y) = z$, since $g: Y \to Z$ is surjective. Then there exists $x \in X$ satisfying $f(x) = y$, since $f: X \to Y$ is surjective. But then $g(f(x)) = z$. It follows that $g \circ f: X \to Z$ is surjective. This proves (ii).

Clearly (iii) follows from (i) and (ii). ∎

1.9 Inverse Functions

Definition Let X and Y be sets, and let $f: X \to Y$ be a function from X to Y. A function $g: Y \to X$ from Y to X is said to be the *inverse* of $f: X \to Y$ if $g(f(x)) = x$ for all $x \in X$ and $f(g(y)) = y$ for all $y \in Y$.

We denote by $f^{-1}: Y \to X$ the inverse of a function $f: X \to Y$, provided that such an inverse exists.

Example Consider the function $f: [1, 2] \to [1, 4]$, where $f(x) = x^2$ for all $x \in [1, 2]$. The inverse of this function is the function $g: [1, 4] \to [1, 2]$, where $g(y) = \sqrt{y}$ for all $y \in [1, 4]$.

Example Consider the function $h: \mathbb{R} \to \mathbb{R}$, where $h(x) = x^2$ for all real numbers x. This function does not have an well-defined inverse. Indeed no function $k: \mathbb{R} \to \mathbb{R}$ has the property that $y = h(k(y))$ for all real numbers y, since this identity clearly cannot be satisfied when $y < 0$.

Lemma 1.4 *Let X and Y be sets. A function $f: X \to Y$ has a well-defined inverse if and only if it is a bijection. Moreover the inverse of a bijection is itself a bijection.*

Proof Let $f: X \to Y$ be a function which has a well-defined inverse $f^{-1}: Y \to X$. Let u and v be elements of X. Then $u = f^{-1}(f(u))$ and $v = f^{-1}(f(v))$. Thus if $u \neq v$ then $f(u) \neq f(v)$. The function $f: X \to Y$ is therefore injective. The function $f: X \to Y$ is also surjective, since $y = f(f^{-1}(y))$ for all $y \in Y$. We have thus shown that if a function $f: X \to Y$ has a well defined inverse then it is both injective and surjective, and is thus a bijection.

Conversely suppose that $f: X \to Y$ is a bijection. Then, given any element y of Y, there exists exactly one element x of X satisfying $f(x) = y$. We therefore define $f^{-1}(y)$ to be the unique element x of X satisfying $f(x) = y$. Clearly $f(f^{-1}(y)) = y$ for all $y \in Y$. Thus $f \circ f^{-1}$ is the identity map of Y. We must also show that $f^{-1} \circ f$ is the identity map of X. Let x be an element of X. Then $f(f^{-1}(f(x))) = f(x)$, since $f \circ f^{-1}$ is the identity map of Y. But $f: X \to Y$ is injective. It follows that $f^{-1}(f(x)) = x$, since the elements x and $f^{-1}(f(x))$ are mapped by f to the same element of the set Y. We have thus shown that if the function $f: X \to Y$ is a bijection then it has a well-inverse.

If $g: Y \to X$ is the inverse of a bijection $f: X \to Y$ then f is the inverse of g, and therefore $g: Y \to X$ must be a bijection. ∎

1.10 Preimages

Let $f: X \to Y$ be a function from a set X to a set Y, and let B be a subset of Y. The *preimage of the set B under the function f* is the set $f^{-1}(B)$ defined such that

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

Remark The preimage $f^{-1}(B)$ of a subset B of Y is defined in this fashion for all functions $f: X \to Y$ from X to Y, irrespective of whether or not that function has a well-defined inverse function. The standard notation $f^{-1}(B)$ adopted for the preimage of the set B reflects that fact that any function $f: X \to Y$ from a set X to a set Y induces a corresponding function from subsets of Y to subsets of X that obviously goes in the reverse direction to the function f.

In cases where the function $f: X \to Y$ does have well-defined inverse $f^{-1}: Y \to X$, the preimage of a subset B of Y under the function f coincides with the image of B under the inverse of the function f, so that, in this case, the notation $f^{-1}(B)$ is unambiguous, and can be taken to represent either the preimage of the set B under the function f, or else the image of B under the function f^{-1}.

Example Let $f: \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x) = x^2$ for all $x \in \mathbb{R}$.

The preimage $f^{-1}([1,4])$ of the interval $[1,4]$ is the union $[-2,-1] \cup [1,2]$ of the intervals $[1,2]$ and $[-2,-1]$.

Lemma 1.5 *Let $f: X \to Y$ be a function between sets X and Y and let B be a subset of Y. Then $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$. Thus the preimage of the complement of any subset of Y is the complement of the preimage of that subset.*

Proof Let x be an element of X. Then

$$\begin{aligned} x \in f^{-1}(Y \setminus B) &\iff f(x) \in Y \setminus B \iff f(x) \notin B \\ &\iff x \notin f^{-1}(B) \iff x \in X \setminus f^{-1}(B). \end{aligned}$$

It follows that the subsets $f^{-1}(Y \setminus B)$ and $X \setminus f^{-1}(B)$ of X contain the same elements, and must therefore be the same subset of X. ∎

Lemma 1.6 *let $f: X \to Y$ be a function from a set X to a set Y, and let $\mathcal{C}$ be any collection of subsets of Y. Then*

$$f^{-1}\left(\bigcup_{B\in\mathcal{C}} B\right) = \bigcup_{B\in\mathcal{C}} f^{-1}(B), \quad f^{-1}\left(\bigcap_{B\in\mathcal{C}} B\right) = \bigcap_{B\in\mathcal{C}} f^{-1}(B).$$

Thus the preimage of any union of subsets of Y is the union of the preimages of those subsets, and the preimage of any intersection of subsets of Y is the intersection of the preimages of those subsets.

Proof Let x be an element of X. Then

$$\begin{aligned} x \in f^{-1}\left(\bigcup_{B\in\mathcal{C}} B\right) &\iff f(x) \in \bigcup_{B\in\mathcal{C}} B \\ &\iff \text{there exists } B \in \mathcal{C} \text{ such that } f(x) \in B \\ &\iff \text{there exists } B \in \mathcal{C} \text{ such that } x \in f^{-1}(B) \\ &\iff x \in \bigcup_{B\in\mathcal{C}} f^{-1}(B). \end{aligned}$$

It follows that the subsets $f^{-1}\left(\bigcup_{B\in\mathcal{C}} B\right)$ and $\bigcup_{B\in\mathcal{C}} f^{-1}(B)$ of X contain the same elements, and must therefore be the same subset of X.

Also

$$\begin{aligned} x \in f^{-1}\left(\bigcap_{B\in\mathcal{C}} B\right) &\iff f(x) \in \bigcap_{B\in\mathcal{C}} B \\ &\iff \text{for all } B \in \mathcal{C},\ f(x) \in B \\ &\iff \text{for all } B \in \mathcal{C},\ x \in f^{-1}(B) \\ &\iff x \in \bigcap_{B\in\mathcal{C}} f^{-1}(B). \end{aligned}$$

It follows that the subsets $f^{-1}\left(\bigcap_{B\in\mathcal{C}} B\right)$ and $\bigcap_{B\in\mathcal{C}} f^{-1}(B)$ of X contain the same elements, and must therefore be the same subset of X. ∎

1.11 Finite and Infinite Sets

A set is said to be *finite* if the number of elements it contains is finite.

A basic result states that if X is a finite set then any injection $f: X \to X$ from the set X to itself is a bijection. Infinite sets do not have this property.

Although the above result seems fairly obvious, we shall give a fairly formal proof.

Let n be a positive integer. We say that a set X has n elements if there exists a bijection $f: \{1, 2, \ldots, n\} \to X$ defined on the set $\{1, 2, \ldots, n\}$ of natural numbers not exceeding n, and mapping this set onto X. We say that a set X has zero elements if it is the empty set. We say that a set X is finite if there exists some non-negative integer n such that X has n elements. If X is a set with n elements, where $n \geq 1$, and if x is some element of X, then the set $X \setminus \{x\}$ has $n - 1$ elements. This fact is readily verified, and is an easy consequence of the fact that, for each integer j between 1 and n there exists a bijection from the set $\{m \in \mathbb{N} : 1 \leq m \leq n - 1\}$ to the set

$$\{m \in \mathbb{N} : 1 \leq m \leq n \text{ and } m \neq j\}.$$

This observation enables us to set up a proof of the required result for finite sets by induction on the number of elements in the set.

Proposition 1.7 *Let X be a finite set. Then any injection $f: X \to X$ is a bijection.*

Proof The result is easily seen to be true when the number of elements in X is zero or one. Suppose that the result is true for all sets with k elements, where k is some natural number. We show that the result is then true for all sets with $k + 1$ elements. Let X be a set with $k + 1$ elements, and let $f: X \to X$ be a function from X to X which is an injection. Suppose that there were to exist some element x of X that was not in the range of f. Let $Y = X \setminus \{x\}$, and let $g: Y \to Y$ be the function defined such that $g(y) = f(y)$ for all $y \in Y$. The function g would then be an injection from the set Y to itself. Moreover the set Y has k elements. The inductive hypothesis therefore ensures that every injection from the set Y to itself is a surjection. Therefore the function g would be a surjection. In particular there would exist some element y of Y such that $g(y) = f(x)$. But then x and y would be distinct elements of X with the property that $f(x) = f(y)$. But the function f is an injection, and therefore this situation cannot arise. We see therefore that a contradiction would arise were there to exist any element x of the set X that was not in the range of the injection f. It follows that the range of the function f must be the whole of the set X. Thus f is a surjection, and is therefore a bijection. We have thus shown that if every injection from a set with k elements to itself is a bijection, then every injection from a set with $k+1$ elements to itself is a bijection. It now follows by induction on the number of elements in the set that every injection from a finite set to itself is a bijection. ∎

Example Consider the function $f: \mathbb{N} \to \mathbb{N}$ from the set of natural numbers to itself defined such that $f(n) = n + 1$ for all natural numbers n. This function is an injection. However it is not a surjection, because the number 1 is not in the range of the function. The function f is thus an example of a function from a set to itself that is an injection but is not a bijection.

A set is said to be *infinite* if it is not finite.

Lemma 1.8 *Let X be an infinite set. Then there exists an injection $f: X \to X$ that is not a bijection.*

Proof No finite list of elements of X can include all elements of X, and therefore there exists an infinite sequence $x_1, x_2, x_3, \ldots$ of elements of X which are distinct (so that $x_j \neq x_k$ whenever $j \neq k$). Let $f: X \to X$ be the function defined such that $f(x_n) = x_{n+1}$ for all natural numbers n, and $f(x) = x$ for all elements of X not included in the sequence $x_1, x_2, x_3, \ldots$. Then the function f is an injective function whose range is $X \setminus \{x_1\}$. This injection is not a bijection. ∎

The following result follows immediately on combining the results of Proposition 1.7 and Lemma 1.8.

Proposition 1.9 *A set X is infinite if and only if there exists an injection $f: X \to X$ that is not a bijection.*

1.12 Countability

Definition A set X is said to be *countable* if there exists an injection $f: X \to \mathbb{N}$ mapping X into the set $\mathbb{N}$ of natural numbers.

Example The set $\mathbb{Z}$ of integers is countable. For there is a well-defined bijection $f: \mathbb{Z} \to \mathbb{N}$ defined such that $f(n) = 2n + 1$ when $n \geq 0$ and $f(n) = -2n$ when $n < 0$. This bijection maps the set of non-negative integers onto the set of odd natural numbers, and maps the set of negative integers onto the set of even natural numbers.

Lemma 1.10 *Any subset of a countable set is countable.*

Proof Let Y be a subset of a countable set X. Then there exists an injection $f\colon X \to \mathbb{N}$ from X to the set $\mathbb{N}$ of natural numbers. The restriction of this injection to set Y gives an injection from Y to $\mathbb{N}$. ∎

Proposition 1.11 *A non-empty set X is countable if and only if there exists a surjective function $g\colon \mathbb{N} \to X$ mapping the set $\mathbb{N}$ of natural numbers onto X.*

Proof Suppose that X is a countable non-empty set. Then there exists an injection $f\colon X \to \mathbb{N}$ from X to $\mathbb{N}$. Let x_0 be some chosen element of the set X. Then there is a well-defined function $g\colon \mathbb{N} \to X$ defined such that $g(f(x)) = x$ for all $x \in X$, and $g(n) = x_0$ for natural numbers n that do not belong to the range $f(X)$ of the function f. (The definition of the function g relies on the fact that, given an element n of the range $f(X)$ of the injection f, there exists exactly one element x of the set X for which $f(x) = n$.) The function g is clearly a surjection, in view of the fact that $x = g(f(x))$ for all $x \in X$.

Conversely let X be a non-empty set, and let $g\colon \mathbb{N} \to X$ be a surjection from $\mathbb{N}$ to X. Given an element x, there exists at least one natural number n for which $g(n) = x$. It follows that there is a well-defined function $f\colon X \to \mathbb{N}$ such that, given any element x of X, $f(x)$ is the smallest natural number n for which $g(n) = x$. Then $g(f(x)) = x$ for all $x \in X$. It follows from this that if x_1 and x_2 are elements of X (not necessarily distinct), and if $f(x_1) = f(x_2)$, then $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. We conclude that distinct elements of the set X get mapped to distinct natural numbers. Thus the function $f\colon X \to \mathbb{N}$ is an injection, and therefore the set X is countable, as required. ∎

Corollary 1.12 *Let $h\colon X \to Y$ be a surjection. Suppose that the set X is countable. Then the set Y is countable.*

Proof There is nothing to prove if the set X is the empty set, since in that case the set Y must also be the empty set. Suppose therefore that the set X is non-empty and countable. It follows from Proposition 1.11 that there exists a surjection $g\colon \mathbb{N} \to X$ from $\mathbb{N}$ to X. The composition $h \circ g\colon \mathbb{N} \to Y$ of g and h is then a surjection from $\mathbb{N}$ to Y (since the composition of two surjections is always a surjection). It then follows from Proposition 1.11 that the set Y is countable, as required. ∎

1.13 Cartesian Products and Unions of Countable Sets

Lemma 1.13 *There exists a bijection between the sets $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$.*

Proof Let $f\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ be the function defined such that

$$f(j,k) = \tfrac{1}{2}(j+k-1)(j+k-2)+k.$$

One can check that this function f is a bijection.

Note that, for each natural number m greater than one, this function f maps the set D_m into the set I_m, where $D_m = \{(j,k)\in\mathbb{N}\times\mathbb{N} : j+k=m\}$ and

$$I_m = \{n\in\mathbb{N} : \tfrac{1}{2}(m-1)(m-2) < n \leq \tfrac{1}{2}m(m-1)\}.$$

Now, given any natural number n, there exists a unique natural number m greater than one such that $\frac{1}{2}(m-1)(m-2) < n \leq \frac{1}{2}m(m-1)$. It follows that each natural number belongs to exactly one of the sets $I_2, I_3, I_4\ldots$. Moreover if n is a natural number, and if $n\in I_m$, where m is a natural number greater than one, then $n = f(m-k,k)$ where $k = n - \frac{1}{2}(m-1)(m-2)$. Moreover $(m-k,k)$ is the unique element of D_n satisfying $f(n-k,k)=n$. These facts ensure that, given any natural number n, there exists exactly one pair (j,k) of natural numbers satisfying $f(j,k)=n$. (These natural numbers j and k satisfy $j+k=m$, where m is the unique natural number greater than one that satisfies the inequalities $\frac{1}{2}(m-1)(m-2) < n \leq \frac{1}{2}m(m-1)$.) Therefore the function f is both injective and surjective, and is thus a bijection, as required. ∎

Remark The function $f\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ used in the proof of Lemma 1.13 is constructed so that

$$f(1,1)=1,$$
$$f(2,1)=2,\quad f(1,2)=3,$$
$$f(3,1)=4,\quad f(2,2)=5,\quad f(1,3)=6,$$
$$f(4,1)=7,\quad f(3,2)=8,\quad f(2,3)=9,\quad f(1,4)=10,\quad \text{etc.}$$

These examples giving the value of (j,k) for small values of j and k should convey the basic scheme used to construct this function f.

Proposition 1.14 *Let X and Y be countable sets. Then the Cartesian product $X\times Y$ of X and Y is a countable set.*

Proof There exist injective functions $g\colon X\to\mathbb{N}$ and $h\colon Y\to\mathbb{N}$, because the sets X and Y are countable. Also there exists a bijection $f\colon\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ from $\mathbb{N}\times\mathbb{N}$ to $\mathbb{N}$ (Lemma 1.13). Let $p\colon X\times Y\to\mathbb{N}$ be the function defined such that $p(x,y) = f(g(x),h(y))$ for all $x\in X$ and $y\in Y$. We claim that the function p is an injection. Let x_1 and x_2 be elements of X (not necessarily distinct), and let y_1 and y_2 be elements of Y. Suppose that $p(x_1,y_1)=p(x_2,y_2)$. Then

$(g(x_1), h(y_1)) = (g(x_2), h(y_2))$, because the function $f\colon \mathbb{N} \to \mathbb{N}$ is an injection, and therefore $g(x_1) = g(x_2)$ and $h(y_1) = h(y_2)$. But the functions g and h are injections. It follows that $x_1 = x_2$ and $y_1 = y_2$, and thus $(x_1, y_1) = (x_2, y_2)$. We have therefore shown that if the elements (x_1, y_1) and (x_2, y_2) of $X \times Y$ are such that $p(x_1, y_1) = p(x_2, y_2)$ then $(x_1, y_1) = (x_2, y_2)$. This shows that the function $p\colon X \times Y \to \mathbb{N}$ is an injection. The existence of such an injection guarantees that the set $X \times Y$ is countable, as required.

Corollary 1.15 *Let $X_1, X_2, \ldots, X_n$ be countable sets. Then the Cartesian product $X_1 \times X_2 \times \cdots \times X_n$ of these sets is a countable set.*

Proof The result follows by induction on the number of sets forming the Cartesian product, because the set $X_1 \times X_2 \times \cdots \times X_n$ may be regarded as the Cartesian product of the sets $X_1 \times X_2 \times \cdots \times X_{n-1}$ and X_n whenever $n > 1$, and the Cartesian product of any two countable sets is countable (Proposition 1.14). ∎

Lemma 1.16 *The set $\mathbb{Q}$ of rational numbers is countable.*

Proof The set $\mathbb{Z}$ of integers and the set $\mathbb{N}$ of natural numbers are countable sets, and therefore the Cartesian product $\mathbb{Z} \times \mathbb{N}$ is a countable set (Proposition 1.14). There is an obvious surjection $g\colon \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$, where $g(z, n) = z/n$ for all integers z and natural numbers n. The result therefore follows immediately on applying Corollary 1.12. ∎

Proposition 1.17 *Let $X_1, X_2, X_3, \ldots$ be a sequence of countable sets Then the union $\bigcup_{n=1}^{\infty} X_n$ of these countable sets is itself a countable set.*

Proof For each natural number n let $g_n\colon X_n \to \mathbb{N}$ be an injective function from X_n to the set $\mathbb{N}$ of natural numbers. (Such injective functions exist because each set X_n is countable.) We shall construct an injective function $h\colon X \to \mathbb{N} \times \mathbb{N}$ from X to $\mathbb{N}$, where $X = \bigcup_{n=1}^{\infty} X_n$.

Given any element x of X, let $h(x) = (n(x), g_{n(x)}(x))$, where $n(x)$ is the smallest natural number with the property that $x \in X_{n(x)}$. (Note that x belongs to at least one of the sets X_n, and therefore this natural number $n(x)$ is well-defined.)

Let x and y be elements of X satisfying $h(x) = h(y)$. We claim that $x = y$. Now if $h(x) = h(y)$ then $n(x) = n(y)$. It follows that $x \in X_n$ and $y \in X_n$, where $n = n(x) = n(y)$. Moreover $g_n(x) = g_n(y)$. But $g\colon X_n \to \mathbb{N}$ is an injective function. It follows that $x = y$. We conclude therefore that the function $h\colon X \to \mathbb{N} \times \mathbb{N}$ is injective.

Now Lemma 1.13 ensures that there exists a bijective function $f\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ from $\mathbb{N}\times\mathbb{N}$ to $\mathbb{N}$. The composition function $f\circ h\colon X \to \mathbb{N}$ is then an injective function from X to $\mathbb{N}$. We conclude therefore that the set X is countable, as required. ∎

Corollary 1.18 *Let $(X_i : i \in I)$ be a collection of countable sets, indexed by a countable set I. Then the union $\bigcup_{i\in I} X_i$ of the sets in this countable collection is a countable set.*

Proof The indexing set I is a countable set. Therefore there exists an injective function $g\colon I \to \mathbb{N}$. It follows that, for each natural number n, there exists at most one element i of the indexing set such that $g(i) = n$. If there exists some element i of I such that $g(i) = n$, let $Y_n = X_i$; otherwise let $Y_n = \emptyset$. Then $Y_1, Y_2, Y_3, \ldots$ is an infinite sequence of countable sets, and clearly $\bigcup_{i\in I} X_i = \bigcup_{n=1}^{\infty} Y_n$. It follows immediately from Proposition 1.17 $\bigcup_{i\in I} X_i$ is a countable set, as required. ∎

We define a *countable union* of sets to be a union of sets where the sets making up the collection can be indexed by some countable sets. Thus the union of a finite number of sets is a countable union of sets. Also the union of an infinite sequence $X_1, X_2, X_3, \ldots$ of sets is a countable union. The result of Corollary 1.18 may be summed up in the statement that *any countable union of countable sets is itself a countable sets.*

1.14 Uncountable Sets

A set that is not countable is said to be *uncountable.* Many sets occurring in mathematics are uncountable. These include the set of real numbers (see Proposition 1.21).

It follows directly from Lemma 1.10 that if a set X has an uncountable subset, then X must itself be uncountable.

It also follows directly from Corollary 1.12 that if $h\colon X \to Y$ is a surjection from a set X to a set Y, and if the set Y is uncountable, then the set X is uncountable.

1.15 Power Sets

Definition Let X be a set. The *power set* $\mathcal{P}(X)$ is defined to be the set of subsets of X.

Proposition 1.19 *Let X be a set. Then there does not exist any surjection from X to the power set $\mathcal{P}(X)$ of X.*

Proof Let $f\colon X \to \mathcal{P}(X)$ be any function from X to $\mathcal{P}(X)$, and let

$$Z_f = \{x \in X : x \notin f(x)\}.$$

Let $x \in X$. Then x belongs to exactly one of the sets Z_f and $f(x)$. It follows that $Z_f \neq f(x)$ for all $x \in X$. We have thus shown that any function $f\colon X \to \mathcal{P}(X)$ determines an element Z_f of $\mathcal{P}(X)$ that does not belong to the range of the function f. Thus no function $f\colon X \to \mathcal{P}(X)$ can be a surjection. ∎

Corollary 1.20 *) The power set $\mathcal{P}(\mathbb{N})$ of the set $\mathbb{N}$ of natural numbers is uncountable.*

Proof It follows from Proposition 1.11 that if the set $\mathcal{P}(\mathbb{N})$ were countable then there would exist a surjection $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$ from $\mathbb{N}$ to $\mathcal{P}$. But it follows from Proposition 1.19 that there are no surjections from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$. Therefore $\mathcal{P}(\mathbb{N})$ cannot be countable. ∎

1.16 The Cantor Set

Definition The *Cantor set* is the set consisting of all real numbers that can be expressed as the sums of infinite series of the form $\sum_{n=1}^{\infty} \frac{2a_n}{3^n}$, where, for each natural number n, either $a_n = 0$ or $a_n = 1$.

We shall show that the Cantor set is an uncountable set.

Let $\mathcal{P}(\mathbb{N})$ denote the set of all subsets of the set $\mathbb{N}$ of natural numbers, and let $f\colon \mathcal{P}(\mathbb{N}) \to \mathbb{R}$ be the function defined such that $f(I) = 2\sum_{n \in I} 3^{-n}$ for all subsets I of $\mathbb{N}$. The range of this function f is the Cantor set. We claim that the function f is injective.

Let I and J be subsets of $\mathbb{N}$, and let $a_1, a_2, a_3, \ldots$ and $b_1, b_2, b_3, \ldots$ be the infinite sequences defined such that $a_n = 1$ if $n \in I$, $a_n = 0$ if $n \notin I$, $b_n = 1$ if $n \in J$ and $b_n = 0$ if $n \notin J$. Then

$$f(I) = \sum_{n=1}^{\infty} \frac{2a_n}{3^n}, \quad f(J) = \sum_{n=1}^{\infty} \frac{2b_n}{3^n}.$$

Suppose that $I \neq J$. Let m be the smallest value of n for which $a_n \neq b_n$. Then

$$f(J) - f(I) = \frac{2(b_m - a_m)}{3^m} + \sum_{n=m+1}^{\infty} \frac{2(b_n - a_n)}{3^n}.$$

Now $|b_n - a_n| \leq 1$ for all natural numbers n, and therefore

$$\left| \sum_{n=m+1}^{\infty} \frac{2(b_n - a_n)}{3^n} \right| \leq \sum_{n=m+1}^{\infty} \frac{2|b_n - a_n|}{3^n} \leq \sum_{n=m+1}^{\infty} \frac{2}{3^n} = \frac{2}{3^{m+1}} \times \frac{1}{1 - \frac{1}{3}} = \frac{1}{3^m}.$$

It follows that

$$\left| f(J) - f(I) - \frac{2(b_m - a_m)}{3^m} \right| \leq \frac{1}{3^m},$$

where $|b_m - a_m| = 1$, and therefore

$$|f(J) - f(I)| \geq \left| \frac{2(b_m - a_m)}{3^m} \right| - \frac{1}{3^m} = \frac{1}{3^m}.$$

We conclude from this that $f(I) \neq f(J)$ when $I \neq J$. It follows from this that the function $f\colon \mathcal{P}(\mathbb{N}) \to \mathbb{R}$ is injective, and therefore defines a bijection between the set $\mathcal{P}(\mathbb{N})$ and the Cantor set. Now $\mathcal{P}(\mathbb{N})$ is uncountable (Corollary 1.20). It follows that that Cantor set is uncountable.

Proposition 1.21 *The set $\mathbb{R}$ of real numbers is uncountable.*

Proof Every subset of a countable set is countable (Lemma 1.10). The Cantor set is an uncountable set that is a subset of the set $\mathbb{R}$ of real numbers. Therefore $\mathbb{R}$ cannot be countable. ∎