Chapter 3

Functions

Topics :

1. General Functions
2. Specific functions
3. Permutations

The concept of *function* is central to mathematics. (The words *map* and *mapping* are synonims for function.) This fundamental notion is the modern extension of the classical concept of a (numerical) function of one or several numerical "variables".

The idea of *symmetry* can be formalized and studied using *permutations*; the related notion of invariance plays an important role in modern geometry and physics. Sets of permutations on finite sets appear naturally (as groups of substitutions) in the study of algebraic equations.

3.1 General functions

In everyday language the word *function* indicates dependence of one varying quantity on another. Intuitively, a function is a "mechanism" that transforms one quantity into another. We shall make this idea more precise.

3.1.1 Definition. Let A and B be sets. A **function** f from A to B, denoted by $f : A \to B$, is a *rule* which associates with each element $x \in A$ a unique element $y \in B$. We write $y = f(x)$ to denote the element y assigned to x by the rule f; we say that y is the **image** of x under f (or the **value** of f at x), and x is a **preimage** of y under f.

We may think of a function as an "abstract machine" that processes an **input** x, in a certain way, to produce *the* **output** $f(x)$. If f is a function from A to B, we often write

$$f : A \to B, \quad x \mapsto f(x).$$

We also say that F is a *mapping* (or *map*) from A to B; it is customary to say that f maps the element x to (the element) $f(x)$. The set of all functions (or mappings) from A to B is denoted by B^A.

Note : We have used → to specify the sets a function is between and ↦ to specify its "rule". This distinction between → and ↦ will be consistent throughout these notes.

A function may be specified by a *list*, such as

$$f : \{a, b, c\} \to \mathbb{R}\,, \quad a \mapsto 1,\ b \mapsto 10 \quad \text{and} \quad c \mapsto 100$$

or by an *algebraic expression*, such as

$$g : \mathbb{Z} \to \mathbb{Z}\,, \quad x \mapsto x^2 + 4.$$

Note : The "mechanism" of a function need not be dictated by an algebraic formula. All that is required is that we carefully specify the allowable inputs and, for each allowable input, the corresponding output.

3.1.2 Examples. Let A be the set of people in a class.

1. There is a function $e : A \to [0, 100]$, which assigns to each person $x \in A$ an examination mark $e(x) \in [0, 100]$.
2. There is a function $g : A \to \{0, 1\}$, where
$$g(x) := \begin{cases} 1, & \text{if } x \text{ is male} \\ 0, & \text{if } x \text{ is female} \end{cases}$$
3. There is a function $b : A \to \{1, 2, 3, \ldots, 366\}$, where $b(x)$ is the unique number which encodes the birthday of x.

We can associate a set of ordered pairs in $A \times B$ to each function from A to B. This set is called the *graph* of the function and is often displayed pictorially to aid in understanding the behaviour of the function.

3.1.3 Definition. Let $f : A \to B$ be a function. The **graph** of the function f is the set of ordered pairs $\{(x, f(x)) \,|\, x \in A\}$.

If A and B are finite sets, we can represent a function f from A to B by making a list of elements in A and a list of elements in B and drawing an arrow from each element in A to the corresponding element in B. Such a drawing is called an **arrow diagram**.

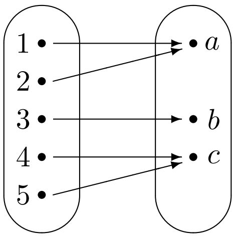
3.1.4 Example. Consider the function

$$f : \{1, 2, 3, 4, 5\} \to \{a, b, c\}$$

given by

$$1 \mapsto a,\ 2 \mapsto a,\ 3 \mapsto b,\ 4 \mapsto c,\ 5 \mapsto c.$$

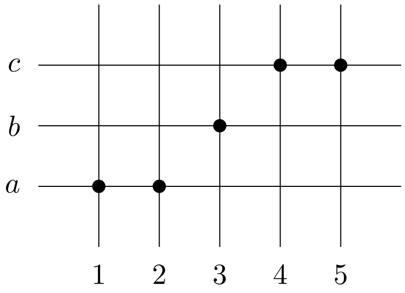
The function f can be represented by the following *arrow diagram* :



Alternatively, the graph of f,

$$G_f = \{(1, a),\ (2, a),\ (3, b),\ (4, c),\ (5, c)\},$$

can be exhibited as follows :



NOTE : It is customary to *identify* a function $f : A \to B$ and its graph $G_f \subseteq A \times B$; that is, to think of a function as *a set of ordered pairs* of elements. In this case, we call – by abuse of language – the exhibition of the set G_f the *graphical representation* (or even the *graph*) of the function f.

3.1.5 DEFINITION. Let f be a function from A to B. We say that the set A is the **domain** of f and the set B is the **codomain** of f. The set $\{f(x) \,|\, x \in A\}$ is called the **range** (or **image**) of f.

NOTE : (1) Although the range $\mathrm{im}\,(f)$ of a function f is always a subset of the codomain, there is no requirement that the range equals the codomain. Thus $\mathrm{im}\,(f) \subseteq B$.

(2) If the domain $\mathrm{dom}\,(f)$ and codomain $\mathrm{codom}\,(f)$ of a function f are understood, we will write simply

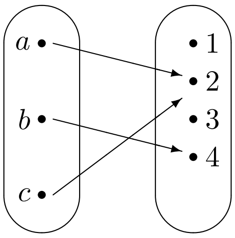
$$y = f(x).$$

As a matter of convention, if we write

$$y = f(x) \quad \text{or} \quad x \mapsto f(x)$$

without defining the domain of f, then we will *always* assume that the domain of f is the set of *all* x for which $f(x)$ is meaningful. For example, $y = \frac{1}{x}$ will have, by this convention, the domain $\operatorname{dom}(f) = \{x \in \mathbb{R} \mid x \neq 0\}$.

3.1.6 Example. Let $A = \{a, b, c\}$ and $B = \{1, 2, 3, 4\}$. Define a function f from A to B by the arrow diagram



(a) Write the domain and the codomain of f.

(b) Find $f(a)$, $f(b)$ and $f(c)$.

(c) What is the range (image) of f ?

(d) Find the preimages of 2, 4, and 1. [If $y \in \operatorname{codom}(f)$, then the *preimage* of y under f is the set $f^{-1}(y) := \{x \in \operatorname{dom}(f) \mid f(x) = y\}$.]

(e) Represent f as a set of ordered pairs.

Solution :

(a) $\operatorname{dom}(f) = \{a, b, c\}$ and $\operatorname{codom}(f) = \{1, 2, 3, 4\}$.

(b) $f(a) = 2$, $f(b) = 4$, and $f(c) = 2$.

(c) $\operatorname{im}(f) = \{2, 4\}$.

(d) $f^{-1}(2) = \{a, c\}$, $f^{-1}(4) = \{b\}$, and $f^{-1}(1) = \emptyset$.

(e) $f = \{(a, 2),\ (b, 4),\ (c, 2)\}$.

3.1.7 Definition. Suppose f and g are functions from A to B. Then f **equals** g, written $f = g$, provided

$$f(x) = g(x) \quad \text{for all } x \in A.$$

3.1.8 Example. Define $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ by the following formulas (for all $x \in \mathbb{R}$) :

$$\begin{aligned} f(x) &= |x| \\ g(x) &= \sqrt{x^2}. \end{aligned}$$

Does $f = g$?

Solution : Yes. Since the *absolute value* of a (real) number equals the square root of its square, $|x| = \sqrt{x^2}$ for all $x \in \mathbb{R}$. Hence $f = g$.

Injective and surjective functions

A function may send several elements of its domain (inputs) to the same element of its codomain (output). In terms of arrow diagrams, this means means that two or more arrows that start in the domain can point to the same element in the codomain. On the other hand, a function may associate a different element of its codomain to each element of its domain, which would mean that no two arrows that start in the domain would point to the same element in the codomain. A function with this property is called *one-to-one.*

3.1.9 Definition. Let $f : A \to B$ be a function. We say that f is **one-to-one** (or **injective**) provided $f(x_1) \neq f(x_2)$, whenever $x_1 \neq x_2$. Symbolically :

$$\boxed{f \text{ is injective} \iff (\forall x_1, x_2 \in A, \text{ if } x_1 \neq x_2 \text{ then } f(x_1) \neq f(x_2)).}$$

In other words, every element of the codomain of a one-to-one function has *at most* one preimage. A one-to-one function is also called an **injection**.

NOTE : (1) We see that a function $f : A \to B$ is one-to-one if and only if the quantification

$$\forall x_1 \forall x_2 \, (x_1 \neq x_2 \; \to \; f(x_1) \neq f(x_2))$$

is TRUE.

(2) Equivalently,

$$\boxed{f \text{ is injective } \iff (\forall x_1, x_2 \in A, \text{ if } \; f(x_1) = f(x_2) \; \text{ then } \; x_1 = x_2).}$$

(3) For a one-to-one function $f : A \to B$, any two distinct elements of the domain A are sent to two distinct elements of the codomain. It follows that the function f is *not* one-to-one if and only if at least two elements of the domain are taken to the same element of the codomain. Symbolically :

$$\boxed{f \text{ is } \textit{not} \text{ injective } \iff (\exists x_1, x_2 \in A, \; \text{ such that } \; x_1 \neq x_2 \; \text{ and } \; f(x_1) = f(x_2)).}$$

3.1.10 EXAMPLE. Let $f : \{a, b, c\} \to \{1, 2, 3, 4\}$ defined by $f(a) = 2$, $f(b) = 3$ and $f(c) = 2$. The function f is *not* one-to-one since $f(a) = f(c)$ and $a \neq c$.

3.1.11 EXAMPLE. Let $A = [0, \infty)$ and let $f : A \to A$ be defined by $f(x) = \frac{5x^2+3}{3x^2+5}$. Is this function one-to-one ?

SOLUTION : To show that f is an injection, we must show that, if $f(a) = f(b)$, then $a = b$. Suppose that $f(a) = f(b)$. Then

$$\frac{5a^2+3}{3a^2+5} = \frac{5b^2+3}{3b^2+5}$$

and so

$$15a^2b^2 + 9b^2 + 25a^2 + 15 = 15a^2b^2 = 9a^2 + 25b^2 + 15\,.$$

This relation simplifies to $16a^2 = 16b^2$, or $a^2 = b^2$. Since $a \geq 0$ and $b \geq 0$, it follows that $a = b$.

There may be an element of the codomain of a function that is not the image of any element in the domain. On the other hand, a function may have the property that *every* element of its codomain is the image of some element of its domain. Such a function is called *onto*.

3.1.12 Definition. Let $f : A \to B$ be a function. We say that f is **onto** (or **surjective**) provided for every element $y \in B$ there is an element $x \in A$ so that $f(x) = y$. Symbolically :

$$\boxed{f \text{ is surjective} \iff \forall y \in B, \exists x \in A \text{ such that } f(x) = y.}$$

In other words, every element of the codomain of an onto function has *at least* one preimage. An onto function is also called a **surjection**.

Note : (1) We see that a function $f : A \to B$ is onto if and only if the quantification

$$\forall y\, \exists x\, (y = f(x))$$

is TRUE.

(2) A function $f : A \to B$ is onto if and only if its range $\operatorname{im}(f)$ equals the codomain B. It follows that the function f is *not* onto if and only if $\operatorname{im}(f) \subset B$. That is, there is at least one element of B that is not an element of $\operatorname{im}(f)$. Symbolically :

$$\boxed{f \text{ is } \textit{not} \text{ surjective} \iff \exists y \in B \text{ such that } \forall x \in A,\ f(x) \neq y.}$$

3.1.13 Example. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{7, 8, 9, 10\}$. Let $f, g : A \to B$ be defined by

$$f : \quad 1 \mapsto 7,\ 2 \mapsto 7,\ 3 \mapsto 8,\ 4 \mapsto 9,\ 5 \mapsto 9,\ 6 \mapsto 10$$

and

$$g : \quad 1 \mapsto 7,\ 2 \mapsto 7,\ 3 \mapsto 7,\ 4 \mapsto 9,\ 5 \mapsto 9,\ 6 \mapsto 10\,,$$

respectively. Investigate for surjectivity these two functions.

Solution : The function f is onto because for each element $b \in B$ we can find one or more elements $a \in A$ such that $f(a) = b$. It is also easy to check that $\operatorname{im}(f) = B$.

However, the function g is *not* onto. Observe that $8 \in B$ but there is no $a \in A$ with $g(a) = 8$. Also, $\operatorname{im}(g) = \{7, 9, 10\} \neq B$.

3.1.14 Example. Let $f : \mathbb{Q} \to \mathbb{Q}$ defined by $x \mapsto 3x + 4$. Prove that f is onto.

Solution : Let $b \in \mathbb{Q}$ be arbitrary. We seek an $a \in \mathbb{Q}$ so that $f(a) = b$.

Let $a = \frac{1}{3}(b - 4)$. (Since b is a rational number, so is a.) Notice that

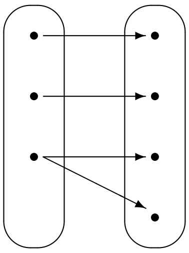
$$f(a) = 3\left[\frac{1}{3}(b-4)\right] + 4 = (b-4) + 4 = b.$$

Therefore the function $f : \mathbb{Q} \to \mathbb{Q}$ is onto.

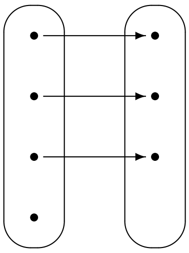
How did we ever "guess" that we should take $a = \frac{1}{3}(b - 4)$? We did not guess, we worked backward ! That is, we solved for a the *equation* $f(a) = b$.

3.1.15 Example. Let S be a finite set, with at least one element, and let $f : 2^S \to \mathbb{Z}^+$ be defined by $f(A) = |A|$ (cardinality of A). This function is not a surjection.

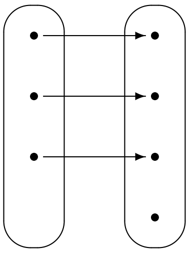
We can use arrow diagrams to exhibit various specific situations.



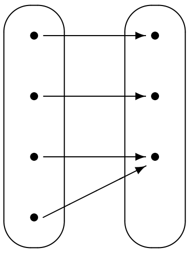
not a function



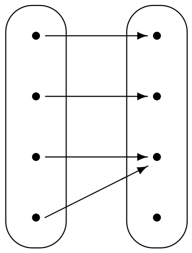
not a function



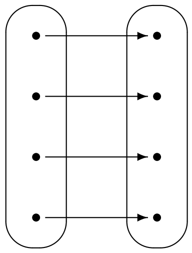
1-1 but not onto



onto but not 1-1



neither 1-1 nor onto



1-1 and onto

3.1.16 Definition. A function f is **bijective** if f is both one-to-one and onto.

Every element of the codomain of a bijective function has *exactly* one preimage. A bijective function is also called a **one-to-one correspondence** (or **bijection**).

3.1.17 Definition. Let A be a (nonempty) set. The **identity function** on A is the function $id_A : A \to A$ defined by

$$id_A(x) := x, \quad x \in A\,.$$

Every identity function is bijective.

3.1.18 Examples. (1) The function $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ is neither injective nor surjective, since $f(-1) = f(1)$ and for $y < 0$ there is no $x \in \mathbb{R}$ such that $y = f(x)$.

(2) The function $g : \mathbb{R} \to [0, \infty)$, $x \mapsto x^2$ is not injective but is surjective.

(3) The function $h : [0, \infty) \to \mathbb{R}$, $x \mapsto x^2$ is injective but is not surjective.

(4) The function $k : [0, \infty) \to [0, \infty)$, $x \mapsto x^2$ is bijective.

The inverse of a function

If f is a one-to-one correspondence from A to B, then there is a function from B to A that "undoes" the action of f; that is, it sends each element of B back to the element of A that it came from. This function is called the *inverse* of f.

3.1.19 Definition. Let $f : A \to B$ be a bijection. The **inverse function** of the given function is the function $f^{-1} : B \to A$ defined by

$$f^{-1}(y) = x \iff f(x) = y.$$

Note : f^{-1} does *not* denote the reciprocal $1/f$.

3.1.20 Example. Find the inverse of the bijective function $f : \{1, 2, 4, 8\} \to \{0, 1, 2, 3\}$ given by

$$1 \mapsto 0,\ 2 \mapsto 1,\ 4 \mapsto 2,\ 8 \mapsto 3\,.$$

Solution : We have (by reversing the arrows) :

$$f^{-1} : \quad 0 \mapsto 1,\ 1 \mapsto 2,\ 2 \mapsto 4,\ 3 \mapsto 8\,.$$

3.1.21 Example. Let $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 3x + 4$. Find the inverse function f^{-1}.

Solution : The given function is a one-to-one correspondence (why ?), and so it makes sense to ask for the inverse function $f^{-1} : \mathbb{R} \to \mathbb{R}$. Let $x \in \mathbb{R}$. Then $f(f^{-1}(x)) = x \iff 3f^{-1}(x) + 4 = x$. Solving for $f^{-1}(x)$, we find that $f^{-1}(x) = \frac{x-4}{3}$. Thus $f^{-1} : \mathbb{R} \to \mathbb{R}, \quad x \mapsto \frac{x-4}{3}$.

Composition of functions

The notion of performing first one function and then another can be defined precisely.

3.1.22 Definition. Let $f : A \to B$ and $g : C \to D$, where $B \subseteq C$. Then the **composition** of g and f, denoted by $g \circ f$, is the function from A to D defined by

$$(g \circ f)(x) := g(f(x)), \quad x \in A.$$

(The symbol $g \circ f$ is read "g composite f").

In other words, $g \circ f$ is the function that assigns to the element $x \in A$ the element assigned by g to $f(x)$.

NOTE : (1) The notation $g \circ f$ means that we do f first and then g. It may seem strange that, although we evaluate f first, we write its symbol after g. Why? When we apply the function $g \circ f$ to an element $a \in A$, as in $(g \circ f)(a)$, the letter f is closer to a and "hits" it first :

$$a \mapsto g(f(a)).$$

(2) The domain of $g \circ f$ is the same as the domain of f :

$$\operatorname{dom}(g \circ f) = \operatorname{dom}(f)\,.$$

(3) For the composition $g \circ f$ to make sense, every output of f must be an acceptable input to g. Properly said, we need $\operatorname{im}(f) \subseteq \operatorname{dom}(g)$.

(4) It is possible that $g \circ f$ and $f \circ g$ both make sense (are defined). It this situation, it may be the case that $g \circ f \neq f \circ g$ (are different functions).

3.1.23 EXAMPLE. Let $A = \{1,2,3,4,5\}$, $B = \{a,b,c,d\}$, $C = \{b,c,d\}$, and $D = \{\Box, \Diamond, \triangle, \bowtie, \heartsuit\}$. Let $f : A \to B$ and $g : C \to D$ be defined by

$$f : \quad 1 \mapsto b,\ 2 \mapsto b,\ 3 \mapsto c,\ 4 \mapsto d,\ 5 \mapsto d\,,$$

and

$$g : \quad b \mapsto \Diamond,\ c \mapsto \bowtie,\ d \mapsto \heartsuit.$$

We can identify these functions with their graphs, and write them as sets of ordered pairs of elements :

$$f = \{(1,b),\ (2,b),\ (3,c),\ (4,d),\ (5,d)\}$$

and

$$g = \{(b,\Diamond),\ (c,\bowtie),\ (d,\heartsuit)\}.$$

Then $g \circ f$ is the function

$$g \circ f = \{(1,\Diamond),\ (2,\Diamond),\ (3,\bowtie),\ (4,\heartsuit),\ (5,\heartsuit)\}\,.$$

For example,

$$(g \circ f)(2) = g(f(2)) = g(b) = \diamond.$$

So $(2, \diamond) \in g \circ f$.

3.1.24 Example. Let $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^2 + 2$ and let $g : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 3x + 4$. Then $g \circ f : \mathbb{R} \to \mathbb{R}$ is the function defined by

$$(g \circ f)(x) = g(f(x)) = g(x^2 + 2) = 3(x^2 + 2) + 4 = 3x^3 + 10$$

and $f \circ g : \mathbb{R} \to \mathbb{R}$ is the function defined by

$$(f \circ g)(x) = f(g(x)) = f(3x + 4) = (3x + 4)^2 + 2 = 9x^2 + 24x + 18.$$

We can see clearly that $g \circ f \neq f \circ g$.

We have seen that composition of functions does not satisfy the *commutativity property.* It does, however, satisfy the *associativity property.*

3.1.25 Proposition. *Let $f : A \to B$, $g : B' \to C$, and $h : C' \to D$, where $B \subseteq B'$, $C \subseteq C'$. Then*

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

Solution : We need to show that the functions $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are the same. First, we see that the domains of the functions are the same, namely the set A. Second, we check that for any $a \in A$, the functions produce the same value. We have

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

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

It is often important to decide whether a function is one-to-one or onto. In this regard, the following results concerning the composition of functions are useful.

3.1.26 PROPOSITION. *Let $f : A \to B$ and $g : C \to D$, where $B \subseteq C$.*

(a) If f and g are injections, then $g \circ f$ is also an injection.

(b) If f and g are surjections, then $g \circ f$ is also a surjection.

(c) If $g \circ f$ is an injection, then f is an injection.

(d) If $g \circ f$ is a surjection, then g is a surjection.

3.1.27 EXAMPLE. Let $f : A \to B$ and $g : B \to A$. Show that if $f \circ g : B \to B$ is the identity function on B and $g \circ f : A \to A$ is the identity function on A, then f and g are bijections, f is the inverse function of g, and g is the inverse function of f.

SOLUTION : We first note that it follows from PROPOSITION 2.3.29 (c) and (d) that both f and g are bijections. We show that g is the inverse function of f, and a similar argument shows that f is the inverse function of g. Let $y \in B$ and let $x = g(y)$. We must show that x is the element of A for which $f(x) = y$. But

$$f(x) = f(g(y)) = f \circ g(y) = id_B(y) = y.$$

3.1.28 DEFINITION. A function $f : A \to B$ is **invertible** provided there is a function $g : B \to A$ such that $f \circ g : B \to B$ is the identity function on B and $g \circ f : A \to A$ is the identity function on A.

NOTE : A function $f : A \to B$ is invertible if and only if it is a bijection.

3.1.29 EXAMPLE. Show that the function $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto 3x + 4$ is a bijection.

SOLUTION : Define $g : \mathbb{R} \to \mathbb{R}, \quad x \mapsto (x - 4)/3$. Let $x \in \mathbb{R}$. Then

$$(g \circ f)(x) = g(f(x)) = g(3x + 4) = \frac{(3x + 4) - 4}{3} = x$$

and

$$(f \circ g)(x) = f(g(x)) = f\left(\frac{x - 4}{3}\right) = 3\left(\frac{x - 4}{3}\right) + 4 = (x - 4) + 4 = x.$$

Therefore, $f : \mathbb{R} \to \mathbb{R}$ is invertible, and thus it is a bijection.

NOTE : Alternatively, one can show that the function f is both one-to-one and onto. This can be done, for instance, by showing that for any given $y \in \mathbb{R}$, the *equation* (in x) $y = 3x + 4$ has a *unique* solution.

3.2 Specific functions

Let $f : A \to B$ be a function. In the general case, the domain A and the codomain B of such a function are completely arbitrary sets. However, important classes of functions exist for specific sets A, B. We shall describe briefly some of these *specific* functions.

(i) $B = \mathbb{R}$. Functions $f : A \to \mathbb{R}$ are referred to as **real-valued functions**. The domain A of f is an arbitrary set; in other words, the inputs of a real-valued function are *not* necessary numbers : they could be any type of objects (e.g. people, books, triangles, sets or even sets of sets).

Two real-valued functions f and g can be combined to form new functions $f + g$, $f - g$, fg, and f/g in a manner similar to the way we add, subtract, multiply, and divide real numbers.

3.2.1 DEFINITION. Let $f : A_1 \to \mathbb{R}$ and $g : A_2 \to \mathbb{R}$, where $A_1 \cap A_2 \neq \emptyset$. Then

$$f + g : A_1 \cap A_2 \to \mathbb{R} \quad \text{is defined by} \quad (f + g)(x) := f(x) + g(x)\,;$$

$$f - g : A_1 \cap A_2 \to \mathbb{R} \quad \text{is defined by} \quad (f - g)(x) := f(x) - g(x)\,;$$

$$f \cdot g : A_1 \cap A_2 \to \mathbb{R} \quad \text{is defined by} \quad (f \cdot g)(x) := f(x) \cdot g(x)\,;$$

$$\frac{f}{g} : A_1 \cap A_2 \setminus \{x \in A_1 \cap A_2 \,|\, g(x) \neq 0\} \to \mathbb{R} \quad \text{is defined by} \quad \left(\frac{f}{g}\right)(x) := \frac{f(x)}{g(x)}\,\cdot$$

3.2.2 Example. Let $f : [0,\infty) \to \mathbb{R}$, $x \mapsto \sqrt{x}+3$ and let $g : (-\infty, 4] \to \mathbb{R}$, $x \mapsto \sqrt{4-x}-1$. Then $(-\infty,4] \cap [0,\infty) = [0,4]$ and

$$f+g : [0,4] \to \mathbb{R} \quad \text{is defined by} \quad (f+g)(x) = \sqrt{x} + \sqrt{4-x} + 2\,;$$

$$f-g : [0,4] \to \mathbb{R} \quad \text{is defined by} \quad (f-g)(x) = \sqrt{x} - \sqrt{4-x} + 4\,;$$

$$f \cdot g : [0,4] \to \mathbb{R} \quad \text{is defined by} \quad (f \cdot g)(x) = \sqrt{x(4-x)} + 3\sqrt{4-x} - \sqrt{x} - 3\,;$$

$$\frac{f}{g} : [0,3) \cup (3,4] \to \mathbb{R} \quad \text{is defined by} \quad \left(\frac{f}{g}\right)(x) = \frac{\sqrt{x}+3}{\sqrt{4-x}-1}\,\cdot$$

Real-valued functions $f : A \to \mathbb{R}$ where $A \subseteq \mathbb{R}$ are usually called *real-valued functions of one real variable* (or **real functions**, for short). The simplest types of real functions are the **polynomials**, of the form

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

with *coefficients* $a_0,\ a_1,\ \ldots, a_n$. Next come the **rational functions**, such as

$$x \mapsto \frac{1}{x}, \quad x \mapsto \frac{1}{1+x^2}, \quad x \mapsto \frac{2x+1}{x^4+3x^2+5}$$

which are quotients of polynomials, and the *trigonometric functions* sin, cos, tan. Other basic real functions are the *exponential function* $\exp_a$, the *power function* $(\cdot)^a$, the *logarithmic function* $\log_a$, and the *inverse trigonometric functions* arcsin, arccos,
arctan.

Note : These real functions (which are commonly referred to as **elementary functions**) are formally defined and their remarkable properties are studied in *Calculus* courses.

The **absolute value** (or **modulus**) **function** is the real function

$$|\cdot| : \mathbb{R} \to \mathbb{R}, \quad x \mapsto |x| := \begin{cases} x & \text{if} \ \ x \geq 0 \\ -x & \text{if} \ \ x < 0. \end{cases}$$

For example, $|1.5| = 1.5, \ | - 0.7| = 0.7, \ |0| = 0.$

NOTE : Geometrically, the absolute value of (the number) x represents the *distance* from the origin of the real line to the point (on the real line) with *coordinate* x.

The absolute value function has some remarkable properties (see APPENDIX B).

3.2.3 EXAMPLE. There is a function $\{\cdot\}_* : \mathbb{R} \to \mathbb{R}$ which associates to each real number x the *distance to the closest integer* (on the real line); that is,

$$\{x\}_* := \min\{|x - n| \mid n \in \mathbb{Z}\}.$$

(ii) $B = \mathbb{Z}$. Functions $f : A \to \mathbb{Z}$ are special cases of real-valued functions. Some of these functions play important roles in discrete mathematics. The *floor* and *ceiling functions* are fundamental.

3.2.4 DEFINITION. The **floor function** is the function

$$\lfloor\cdot\rfloor : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}.$$

$\lfloor x \rfloor$ is the greatest integer which is less than or equal to x; for example, $\lfloor 1.5 \rfloor = 1, \ \lfloor -0.7 \rfloor = -1, \ \lfloor \pi \rfloor = 3.$

3.2.5 DEFINITION. The **ceiling function** is the function

$$\lceil\cdot\rceil : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \lceil x \rceil := \min\{n \in \mathbb{Z} \mid n \geq x\}.$$

$\lceil x \rceil$ is the least integer which is greater than or equal to x; for example, $\lceil 1.5 \rceil = 2, \ \lceil -0.7 \rceil = 0, \ \lceil \pi \rceil = 4.$

Both these functions have some remarkable properties (see APPENDIX B). Other interesting (and useful) examples are given in what follows.

3.2.6 Examples.

1. The **signum function** is the function

$$\operatorname{sgn} : \mathbb{R} \to \mathbb{Z}, \quad x \mapsto \begin{cases} \dfrac{x}{|x|} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

2. The **Dirichlet function** is the function

$$\delta : \mathbb{R} \to \{0, 1\}, \quad x \mapsto \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q}. \end{cases}$$

3. The **unit-step function** (at $a \in \mathbb{R}$) is the function

$$u_a : \mathbb{R} \to \{0, 1\}, \quad x \mapsto u_a(x) := \begin{cases} 1 & \text{if } \ x \geq a \\ 0 & \text{if } \ x < a. \end{cases}$$

Note : Both the Dirichlet function and the unit-step function are examples of *characteristic functions.* The general concept can be described as follows. Let X be a (fixed) set and let 2^X denote the power set (i.e. the set consisting of all the subsets, including the empty set) of X. Given $A \in 2^X$, the **characteristic function** of A is the function

$$\varphi_A : X \to \{0, 1\}, \quad x \mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } \ x \notin A. \end{cases}$$

Equal subsets (of X) have, by definition, equal corresponding characteristic functions. It turns out that there is a one-to-one correspondence between the power set 2^X and the set $\{0,1\}^X$ (of all functions $X \to \{0,1\}$) : the function

$$\Phi : 2^X \to \{0,1\}^X, \quad A \mapsto \varphi_A$$

is a *bijection.* In other words, each (sub)set may be viewed as a function, its characteristic function, and any such function determines uniquely the (sub)set; this allows us to *identify*, whenever appropriate, a (sub)set with its characteristic function. We can see that $\delta = \varphi_{\mathbb{Q}}$ (the Dirichlet function δ is the characteristic function of the set of rational numbers) and $u_a = \varphi_{[a,\infty)}$ (the unit-step function u_a is the characteristic function of the interval $[a, \infty)$ of real numbers).

(iii) $A \subseteq \mathbb{N}$ Functions $f : A \to B$ where A is an infinite subset of $\mathbb{N}$ (usually either the set $\mathbb{N}$ or the set of positive integers $\mathbb{Z}^+$) are called **sequences** (of elements of B).

3.2.7 Example. The *sequence*

$$1, \; -\frac{1}{2}, \; \frac{1}{3}, \; -\frac{1}{4}, \; \cdots, \; \frac{(-1)^n}{n+1}, \; \cdots$$

can be thought of as the function

$$f : \mathbb{N} \to \mathbb{R}, \quad n \mapsto f(n) := \frac{(-1)^n}{n+1}\cdot$$

Sequences of numbers will be encountered later (see chapters 4-6).

(iv) $A = B$. *Bijective* functions $f : A \to A$ where A is an arbitrary set are called **permutations** (or **symmetries**) of A. The set $\mathsf{Sym}\,(A)$ of all permutations of A has a remarkable algebraic structure and plays a major role in many areas of mathematics.

Note : When the set A (usually infinite) is equipped with some "geometric structure", it is customary to refer to a permutation (of A) as a *transformation* on the "space" A.

The case when A is a *finite* set will be considered in the following section.

3.3 Permutations

When dealing with *discrete* (usually finite) objects, a permutation is best viewed as a *rearrangement* of objects. This simple idea can be made precise.

Let X be a finite, *ordered* set with n elements. These are our distinct objects we want to "rearrange". We may assume that $X = \{1, 2, 3, \cdots, n\}$. (We identify each object with its"position" in the ordered set : the first, second, third, etc.)

3.3.1 Definition. A bijection $\alpha : \{1, 2, 3, \cdots, n\} \to \{1, 2, 3, \cdots, n\}$ is called a **permutation on n elements**.

The set of all permutations on n elements is denoted by S_n; it is usually referred to as the *symmetric group* of order n.

3.3.2 Example. Let $X = \{1, 2, 3, 4, 5\}$ and let $\alpha : X \to X$ be defined by

$$\alpha = \{(1,2),\ (2,4),\ (3,1),\ (4,3),\ (5,5)\}.$$

Since α is a one-to-one and onto function (i.e. a bijection) from X to X, it is a permutation (on 5 elements); we write $\alpha \in S_5$.

Let α be an arbitrary permutation on n elements (or a permutation of *degree* n). We can express α as a $2 \times n$ array of integers. The top row contains the integers 1 through n in their usual order, and the bottom row contains $\alpha(1)$ through $\alpha(n)$:

$$\alpha = \begin{bmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{bmatrix}.$$

Note : (1) The numbers $\alpha(1),\ \alpha(2),\ \dots,\ \alpha(n)$ are the numbers $1, 2, \dots, n$ in some order.

(2) The top row in the *array notation* is not strictly necessary. We could express the permutation α simply by reporting the bottom row; all the information we need is there. We could write $\alpha = \begin{bmatrix} \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{bmatrix}$. This notation is reasonable only when n is small. On the other hand, this is a reasonable way to store a permutation into a computer.

3.3.3 Example. For the permutation (on 5 elements)

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix}$$

$\alpha(1) = 2,\ \alpha(2) = 4,\ \alpha(3) = 1,\ \alpha(4) = 3$ and $\alpha(5) = 5$.

3.3.4 Example. The identity function $id_{\{1,2,\ldots,n\}}$ is a permutation (on n elements) and therefore in S_n. We usually denote the **identity permutation** by the lowercase Greek letter ι (iota). Thus

$$\iota := \begin{bmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{bmatrix} \in S_n.$$

Permutations (on the same number of elements) can be *multiplied* by consecutive application. Let $\alpha, \beta \in S_n$. The function

$$\beta\alpha : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}, \quad k \mapsto \beta\left(\alpha(k)\right)$$

is the **product** (or **composition**) of the permutations α and β.

Note : Permutations are functions and $\beta\alpha$ is just the composite function $\beta \circ \alpha$. Permutation α acts first and then permutation β acts on the result of α.

The following result lists important properties of S_n.

3.3.5 Proposition. *Consider the set S_n. Then (for $\alpha, \beta, \gamma \in S_n$) :*

(G1) $\beta\alpha \in S_n$.

(G2) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

(G3) $\alpha\iota = \iota\alpha$.

(G4) $\alpha^{-1} \in S_n$ *and* $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \iota$.

Note : The properties listed above may be summarized by saying that S_n is a *group* (with respect to the composition of permutations).

3.3.6 Example. The product of permutations

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{bmatrix}$$

is

$$\begin{aligned}\beta\alpha &= \begin{bmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{bmatrix}\begin{bmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 3 & 2\end{bmatrix}\\ &= \begin{bmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{bmatrix}.\end{aligned}$$

Also

$$\begin{aligned}\alpha\beta &= \begin{bmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 3 & 2\end{bmatrix}\begin{bmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{bmatrix}\\ &= \begin{bmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{bmatrix}.\end{aligned}$$

Note : The product of permutations is, in general, *not* commutative. More precisely, the symmetric group S_n is not commutative for $n \geq 3$.

If a permutation maps $a \mapsto b$, then its inverse maps $b \mapsto a$. Thus the inverse of the permutation

$$\alpha = \begin{bmatrix}1 & 2 & \dots & n\\ a_1 & a_2 & \dots & a_n\end{bmatrix}$$

is simply

$$\alpha^{-1} = \begin{bmatrix}a_1 & a_2 & \dots & a_n\\ 1 & 2 & \dots & n\end{bmatrix}.$$

3.3.7 Example. Let

$$\alpha = \begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 4 & 5 & 1 & 3 & 2 & 7 & 6\end{bmatrix} \in S_7.$$

Find α^{-1}.

Solution : We have

$$\begin{aligned}\alpha^{-1} &= \begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 4 & 5 & 1 & 3 & 2 & 7 & 6\end{bmatrix}^{-1} = \begin{bmatrix}4 & 5 & 1 & 3 & 2 & 7 & 6\\ 1 & 2 & 3 & 4 & 5 & 6 & 7\end{bmatrix}\\ &= \begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 3 & 5 & 4 & 1 & 2 & 7 & 6\end{bmatrix}.\end{aligned}$$

Cycle notation

For another look at permutations we consider the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix}$, an element of S_5. The **cycle notation** for α is as follows :

$$\alpha = (1,2,4,3)(5).$$

Let us explain what this notation means. The two lists in parentheses, $(1,2,4,3)$ and (5), are called **cycles**. The cycle $(1,2,4,3)$ means that

$$1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1\,.$$

In other words,

$$\alpha(1) = 2,\ \alpha(2) = 4,\ \alpha(4) = 3, \quad \text{and} \quad \alpha(3) = 1.$$

Each number k is followed by $\alpha(k)$. Taken literally, if we began the cycle with 1, we would go on for ever :

$$(1,2,4,3,1,2,4,3,1,2,4,3,\dots).$$

Instead, when we reach the first 3, we write a close parentheses meaning "return to the start of the cycle". Thus $(1,\ \dots,\ 3)$ means that $\alpha(3) = 1$.

What does the lonely (5) mean ? It means $\alpha(5) = 5$.

NOTE : (1) A cycle is a permutation. For example,

$$(1,2,4,3) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix} \quad \text{and} \quad (5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}.$$

(2) A cycle may be written starting with *any* of its elements. For example,

$$(1,2,4,3) = (2,4,3,1) = (4,3,1,2) = (3,1,2,4).$$

However, the *cyclic order* must be kept. For example,

$$(1,2,4,3) \neq (2,1,4,3).$$

(3) A cycle $(a_1, a_2, \dots, a_k)$ is called a cycle of length k (or an k-cycle).

3.3.8 Example. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 6 & 3 & 8 & 1 & 4 & 9 \end{bmatrix} \in S_9.$$

Express α in cycle notation.

Solution : Note that $\alpha(1) = 2$, $\alpha(2) = 7$, and $\alpha(7) = 1$. So far we have

$$\alpha = (1, 2, 7) \cdots .$$

The first element we have not considered is 3. Restarting from 3, we have $\alpha(3) = 5$ and $\alpha(5) = 3$, so the next cycle is $(3, 5)$. So far we have

$$\alpha = (1, 2, 7)(3, 5) \cdots .$$

The next element we have yet to consider is 4. We have $\alpha(4) = 6$, $\alpha(6) = 8$, and $\alpha(8) = 4$ to complete the cycle. The next cycle is $(4, 6, 8)$. Thus far we have

$$\alpha = (1, 2, 7)(3, 5)(4, 6, 8) \cdots .$$

Finally, we have $\alpha(9) = 9$, so the last cycle is just (9). The permutation α in cyclic notation is

$$\alpha = (1, 2, 7)(3, 5)(4, 6, 8)(9).$$

Note : Since a cycle of length 1 is just the identity permutation, it can be dropped (as long as the degree of the permutation is remembered). For example,

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{bmatrix} = (1, 3)(2)(4)(5) = (1, 3) \in S_5.$$

Does the cycle notation method work for all permutations (on n elements) ? The answer is *yes*. More precisely, *we can write any permutation* $\alpha \in S_n$ *as a product of pairwise disjoint cycles*; that is, no two cycles have common elements.

Note : Any two disjoint cycles commute.

3.3.9 Example. Consider the cycles $(1,2),\ (1,3),\ (3,4) \in S_4$. Then

$$(1,2)(3,4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = (3,4)(1,2).$$

Does $(1,2)(1,3) = (1,3)(1,2)$?

Solution : The answer is *no.* Indeed,

$$(1,2)(1,3) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} = (1,3)(1,2).$$

We can say more. Is it possible to write the same permutation as a product of disjoint cycles in two different ways ? At first glance, the answer is *yes.* For example,

$$\alpha = (1,2,7)(3,5)(4,6,8)(9) = (5,3)(6,8,4)(9)(7,1,2)\,;$$

both represent the permutation $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 5 & 6 & 3 & 8 & 1 & 4 & 9 \end{bmatrix}$. However, on closer inspection, we see that the two representations of α have the same cycles; the cycles $(1,2,7)$ and $(7,1,2)$ both say the same thing, namely, $\alpha(1) = 2,\ \alpha(2) = 7,$ and $\alpha(7) = 1$. One can prove that *there is only one way to write α as a product of disjoint cycles.* The following general result holds.

3.3.10 Proposition. *Every permutation on a finite set can be decomposed into pairwise disjoint cycles. Furthermore, this decomposition is unique up to rearranging the cycles and the cyclic order of the elements within cycles.*

The cycle notation is handy for doing calculations with permutations (on a finite set). The most basic operations are taking the inverse of a permutation and the composition of two permutations.

Let us begin with calculating the inverse of a permutation. An important observation is the following : if $(a,b,c,\dots)$ is a cycle, then its inverse is

$(\ldots, c, b, a)$. Since any permutation $a \in S_n$ decomposes into pairwise disjoint cycles, we get a simple rule for calculating the inverse of α :

$$\alpha = \alpha_1\alpha_2\cdots\alpha_r \quad \Rightarrow \quad \alpha^{-1} = \alpha_1^{-1}\alpha_2^{-1}\cdots\alpha_r^{-1}.$$

3.3.11 Example. Let $\alpha = (1,2,7,9,8)(5,6,3)(4) \in S_9$. Calculate α^{-1}.

Solution : We have

$$\alpha^{-1} = (8,9,7,2,1)(3,6,5)(4) = (8,9,7,2,1)(3,6,5).$$

Let us explore how to compute the composition of two permuations.

3.3.12 Example. Let $\alpha, \beta \in S_9$ be given by

$$\alpha = (1,3,5)(4,6)(2,7,8,9) \quad \text{and} \quad \beta = (1,4,7,9)(2,3)(6,8).$$

Compute $\alpha\beta$.

Solution : We calculate $\alpha\beta(k)$ for all $k \in \{1,2,3,4,5,6,7,8,9\}$. We begin with $\alpha\beta(1)$. We have $\alpha\beta(1) = \alpha(4) = 6$. Thus far we can write

$$\alpha\beta = (1,6,\ldots$$

To continue the cycle, we calculate $\alpha\beta(6)$. We have $\alpha\beta(6) = \alpha(8) = 9$. Now we have

$$\alpha\beta = (1,6,9,\ldots$$

Continuing in this fashion, we get

$$1 \mapsto 6 \mapsto 9 \mapsto 3 \mapsto 7 \mapsto 2 \mapsto 5 \mapsto 1$$

and we have completed a cycle ! Thus $(1,6,9,3,7,2,5)$ is a cycle of $\alpha\beta$. Notice that 4 is not on this cycle, so we start over computing $\alpha\beta(4)$. We get

$$4 \mapsto 8 \mapsto 4.$$

The two cycles $(1,6,9,3,7,2,5)$ and $(4,8)$ exhaust all the elements of $\{1,2,3,4,5,6,7,8,9\}$, and so we are finished. We have found

$$\alpha\beta = (1,6,9,3,7,2,5)(4,8).$$

Transpositions

The simplest permutation is the identity permutation. The identity permutation ι maps every element into itself.

The next simplest type of permutation is a *transposition.* Transpositions map almost all elements to themselves, except that they exchange one pair of elements. For example,

$$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{bmatrix} = (2,5)$$

is a transposition (of degree 5). Thus

3.3.13 Definition. A **transposition** is a cycle of length 2.

We explore the expression of permutations as products of transpositions. There is a nice trick for converting a cycle into a composition of transpositions.

3.3.14 Example. Let $\pi = (1,2,3,4,5)$. Write π as a composition of transpositions.

Solution : We have

$$\pi = (1,2,3,4,5) = (1,5)(1,4)(1,3)(1,2).$$

3.3.15 Example. Let $\sigma = (1,2,3,4,5)(6,7,8)(10,11) \in S_{11}$. Write σ as a product of transpositions.

Solution : We have

$$\sigma = (1,5)(1,4)(1,3)(1,2)(6,8)(6,7)(10,11).$$

Let α be any permutation (on a finite set). Write α as a product of cycles. Using the technique from Example 3.3.2, we can rewrite each of its cycles as a composition of transpositions. Because the cycles are pairwise disjoint, there is no effect of one cycle on another. Thus we can simply string together the transpositions for the various cycles into one long product of transpositions.

What about the identity permutation ι ? Can it also be represented as a product of transpositions ? Yes. We can write, for instance,

$$\iota = (1,2)(1,2).$$

Let us summarize what we have shown here.

3.3.16 PROPOSITION. *Every permutation on a finite set can be decomposed into transpositions.*

The decomposition of permutations into transpositions is *not* unique ! For example, we can write

$$\begin{aligned}(1,2,3,4) &= (1,4)(1,3)(1,2)\\ &= (1,2)(2,3)(3,4)\\ &= (1,2)(1,4)(2,3)(1,4)(3,4).\end{aligned}$$

These ways of writing $(1,2,3,4)$ are *not* simple rearrangements of one another. We see that they do not even have the same number of transpositions. However, they do have something in common. In all three cases, we used an odd number of transpositions.

The following important general result holds.

3.3.17 PROPOSITION. *Let $\alpha \in S_n$. Let α be decomposed into transpositions as*

$$\begin{aligned}\alpha &= \tau_1\tau_2\cdots\tau_a\\ \alpha &= \sigma_1\sigma_2\cdots\sigma_b.\end{aligned}$$

Then a and b have the same parity; that is, they are both odd or even.

The key to proving this result is the following fact, given without proof (the proof, however, takes a little work !) : *If the identity permutation is written as a composition of transpositions, then that composition must use an even number of transpositions.*

PROOF (OF PROPOSITION 3.3.5) : Let α be a permutation decomposed (into transpositions) as

$$\begin{aligned} \alpha &= \tau_1\tau_2\cdots\tau_a \\ \alpha &= \sigma_1\sigma_2\cdots\sigma_b. \end{aligned}$$

Then we can write

$$\alpha^{-1} = \sigma_b\sigma_{b-1}\cdots\sigma_2\sigma_1$$

and so

$$\iota = \alpha\alpha^{-1} = \tau_1\tau_2\cdots\tau_a\sigma_b\cdots\sigma_2\sigma_1.$$

This is a decomposition of ι into $a+b$ transpositions, hence $a+b$ is even, and so a and b have the same parity. □

The signature of a permutation

The foregoing result enables us to separate permutations into two disjoint categories: those that can be expressed as the composition of an even number of transpositions and those that can be expressed as the composition of an odd number of transpositions.

3.3.18 DEFINITION. Let α be a permutation on a finite set. We call α **even** provided it can be written as the composition of an even number of transpositions. Otherwise it can be written as the composition of an odd number of transpositions, in which case we call α **odd**.

The **signature** of a permutation $\alpha \in S_n$, denoted by $\operatorname{sgn}(\alpha)$, is $+1$ for even permutations and -1 for odd permutations.

3.3.19 EXAMPLE. What is the signature of $(1,2,3,4)$?

SOLUTION : We have

$$\operatorname{sgn}(1,2,3,4) = \operatorname{sgn}(1,4)(1,3)(1,2) = -1.$$

The function

$$h : S_n \to \{-1, 1\}, \qquad \alpha \mapsto \operatorname{sgn}(\alpha)$$

is clearly a surjection. Moreover, it preserves the "group structure"; that is, (for $\alpha, \beta \in S_n$)

$$h(\alpha\beta) = h(\alpha) \cdot h(\beta).$$

Note : The set (in fact, *subgroup*) $A_n = h^{-1}(1)$ (of all even permutations on n elements) is referred to as the *alternating group* on n elements.

3.4 Exercises

Exercise 31 Recall the definitions of the floor function, the ceiling function, the absolute value function, and of the unit-step function. Then sketch the graph of

(a) $y = \lfloor x \rfloor$.

(b) $y = \lceil x \rceil$.

(c) $y = \lfloor x - 1 \rfloor$.

(d) $y = \lceil x - 1 \rceil$.

(e) $y = 1 + \lfloor x \rfloor$.

(f) $y = 2 - \lceil x \rceil$.

(g) $y =\mid x \mid$.

(h) $y =\mid x - 2 \mid$.

(i) $y =\mid x + 2 \mid$.

(j) $y = 1- \mid x \mid$.

(k) $y = u_2(x)$.

(l) $y = u_0(x)$.

(m) $y = u_{-1}(x)$.

(n) $y = x^2 u_3(x)$.

(o) $y = 1 - u_1(x)$.

(p) $y = (1 - u_3(x))u_2(x)$.

Exercise 32 Investigate the following functions for injectivity, surjectivity, and bijectivity. If the function is bijective, find its inverse.

(a) $f : \mathbb{N} \to \mathbb{N}\,, \quad n \mapsto n^2 + 1.$

(b) $g : \mathbb{Z} \to \mathbb{Z}\,, \quad n \mapsto n^3.$

(c) $h : \mathbb{R} \to \mathbb{Z}\,, \quad x \mapsto \lfloor x \rfloor.$

(d) $i : \mathbb{R} \to \mathbb{Z}\,, \quad x \mapsto \lceil x \rceil.$

(e) $j : \mathbb{R} \to \mathbb{R}\,, \quad x \mapsto |x|.$

(f) $k : [0, \infty) \to [0, \infty)\,, \quad x \mapsto |x|.$

(g) $l : (-\infty, 0] \to [0, \infty)\,, \quad x \mapsto |x|.$

(h) $m : \mathbb{R} \to \mathbb{R}\,, \quad x \mapsto x^4.$

(i) $n : [0, \infty) \to [0, \infty)\,, \quad x \mapsto x^4.$

(j) $u : \mathbb{R} \to \mathbb{R}\,, \quad x \mapsto \begin{cases} x^2, & \text{if } x \geq 0 \\ 2x, & \text{if } x < 0. \end{cases}$

(k) $v : (0, \infty) \to (0, \infty)\,, \quad x \mapsto \dfrac{7x + 8}{8x + 7}\,.$

(l) $w : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{2\}\,, \quad x \mapsto \dfrac{2x + 1}{x - 2}\,.$

Exercise 33 Write down *all* functions $f : A \to B$ and then indicate which are one-to-one and which are onto.

(a) $A = \{1, 2, 3\}$ and $B = \{4, 5\}$.

(b) $A = \{1, 2\}$ and $B = \{3, 4, 5\}$.

(c) $A = \{1, 2\}$ and $B = \{3, 4\}$.

Exercise 34 Give an example of a function from $\mathbb{N}$ to $\mathbb{N}$ that is

(a) one-to-one but not onto ;

(b) onto but not one-to-one ;

(c) both one-to-one and onto (but different from the identity function) ;

(d) neither one-to-one nor onto.

Exercise 35 Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be two functions.

(a) If f and g are both one-to-one, is $f+g$ also one-to-one ?

(b) If f and g are both one-to-one, is $f \cdot g$ also one-to-one ?

(c) If f and g are both one-to-one, is $f \circ g$ also one-to-one ?

(d) If f and g are both onto, is $f+g$ also onto ?

(e) If f and g are both onto, is $f \cdot g$ also onto ?

(f) If f and g are both onto, is $f \circ g$ also onto ?

Justify your answers.

Exercise 36 Let

$$f : \mathbb{R} \to \mathbb{R}\,, \quad x \mapsto ax+b \quad \text{and} \quad g : \mathbb{R} \to \mathbb{R}\,, \quad x \mapsto cx+d$$

where a, b, c, and d are constants. Determine for which constants a, b, c, and d it is true that $f \circ g = g \circ f$.

Exercise 37 Express the following permutations in cycle notation.

(a) $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{bmatrix}$.

(b) $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{bmatrix}$.

(c) $\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{bmatrix}$.

(d) $\gamma^2 := \gamma\gamma$, where γ is the permutation from part (c).

(e) γ^{-1}, where γ is the permutation from part (c).

(f) $\iota \in S_5$.

(g) $\delta = (1,2)(2,3)(3,4)(4,5)(5,1)$.

Exercise 38 Let $\pi, \sigma, \tau \in S_9$ be given by

$$\begin{aligned} \pi &= (1)(2,3,4,5)(6,7,8,9), \\ \sigma &= (1,3,5,7,9,2,4,6,8), \\ \tau &= (1,9)(2,8)(3,5)(4,6)(7). \end{aligned}$$

Calculate :

(a) $\pi\sigma$; (b) $\sigma\pi$; (c) π^2; (d) π^{-1}; (e) σ^{-1}; (f) τ^2; (g) τ^{-1}.

Exercise 39 Find

(a) $a, b, c, d,$ and e when

$$(1,3,4)(2,5) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{bmatrix}.$$

(b) $a, b,$ and c when

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{bmatrix} = (1, a, b)(3, c).$$

Exercise 40 Exhibit

(a) the 6 elements of S_3 in cycle notation.

(b) the 24 elements of S_4 in cycle notation.

Exercise 41 Prove or disprove :

(a) For all $\alpha, \beta \in S_n, \quad \alpha\beta = \beta\alpha.$

(b) If τ and σ are transpositions, then $\tau\sigma = \sigma\tau.$

(c) For all $\alpha, \beta \in S_n, \quad (\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}.$

(d) For all $\alpha, \beta \in S_n, \quad (\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}.$

Exercise 42 Let $\alpha, \beta, \gamma \in S_n.$

(a) Prove that if $\alpha\beta = \beta$, then $\alpha = \iota.$

(b) Prove that if $\alpha\beta = \alpha\gamma$, then $\beta = \gamma.$

Exercise 43 Write out the following products in cycle notation :

$$(1,2)(1,3), \quad (1,2)(1,3)(1,4), \quad (1,2)(1,3)(1,4)(1,5), \quad (1,2)(1,3)\cdots(1,n).$$

Exercise 44 Express each of the following permutations as products of transpositions :

$$(2,3,4), \quad (2,4,6,8), \quad (1,2)(3,4,5)(6,7,8,9), \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 8 & 3 & 1 & 5 & 7 & 4 & 2 \end{bmatrix}.$$

Exercise 45 For each of the permutations listed, write the permutation as a composition of transpositions, and then determine if the permutation is even or odd.

(a) $(1, 2, 3, 4, 5)$.

(b) $(1, 3)(2, 4, 5)$.

(c) $[(1, 3)(2, 4, 5)]^{-1}$.

(d) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{bmatrix}$.