Course 2BA1: Michaelmas Term 2002
Section 2: Sets and Functions

David R. Wilkins

Contents

2 Sets and Functions

2.1 Sets

A *set* is a collection of entities. (This collection may be empty.) The entities belonging to a set are referred to as *elements* of the set. If a is an element of a set A then we denote this fact by writing $a \in A$.

Two sets are said to be identical, or to be equal to one another, if and only if they have the same elements. Thus if A and B denote sets, then

$A = B$ if and only if every element of A is an element of B and every element of B is an element of A.

If we have a list of entities, we denote the set consisting of these entities by enclosing the list within braces $\{\ldots\}$. For example the set consisting of the colours red, green and blue can be denoted by $\{\text{red}, \text{green}, \text{blue}\}$.

Note that the order in which elements are specified in such a list is irrelevant. For example, the set consisting of the two people Alice and Bob may be written either as $\{\text{Alice}, \text{Bob}\}$ or as $\{\text{Bob}, \text{Alice}\}$. In other words,

$$\{\text{Alice}, \text{Bob}\} = \{\text{Bob}, \text{Alice}\}.$$

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

Example The set $\mathbb{N}$ consisting of all natural numbers is an infinite set, as is the set $\mathbb{Z}$ consisting of all integers.

One set, the *empty set*, deserves special mention. This set is denoted by $\emptyset$. It has no elements.

The elements of a given set may themselves be sets (and thus have elements of their own).

2.2 Unions, Intersections and Complements of Sets

Let A and B be sets. We define the *union* $A \cup B$ of A and B to be the set consisting of all elements that belong to A or to B (or to both). We define the *intersection* $A \cap B$ of A and B to be the set consisting of all elements that belong to both A and B. We also define $A \setminus B$ to be the set consisting of elements of A that do not belong to B. If every element of B belongs to A (so that B is a *subset* of A), then $A \setminus B$ is customarily referred to as the *complement* of B in A.

Example Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{4, 5, 6, 7, 8\}$. Then

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5, 6, 7, 8\}, \\ A \cap B &= \{4, 5\}, \\ A \setminus B &= \{1, 2, 3\}, \\ B \setminus A &= \{6, 7, 8\}. \end{aligned}$$

Example Let $\mathbb{Z}$ be the set of all integers, and let $2\mathbb{Z}$ denote the set of all even integers (i.e., all integers that are divisible by two). Then $\mathbb{Z} \setminus 2\mathbb{Z}$ is the set of all odd integers (i.e., all integers that are not divisible by two). We

see that $2\mathbb{Z} \cup (\mathbb{Z} \setminus 2\mathbb{Z}) = \mathbb{Z}$ (i.e., the set of integers is the union of the set of even integers and the set of even integers, or in other words, every integer is even or odd). Also $2\mathbb{Z} \cap (\mathbb{Z} \setminus 2\mathbb{Z}) = \emptyset$ (i.e., the intersection of the set of even integers and the set of odd integers is empty, or in other words, no integer is both even and odd).

One may also form unions and intersections of three or more sets. If A, B and C are sets, then $A \cup B \cup C$ denotes the union of the three sets A, B and C, and consists of all elements that belong either to A or to B or to C. Similarly $A \cap B \cap C$ denotes the intersection of the three sets A, B, C. An entity x is an element of the intersection $A \cap B \cap C$ if and only if it is an element of A and also of B and of C. Analogous notations are used for unions and intersections of four or more sets.

Let A, B and C be sets. One can readily verify the following identities:

$$\begin{aligned}
A \cup A &= A, \\
A \cap A &= A, \\
A \cup B &= B \cup A, \\
A \cap B &= B \cap A, \\
(A \cup B) \cup C &= A \cup (B \cup C) = A \cup B \cup C, \\
(A \cap B) \cap C &= A \cap (B \cap C) = A \cap B \cap C, \\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), \\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C), \\
(A \cap B) \cup (A \setminus B) &= A, \\
(A \cap B) \cap (A \setminus B) &= \emptyset, \\
A \cup B &= (A \cap B) \cup (A \setminus B) \cup (B \setminus A), \\
A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C), \\
A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C).
\end{aligned}$$

Example Let us verify that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ for all sets A, B and C. Now, given any sets D and E a standard and useful method for proving that they are in fact the same set is to show that every element of D belongs to E and that every element of E belongs to D. For then it follows that the sets D and E have the same elements, and therefore $D = E$.

So let A, B and C be sets, let $D = A \cap (B \cup C)$ and let $E = (A \cap B) \cup (A \cap C)$. Let x be an element of D. Then $x \in A$. Also either $x \in B$ or $x \in C$ (or both). If $x \in B$ then $x \in A \cap B$, (since we also know that $x \in A$). But every element of $A \cap B$ is an element of the union $(A \cap B) \cup (A \cap C)$, which is E. Therefore $x \in E$. Similarly if $x \in C$, then $x \in A \cap C$, and hence $x \in E$.

Thus we have seen that an element of D belongs to E in each of the two cases when $x \in B$ and when $x \in C$. We conclude that every element of D belongs to E.

Now let x be an element of E. Then either $x \in A \cap B$ or $x \in A \cap C$. In the first case $x \in B$, and in the second case $x \in C$, so that in either case $x \in B \cup C$. Moreover $x \in A$ in both cases. It follows that every element of E belongs to the intersection of A and $B \cup C$. This intersection is the set D. Thus every element of E belongs to D.

We have shown that the sets D and E have the same elements. Therefore D and E are in fact the same set, and so $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Example Let us verify that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ for all sets A, B and C. Let x be an element of $A \setminus (B \cup C)$. We must show that x belongs to the set of the right hand side of the above equality. Now $x \in A \setminus (B \cup C)$, and therefore x belongs to A but does not belong to $B \cup C$. In particular, x does not belong to B, nor to C. It follows that $x \in A \setminus B$, and also $x \in A \setminus C$. But then $x \in (A \setminus B) \cap (A \setminus C)$. We have thus shown that every element of $A \setminus (B \cup C)$ is an element of $(A \setminus B) \cap (A \setminus C)$.

Now let x be any element of $(A \setminus B) \cap (A \setminus C)$. Then $x \in (A \setminus B)$ and $x \in (A \setminus C)$. The element therefore cannot belong to B. Nor can it belong to C. But $x \in A$. We conclude therefore that x is an element of A that does not belong to $B \cup C$. (Every element of $B \cup C$ must belong either to B or to C.) Thus any element x of $(A \setminus B) \cap (A \setminus C)$ belongs to $A \setminus (B \cup C)$. We conclude that the sets $A \setminus (B \cup C)$ and $(A \setminus B) \cap (A \setminus C)$ are in fact the same set, since we have shown that an element of either is an element of the other. Thus $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

2.3 Subsets and Power Sets

Definition Let A and B be sets. We say that the set B is a *subset* of A if every element of B is an element of A. If B is a subset of A then we denote this fact by writing either $B \subset A$ or $A \supset B$.

The empty set $\emptyset$ is a subset of every set. Morover any set is a subset of itself (i.e., $A \subset A$ for any set A). Thus a non-empty set A always has at least two subsets, namely $\emptyset$ and A itself.

Let A and B be sets. If $A \subset B$ and $B \subset A$ then $A = B$. For if $A \subset B$ and $B \subset A$ then every element of A is an element of B, and also every element of B is an element of A. But then the sets A and B have the same elements, and therefore these sets are in fact the same set.

Definition Let A be a set. The *power set* $\mathcal{P}A$ is the set whose elements are the subsets of A.

Example Let A be a set consisting of exactly one element a, so that $A = \{a\}$. Then the subsets of A are the empty set $\emptyset$ and A itself. It follows that the power set $\mathcal{P}A$ of A is given by $\mathcal{P}A = \{\emptyset, A\}$ in this case. Note that the set A has 1 element and that its power set $\mathcal{P}A$ has 2 elements.

Example Let $A = \{1, 2\}$. Then $\mathcal{P}A = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Note that the set A has 2 elements and that its power set $\mathcal{P}A$ has 4 elements.

Example Let A be the set consisting of the three colours red, green and blue. Let us for convenience denote these colours by R, G and B. Thus $A = \{\mathrm{R}, \mathrm{G}, \mathrm{B}\}$. Going systematically through the subsets of A with 0, 1, 2, and 3 elements, we see that the power set of A is given by the following:

$$\mathcal{P}A = \{\emptyset, \{\mathrm{R}\}, \{\mathrm{G}\}, \{\mathrm{B}\}, \{\mathrm{G}, \mathrm{B}\}, \{\mathrm{B}, \mathrm{R}\}, \{\mathrm{R}, \mathrm{G}\}, \{\mathrm{R}, \mathrm{G}, \mathrm{B}\}\}\,.$$

Note that the set A has 3 elements and its power set $\mathcal{P}A$ has 8 elements.

Example Let A be a set consisting of the four elements a, b, c and d. Then the power set $\mathcal{P}A$ of A consists of the following subsets of A: the empty set $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{d\}$, $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$, $\{c, d\}$, $\{b, c, d\}$, $\{a, c, d\}$, $\{a, b, d\}$, $\{a, b, c\}$ and $\{a, b, c, d\}$. Thus the set A has one subset with no elements, four subsets with exactly one element, six subsets with exactly two elements, four subsets with exactly three elements, and one subset with exactly four elements. Note that the set A has 4 elements and its power set $\mathcal{P}A$ has 16 elements.

The pattern emerging from the above examples would lead one to conjecture the following theorem on the number of elements in the power set of a finite set, which we now proceed to state and prove.

Theorem 2.1 *If a finite set A has exactly n elements, then its power set $\mathcal{P}A$ has exactly 2^n elements.*

Proof Let A be a set with n elements, where $n > 0$. Choose an element a of A, and let B be the subset of A consisting of all elements of A apart from a (i.e., B is the complement $A \setminus \{a\}$ of $\{a\}$ in A). The set B has $n - 1$ elements. Now for each subset C of B there exist exactly two subsets of A whose intersection with B is the set C; these subsets are C itself and $C \cup \{a\}$ (i.e., the subset of A obtained by adjoining the element a to C). It follows that the set A has twice as many subsets as the set B.

If A has just one element then its power set $\mathcal{P}A$ has two elements. Indeed if $A = \{a\}$ then $\mathcal{P}A = \{\emptyset, A\}$.

An easy application of the Principle of Mathematical Induction proves that a if finite set has n elements then its power set has 2^n elements. Indeed this result holds for all sets with just one element, and if, for any natural number m, the result holds for all sets with m elements, then it also holds for all sets with $m+1$ elements, since we have already seen that the addition of an element to a set doubles the number of subsets which it contains. ∎

2.4 The Specification of Sets

We come now to consider a standard method for specifying sets in terms of the properties satisfied by their elements.

Suppose we wish to specify the subset of a given set A consisting of all elements of A that satisfy a given condition. Such a set is specified by the following:

$$\{a \in A : \textit{condition}\}$$

where '*condition*' is to be replaced in the above by the specific condition that an element a of the set A has to satisfy in order to belong to the subset being specified, as in the following examples.

Example Suppose we wish to specify the set consisting of all natural numbers greater than 7. This set can be specified as

$$\{n \in \mathbb{N} : n > 7\}.$$

Here $\mathbb{N}$ denotes the set of natural numbers. Note that this set can also be specified as

$$\{n \in \mathbb{Z} : n > 7\},$$

where $\mathbb{Z}$ denotes the set of integers (i.e., whole numbers). (Integers may be positive, negative or zero, but those integers n which also satisfy the condition $n > 7$ are positive, and are therefore natural numbers.)

Example The set of real numbers is denoted by $\mathbb{R}$. Therefore the set of real numbers whose squares are greater than 7 may be denoted by

$$\{x \in \mathbb{R} : x^2 > 7\}.$$

Example What is $\{x \in \mathbb{R} : x^2 < -7\}$?

Now the square of a real number x is always non-negative, whether x be positive, negative or zero. Therefore there are no real numbers x satisfying $x^2 < -7$. We conclude that $\{x \in \mathbb{R} : x^2 < -7\}$ is simply a somewhat complicated way of specifying the empty set $\emptyset$.

Example How many elements are there in the set $\{x \in \mathbb{R} : x^2 = 1\}$?

In other words, how many real numbers are there whose squares are equal to 1. There are exactly two, namely $+1$ and -1. Thus $\{x \in \mathbb{R} : x^2 = 1\} = \{-1, 1\}$. This set has two elements.

Example The set of real numbers that are less than -7 or greater than 4 may be denoted by

$$\{x \in \mathbb{R} : x < -7 \text{ or } x > 4\}$$

Example Note that $\{x \in \mathbb{R} : x < -7 \text{ and } x > 4\}$ is simply another somewhat complicated way of specifying the empty set.

Definition Let a and b be real numbers with $a \leq b$. We define

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}, \quad (a, b) = \{x \in \mathbb{R} : a < x < b\},$$

$$[a, b) = \{x \in \mathbb{R} : a \leq x < b\}, \quad (a, b] = \{x \in \mathbb{R} : a < x \leq b\}.$$

Thus $[a, b]$ denotes the set consisting of all real numbers x that satisfy $a \leq x \leq b$, and the other sets are defined similarly. (Note that if $a = b$ then (a, b), $[a, b)$ and $(a, b]$ are all the empty set, and $[a, b]$ is the set $\{a\}$ consisting of the single element a.)

2.5 Binary Relations

A *binary* relation on a set specifies relations between pairs of elements from the set.

Example The relations $=$ ('equals'), $\neq$ ('not equal to'), $<$ ('less than'), $>$ ('greater than'), $\leq$ ('less than or equal to') and $\geq$ ('greater than or equal to') are all binary relations on the set $\mathbb{R}$ of real numbers.

Example Let A be a set, and let $\mathcal{P}A$ be the power set of A (i.e., the set whose elements are the subsets of A). Then $\subset$ is a binary relation on $\mathcal{P}A$, where two subsets B and C of A satisfy $B \subset C$ if and only if B is a subset of C.

If one has a relation R on a set A, then, given two elements x and y of A, either x is related to y, in which case we may write xRy, or else the element is not related to y.

Definition Let R be a relation on a set A.

The relation R is said to be *reflexive* when it has the following property: xRx for all elements x of the set A.

The relation R is said to be *symmetric* when it has the following property: if x and y are elements of the set A, and if xRy, then yRx.

The relation R is said to be *transitive* when it has the following property: if x, y and z are elements of the set A, and if xRy and yRz, then xRz.

An *equivalence relation* is a relation that is reflexive, symmetric and transitive.

Example The relation $<$ ('less than') on the set $\mathbb{R}$ of real numbers is neither reflexive nor symmetric, but it is transitive. Indeed there is no real number x satisfying $x < x$. Moreover there are no pairs of real numbers x and y satisfying both $x < y$ and $y < x$. However, if x, y and z are real numbers, and if $x < y$ and $y < z$, then $x < z$, and therefore the relation $<$ on $\mathbb{R}$ is transitive.

Example Let A be a non-empty set, and let $\mathcal{P}A$ be the power set of A. The relation $\subset$ on $\mathcal{P}A$ is reflexive and transitive, but is not symmetric. Indeed every subset of A is a subset of itself and therefore $B \subset B$ for all $B \in \mathcal{P}A$, showing that the relation $\subset$ on $\mathcal{P}A$ is reflexive. If B, C and D are subsets of A, and if $B \subset C$ and $C \subset D$, then $B \subset D$ (for if every element of B is an element of C and if every element of C is an element of D then clearly every element of B is an element of D), and therefore the relation $\subset$ on $\mathcal{P}A$ is transitive. It is not the case however that $B \subset C$ always implies that $C \subset B$. Indeed subsets B and C of A satisfy both $B \subset C$ and $C \subset B$ if and only if $B = C$. Thus the relation $\subset$ on $\mathcal{P}A$ is not symmetric.

Example The relation $=$ ('equals') on the set $\mathbb{R}$ of real numbers is an equivalence relation. However none of the relations $\neq$ ('not equal to'), $<$ ('less than'), $>$ ('greater than'), $\leq$ ('less than or equal to') or $\geq$ ('greater than or equal to') are equivalence relations on $\mathbb{R}$.

2.6 Congruences

Let m be a positive integer. We say that two integers x and y are *congruent modulo* m if $x - y$ is divisible by m. If x and y are congruent modulo m, then we denote this fact by writing

$$x \equiv y \pmod{m}.$$

Lemma 2.2 *Let m be a positive integer, and let x, y and z be integers. Then the following results hold:*

(i) $x \equiv x \pmod{m}$;

(ii) *if* $x \equiv y \pmod{m}$ *then* $y \equiv x \pmod{m}$;

(iii) *if* $x \equiv y \pmod{m}$ *and* $y \equiv z \pmod{m}$ *then* $x \equiv z \pmod{m}$.

The relation of congruence modulo m is thus reflexive, symmetric and transitive, and is therefore an equivalence relation on the set $\mathbb{Z}$ of integers.

Proof Clearly $x \equiv x \pmod{m}$ for any integer x, since $x - x = 0$, and 0 is divisible by any non-zero integer.

If $x \equiv y \pmod{m}$ then $x - y$ is divisible by m. But then $y - x$ is also divisible by m, and hence $y \equiv x \pmod{m}$.

If $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$ then both $x - y$ and $y - z$ are divisible by m. But $x - z = (x - y) + (y - z)$ and the sum of two integers divisible by m is itself an integer divisible by m. Therefore $x - z$ is divisible by m, and hence $x \equiv z \pmod{m}$. ∎

Congruences play an important role in the study of the theory of numbers, and in applications of that theory to practical problems in areas such as cryptography.

One well known theorem, due to Pierre de Fermat, states that if p is any prime number then $x^p \equiv x \pmod{p}$ for all integers x. This result is sometimes referred to as *Fermat's Little Theorem*. This property of prime numbers is not shared by all natural numbers. For example $2^6 = 64$ and $64 \equiv 4 \pmod{6}$. But the numbers 2 and 4 are not congruent modulo 6 (since $4 - 2$ is not divisible by 6). Therefore the congruence $x^6 \equiv x \pmod{6}$ does not hold when $x = 2$.

2.7 Partitions and Equivalence Relations

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

Example Let $\mathbb{Z}$ be the set of integers, let O be the set of odd integers, and let E be the set of even integers. Every integer is either even or odd, and no integer is both even and odd. Therefore any integer belongs to exactly one of the sets O and E. Thus the collection consisting of the sets O and E is a partition of the set $\mathbb{Z}$ of integers.

There is a close connection between partitions and equivalence relations. We recall that an equivalence relation $\sim$ on a set A is a binary relation on A with the following properties:

(i) $x \sim x$ for all elements x of A (i.e., $\sim$ is *reflexive*);

(ii) if x and y are elements of A and if $x \sim y$ then $y \sim x$ (i.e., $\sim$ is *symmetric*);

(iii) if x, y and z are elements of A, and if $x \sim y$ and $y \sim z$ then $x \sim z$ (i.e., $\sim$ is *transitive*).

Definition Let $\sim$ be an equivalence relation on a set A, and let x be an element of A. The *equivalence class* $[x]$ of the element x is the subset of A defined as follows:

$$[x] = \{a \in A : a \sim x\}.$$

Example Let m be a positive integer. There is then an equivalence relation on the set $\mathbb{Z}$, where two elements x and y are related if and only if $x - y$ is divisible by m. (In other words, integers x and y are related if and only if $x \equiv y \pmod{m}$.) The equivalence class $[n]_m$ of an integer n thus consists of all integers x that are congruent to n modulo m. This equivalence class is referred to as the *congruence class* of n modulo m. An integer x belongs to the congruence class $[n]_m$ of n modulo m if and only if $x - n$ is divisible by m.

Now, given any integer x, exactly one of the integers

$$x, x-1, x-2, \ldots, x-m+1$$

between $x - m + 1$ and x is divisible by m. It follows that the integer x belongs to exactly one of the congruence classes $[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m$. These congruence classes modulo m therefore constitute a partition of the set $\mathbb{Z}$ of integers.

Theorem 2.3 *Let $\sim$ be an equivalence relation on a set A. Then every element of A belongs to exactly one equivalence class. Thus the collection of equivalence classes is a partition of the set A.*

Proof Let x be an element of A. Then $x \sim x$ (since the relation $\sim$ is reflexive), and therefore $x \in [x]$. Thus every element x of A belongs to its own equivalence class $[x]$. We see from this that each element of A belongs to at least one equivalence class.

To complete the proof we must show that each element of A belongs to at most one equivalence class. Let x and y be elements of A. We shall show that if the equivalence classes $[x]$ and $[y]$ have at least one element in common then $[x] = [y]$.

Suppose then that there exists an element z of A that belongs to both $[x]$ and $[y]$. Then $z \sim x$ and $z \sim y$. But then $x \sim z$ (since the relation $\sim$ is symmetric), and hence $x \sim y$ (since $x \sim z$, $z \sim y$, and the relation $\sim$ is transitive). Moreover $y \sim x$, since the relation $\sim$ is symmetric. If a is an element of A and if $a \in [x]$ then $a \sim x$ and $x \sim y$, and therefore $a \in [y]$. Similarly if $a \in [y]$ then $a \sim y$ and $y \sim x$, and therefore $a \in [x]$. Thus every element of $[x]$ is an element of $[y]$, and every element of $[y]$ is an element of $[x]$. It follows that $[x] = [y]$.

We have proved that if equivalence classes $[x]$ and $[y]$ have at least one element in common then they coincide (i.e., they are in fact the same equivalence class). It follows that an element of A cannot belong to more than one equivalence class.

We have proved that every element of A belongs to exactly one equivalence class, since an element of A belongs to at least one equivalence class but cannot belong to more than one equivalence class. Thus the collection of equivalence classes is a partition of the set. ∎

Remark We have seen how every equivalence relation on a set gives rise to a partition of that set. On the other hand, any partition of the set gives rise to an equivalence relation on that set: two elements of the set are related if and only if they belong to the same subset in the partition. It follows that equivalence relations and partitions correspond to one another: to each equivalence relation on a set there is a corresponding partition of the set, and vice versa.

2.8 Partial Orders and Lattices

Definition Let A be a set. A binary relation R on A is said to be *anti-symmetric* if it has the following property:

if x and y are elements of A, and if xRy and yRx, then $x = y$.

Definition A *partial order* on a set is a relation on that set which is reflexive, transitive and anti-symmetric.

Let $\preceq$ denote a relation on a set A. We see that this relation is a partial order on the set A if and only if it has the following three properties:

(i) $x \preceq x$ for all elements x of A;

(ii) if x, y, and z are elements of A, and if $x \preceq y$ and $y \preceq z$, then $x \preceq z$;

(iii) if x and y are elements of A, and if $x \preceq y$ and $y \preceq x$, then $x = y$.

Example The relation $\leq$ ('less than or equal to') is a partial order on the set $\mathbb{R}$ of real numbers. (It clearly possesses all three properties listed above.) It is also a partial order when considered as a relation on the set $\mathbb{Z}$ of integers, or on the set $\mathbb{N}$ of natural numbers.

Example Let A be a set. The relation $\subset$ is a partial order on the power set $\mathcal{P}A$ of A, where subsets B and C satisfy $B \subset C$ if and only if B is a subset of C (i.e., if and only if every element of B belongs also to C).

Definition A *partially ordered set* (or *poset*) $(A, \preceq)$ consists of a set A, which is provided with a partial order $\preceq$ defined on the set.

Let $(A, \preceq)$ be a partially ordered set, and let B be a subset of A. An element l of A is said to be a *lower bound* of B if $l \preceq b$ for all elements b of B. An element l of A is said to be the *greatest lower bound* of B if l is a lower bound of B and if $l' \preceq l$ for all lower bounds l' of B. If such a greatest lower bound exists, we shall denote it by $\operatorname{glb} B$.

It is worth noting that a subset B of A can have at most one greatest lower bound. For if l and l' denote elements of A (not necessarily distinct), and if l and l' are greatest lower bounds of B then $l' \preceq l$ and $l \preceq l'$ and therefore $l = l'$ (since the relation $\preceq$ on A is anti-symmetric).

We can define in a similar fashion the notion of a *least upper bound* of a subset of A. An element u of A is said to be an *upper bound* of a subset B of A if $b \preceq u$ for all elements b of B. An element u of A is said to be the *least upper bound* of B if u is an upper bound of B and if $u \preceq u'$ for all upper bounds u' of B. A subset B of A can have at most one least upper bound. If such a least upper bound exists, we shall denote it by $\operatorname{lub} B$.

Example Consider the partially ordered set $(\mathbb{R}, \leq)$. Any finite subset B of $\mathbb{R}$ has both a greatest lower bound and a least upper bound. The greatest lower bound of B in this case is the smallest real number belonging to B, and the least upper bound is the largest real number belonging to B.

Example Let A be a set, and let $\mathcal{P}A$ be the power set of A (i.e., the set whose elements are the subsets of A). Then $(\mathcal{P}A, \subset)$ is a partially ordered set (i.e., the relation $\subset$ is a partial order on the power set $\mathcal{P}A$ of A). Given subsets B and C of A one can readily verify that

$$\operatorname{glb}\{B, C\} = B \cap C, \quad \operatorname{lub}\{B, C\} = B \cup C.$$

Indeed $B \cap C \subset B$ and $B \cap C \subset C$, and therefore $B \cap C$ is a lower bound of $\{B, C\}$. Moreover if D is any subset of A that is a lower bound of $\{B, C\}$

then $D \subset B$ and $D \subset C$, hence the elements of D must belong to both B and C, hence $D \subset B \cap C$. This shows that $\mathrm{glb}\{B, C\} = B \cap C$. A similar argument shows that $\mathrm{lub}\{B, C\} = B \cup C$.

Example Let $(\mathbb{N}, \leq)$ be the partially ordered set (poset) consisting of the set $\mathbb{N}$ of natural numbers, together with the usual partial order $\leq$. Let B be the subset of $\mathbb{N}$ consisting of all the even natural numbers (i.e., $B = \{2, 4, 6, 8, \ldots\}$). The set B has a greatest lower bound. Indeed $\mathrm{glb}\, B = 2$. But the set B has no least upper bound. Indeed the set has no upper bound: no natural number has the property that it is greater than or equal to all even natural numbers.

Definition A partially ordered set $(A, \preceq)$ is said to be a *lattice* if, given any two elements x and y of the set A, there exists an element $\mathrm{glb}\{x, y\}$ of A that is the greatest lower bound of the set $\{x, y\}$ and an element $\mathrm{lub}\{x, y\}$ that is the least upper bound of the set $\{x, y\}$.

Example $(\mathbb{R}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{N}, \leq)$ are lattices (where two numbers x and y satisfy $x \leq y$ if and only if x is less than or equal to y).

Example Let A be a set, and let $\mathcal{P}A$ denote the power set of A. Then $(\mathcal{P}A, \subset)$ is a lattice. Indeed, if B and C are elements of $\mathcal{P}A$ then they are subsets of A. Moreover we have already seen that

$$\mathrm{glb}\{B, C\} = B \cap C, \quad \mathrm{lub}\{B, C\} = B \cup C,$$

and $B \cap C$ and $B \cup C$ are elements of $\mathcal{P}$ (since they are obviously subsets of A). It follows that contains the greatest lower bound and least upper bound of the set $\{B, C\}$ for all elements B and C of $\mathcal{P}A$ (i.e., for all subsets B and C of A).

2.9 Cartesian Products of Sets

Let A and B be sets. The *Cartesian product* $A \times B$ of the sets A and B is defined to be the set of all *ordered pairs* (a, b) with $a \in A$ and $b \in B$.

Such an ordered pair (a, b) is comprised of two elements a and b, where the first element a is taken from the set A, and the second element b is taken from the set B. If (a_1, b_1) and (a_2, b_2) are ordered pairs of this type then $(a_1, b_1) = (a_2, b_2)$ if and only if $a_1 = a_2$ and $b_1 = b_2$.

Example Points of the plane are specified in Cartesian coordinates by means of ordered pairs (x, y), where x and y are real numbers. The set of such ordered pairs is the set $\mathbb{R} \times \mathbb{R}$ (the Cartesian product of two copies of the set $\mathbb{R}$ of real numbers).

Example Let $A = \{1, 2, 3\}$ and $B = \{1, 2\}$. Then

$$A \times B = \{(1, 1), (2, 1), (3, 1), (1, 2), (2, 2), (3, 2)\}.$$

Note that, in this example, the number of elements of the set $A \times B$ (i.e., 6) is the product of the number of elements of A (i.e., 3) and the number of elements of B (i.e., 2).

Suppose that A and B are finite sets. Let m and n be the number of elements in A and B respectively. Then the number of elements of the Cartesian product $A \times B$ is mn. Indeed an element of $A \times B$ is an ordered pair (a, b) with $a \in A$ and $b \in B$. There are m ways to choose the element a from A, and, for each such choice, there are n ways to choose the element b from B.

One may form the Cartesian product of any number of sets. Suppose that $A_1, A_2, \ldots A_n$ are sets. The *Cartesian product* of these sets is the set $A_1 \times A_2 \times \cdots \times A_n$ consisting of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ with $a_i \in A_i$ for $i = 1, 2, \ldots, n$.

Example Points of three dimensional space are specified in Cartesian co-ordinates by means of ordered triples (x, y, z), where x, y and z are real numbers. The set of such ordered triples is the set $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

Let $A_1, A_2, \ldots, A_n$ be sets, and let $(c_1, c_2, \ldots, c_n)$ and $(d_1, d_2, \ldots, d_n)$ be elements of the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ of these sets. Then $(c_1, c_2, \ldots, c_n) = (d_1, d_2, \ldots, d_n)$ if and only if $c_i = d_i$ for $i = 1, 2, \ldots, n$ (i.e., if and only if $c_1 = d_1$, $c_2 = d_2$, etc.).

A Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ of finite sets $A_1, A_2, \ldots, A_n$ is itself a finite set: the number of elements of the Cartesian product is equal the product of the number of elements of the individual sets $A_1, A_2, \ldots, A_n$.

Example If the sets A, B and C have 3, 5 and 7 elements respectively then their Cartesian product has 105 elements, since $105 = 3 \times 5 \times 7$.

Example Suppose that one to construct a database containing information on students taking a course such as 2BA1. Each record in the database is to specify the student number, the name, and the degree programme being followed by the student. Let I be the set consisting of all strings of eight decimal digits, let N be a set containing all the student names, and let D be the set of all degree programmes taught at Trinity College Dublin. Then a record in the database determines an element of the set $I \times N \times D$, such as

$$(63009987, \text{Síle Ní Shé}, \text{CSLL German}).$$

The collection of all such records contained in the database can be viewed as a subset of the Cartesian product $I \times N \times D$ of the set I, N and D. The language of sets and Cartesian products is used in discussions of *relational databases*.

A subset of the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ of sets $A_1, A_2, \ldots, A_n$ is sometimes referred to as an *n-ary relation* on the sets $A_1, A_2, \ldots, A_n$.

2.10 Functions between Sets

Definition Let A and B be sets. A *function* $f: A \to B$ from A to B assigns to each element a of A an element $f(a)$ of B. The set A on which the function is defined is referred to as the *domain* of the function $f: A \to B$. The set B into which the domain is mapped by f is referred to as the *codomain* of the function f.

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

Example There is a function $r: \mathbb{R} \setminus \{0\} \to \mathbb{R}$, where $r(x) = 1/x$ for all non-zero real numbers x. The domain of this function is the set $\mathbb{R} \setminus \{0\}$ of all non-zero real numbers (i.e., the set $\{x \in \mathbb{R} : x \neq 0\}$). The domain of this function cannot be extended to the entire set $\mathbb{R}$ of real numbers since the reciprocal of zero is not defined. According the above definition the value of a function must be defined at all elements of its domain.

Example Let A be the set of letters in the English alphabet (including both upper-case and lower-case letters). Then there is a function $f: A \to \mathbb{N}$ which sends each letter to its ASCII code. Then, for example, $f(\mathbf{A}) = 65$, $f(\mathbf{B}) = 66$, $f(\mathbf{a}) = 97$ and $f(\mathbf{b}) = 98$.

Given any set A, there is a function $1_A: A \to A$ from the set A to itself which sends each element a of A to itself. This function is referred to as the *identity function* on A.

Definition Let A and B be sets, and let $f: A \to B$ be a function from A to B. The *range* of the function f is the subset $f(A)$ of B defined by

$$f(A) = \{b \in B : b = f(a) \text{ for some } a \in A\}.$$

In other words, the *range* of a function is the set consisting of all elements of the codomain of the function that are images under the function of elements of its domain.

Definition Let A be a set. A *Boolean function* on A is a function $f: A \to \{T, F\}$ whose domain is A and whose codomain is the set $\{T, F\}$ whose elements are the *truth values* $T = \text{true}$ and $F = \text{false}$.

2.11 Compositions of Functions

Let A, B and C be sets, let $f: A \to B$ be a function A to B, let $g: B \to C$ be a function from B to C. Then there is a function $g \circ f: A \to C$ obtained by composing the functions f and g. This function is defined at each element a of A by the formula $(g \circ f)(a) = g(f(a))$. (In other words, in order to apply the composition function $g \circ f$ to an element a of A, we first apply the function f to the element a, and then we apply the function g to the resulting element $f(a)$ of B to obtain an element $g(f(a))$ of C.

Example Let $\mathbb{R}$ denote the set of real numbers, and let $f: \mathbb{R} \to \mathbb{R}$ and $g: \mathbb{R} \to \mathbb{R}$ be the functions defined by $f(x) = (x + 1)^2$ and $g(x) = \sin x$ for all real numbers x. Then $g \circ f = h$ where $h: \mathbb{R} \to \mathbb{R}$ is the function defined by $h(x) = \sin(x + 1)^2$ for all real numbers x. Also $f \circ g = k$, where $k: \mathbb{R} \to \mathbb{R}$ is the function defined by $k(x) = (\sin x + 1)^2$ for all real numbers x.

Remark Note that '$g \circ f$' denotes the composition function 'f followed by g'. The functions are specified in this order (which may at first seem odd) in order that $(g \circ f)(a) = g(f(a))$ for all elements a of the domain A of the function f.

2.12 The Graph of a Function

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

$$\Gamma(f) = \{(a, b) \in A \times B : b = f(a)\}.$$

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

Remark In some books, including many textbooks on discrete mathematics written for students of computer science, a function from a set A to a set B is formally defined as a subset of the Cartesian product $A \times B$ with the property that for each element a of A there exists exactly one element b of B for which the ordered pair (a, b) belongs to the given subset. In essence, in this approach, functions are being identified with their graphs.

2.13 The Inverse of a Function

Definition Let A and B be sets, and let $f: A \to B$ be a function from A to B. A function $g: B \to A$ from B to A is said to be the *inverse* of the function f if $g(f(a)) = a$ for all elements a of A and $f(g(b)) = b$ for all elements b of B. If there exists a function $g: B \to A$ that is the inverse of $f: A \to B$, then the function f is said to be *invertible* and the inverse of a function $f: A \to B$ is denoted by $f^{-1}: B \to A$.

Example Let $\mathbb{R}^+$ denote the set of all non-negative real numbers, and let $q: \mathbb{R}^+ \to \mathbb{R}^+$ denote the function defined by $q(x) = x^2$ for each non-negative real number x. This function is invertible, and its inverse $q^{-1}: \mathbb{R}^+ \to \mathbb{R}^+$ is given by $q^{-1}(x) = \sqrt{x}$, where, for each non-negative real number x, $\sqrt{x}$ denotes the unique non-negative real number that is a square root of x.

Example Let A be the set of letters in the English alphabet (including both upper-case and lower-case letters), and let

$$I = \{n \in \mathbb{N} : 65 \leq n \leq 90 \text{ or } 97 \leq n \leq 122\}.$$

There is then a function $f: A \to I$ that sends each letter of the alphabet to its ASCII code. The inverse function $f^{-1}: I \to A$ sends each natural number within the specified ranges to the letter of the English alphabet which it represents. Thus, for example, $f^{-1}(65) = \mathbf{A}$, $f^{-1}(66) = \mathbf{B}$, $f^{-1}(90) = \mathbf{Z}$, $f^{-1}(97) = \mathbf{a}$, $f^{-1}(98) = \mathbf{b}$ and $f^{-1}(122) = \mathbf{z}$.

2.14 Injective, Surjective and Bijective Functions

Many functions are not invertible. The following example illustrates some of the reasons why certain functions may not be invertible.

Example Let W be the set of all English words occurring as headwords in some specified dictionary, let $\mathbb{N}$ denote the set of natural numbers and let $\lambda: W \to \mathbb{N}$ denote the function that sends each word to its length. (Thus, for example, $\lambda(\textbf{to}) = 2$ and $\lambda(\textbf{indecipherable}) = 14$.) This function $\lambda: W \to \mathbb{N}$ is not invertible.

One feature of this function which results in its not being invertible is the fact that there are natural numbers that are the image of more than one word. For example

$$\lambda(\textbf{to}) = \lambda(\textbf{by}) = \lambda(\textbf{at}) = 2.$$

$$\lambda(\textbf{physical}) = \lambda(\textbf{computer}) = 8.$$

If one were to seek to define function $\mu: \mathbb{N} \to W$ that was the inverse of $\lambda: W \to \mathbb{N}$ then one would run into problems in seeking to define values such as $\mu(2)$ and $\mu(8)$. Indeed if such an inverse function $\mu: \mathbb{N} \to W$ were to exist, then it would have to satisfy $\mu(\lambda(\alpha)) = \alpha$ for all words α in the dictionary. In particular we would have $\mu(\lambda(\textbf{physical})) = \textbf{physical}$ and $\mu(\lambda(\textbf{computer})) = \textbf{computer}$. But $\mu(\lambda(\textbf{physical})) = \mu(8)$, and $\mu(\lambda(\textbf{computer})) = \mu(8)$, and therefore the inverse function $\mu: \mathbb{N} \to W$ would also have to satisfy $\mu(\lambda(\textbf{physical})) = \mu(\lambda(\textbf{computer}))$, and therefore the words '**physical**' and '**computer**' would have to be identical, which is clearly not the case. This demonstrates the impossibility of finding an inverse function to λ.

Another type of problem can also arise in seeking to define an inverse $\mu: \mathbb{N} \to W$ to the function $\lambda: W \to \mathbb{N}$. How do we define $\mu(1000)$? Now the inverse function μ would have to satisfy $\lambda(\mu(n)) = n$ for all natural numbers, and in particular would have to satisfy $\lambda(\mu(1000)) = 1000$. Therefore $\mu(1000)$ would have to be a headword in the specified dictionary with 1000 letters! We take it for granted that no such headword exists.

Definition Let A and B be sets, and let $f: A \to B$ be a function from A to B. We say that the function f is *injective* if $f(x) \neq f(y)$ for all elements x and y of A with $x \neq y$. We say that the function f is *surjective* if, given any element b of B, there exists some element a of A such that $f(a) = b$. We say that the function f is *bijective* if it both injective and surjective.

Thus a function is injective if and only if distinct elements of its domain get mapped to distinct elements of its codomain. A function is surjective if every element of the codomain is the image of some element of the domain.

Example Let $\mathbb{R}^+$ denote the set of non-negative real numbers, and let $q\colon \mathbb{R}^+ \to \mathbb{R}^+$ be the function given by $q(x) = x^2$ for all non-negative real numbers x. Let x and y be non-negative real numbers. If $x < y$ then $x^2 < y^2$. If $x > y$ then $x^2 > y^2$. But if $x \neq y$ then either $x < y$ or $x > y$. It follows that if $x \neq y$ then $x^2 \neq y^2$. The function $q\colon \mathbb{R}^+ \to \mathbb{R}^+$ is therefore injective. Also, given any non-negative real number x, there exists a non-negative real number $\sqrt{x}$ whose square is equal to x. It follows that the function $q\colon \mathbb{R}^+ \to \mathbb{R}^+$ is both injective and surjective. It is therefore bijective. This function also has an inverse $q^{-1}\colon \mathbb{R}^+ \to \mathbb{R}^+$, where $q^{-1}(x) = \sqrt{x}$ for all non-negative real numbers x.

Example Let $s\colon \mathbb{R} \to \mathbb{R}$ by the function given by $s(x) = x^2$ for all real numbers x. This function is not injective. For example, -2 and 2 are distinct elements of $\mathbb{R}$, but $s(-2) = 4 = s(2)$. Moreover the function is not surjective, since any negative real number such as -4 is not in the range of the function. This function $s\colon \mathbb{R} \to \mathbb{R}$ is neither injective nor surjective. Moreover one can easily satisfy oneself that it does not have an inverse. (Such an inverse, were it to exist, would have to be defined for *all* real numbers, not merely the non-negative ones.)

Remark Note that the expressions defining the values $q(x)$ and $s(x)$ of the functions of the previous two examples are the same, but these two functions have different domains and different codomains, and are therefore regarded as being different functions. In determining whether or not functions are injective or surjective, it is crucial to take into account the domain and codomain given in the specification of the function.

One can readily verify that the composition of two injections is itself an injection, and that the composition of two surjections is itself a surjection. It follows directly that the composition of two bijections is a bijection.

Theorem 2.4 *A function $f\colon A \to B$ is invertible if and only if it is both injective and surjective.*

Proof First we show that an invertible function must be both injective and surjective. Suppose that the function $f\colon A \to B$ has an inverse $g\colon B \to A$. Then $g(f(a)) = a$ for all elements a of the domain A, and $f(g(b)) = b$ for all elements b of the codomain B. Let x and y be elements of A. If $f(x) = f(y)$ then $x = g(f(x)) = g(f(y)) = y$. Thus $f(x)$ and $f(y)$ cannot be equal unless $x = y$. It follows that if $x \neq y$ then $f(x) \neq f(y)$. We see therefore that an invertible function must be injective.

An invertible function must also be surjective. For if $g: B \to A$ is an inverse of $f: A \to B$ then $f(g(b)) = b$ for all elements b of the codomain B, and thus there exists at least one element of the domain, namely $g(b)$, which is mapped by f to the element b.

We have now shown that an invertible function must be both injective and surjective. It remains to show that a function that is both injective and surjective is invertible.

Let $f: A \to B$ be a function that is both injective and surjective. Let b be an element of the set B. There exists at least one element x of A satisfying $f(x) = b$, since the function f is surjective. If y is an element of A and if $y \neq x$, then $f(y) \neq f(x)$, because the function f is injective, and therefore $f(y) \neq b$. We conclude that, for each element b of B, there exists exactly one element x of the set A satisfying $f(x) = b$; let us denote this element by $g(b)$. We obtain in this way a function $g: B \to A$ such that, for each element b of B, $g(b)$ is the unique element x of A satisfying $f(x) = b$.

Clearly $f(g(b)) = b$ for all elements b of B. In order to prove that the function $g: B \to A$ is the inverse of $f: A \to B$, we must also prove that $g(f(a)) = a$ for all elements a of A. Let a be an element of the set A. Now $f(g(b)) = b$ for all elements b of B; letting $b = f(a)$, we see that $f(g(f(a))) = f(a)$. But then $g(f(a))$ and a are both elements of A that are mapped by f to the element $f(a)$ of B. It follows that $g(f(a)) = a$, since the function f is injective. We have thus shown that $g(f(a)) = a$ for any element a of the domain A of the function f. We conclude that the function $g: B \to A$ is indeed the inverse of $f: A \to B$, and thus the function f is invertible, as required. ∎

The above theorem shows that a function between sets is invertible if and only if it is a bijection.

Example Let $q: [-3, 1] \to [0, 9]$ be the function defined by $q(x) = x^2$ for all $x \in [-3, 1]$, where

$$[-3, 1] = \{x \in \mathbb{R} : -3 \leq x \leq 1\} \quad \text{and} \quad [0, 9] = \{x \in \mathbb{R} : 0 \leq x \leq 9\}.$$

(We recall that, given any real numbers a and b satisfying $a \leq b$, the set of real numbers x satisfying $a \leq x \leq b$ is denoted by $[a, b]$.) The function $q: [-3, 1] \to [0, 9]$ is surjective, since for each real number y satisfying $0 \leq y \leq 9$, there exists at least one real number x satisfying $-3 \leq x \leq 1$ such that $q(x) = y$; one such real number x is given by $x = -\sqrt{y}$, where $\sqrt{y}$ denotes the positive square root of y. However the function q is not injective. Indeed $q(1) = q(-1) = 1$. The function $q: [-3, 1] \to [0, 9]$ is therefore not bijective, and hence is not invertible.

Example Let $f\colon [0,2] \to [0,2]$ and $g\colon [0,2] \to [0,2]$ be the functions defined by

$$f(x) = \begin{cases} x^2 & \text{if } 0 \leq x \leq 1; \\ 3 - x & \text{if } 1 < x \leq 2; \end{cases}$$

$$g(x) = \begin{cases} x^2 & \text{if } 0 \leq x < 1; \\ 3 - x & \text{if } 1 \leq x \leq 2. \end{cases}$$

The function $f\colon [0,2] \to [0,2]$ is not injective since $f(1) = f(2) = 1$. This function is not surjective, since there is no element x of the domain $[0,2]$ for which $f(x) = 2$. The function f is thus not bijective, and hence is not invertible. The function $g\colon [0,2] \to [0,2]$, on the other hand, is invertible, with inverse given by

$$g^{-1}(x) = \begin{cases} \sqrt{x} & \text{if } 0 \leq x < 1; \\ 3 - x & \text{if } 1 \leq x \leq 2. \end{cases}$$

It follows from this that the function $f\colon [0,2] \to [0,2]$ must be both injective and surjective.

2.15 Partial Mappings

There is a generalization of the concept of a function between sets that is used in theoretical computer science. This is the concept of a *partial mapping*.

A *partial mapping* (or *partial function*) $f\colon A \nrightarrow B$ associates to some (but not necessarily all) elements a of A a corresponding element $f(a)$ of B. Partial mappings may be used in computer science to represent functions that are not defined for all their input values. For example, suppose that one has an algorithm which takes as input a natural number n and which, if it terminates, returns some other natural number $f(n)$. However there may be values of n for which the algorithm does not terminate, and for such values, the return value $f(n)$ is not defined. This situation is then represented by a partial mapping $f\colon \mathbb{N} \nrightarrow \mathbb{N}$.

The *domain* of a partial mapping $f\colon A \nrightarrow B$ is defined to be the subset of A consisting of all elements a of A for which $f(a)$ is defined. The *range* of the partial mapping $f\colon A \nrightarrow B$ is defined to be the subset of B consisting of all elements of B that are of the form $f(a)$ for some element a of the domain of the partial mapping.

A partial mapping $f\colon A \nrightarrow B$ is said to be *total* if its domain is the whole of A. Thus a partial mapping $f\colon A \nrightarrow B$ is total if and only if it is in fact a function from A to B.

A theory of partial mappings may be developed that generalizes the theory of functions between sets.