# An Elementary Overview of Mathematical Structures

## Algebra, Topology and Categories

**Marco Grandis**

World Scientific

*Published by*

World Scientific Publishing Co. Pte. Ltd.
5 Toh Tuck Link, Singapore 596224
*USA office:* 27 Warren Street, Suite 401-402, Hackensack, NJ 07601
*UK office:* 57 Shelton Street, Covent Garden, London WC2H 9HE

Library of Congress Control Number: 2020032226

**British Library Cataloguing-in-Publication Data**
A catalogue record for this book is available from the British Library.

**AN ELEMENTARY OVERVIEW OF MATHEMATICAL STRUCTURES**
**Algebra, Topology and Categories**

ISBN 978-981-122-031-9 (hardcover)
ISBN 978-981-122-032-6 (ebook for institutions)
ISBN 978-981-122-033-3 (ebook for individuals)

For any available supplementary material, please visit
https://www.worldscientific.com/worldscibooks/10.1142/11828#t=suppl

Desk Editor: Soh Jing Wen

Printed in Singapore

# Contents

# Introduction

## 0.1 Structures in Mathematics

The focus of various sectors of Mathematics has shifted, in the last century, from equations to structures. The reader has likely encountered some of them, in Mathematics or related sciences.

*Algebra* denotes now the study of algebraic structures, like groups and fields, vector spaces, lattices and Boolean algebras: all these are sets equipped with some operations, satisfying some conditions.

*Topology* deals with the study of continuity, based on metric spaces, topological spaces, uniform spaces, etc. Algebro-topological structures, from topological groups to Banach and Hilbert spaces, are at the roots of Functional Analysis.

Furthermore, each of these structures has transformations that preserve the structure, like the *homomorphisms* of an algebraic structure or the *continuous mappings* of topological spaces. Collecting all the structures of a given type, with the appropriate transformations, we form a higher structure called a 'category'; for instance, the category $\mathsf{Gp}$ of all groups and their homomorphisms (with their composition law), or the category $\mathsf{Top}$ of all topological spaces and their continuous mappings.

*Categories* can now be investigated, along the same lines used for algebraic or topological structures; we arrive thus at a theory of mathematical structures.

## 0.2 A structural perspective

We want to present a general, elementary overview of these frameworks: the main algebraic structures in the first two chapters, then the main topological ones in Chapters 3 and 4, all of them organised in categories in Chapters 5 and 6.

In all these structures, the basic facts are *governed by universal properties* that follow and repeat the same pattern. Listing a few examples of the many cases dealt with, we have:

- the cartesian product of structures of the same kind (in 1.2.3, 1.3.4, 1.4.8, etc.),

- the free group on a set, or the free ring, or the free structure of a certain kind (in 1.6.3, 5.4.2, etc.),

- the field of fractions of an integral ring (in 2.2.4),

- the completion of a metric space (in 4.5.6),

- the Hausdorff space associated to a general topological space (in 6.5.1),

- the universal compactification of a topological space (in 6.6.5).

Loosely speaking, in each case we want to find the 'best solution' of a problem, with respect to the structures that we are considering and their transformations; this solution is determined up to 'isomorphism', i.e. an invertible transformation in the theory we are considering. Highlighting this fact should help the reader to have a better understanding of these constructions, and hopefully a deeper one.

A general formalisation of a universal property will be given within Category Theory, in Section 5.4, but the various instances we are interested in can be made precise from the start, as the reader can see in the examples listed above.

This perspective involves Category Theory itself: for instance, the cartesian product of categories (in 5.2.5) is governed by the same universal property as all cartesian products.

## 0.3 An inductive approach

This book draws on the author's experience, while teaching courses of Algebra, or Topology, or Category Theory, or Calculus.

Notions are presented in a concrete, 'inductive' way, starting from elementary examples. Then their theory is developed, with new examples and many exercises. Rich structures are often presented before the more general ones, formally simpler but didactically more abstract – in the same way as, in the historical construction of mathematics, the former often preceded the latter.

Whenever possible, the reader is guided to build the theory, through a series of exercises. The unfolding – and beauty – of mathematics combines and alternates 'natural parts', where everything seems to go on by itself, with sudden turns where new directions or unexpected results appear; the reader should learn to work out the natural developments, and to realise the power of real advances.

Each chapter and section has its own introduction; many references for further reading or study are given.

## 0.4 Borders and links

This book is reasonably self contained. We assume, from the beginning, the existence of the field $\mathbb{R}$ of real numbers, satisfying the axioms listed in Section 1.1; this framework, the heritage of centuries of thinking and research, is a source of inspiration and examples for our study of algebraic and topological structures.

Some basic issues of Set Theory are reviewed in Section 1.2. Hints at a foundational setting of Mathematics, where everything is constructed *ab ovo*, can be found in Subsection 4.6.7.

Calculus is not studied here. The basic transcendental functions – exponential and logarithm, sine and cosine – are only used in a marginal way, e.g. for linear groups and complex numbers.

However, the properties of continuous real functions are explored in Chapters 3 and 4. Limits of functions ‘at infinity’ are interpreted by compactifications of euclidean spaces, in Section 4.3.

Some unusual links with Calculus and Physics also appear in the first chapters on algebraic structures: for instance, the interpretation of a linear differential equation with constant coefficients as a linear equation, in a module of $C^\infty$-functions over a polynomial ring (in Subsection 2.6.8), or the interpretation of physical dimensions as elements of a vector space over the rational field, written in multiplicative notation (in Remark 2.3.6(b)).

## 0.5 Notation and conventions

Weak inclusion of sets is denoted by the symbol $\subset$, instead of the more usual $\subseteq$, which is not used here. General notation for number sets and other issues can be found at the beginning of Section 1.1.

A part marked with * is out of the main line of exposition. It may refer to issues dealt with further down, or be addressed to readers with some knowledge of the subject which is being analysed, or give references for higher topics.

Most exercises have a solution or convenient hints. These are deferred to the last chapter, or can be found below the exercise when they are important for the sequel. Easy exercises or exercises marked with * can be left to the reader.

## 0.6 Acknowledgements

I developed the approach to teaching mentioned above at my Department, beginning in a climate of discussion and experimentation which was alive in the late 1960's and the 1970's.

I inherited in part this approach from Gabriele Darbo, my professor and dear friend, together with my interest in Algebraic Topology, Homological Algebra and Category Theory.

I discussed the didactical solutions of this book with many colleagues, in particular with Ettore Carletti and Giacomo Caviglia, receiving helpful suggestions on its organisation.

I would also like to thank Dr Lim Swee Cheng, Ms Tan Rok Ting, and Ms Soh Jing Wen, at World Scientific Publishing Co., for their kind, effective help in the publication of this book, together with Mr Loo Chuan Min, the author of the cover.

Diagrams and figures are composed with 'xy-pic', by K.H. Rose and R. Moore – a free package.

# 1
# Algebraic structures, I

An algebraic structure is a set equipped with some operations satisfying some conditions – the axioms of the structure that we are considering.

A mapping $f\colon X \to Y$ between two structures of the same kind is called a 'homomorphism' when it preserves the operations of the structure, and an 'isomorphism' if – moreover – it is bijective. Then the inverse mapping is also a homomorphism, and the objects $X, Y$ have, essentially, the same structure.

The algebraic properties of the set $\mathbb{R}$ of real numbers, with respect to the main operations (addition and multiplication), are well known: properties of associativity, commutativity, distributivity, etc. We begin by listing them in Section 1.1, exploring their consequences, and how they can be extended to other set of numbers, or other sets.

All the main algebraic structures get out of this analysis, from groups to fields and vector spaces; they are explored in this chapter and the next. Some elementary points of Set Theory are reviewed in Section 1.2; we also need something about ordered sets, dealt with in Section 1.4.

Historically, group theory begins with Évariste Galois, in the 1830's, and Arthur Cayley in the 1850's. Vector spaces on the real field were formally introduced by Giuseppe Peano in 1888, as 'linear systems' [Pe].

The real development of the theory of groups and rings began in the first decades of the last century, under the impulsion of Emmy Noether.

Van der Waerden's 'Moderne Algebra', in 1940, was a milestone in this process: the book had many translations and augmented editions, as 'Modern Algebra', and later as 'Algebra' [Wa], in 1991. The dropping of 'Modern', in the title, reflects the fact that 'Algebra' denotes now – in Mathematics – the study of all algebraic structures: algebraic equations, the origins of this discipline, are just a part of it.

Serge Lang's [La2] is also a general textbook on this discipline. Books on the main algebraic structures will be cited in the appropriate section.

## 1.1 Introducing fields and vector spaces

The set $\mathbb{R}$ of real numbers contains the set $\mathbb{N}$ of natural numbers $0, 1, 2, ..., n, ...$ used to count the elements of a finite set. It also contains the set $\mathbb{Z}$ of all integers

$$... -2,\ -1,\ 0,\ 1,\ 2,\ ...$$

and the set $\mathbb{Q}$ of rational numbers, i.e. the quotients $h/k$ of two integers, with $k \neq 0$.

We write as $\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ the same sets without 0. The letter $n$ usually stands for a natural number; saying $n \geqslant 1$ we mean $n \in \mathbb{N}^*$.

The elementary construction of the set $\mathbb{C}$ of complex numbers will be dealt with in the first part of Section 2.7; it can also be read after the present section.

We use as of now some basic notation for sets, that will be reviewed in Section 1.2. Writing $A \subset X$ (or $X \supset A$) we mean that $A$ is a subset of $X$, and $X$ is a superset of $A$: in other words, every element of $A$ belongs to $X$; the sets can be equal.

If $A$ and $B$ are subsets of $X$, $A \cup B$ denotes their union and $A \cap B$ denotes their intersection, while $A \setminus B$ is the set of elements of $A$ which do not belong to $B$. The complement $X \setminus A$ is also written as $C_X A$.

The symbol $\{x_1, ..., x_n\}$ denotes the set formed by the elements of this list. In particular, the set $\{x\}$ has a unique element, and is called a *singleton*; we can write $\{*\}$ to avoid choosing a name for the element, when this is not relevant.

### *1.1.1 The real field and other fields*

The set $\mathbb{R}$ of real numbers, also called the *real line*, comes with two main operations, the addition, or sum, $x + y$ and the multiplication, or product, $x.y$ (often written as $xy$), which are defined for all $x, y \in \mathbb{R}$.

Their main properties can be listed as follows.

(A.1) (*Associativity of the sum*) For every $x, y, z \in \mathbb{R}$ we have: $x + (y + z) = (x + y) + z$.

The result of both procedures can be written as $x + y + z$. Similarly, a finite sum of real numbers $x_1 + x_2 + ... + x_n$ has a precise meaning.

(A.2) (*Identity of the sum*) There is a real number 0 such that, for all $x \in \mathbb{R}$: $0 + x = x = x + 0$.

This element is uniquely determined and called the *identity* of the sum. In fact, if $0'$ also satisfies the same relations, we deduce that: $0' = 0 + 0' = 0$ (using first the fact that 0 is an identity, and then the fact that $0'$ is also).

(A.3) (*Opposite element*) For every $x \in \mathbb{R}$ there is some $x' \in \mathbb{R}$ such that $x + x' = 0 = x' + x$.

This element is determined by $x$ and called the *opposite*, or *additive inverse*, of $x$; it is written as $-x$. In fact, if $x''$ also satisfies the same relations, we deduce that:

$$x' = 0 + x' = (x'' + x) + x' = x'' + (x + x') = x'' + 0 = x'',$$

using first the fact that 0 is an identity, then a property of $x''$, then associativity, then a property of $x'$, then again a property of 0.

(A.4) (*Commutativity of the sum*) For every $x$, $y \in \mathbb{R}$ we have: $x + y = y + x$.

The reader will note that, taking this into account, one could write (A.2) and (A.3) in a simplified form. We prefer to avoid this shortcut, for future developments where commutativity is not assumed.

(A.5) (*Associativity of the product*) For every $x, y, z \in \mathbb{R}$ we have: $x(yz) = (xy)z$.

Again, this allows us to write iterated products, like $xyz$ and $x_1x_2 \ldots x_n$, without parentheses.

(A.6) (*Distributivity of the product over the sum*) For every $x, y, z \in \mathbb{R}$ we have:

$$x(y + z) = xy + xz, \qquad (x + y)z = xz + yz.$$

As usual, it is understood that $xy + xz$ means $(xy) + (xz)$: by default, a product has priority over a sum.

(A.7) (*Identity of the product*) There is a real number 1 such that, for all $x \in \mathbb{R}$: $1.x = x = x.1$.

This element is uniquely determined and called the *identity* of the product, or also the *unit* of $\mathbb{R}$. The proof is the same as in (A.2), changing notation from sum to product: if $1'$ satisfies the same relations, we deduce that: $1' = 1.1' = 1$.

(A.8) (*Commutativity of the product*) For every $x, y \in \mathbb{R}$ we have: $xy = yx$.

Also here we could simplify the other axioms using this property; but we do not.

(A.9) (*Inverse element*) $1 \neq 0$, and for every $x \neq 0$ there is some $y$ such that $xy = 1 = yx$.

This element $y$ is determined by $x$; it is written as $x^{-1}$ and called the *inverse* of $x$. The proof is the same as in (A.3), changing sum to product. The property $1 \neq 0$ cannot be deduced from the others, as the 'null ring' will show, below.

More generally, a set $K$ equipped with two operations satisfying the previous properties is called a *field*. The properties (A.1–9) are called *the axioms of fields*. The set of real numbers, equipped with its sum and multiplication, is called the *real field*.

The set $\mathbb{Q}$ of rational numbers is also a field, with the same operations of real numbers (restricted to $\mathbb{Q}$): see Exercise 1.1.3(i). It is called the *rational field.*

*The field $\mathbb{C}$ of *complex numbers* is constructed in Section 2.7.*

### *1.1.2 The ring of integers and other rings*

The set of integers $\mathbb{Z}$, with its addition and multiplication, satisfies all the axioms above, except (A.9); it is called the *ring of integers.*

More generally, a set $R$ equipped with two operations that satisfy the axioms (A.1–6) is called a *ring.* It is a *unital ring* if also (A.7) holds true, and a *commutative ring* if (A.8) is satisfied.

$\mathbb{Z}$ is thus a commutative unital ring, and is not a field. Rings of square matrices will give examples of unital rings that are not commutative, in Section 2.6. (Note that, in a ring, the addition is always assumed to be commutative.)

The singleton $\{0\}$, with the operation $0 + 0 = 0 = 0.0$ (the only possible one), is a commutative unital ring, called the *trivial ring*, or the *null ring.* Note that the additive and multiplicative identities coincide – the only point of the axioms of fields that is not satisfied here. (The name of the unique element is of no relevance.)

In a unital ring $R$, an element $x$ is said to be *invertible* if there is some $y \in R$ such that $xy = 1 = yx$. Then $y$ is determined by $x$, and written as $x^{-1}$. These elements form the set $\mathrm{Inv}(R)$, analysed in Exercise 1.1.3(f) below.

For instance, $\mathrm{Inv}(\mathbb{Z}) = \{-1, 1\}$. In a ring, the set $R \setminus \{0\}$ is often written as $R^*$; thus, a non-trivial commutative unital ring $R$ is a field if and only if $\mathrm{Inv}(R) = R^*$.

### *1.1.3 Exercises and complements*

For a beginner, it is important to understand how the axioms (A.1–9) are indeed the foundation of our use of the basic operations of real numbers.

This can be done with the following exercises, stated for a ring $R$, under additional hypotheses when it is the case; all of them hold for a field. Solutions can be found below.

(a) In a ring $R$ we have:

$$-0 = 0, \qquad -(-x) = x, \qquad -(x + y) = (-x) + (-y). \tag{1.1}$$

(b) (*Cancellation law of the sum*) In a ring $R$, from $x + y = x + z$ it follows that $y = z$.

(c) For every $x \in R$ we have: $x.0 = 0 = 0.x$. A unital ring where $0 = 1$ is trivial (a singleton). A unital ring where 0 is invertible is trivial.

(d) For every $x, y \in R$ we have:

$$x.(-y) = -\,xy = (-x).y, \qquad (-x).(-y) = xy. \tag{1.2}$$

(e) One defines the *difference* $x - y = x + (-y)$. Prove that the product distributes over this 'derived' operation.

(f) If $R$ is unital, the set $\mathrm{Inv}(R)$ of invertible elements contains the unit 1. If $x$ and $y$ are invertible, also $x^{-1}$ and $xy$ are, and

$$1^{-1} = 1, \qquad (x^{-1})^{-1} = x, \qquad (xy)^{-1} = y^{-1}.x^{-1}. \tag{1.3}$$

Therefore the set $\mathrm{Inv}(R)$ inherits a multiplication from the ring; this operation is associative, has an identity (the unit of the ring), and every element has an inverse. *(This will be expressed saying that $\mathrm{Inv}(R)$ is a group.)*

(g) (*Cancellation laws of the product*) If $x \in \mathrm{Inv}(R)$, from $xy = xz$ it follows that $y = z$. Similarly, if $yx = zx$ then $y = z$.

Thus, in a field, this multiplicative cancellation holds for the elements $x \neq 0$. The same is true in any ring which is contained in a field, with the 'same' operations, like $\mathbb{Z} \subset \mathbb{Q}$. (But we will see rings where there exist elements $x, y \neq 0$ with $xy = 0$.)

(h) In a field $K$ one defines the *quotient* $x/y = x.y^{-1}$, provided that $y \neq 0$. Prove that $(xz)/(yz) = x/y$, if $y, z \neq 0$.

(i) The set $\mathbb{Q}$ of rational numbers inherits from $\mathbb{R}$ the structure of a field.

(j) A field can be finite: for instance, one can form a field $\mathbb{F}_2 = \{0, 1\}$ consisting of two distinct elements, which can be viewed as 'even' and 'odd'.

*Solutions.* (a) Obviously 0 is the opposite of itself, $x$ is the opposite of $-x$, and $(-x)+(-y)$ is the opposite of $x + y$. Let us note that, without the commutativity of the sum, in (A.4), we should compute the opposite of $x + y$ as $(-y) + (-x)$.

(b) Add $-x$ to each member of the equation.

(c) We have: $x.0+0 = x.0 = x.(0+0) = x.0+x.0$; cancelling $x.0$ we get $0 = x.0$.

(d) We have: $x.y + x.(-y) = x(y + (-y)) = x.0 = 0$, which means that $x.(-y)$ is the opposite of $xy$. The rest is an obvious consequence.

(e) Applying previous results, we have:

$$x(y - z) = x(y + (-z)) = xy + x(-z) = xy + (-xz) = xy - xz,$$

and symmetrically.

(f) As in (a); here the product is not assumed to be commutative.

(g) One multiplies by $x^{-1}$, at the left or the right.

(h) In fact $(xz)/(yz) = x.z.y^{-1}.z^{-1} = x.y^{-1}$.

(i) The rational numbers are 'stable' in $\mathbb{R}$ under sum, product and all the derived items considered in properties (A.1–9), as shown by the following well-known formulas of the 'calculus of fractions', for $a, b, c, d \in \mathbb{Z}$ and $b, d \neq 0$

$$\begin{aligned} a/b + c/d &= (ad + bc)/(bd), \qquad & 0 &= 0/1, \qquad & -(a/b) &= (-a)/b, \\ (a/b).(c/d) &= (ac)/(bd), & 1 &= 1/1, & (b/d)^{-1} &= d/b. \end{aligned}$$

(j) Following the interpretation of the elements $0, 1$ as 'even' and 'odd', we define the operations in $\mathbb{F}_2$ as:

$$\begin{aligned} 0 + 0 = 1 + 1 &= 0, \qquad & 0 + 1 = 1 + 0 &= 1, \\ 0.0 = 0.1 = 1.0 &= 0, & 1.1 &= 1. \end{aligned}$$

(Note that, here, $1 + 1$ is not defined as in $\mathbb{Z}$ and $\mathbb{R}$.)

These operations satisfy the axioms of fields. A direct proof, here, would be tiresome and of little interest: the reader can wait until this result will follow from a general construction, that will give a finite field having any prime number $p$ of elements (in 2.1.6(c)).

### *1.1.4 Subrings and subfields*

A *subring* of a ring $R$ is a subset $R'$ that satisfies the following conditions:

(i) if $x, y \in R'$ then $x + y \in R'$,

(ii) $0 \in R'$,

(iii) if $x \in R'$ then $-x \in R'$,

(iv) if $x, y \in R'$ then $xy \in R'$.

Among them we always have the *null* subring $\{0\}$ and the *total* subring $R$. A subring of a ring is a ring, with the restricted operations.

For a unital ring, a *unital subring* is assumed to contain the unit of the ring.

In a field $K$, a *subfield* $K'$ of $K$ is a unital subring that also satisfies

(v) if $x \in K'$ and $x \neq 0$, then $x^{-1} \in K'$.

A subfield of a field is a field. $\mathbb{Q}$ is a subfield of $\mathbb{R}$, while $\mathbb{Z}$ is a unital subring of both, but not a subfield.

A subring or subfield is said to be *proper* if it is not the total one.

*Exercises and complements.* The solutions can be found in Section 7.1.

(a) Prove that, in the definition of a subring, conditions (ii) and (iii) cannot be left out.

(b) The set $2\mathbb{Z}$ of all even integers forms a non-unital subring of $\mathbb{Z}$. There are infinitely many others. The only unital subring of $\mathbb{Z}$ is the total one.

(c) The rational field $\mathbb{Q}$ has no proper subfields. Any subfield of $\mathbb{R}$ contains $\mathbb{Q}$, that is called the *minimal subfield* of $\mathbb{R}$. (This topic will be developed in 2.2.1.)

### 1.1.5 Homomorphisms of rings

Let $R, S$ be rings. A mapping $f\colon R \to S$ is said to be a *homomorphism* (of rings) if it preserves sum and multiplication, in the sense that, for all $x, y \in R$

(i) $f(x+y) = f(x) + f(y)$,

(ii) $f(xy) = f(x).f(y)$.

One can write

$$f(x +_R y) = f(x) +_S f(y), \qquad f(x \cdot_R y) = f(x) \cdot_S f(y),$$

to distinguish the operations of our rings. This is only done when useful.

The homomorphism $f$ also preserves the identity of the sum and all opposites.

In fact $f(0_R) = 0_S$, as follows from $f(0) = f(0+0) = f(0) + f(0)$, cancelling $f(0)$ in $S$. Moreover, for $x \in R$, $f(x) + f(-x) = f(x-x) = f(0) = 0$.

The identity mapping $R \to R$ of a ring is a homomorphism, written as $\mathrm{id}\,R$. Given two consecutive homomorphisms $f\colon R \to S$ and $g\colon S \to T$, the composed mapping $gf\colon R \to T$ is a homomorphism: it takes any $x \in R$ to the element $g(f(x))$ of $T$. It will also be written as $g.f$, when useful.

This *partial composition law* is associative (whenever legitimate): given a third consecutive homomorphism $h\colon T \to U$, we have

$$h(gf) = (hg)f,$$

as both composites take any $x \in R$ to the element $h(g(f(x)))$ of $U$. Moreover, an identity homomorphism acts as an identity, for every legitimate composition: for a homomorphism $f\colon R \to S$ we have

$$f.(\mathrm{id}\,R) = f = (\mathrm{id}\,S).f. \tag{1.4}$$

If $R'$ is a subring of $R$, the inclusion $R' \to R$ is a homomorphism. We have already considered some of them

$$\{0\} \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R}. \tag{1.5}$$

An *isomorphism* $f\colon R \to S$ of rings is a homomorphism that has an inverse: there is a homomorphism $g\colon S \to R$ such that $gf = \mathrm{id}\,R$ and $fg = \mathrm{id}\,S$. This is equivalent to saying that the homomorphism $f$ is bijective, i.e. injective and surjective, and $g$ is the inverse mapping (see Exercise 1.1.6(c)).

When this is the case, we say that the rings $R$ and $S$ are *isomorphic*, and write $R \cong S$. The inverse homomorphism is written as $f^{-1}$.

### *1.1.6 Exercises and complements*

The following properties are important; their proof can be found below.

(a) For all rings $R, S$ the constant mapping $R \to S$ at $0_S$ is a homomorphism, called the null homomorphism. If $R, S$ are unital rings, a *unital homomorphism* $f\colon R \to S$, or *homomorphism of unital rings*, is a homomorphism that preserves the unit (and can only be null when $S$ is the null ring). If $K$ is a field, there are no unital homomorphisms $K \to \mathbb{Z}$.

(b) Given two fields $K$ and $K'$, a *homomorphism* (of fields) $f\colon K \to K'$ is defined as a homomorphism of unital rings. Prove that it preserves all inverses, and that it is necessarily injective.

(c) An isomorphism $f\colon R \to S$ is bijective. Conversely, if $f\colon R \to S$ is a bijective homomorphism of rings, the inverse mapping is a homomorphism. The same holds for homomorphisms of unital rings.

(d) Isomorphism is an equivalence relation between rings.

(e) An isomorphism $f\colon R \to S$ of rings, between unital rings, is necessarily unital; more generally, this holds for every surjective homomorphism of rings whose domain is a unital ring.

*Solutions.* (a) The first point is obvious. If $f\colon K \to \mathbb{Z}$ is a unital homomorphism, $f(1_K + 1_K) = 2$, therefore $1_K + 1_K \neq 0_K$, and 2 should be invertible in $\mathbb{Z}$.

(b) First, if $x \neq 0$ in $K$, then $f(x).f(x^{-1}) = f(x.x^{-1}) = f(1) = 1$. Secondly, suppose that $x, y \in K$ and $f(x) = f(y)$. Therefore $f(x - y) = 0$ is not invertible in $K'$, and $x - y = 0$, which means that $x = y$.

(c) The inverse mapping $g$ is also a homomorphism, as we can cancel $f$ in the following equalities

$$f(g(x) + g(y)) = f(g(x)) + f(g(y)) = x + y = f(g(x + y)),$$
$$f(g(x).g(y)) = f(g(x)).f(g(y)) = x.y = f(g(x.y)).$$

In the unital case one cancels $f$ in: $f(g(1_S)) = 1_S = f(1_R)$.

(d) Reflexivity comes from the identity mapping $\mathrm{id}\, R$ of any ring. Symmetry follows from the definition, and transitivity from composing two consecutive isomorphisms.

In fact, the composite $gf$ of two consecutive isomorphisms $f\colon R \to S$ and $g\colon S \to T$ is an isomorphism, with inverse $f^{-1}.g^{-1}\colon T \to R$.

(e) Plainly, the element $f(1_R)$ is a unit for every element $f(x)$ of $S$.

### *1.1.7 Vector spaces on a field*

The reader likely knows that many physical quantities – like velocity, acceleration, force – are expressed by a vector. Vectors can be added and multiplied by real numbers, forming a ‘vector space’, an algebraic structure which appears everywhere in Mathematics and Physics.

We begin by an important instance, likely known in some form to the reader: the set $F(T, \mathbb{R})$ of all functions $f\colon T \to \mathbb{R}$ defined on a set $T$, with values in the real field.

This set has two basic operations (for $f, g \in F(T, \mathbb{R})$ and $\lambda \in \mathbb{R}$):

$$\begin{gathered}(f+g)(t) = f(t) + g(t),\\ (\lambda f)(t) = \lambda.f(t).\end{gathered} \tag{1.6}$$

The first operation acts on two functions $f, g\colon T \to \mathbb{R}$, yielding their *sum* $f + g$; this is computed pointwise, at each $t \in T$, by a sum $f(t) + g(t)$ of real numbers. The second operation acts on a number $\lambda \in \mathbb{R}$ and a function $f\colon T \to \mathbb{R}$, yielding their *scalar multiplication* $\lambda f$ (also written as $\lambda.f$); again, this is computed pointwise, by products $\lambda.f(t)$ in $\mathbb{R}$.

In this context a function $f \in F(T, \mathbb{R})$ is called a *vector*, a number $\lambda \in \mathbb{R}$ is called a *scalar* and the set $F(T, \mathbb{R})$ is called a *vector space*, or a *linear space*, on the real field.

More generally, we can replace the real field with any field $K$. A *vector space on the field $K$* is a set $X$ equipped with two operations: the *sum* $x + y$ (for $x, y \in X$) and the *scalar multiplication* $\lambda x$ (for $x \in X$ and $\lambda \in K$). In both cases the result is an element of $X$; these elements are called *vectors*, while the elements of $K$ are called *scalars*. The following axioms must be satisfied.

(VS.1) (*Associativity of the sum*) For every $x, y, z \in X$ we have: $x + (y + z) = (x + y) + z$.

(VS.2) (*Identity of the sum*) There is a vector $0 \in X$ such that, for all $x \in X$: $0 + x = x = x + 0$.

(VS.3) (*Opposite element*) For every $x \in X$ there is some $x' \in X$ such that $x + x' = 0 = x' + x$.

(VS.4) (*Commutativity of the sum*) For every $x, y \in X$ we have: $x + y = y + x$.

(VS.5) (*Distributive property, I*) For every $x, y \in X$ and $\lambda \in K$ we have: $\lambda(x + y) = \lambda x + \lambda y$.

(VS.6) (*Distributive property, II*) For every $x \in X$ and $\lambda, \mu \in K$ we have: $(\lambda + \mu).x = \lambda x + \mu x$.

(VS.7) (*Compatibility*) For every $x \in X$ and $\lambda, \mu \in K$ we have: $(\lambda\mu).x = \lambda.(\mu x)$.

(VS.8) (*Unitarity*) For every $x \in X$ we have: $1.x = x$.

The reader will note that the axioms (VS.1–4) coincide with the axioms

(A.1–4), for the sum in a field. (In both cases, as we will see in Section 1.3, we are saying that our structure is a *commutative group*, with respect to the sum.) Also here the *null vector* 0 is uniquely determined; the vector opposite to a vector $x$ is determined by the latter, and written as $-x$; the cancellation law of the sum holds true.

The axioms (VS.5) and (VS.6) are distributive properties of the scalar multiplication, with respect to the sum of vectors or scalars. Usually the context is sufficient to distinguish the null vector from the null scalar; otherwise, the null vector can be written as $\underline{0}$, or $0_X$.

(In Physics and Mathematical Physics, vectors are often distinguished by special characters, either underlined, or boldface, or marked with an arrow.)

The structure of vector spaces will be studied in Section 2.3, but a reader can find attractive (and certainly useful) to explore as of now their notions of homomorphism, isomorphism and substructure, with respect to a fixed field of scalars.

*Exercises and complements.* (a) For every set $T$, the set $F(T, \mathbb{R})$ equipped with the operations defined above is indeed a real vector space. More generally, any field $K$ gives a vector space $F(T, K)$ of functions $f\colon T \to K$. *(There is also a pointwise product of functions $(fg)(t) = f(t).g(t)$, which makes $F(T, \mathbb{R})$ into a $K$-*algebra*, see 2.5.1.)*

(b) A singleton $\{x\}$ has a unique structure of vector space on $K$, with $x + x = x$ and $\lambda x = x$. We have thus the *trivial*, or *null*, vector space on the field $K$, often written as $\{0\}$.

The vector space $F(T, K)$ is trivial when $T = \emptyset$: it has one element, the unique mapping $\emptyset \to K$ (see 1.2.1).

(c) For a positive integer $n$, the set $K^n = K \times ... \times K$ of $n$-tuples $x = (x_1, ..., x_n)$ of elements of $K$ is a vector space on the field $K$, with the following operations

$$\begin{gathered}(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n), \\ \lambda(x_1, ..., x_n) = (\lambda x_1, ..., \lambda x_n).\end{gathered} \tag{1.7}$$

For $n = 1$ we get the set $K$ as a vector space on itself.

In particular, $\mathbb{R}^n$ is a vector space on the real field $\mathbb{R}$, formed of all the $n$-tuples $x = (x_1, ..., x_n)$ of real numbers. We assume that the reader is familiar with the representation of $\mathbb{R}$ as a line, of $\mathbb{R}^2$ as a plane and $\mathbb{R}^3$ as the three-dimensional space (after a system of cartesian coordinates is fixed in each of these geometrical structures).

(d) For the finite set $T = \{1, ..., n\}$, the vector space $F(T, K)$ can be identified with $K^n$.

(e) For every vector $x$ in a vector space $X$ we have: $0.x = \underline{0}$ and $(-1).x = -x$.

(f) (*Cancellation law of the scalar multiplication*) If $\lambda \neq 0$, from $\lambda x = \lambda y$ it follows that $x = y$.

(g) An expression $\lambda x + \mu y$ is called a *linear combination of the vectors* $x, y$ *with scalar coefficients* $\lambda, \mu$. More generally we have linear combinations

$$\textstyle\sum_i \lambda_i x_i = \lambda_1 x_1 + ... + \lambda_n x_n \qquad (\lambda_i \in K,\ x_i \in X). \tag{1.8}$$

### 1.1.8 The natural order of the real field

We come back to examining the set $\mathbb{R}$ of real numbers. After addition and sum, governed by the axioms (A.1–9), in 1.1.1, the set $\mathbb{R}$ is equipped with a binary relation $x \leqslant y$, called the *natural order of real numbers.*

The main new properties are listed below, as (A.10–16).

(A.10) (*Reflexivity*) For every $x \in \mathbb{R}$ we have: $x \leqslant x$.

(A.11) (*Transitivity*) For every $x, y, z \in \mathbb{R}$, if $x \leqslant y$ and $y \leqslant z$ then $x \leqslant z$.

(A.12) (*Anti-symmetry*) For every $x, y \in \mathbb{R}$, if $x \leqslant y$ and $y \leqslant x$ then $x = y$.

(A.13) (*Totality*) For every $x, y \in \mathbb{R}$ we have $x \leqslant y$ or $y \leqslant x$.

This group of axioms only deals with the order relation; it says that $\mathbb{R}$, equipped with the relation $x \leqslant y$, is a *totally ordered set.* The relation $x \leqslant y$ is also written as $y \geqslant x$, while $x < y$ (and $y > x$) means that $x \leqslant y$ and $x \neq y$.

One can rewrite the axioms (A.10–15) using the relation $x < y$ (see Exercise 1.1.9(a)), but this is not convenient in the general theory of ordered sets.

(A.14) (*Addition and order*) For every $x, y, z \in \mathbb{R}$, if $x \leqslant y$ then $x + z \leqslant y + z$.

(A.15) (*Multiplication and order*) For every $x, y, z \in \mathbb{R}$, if $x \leqslant y$ and $z \geqslant 0$ then $xz \leqslant yz$.

These two axioms state the compatibility of the order relation with the main operations. Globally, the axioms (A.1–15) say that $\mathbb{R}$, equipped with addition, multiplication and order, is a *totally ordered field.* Note that we have written the compatibility conditions (A.14–15) in a form that takes advantage of the commutativity of both operations.

The rational field $\mathbb{Q}$, with the natural order, is also a totally ordered field.

(A.16) (*Completeness*) Every subset $A$ of $\mathbb{R}$ which is non-empty and *upper bounded* has a *least upper bound*, written as $\sup A$.

Now, the axioms (A.1–16) say that $\mathbb{R}$ is a *complete totally ordered field.* We will see that this list of axioms determines the real field, up to isomorphism, i.e. up to a bijection that preserves addition, multiplication and order (see 2.2.7).

To make sense of the last axiom, we examine now various notions for a subset $A$ of $\mathbb{R}$, related to the ordering. We take advantage of the reversion symmetry $r(x) = -x$, which reverses the order of $\mathbb{R}$ (by Exercise 1.1.9(b)); the image of $A$ under this symmetry is written as:

$$-A = \{-x \mid x \in A\} = \{x \in \mathbb{R} \mid -x \in A\}. \qquad (1.9)$$

The subset $A$ is said to be *upper bounded* if it has an upper bound in $\mathbb{R}$, i.e. there is some $k \in \mathbb{R}$ such that $x \leqslant k$, for all $x \in A$. Symmetrically, $A$ is said to be *lower bounded* if there is some lower bound $h \in \mathbb{R}$, with $h \leqslant x$ for all $x \in A$; it is said to be *bounded* if it satisfies both conditions. Plainly, $A$ is lower bounded if and only if $-A$ is upper bounded.

We write as $\max A$ the *greatest element*, or *maximum*, of $A$, if it exists: it is a real number $a$ such that:

$$a \in A, \qquad \text{for every } x \in A,\ x \leqslant a. \tag{1.10}$$

It is uniquely determined, because of the anti-symmetry property of the order. Symmetrically, $\min A$ denotes the *least element*, or *minimum*, of $A$, if it exists; then $-\min A = \max(-A)$.

We write as $\sup A$ the *least upper bound* of $A$, if it exists

$$\sup A = \min \{k \in \mathbb{R} \mid \text{for every } x \in A,\ x \leqslant k\}. \tag{1.11}$$

It is characterised as the real number $\alpha$ such that:

(i) for every $x \in A$, $x \leqslant \alpha$,

(ii) if $k \in \mathbb{R}$ and for every $x \in A$, $x \leqslant k$, then $\alpha \leqslant k$.

Plainly, $A$ has a maximum if and only if the supremum of $A$ exists and belongs to $A$; then $\max A = \sup A$.

Symmetrically, we write as $\inf A$ the *greatest lower bound* of $A$, if it exists; then $-\inf A = \sup(-A)$. The completeness axiom is equivalent to saying that every subset of $\mathbb{R}$ which is non-empty and lower bounded has a greatest lower bound.

### *1.1.9 Exercises and complements*

(a) Write a set of axioms for the relation $x < y$, equivalent to the previous (A.10–15).

(b) Consider the *reversion symmetry* $r \colon \mathbb{R} \to \mathbb{R}$ defined by $r(x) = -x$, and note that this mapping is *involutive*, i.e. inverse to itself: $rr = \mathrm{id}\,\mathbb{R}$ (and therefore bijective).

Prove that $r$ reverses the order relation: if $x \leqslant y$ then $-x \geqslant -y$. Prove also that $x \leqslant y$ and $z \leqslant 0$ imply $xz \geqslant yz$.

(c) Prove that $x^2 \geqslant 0$, for every $x \in \mathbb{R}$; this implies that $0 < 1$ (an 'obvious' fact, but also a consequence of the axioms) and $x < x + 1$, for every $x$.

(d) (*Modulus*) The *modulus*, or *absolute value*, of the real number $x$ is defined as:

$$|x| = x, \text{ for } x \geqslant 0, \qquad |x| = -x, \text{ for } x \leqslant 0, \tag{1.12}$$

so that, for every $x \in \mathbb{R}$, $|x| \geqslant 0$, and $|x| = 0$ if and only if $x = 0$. Note that $x \leqslant |x|$, $|-x| = |x|$ and $|x|^2 = x^2$. There are other important properties, for $x, y, z \in \mathbb{R}$

$$\begin{aligned} |x+y| &\leqslant |x|+|y| && (\textit{subadditive property}), \\ |xy| &= |x|.|y| && (\textit{multiplicative property}), \\ |x-y|+|y-z| &\geqslant |x-z| && (\textit{triangle inequality}). \end{aligned} \tag{1.13}$$

(e) For the empty subset, every real number is (trivially) a lower and upper bound; there is no inf nor sup. The total subset has no lower nor upper bound in $\mathbb{R}$. The subset $A = \{x \in \mathbb{R} \mid x > 0\}$ of all positive real numbers has $\inf A = 0$, no minimum and no upper bound.

(f) (*The integral part*) Every $x \in \mathbb{R}$ has an *integral part* in $\mathbb{Z}$

$$[x] = \max\{k \in \mathbb{Z} \mid k \leqslant x\}, \tag{1.14}$$

that satisfies the following inequalities

$$[x] \leqslant x < [x] + 1. \tag{1.15}$$

In particular, for every $x \in \mathbb{R}$, there is an integer $> x$.

## 1.2 Sets and algebraic structures

Mathematics is built with some *primitive* items: these are not defined but their use has to respect some rules. At an informal level, these primitive terms have a concrete meaning, which guides our use.

The foundation commonly used is Set Theory. Here we only give a brief, informal review of some basic notions about sets, that will be used throughout the book. This approach will necessarily leave some points undefined, without affecting our use.

Formal Set Theory is a complex subject, outside of our scopes. An interested reader is referred to [Ha, Kap, Je, Fk]; the first two books are more elementary.

### *1.2.0 Sets and elements*

We think of a *set* $X$ as a 'collection of elements'. The expression $x \in X$ is read as $x$ *is an element of* $X$, or $x$ *belongs to* $X$, or $x$ *is in* $X$.

The sets $X, Y$ are *equal* (written as $X = Y$) if and only if they have the same elements.

The relation $X \subset Y$, read as $X$ *is contained in* $Y$, or $X$ *is a subset of* $Y$, means that every element of $X$ also belongs to $Y$. Equivalently we write

$Y \supset X$, read as $Y$ *contains* $X$, or $Y$ *is a superset of* $X$. Thus $X = Y$ is equivalent to the conjunction: $X \subset Y$ and $Y \subset X$.

$X$ is a *proper subset* of $Y$ if $X \subset Y$ and $X \neq Y$, a derived notion of marginal importance.

The *empty set* $\emptyset$ is defined by having no elements, and is contained in any set. A *singleton* $\{x\}$ is defined by having a unique element, namely $x$. One writes as $\{x_1, x_2, ..., x_n\}$ the set whose elements are specified in the list (and nothing else).

Curly brackets are also used to denote the subset of a set formed by the elements satisfying a certain property, as in the following examples:

$$\{x \in \mathbb{N} \mid x^2 = x\} = \{0, 1\}, \qquad \{x \in \mathbb{N} \mid x \text{ is even}\}. \tag{1.16}$$

*Remarks.* (a) Different letters or symbols can denote the same thing. Thus, if $n \geqslant 1$, the set $\{x_1, x_2, ..., x_n\}$ has at least one element and at most $n$; it has precisely $n$ elements if and only if all $x_i$ are different. Even when we speak of "*two elements* $x, y$", the common use in mathematics does not assume that they are different: this should be explicitly said, if needed.

(b) The expression "$x$ *is an element of* $X$" is a relation between sets, and does not mean that $x$ has a different status. This relation is subject to various axioms, which imply that $x \in x$ cannot happen. It is also well known that one cannot form 'the set of all sets'.

(c) The procedure exemplified in (1.16) describes *a subset of a given set*. The reader probably knows that an illegitimate use, like $S = \{x \mid x \notin x\}$ leads to a contradiction, *Russell's paradox*: $S \in S$ implies $S \notin S$, and conversely.

An expression $\{x \mid p(x)\}$, where $p(x)$ is some property in the variable $x$, is only acceptable when we are leaving understood that $x$ is required to belong to some set, specified by the context.

### 1.2.1 Mappings and cardinals

A *mapping* $f \colon X \to Y$ *from the set* $X$ *to the set* $Y$ is defined by a formula $f(x)$ that transforms every element $x$ of the set $X$ into a unique element $f(x)$ of the set $Y$, read as "$f$ of $x$". The notation $x \mapsto f(x)$ denotes the action of $f$ on an element of $X$.

The mapping $f$ is said to be defined on $X = \operatorname{Dom} f$, the *domain* of $f$, and to take values in $Y = \operatorname{Cod} f$, the *codomain* of $f$. All the mappings $X \to Y$ are elements of a set, written as $\operatorname{Map}(X, Y)$, or also as $Y^X$ (a 'cartesian power': see (1.30)).

We also speak of a *function* $f \colon X \to Y$; this term is commonly used when the codomain $Y$ is the real field, as in 1.1.7, where the set $\operatorname{Map}(T, \mathbb{R})$ is written as $F(T, \mathbb{R})$.

Given two *consecutive mappings* $f \colon X \to Y$ and $g \colon Y \to Z$ (where the codomain of $f$ coincides with the domain of $g$), the *composed mapping* is written as $gf$, or $g.f$, and defined as:

$$gf\colon X \to Z, \qquad (gf)(x) = g(f(x)) \qquad\qquad (\text{for } x \in X). \tag{1.17}$$

Composition is associative (when legitimate): given a third mapping $h\colon Z \to T$ we have: $h(gf) = (hg)f$. Moreover, every set $X$ has an *identity mapping*, written as $\mathrm{id}\, X$ or $1_X$

$$\mathrm{id}\, X\colon X \to X, \qquad (\mathrm{id}\, X)(x) = x \qquad\qquad (\text{for } x \in X), \tag{1.18}$$

which acts as an identity for legitimate compositions: $f.(\mathrm{id}\, X) = f$ and $(\mathrm{id}\, Y).f = f$, for $f\colon X \to Y$.

A mapping $f\colon X \to Y$ is *injective* if, for all $x, x' \in X$, the relation $f(x) = f(x')$ implies $x = x'$. It is *surjective* if, for every $y \in X$, there exists some $x \in X$ such that $f(x) = y$.

The mapping $f\colon X \to Y$ is *bijective*, or a *bijection*, or a *bijective correspondence*, if it is injective and surjective; equivalently, this means that for every $y \in X$ there exists a unique $x \in X$ such that $f(x) = y$. We can then construct a mapping $g\colon Y \to X$, backwards, letting

$$g(y) = x \;\text{ if and only if }\; f(x) = y \qquad (\text{for } y \in Y,\ x \in X), \tag{1.19}$$

and we say that the sets X, Y are *equipotent*.

A mapping $f\colon X \to Y$ is *invertible* if there is a mapping $g\colon Y \to X$ such that $gf = \mathrm{id}\, X$ and $fg = \mathrm{id}\, Y$. Plainly, this is the case if and only if $f$ is bijective. The inverse function $g$, constructed as in (1.19), is determined by $f$, and can be written as $f^{-1}$.

An *indexed family* $x = (x_i)_{i \in I}$ of elements of $X$ is a mapping $x\colon I \to X$, written in *index notation*; the domain $I$ is then called *the set of indices* of the family.

For each set $X$ there is a unique mapping $\emptyset \to X$, and therefore a unique *empty family* $(x_i)_{i \in \emptyset}$ of elements of $X$.

For a finite set, $\sharp X$ will denote the (natural) number of its elements. More generally, each set $X$ has an equipotent *cardinal set* $\sharp X$, and two sets $X, Y$ have the same cardinal if and only if there exists a bijection $X \to Y$. The smallest infinite cardinal is $\aleph_0 = \sharp\mathbb{N}$, read as 'aleph-zero'. (Something more on cardinals will be said in Subsection 1.7.8.)

Plainly, a subset of a finite set $X$ with the same cardinal must be the total one. The reader may know that this fact is no longer true for an infinite set $X$: see Exercise (e) below.

*Exercises and complements.* (a) (*Commutative diagrams*) Mappings between sets (or structured sets) can be represented by vertices and arrows in a *diagram*, as in the examples below, to make evident their relationship and which compositions are legitimate

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "h"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"'] \arrow[dr, "d"] & B \arrow[d, "k"] \\ C \arrow[r, "g"'] & D \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, shift left, "u"] & Y \arrow[l, shift left, "v"] \end{tikzcd} \tag{1.20}$$

As an important property, we say that such a diagram is *commutative* if:

- whenever we have two 'paths' of consecutive arrows, from a certain object to another, the two composed mappings are the same,

- whenever we have a 'loop' of consecutive arrows, from an object to itself, then the composed mapping is the identity of that object.

Thus, the first diagram above is commutative if and only if $gf = h$. For the second, commutativity means that $kf = d = gh$. For the third, it means that $vu = \mathrm{id}\, X$ and $uv = \mathrm{id}\, Y$ (so that these mappings are inverse to each other).

(b) If $X$ and $Y$ are finite sets, with $m$ and $n$ elements, then the set $Y^X = \mathrm{Map}(X, Y)$ has $n^m$ elements.

(c) In particular, for $X = \emptyset$, the set $Y^\emptyset = \mathrm{Map}(\emptyset, Y)$ is a singleton (also when $Y = \emptyset$), and $n^0 = 1$. *In the context of natural numbers*, $0^0$ is defined and equal to 1. (The reader likely knows that, in the context of real numbers, the expression $0^0$ is preferably left undefined.)

(d) For consecutive mappings $f\colon X \to Y$ and $g\colon Y \to Z$

- if $f$ and $g$ are injective (resp. surjective, bijective), so is the composed mapping $gf$,
- if $gf$ is injective, then $f$ is also; if $gf$ is surjective, then $g$ is also.

(e) The set $2\mathbb{N}$ of even natural numbers has the same cardinal as $\mathbb{N}$, as the mapping $f\colon \mathbb{N} \to 2\mathbb{N}$ defined by the formula $f(n) = 2n$ is bijective.

(f) Let us note that the mapping $\mathbb{N} \to \mathbb{N}$ defined by the same formula is not surjective. Injectivity and surjectivity of a mapping $f\colon X \to Y$ only make sense *with respect to assigned sets*, as a domain and a codomain.

*(g) As another example, the mapping $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, is neither injective nor surjective, as $f(-1) = f(1)$ and we have seen that $f(x) \geqslant 0$, for all $x \in \mathbb{R}$.

But the reader likely knows (and will also find in 1.7.4) that, taking restrictions to the interval $J = \{x \in \mathbb{R} \mid x \geqslant 0\}$:

- the mapping $g\colon J \to \mathbb{R}$ defined by the same formula is injective, not surjective,

- the mapping $h\colon \mathbb{R} \to J$ defined by the same formula is surjective, not injective,

- the mapping $k\colon J \to J$ defined by the same formula is bijective, and its inverse is the *main* square root $\sqrt{-}\colon J \to J$.

We also note that an expression like 'the square roots of the number $x$' (or the formula $\pm\sqrt{x}$) does not define a mapping $J \to \mathbb{R}$, as it takes *two* values on each positive number. (Multi-valued relations *can* be considered, with due care, but are not mappings.)

### 1.2.2 The power set

Every set $X$ has a *power set* $\mathcal{P}X$, whose elements are the subsets of $X$:

$$A \in \mathcal{P}X \quad \Leftrightarrow \quad A \subset X, \tag{1.21}$$

where the symbol $\Leftrightarrow$ stays for 'if and only if' (also written as 'iff').

The relation of (weak) inclusion $A \subset B$ in $\mathcal{P}X$ is an order relation (see Section 1.4). In other words, for all $A, B, C \in \mathcal{P}X$ we have

$$\begin{aligned} &A \subset A && (\textit{reflexivity}),\\ &A \subset B \subset C \;\Rightarrow\; A \subset C && (\textit{transitivity}),\\ &A \subset B \subset A \;\Rightarrow\; A = B && (\textit{anti-symmetry}), \end{aligned} \tag{1.22}$$

where the symbol $\Rightarrow$ stays for 'implies'.

The least element of $\mathcal{P}X$ is the *empty subset* $\emptyset$; the greatest element is the *total subset* $X$.

The set $\mathcal{P}X$ has two main operations, called *union* and *intersection*

$$\begin{aligned} A \cup B &= \{x \in X \mid x \in A \text{ or } x \in B\},\\ A \cap B &= \{x \in X \mid x \in A \text{ and } x \in B\}. \end{aligned} \tag{1.23}$$

Let us note that 'or' is (always) meant in the inclusive sense, which admits that both conditions can hold: $A \cap B \subset A \cup B$. The algebraic properties of these operations will be examined in Section 1.4. Two subsets $A, B$ are said to be *disjoint* when $A \cap B = \emptyset$; otherwise, we say that $A$ *meets* $B$. The set $A \cap B$ is also called the *trace* of $A$ on $B$, or the *trace* of $B$ on $A$.

More generally, we can start from a family $(A_i)_{i \in I}$ of subsets of $X$, indexed by a set $I$ (possibly infinite), and consider their union and intersection:

$$\begin{aligned} \textstyle\bigcup_i A_i &= \{x \in X \mid \text{ there exists } i \in I \text{ such that } x \in A_i\},\\ \textstyle\bigcap_i A_i &= \{x \in X \mid \text{ for all } i \in I,\ x \in A_i\}. \end{aligned} \tag{1.24}$$

The empty family of subsets has union $\emptyset$ and intersection $X$. We also recall that $A \setminus B$ is the set of elements of $A$ which do not belong to $B$.

A mapping $f \colon X \to Y$ induces two mappings

$$f_* \colon \mathcal{P}X \to \mathcal{P}Y, \qquad f^* \colon \mathcal{P}Y \to \mathcal{P}X, \tag{1.25}$$

where $f_*$ takes a subset $A \subset X$ to its *image* $f(A) \subset Y$, while $f^*$ takes a subset $B \subset X$ to its *preimage* $f^{-1}(B) \subset X$

$$\begin{aligned} f(A) &= \{y \in Y \mid \text{ there exists } x \in A \text{ such that } y = f(x)\},\\ f^{-1}(B) &= \{x \in X \mid f(x) \in B\}. \end{aligned} \tag{1.26}$$

In particular, the subset $\operatorname{Im} f = f(X) \subset Y$ is said to be the *image of the* *mapping* $f$; the latter is surjective if and only if $\operatorname{Im} f = Y$. One often writes $f(A)$ in the shortened form $\{f(x) \mid x \in A\}$. Note also that, for a bijective mapping $f$, the preimage $f^{-1}(B)$ is the same as the image of $B$ with respect to the inverse mapping $f^{-1}$, and there is no conflict of notation.

This topic, the *transfer of subsets along a mapping*, will be further examined in 6.4.3.

*Exercises and complements.* (a) Given a mapping of sets $f\colon X \to Y$, the mapping $f_*\colon \mathcal{P}X \to \mathcal{P}Y$ of direct images preserves the unions, but need not preserve intersections, including the empty one.

On the other hand, the preimage-mapping $f^*\colon \mathcal{P}Y \to \mathcal{P}X$ preserves all unions and intersections.

(b) If $I$ is a set, and for each $i \in I$ we have a set $A_i$ (defined by some 'well-formed formula'), one assumes the existence of a set $X$ that contains all $A_i$. Thus all $A_i$ belong to $\mathcal{P}X$, and form an indexed family $(A_i)_{i\in I}$ in the latter.

The formulas (1.24), for union and intersection, make sense also in this case, as their result does not depend on the superset $X$ we are using, *with one exception*: the intersection of the empty family is only defined for a specified superset $X$.

(c) For each set $X$, there is a canonical bijection

$$\chi\colon \mathcal{P}X \to \operatorname{Map}(X, \{0,1\}), \tag{1.27}$$

that takes a subset $A \subset X$ to its *characteristic function* $\chi_A\colon X \to \{0,1\}$.

The latter is defined on each $x \in X$ as

$$\chi_A(x) = 1, \quad \text{if } \ x \in A, \qquad\qquad \chi_A(x) = 0, \ \text{otherwise}. \tag{1.28}$$

Loosely speaking, the term 'canonical' highlights the fact that $\chi$ is defined by an explicit formula, not depending on choice.

(d) Therefore, if $X$ is finite, with $n \geqslant 0$ elements, the power set $\mathcal{P}X$ has $2^n$ elements. From combinatorics, we know that $X$ has $\binom{n}{k}$ subsets of $k$ elements, for $0 \leqslant k \leqslant n$; this gives again $\sharp(\mathcal{P}X) = 2^n$.

(e) For every set $X$, $\sharp X \leqslant \sharp\mathcal{P}X$. (Set theory proves that $\sharp X < \sharp\mathcal{P}X$, see 1.7.8.)

### *1.2.3 Cartesian products and their universal property*

Let $(A_i)_{i\in I}$ be a family of sets, indexed by a set $I$. As we have seen (in 1.2.2(b)), there is some set $X$ such that $A_i \subset X$ for all indices $i$, and we can take $X = \bigcup_i A_i$. The *cartesian product* $A = \prod_{i\in I} A_i$ is defined as a subset of the set $\operatorname{Map}(I, X)$

$$A = \{x\colon I \to X \mid x(i) \in A_i, \ \text{for all } i \in I\}. \tag{1.29}$$

An element $x$ is generally written as an indexed family $(x_i)_{i\in I}$, or simply as $(x_i)$.

In particular, if all the factors $A_i$ are the same set $X$, we have a *cartesian power*

$$X^I = \textstyle\prod_{i\in I} X = \operatorname{Map}(I, X). \tag{1.30}$$

Coming back to the general case, the cartesian product comes with a family of *cartesian projections*

$$p_i \colon A \to A_i, \qquad\qquad p_i((x_i)_{i \in I}) = x_i, \tag{1.31}$$

which allows us to formalise our construction, in a way that can be adapted to any kind of structured sets we will consider – a unifying approach already stressed in the general Introduction, in Section 0.2.

The cartesian product of a family of sets $(A_i)_{i \in I}$ can be viewed as a set $A$ provided with a family of mappings $p_i \colon A \to A_i$ (for $i \in I$), satisfying the following *universal property of the product* (of sets):

(i) for every similar pair $(B, (f_i \colon B \to A_i)_{i \in I})$ formed of set $B$ and a family of mappings $f_i \colon B \to A_i$, there exists precisely one mapping $f \colon B \to A$ such that

$$\begin{tikzcd} B \arrow[r, dashed, "f"] \arrow[dr, "f_i"'] & A \arrow[d, "p_i"] \\ & A_i \end{tikzcd} \qquad\qquad p_i f = f_i \ \ (\text{for } i \in I). \tag{1.32}$$

In fact, all these triangles commute (as defined in 1.2.1(a)) if and only if the mapping $f \colon B \to A$ is defined as $f(y) = (f_i(y))_{i \in I}$, for all $y \in B$.

It is crucial to note that the universal property determines its solution *up to a unique bijection.* In fact, if the pair $(A', (q_i)_{i \in I})$ is also a solution of (i), we have two (well determined) mappings

$$\begin{aligned} &f \colon A' \to A, \qquad && p_i f = q_i \qquad && (\text{for } i \in I), \\ &g \colon A \to A', \qquad && q_i g = p_i \qquad && (\text{for } i \in I), \end{aligned} \tag{1.33}$$

and they are inverse to each other. This comes out of the fact that

$$q_i.(gf) = p_i f = q_i = q_i.\mathrm{id}\, A',$$

for all indices $i$, so that $gf = \mathrm{id}\, A'$; similarly, $fg = \mathrm{id}\, A$.

A binary product is written as $X_1 \times X_2$, and an element is written as an (ordered) *pair* $(x_1, x_2)$, with $x_1 \in X_1$ and $x_2 \in X_2$. This is an indexed family (on the set $I = \{1, 2\} \subset \mathbb{N}$), and determines its *first term* $x_1$ and its *second term* $x_2$; therefore $(x_1, x_2) = (y_1, y_2)$ if and only if $x_1 = y_1$ and $x_2 = y_2$.

Similarly, in a finite product $X_1 \times X_2 \times ... \times X_n$, an element is written as an (ordered) *n-tuple* $(x_1, x_2, ..., x_n)$, with $x_i \in X_i$.

*Exercises and complements.* (a) If in formula (1.29) we replace the set $X = \bigcup A_i$ with any set $X'$ which contains all the sets $A_i$, we get a set $A' \subset \mathrm{Map}(I, X')$ related to $A$ by a canonical bijection.

(b) The reader is warned that the cartesian projections $p_i \colon A \to A_i$ of a product are *not always* surjective. This fails whenever some factor $A_i$ is empty (so that the product is empty) and some other factor is not. Outside of this situation, the axiom of choice allows us to conclude that all projections are surjective (see 1.7.6).

(c) A unary product, of a family $(A)$ consisting of a single term, is the set $A$ with its identity projection. The product of the empty family $(A_i)_{i\in\emptyset}$ of sets has one element, the empty mapping $\emptyset \to X$ (however we choose the superset $X$), with no projection.

(d) (*Disjoint unions*) Given a family $(A_i)_{i\in I}$ of sets, we construct their 'disjoint union', namely the set

$$A = \bigcup\nolimits_i A_i \times \{i\}, \tag{1.34}$$

where we have replaced the original $A_i$ with a set $B_i = A_i \times \{i\}$ in obvious bijection with the former, so that the new sets are pairwise disjoint: if $i \neq j$ then $B_i \cap B_j = \emptyset$.

This set comes equipped with a family of mappings

$$u_i \colon A_i \to A, \qquad\qquad u_i(x) = (x, i), \tag{1.35}$$

which satisfies the following *universal property of the sum* (of sets):

(ii) for every similar pair $(B, (f_i \colon A_i \to B)_{i\in I})$ formed of set $B$ and a family of mappings $f_i : A_i \to B$, there exists precisely one mapping $f : A \to B$ such that

$$\begin{tikzcd} A \arrow[r, dashed, "f"] & B \\ A_i \arrow[u, "u_i"] \arrow[ru, "f_i"'] & \end{tikzcd} \qquad\qquad fu_i = f_i \ \ (\text{for } i \in I). \tag{1.36}$$

Also here the solution of the universal property is 'essentially unique', *up to a unique bijection*. Note also that this property is 'dual' to the universal property of the product, in the sense that any of them is turned into the other 'by reversing the arrow of each mapping'; all this will be made precise within category theory, in Chapter 5.

(e) If, in the previous point, all $A_i$ coincide with a set $X$, their disjoint union (1.34) is the cartesian product $X \times I$.

### *1.2.4 Equivalence relations and quotient sets*

A *relation* $R$ in a set $X$ is a subset $R \subset X \times X$. When $(x, y) \in R$, we say that $x$ is $R$-*related* to $y$; this is often written as $x\,R\,y$.

The relation $R$ is said to be:

(i) *reflexive* if, for all $x \in X$, we have $x\,R\,x$,

(ii) *symmetric* if, for all $x, y \in X$, $x\,R\,y$ implies $y\,R\,x$,

(iii) *transitive* if, for all $x, y, z \in X$, $x\,R\,y$ and $y\,R\,z$ imply $x\,R\,z$.

We say that $R$ is an *equivalence relation* when these three properties are satisfied. Then, for each $x \in X$, the *equivalence class* of $x$ (with respect to $R$) is the subset

$$[x] = \{x' \in X \mid x\,R\,x'\} \subset X, \tag{1.37}$$

also written as $[x]_R$ or $\overline{x}$. The element $x$ is said to be a *representative* of the class $[x]$; the element $x'$ is also if and only if $x\,R\,x'$.

The *quotient of the set* $X$ *modulo* $R$, written as $X/R$, is the set of all equivalence classes of $X$.

Formally, $X/R$ is a subset of $\mathcal{P}X$; but we generally think of $X/R$ in a more intuitive way, as if we had 'identified' all the elements of $X$ which lie in the same equivalence class. Thus, the equivalence relation $x = \pm x'$ (more formally: $x = x'$ *or* $x = -x'$) in the real line can be described as: 'the relation that identifies each number with the opposite one'.

The *canonical projection*

$$p\colon X \to X/R, \qquad p(x) = [x] \quad (\text{for } x \in X), \tag{1.38}$$

is always surjective.

The equivalence relations of a set $X$ are ordered by inclusion $R \subset R'$ (as subsets of $X \times X$). The *finest*, or smallest, is the equality relation $x = y$ in $X$, determined by the *diagonal* of the product $X \times X$

$$\Delta_X = \{(x, y) \in X \times X \mid x = y\}. \tag{1.39}$$

The *coarsest*, or largest, is the relation $x, y \in X$, determined by the total subset $X \times X$.

A mapping $f\colon X \to Y$ has an *associated equivalence relation* $R_f$ on $X$:

$$xR_fx' \ \text{ if and only if } \ f(x) = f(x'). \tag{1.40}$$

There is a unique mapping $g\colon X/R_f \to Y$ such that

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "p"'] & Y \\ X/R \arrow[ur, dashed, "g"'] & \end{tikzcd} \qquad f = gp. \tag{1.41}$$

In fact, we can (and must) define $g([x]) = f(x)$, for all $x \in X$. The mapping $f$ is injective if and only if $R_f$ is the equality relation.

*Exercises and complements.* (a) The quotient of the set $X$ modulo the finest equivalence relation $\Delta_X$ is in canonical bijection with $X$ itself. The quotient of the set $X$ modulo the coarsest equivalence relation is a singleton if $X \neq \emptyset$, and is empty otherwise.

(b) In the set of all straight lines of the euclidean plane (or the euclidean 3-dimensional space), *parallelism* is an equivalence relation. The quotient set can be interpreted as the set of *directions* of the plane (or the space).

(c) (*Partitions*) A *partition* of a set $X$ is a family of disjoint subsets $(A_i)_{i\in I}$ that *cover* $X$

$$X = \bigcup_{i\in I} A_i, \qquad A_i \cap A_j = \emptyset \quad \text{(for } i \neq j \text{ in } I\text{)}. \tag{1.42}$$

This amounts to giving an equivalence relation $R$ in the set $X$.

(d) Every binary relation $R$ on the set $X$ *generates* an equivalence relation $E$, the least equivalence relation of $X$ containing $R$.

### 1.2.5 The canonical factorisation

A mapping $f\colon X \to Y$ between sets has a *canonical factorisation*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "p"'] & Y \\ X/R_f \arrow[r, "g"'] & \operatorname{Im} f \arrow[u, "m"'] \end{tikzcd} \qquad f = mgp, \tag{1.43}$$

where:

- the (surjective) mapping $p$ is the canonical projection of the domain $X$ onto its quotient modulo the associated equivalence relation $R_f$,

- the (injective) mapping $m$ is the inclusion of the image $\operatorname{Im} f$ into the codomain $Y$,

- the (bijective) mapping $g\colon X/R_f \to \operatorname{Im} f$ is defined by $g([x]) = f(x)$ (for $x \in X$), and is the only mapping such that $f = mgp$.

From (1.43), we can deduce a factorisation of $f$ formed of a surjective and an injective mapping

$$f = (mg).p, \tag{1.44}$$

which is ‘essentially unique’, as made precise in the exercise below.

(Strictly speaking, there are infinitely many such factorisations, including $f = m.(gp)$.)

*Exercises and complements.* (a) Prove the following property of ‘essential uniqueness’, up to a determined bijection.

Given two factorisations $f = mp = m'p'$, where the mappings $p, p'$ are surjective and $m, m'$ are injective, there is precisely one bijection $i$ such that the following diagram commutes

$$\begin{tikzcd} X \arrow[r, "p"] \arrow[d, equal] & A \arrow[r, "m"] \arrow[d, dashed, "i"] & Y \arrow[d, equal] \\ X \arrow[r, "p'"'] & A' \arrow[r, "m'"'] & Y \end{tikzcd} \qquad p' = ip, \quad m'i = m. \tag{1.45}$$

### *1.2.6 Induction*

Let $A \subset \mathbb{N}$. If the following conditions are satisfied

$(i)$ $\quad 0 \in A$ (*initial step*),

$(ii)$ $\quad$ for every $n \in A$, $n + 1 \in A$ (*inductive step*),

we conclude that $A = \mathbb{N}$. (A well-known procedure, called *a proof by induction.*)

In fact, if there is some natural number that is not in $A$, we can let $m$ be the least of them. But $m > 0$, by (i), and therefore $m - 1$ must be in $A$. Applying (ii) we get $m \in A$, a contradiction.

If we replace the initial step with $n_0 \in A$, the conclusion says that $A$ contains all the natural numbers $\geqslant n_0$.

*Exercises and complements.* (a) Prove by induction that the sum $s_n = 0 + 1 + 2 + ... + n$ (of integers) can be expressed as $n(n + 1)/2$, for all $n \in \mathbb{N}$.

(b) (*Complete induction*) Replacing the inductive step (ii) by the following (apparently) weaker assumption:

(ii′) for every $n \in \mathbb{N}^*$, if $\{0, 1, ..., n - 1\} \subset A$ then $n \in A$,

the conclusion still holds: $A = \mathbb{N}$. The procedure is now called *a proof by complete induction.*

(c) (*Prime factor decomposition*) Let us recall that a natural number $p > 1$ is said to be *prime* if it has no proper divisor in $\mathbb{N}$: if $p = ab$ then $a = 1$ or $a = p$. Prove that any natural number $n > 1$ is a product of prime numbers. (One can add 1, as the product of the empty family of prime numbers.)

### *1.2.7 Structures and categories*

A set can carry structures of various kinds. We have seen various examples in Section 1.1:

- algebraic structures, defined by operations, like fields, rings, and so on,

- order structures, defined by a relation, like ordered and preordered sets,

- ordered algebraic structures, like ordered fields,

and will see other kinds later, like the topological and the algebro-topological structures.

In each of these kinds, there are ‘privileged mappings’, or *morphisms*, that preserve the structure in a specified sense, like homomorphisms of fields, or order preserving mappings between ordered sets, or order preserving homomorphisms between ordered fields. In each kind, the morphisms are closed under composition, and include the identity of each object. This partial composition law is associative (whenever legitimate), and any identity morphism acts as an identity for every legitimate composition.

These objects and morphisms form thus a *category of structured sets.* This topic will be investigated in Chapter 5, but it will be useful to present now – informally – its basic elements.

In each category, a morphism $f\colon X \to Y$ is said to be an *isomorphism* if it admits an inverse, i.e. a backward morphism $g : Y \to X$ (of the category that we are considering) such that $gf = \mathrm{id}\, X$ and $fg = \mathrm{id}\, Y$. By the usual proof (as in Section 1.1), the morphism $g$ is determined by $f$, and can be written as $f^{-1}$. The isomorphism relation $X \cong Y$, meaning that there exists an isomorphism $X \to Y$ (in the category that we are considering) is an equivalence relation.

A morphism $X \to X$ is called an *endomorphism* of $X$, and an *automorphism* if it is invertible.

In any category of structured sets, an isomorphism is necessarily a bijective mapping. The converse need not be true. For instance the identity mapping $\mathrm{id}\,\mathbb{R}$ gives an order-preserving mapping

$$f\colon (\mathbb{R}, =) \to (\mathbb{R}, \leqslant), \tag{1.46}$$

from the set $\mathbb{R}$ equipped with the discrete order, to the same set equipped with the natural order; this is not an isomorphism of ordered sets, because the inverse mapping (of sets) is not order-preserving, and does not belong to the category that we are considering. The same example works in the category of ordered fields, and similar ones will be given for topological spaces.

However, it is important to remark once for all that in a 'category of (pure) algebraic structures' every bijective morphism is an isomorphism: in each case this can be proved as in Exercise 1.1.6(c), for rings.

The *transport of a structure*, along a bijection, is also a useful tool. For instance, suppose that $K$ is an ordered field, $A$ is a set and $f\colon K \to A$ is a bijective mapping. Then there is one and only one structure of ordered field on $A$ that makes $f$ into an isomorphism (of ordered fields): in fact each element of $A$ can be written in a unique way as $f(x)$ (with $x \in K$), and we can (and must) let, for all $x, y \in K$:

$$\begin{gathered} f(x) + f(y) = f(x+y), \qquad f(x).f(y) = f(x.y), \\ f(x) \leqslant f(y) \quad \Leftrightarrow \quad x \leqslant y. \end{gathered} \tag{1.47}$$

We have already seen some instance of a *universal property.* It is an important issue, that will be developed in various forms, in all the structures we will consider: either algebraic, or order-like, or topological, or some combination of the previous kinds. A general definition can be given within category theory, as we will see in Section 5.4 and exploit thereafter.

### 1.2.8 Algebraic structures and equational algebras

Let us reconsider, more formally, the algebraic structure of rings.

A ring $R$ is usually presented as a set equipped with two binary operations (in additive and multiplicative notation, respectively)

$$\begin{aligned} \sigma_R &\colon R^2 \to R, &\qquad \sigma_R(x,y) &= x+y, \\ \mu_R &\colon R^2 \to R, &\qquad \mu_R(x,y) &= xy, \end{aligned} \tag{1.48}$$

satisfying the axioms (A.1–6).

It can also be presented as a set $R$ equipped with four operations, adding to the previous ones a *unary* operation and a *constant*, or *zero-ary* operation

$$\begin{aligned} \omega_R &\colon R \to R, &\qquad \omega_R(x) &= -x, \\ \zeta_R &\colon R^0 \to R, &\qquad \zeta_R(*) &= 0, \end{aligned} \tag{1.49}$$

defined, respectively, on $R^1 = R$ and the singleton $R^0 = \{*\}$.

The second presentation, if more complex, has a crucial advantage: now the axioms of the structure can be written in *equational form*, only depending on the universal quantifier *for all*, applied to all the elements of $R$. In the present case, we require that, *for all* $x, y, z \in R$

$$\begin{gathered} x+(y+z) = (x+y)+z, \qquad x+0 = x = 0+x, \\ x+(-x) = 0 = (-x)+x, \qquad x+y = y+x, \\ x(yz) = (xy)z, \\ x(y+z) = xy+xz, \qquad (x+y)z = xz+yz. \end{gathered} \tag{1.50}$$

An algebraic structure which can be presented in such a form will be called an *equational algebraic structure*, or an *equational algebra*, and their complex will be called a *variety of algebras*; the homomorphisms are always defined as the mappings that preserve all the operations. (The study of varieties of algebras is the subject of Universal Algebra [Gr1, Coh]. A brief presentation of this discipline can be found in [G4].)

Other equational algebraic structures, to be studied later, include: semigroups, monoids, groups, commutative groups, unital rings, modules on a ring, vector spaces on a field, lattices, boolean algebras, etc.

Automatically, a variety of algebras $\mathcal{V}$ has important properties: let us simply mention here that the cartesian product $A \times B$ of two algebras in $\mathcal{V}$, equipped with the componentwise extension of all the operations of the structure, is again an algebra in $\mathcal{V}$.

Fields are an important example of an algebraic structure *which is not equational*, as readily detected by the fact that the cartesian product $K \times K'$ of two fields is a unital ring, but not a field: the element $(1,0)$ cannot have an inverse, as $(1,0).(x,y) = (x,0) \neq (1,1)$.

seen in Exercise 1.1.3(f). Of course this group is still written in multiplicative notation. For a field $K$, the group $\mathrm{Inv}(K) = K^*$ is formed of all non-zero elements of $K$.

(d) The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are abelian groups, with respect to their (usual) addition.

The sets $\mathbb{Q}^*$, $\mathbb{R}^*$ are commutative groups, with respect to multiplication. The set $\mathrm{Inv}(\mathbb{Z}) = \{-1, 1\}$ is also a commutative group.

(e) Prove that the power set $\mathcal{P}X$ of any set $X$ is an abelian group with respect to the *symmetric difference*

$$A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A). \tag{1.53}$$

In this abelian group *each element is opposite to itself.*

(f) Adding binary intersection, $(\mathcal{P}X, \Delta, \cap)$ is a commutative unital ring.

If $X = \emptyset$, $\mathcal{P}X$ is the null ring. If $X$ is a singleton, the ring $\mathcal{P}X$ has two elements, $\emptyset$ and $X$, and is isomorphic to the two-element field $\mathbb{F}_2$ of Exercise 1.1.3(j).

(g) In an abelian group, the sum $\sum_{i\in I} x_i$ of a finite family of elements makes sense without any ordering on the set of indices $I$, because the operation is associative and commutative. The sum of the empty family is defined to be 0.

It will be useful to extend this notation to an *essentially finite sum* $\sum_{i\in I} x_i$, where the set of indices $I$ is arbitrary but the family $(x_i)$ is *quasi null*: this means that its *support* $J = \{i \in I \mid x_i \neq 0\}$ is a finite subset of $I$. Then we let $\sum_{i\in I} x_i = \sum_{i\in J} x_i$.

(h) Abelian groups from a variety of algebras, in the sense of 1.2.8.

### *1.3.1 Homomorphisms, subgroups and kernels*

A *homomorphism* $f\colon A \to B$ *of abelian groups* is a mapping that preserves the operation:

$$f(x + y) = f(x) + f(y) \qquad \text{(for } x, y \in A). \tag{1.54}$$

(One can write $f(x +_A y) = f(x) +_B f(y)$, when useful to distinguish the operations.) It follows that $f$ preserves the identity of the sum, all opposites and all differences, as we have verified in 1.1.5.

As examined in 1.2.7 for any algebraic structure, two consecutive homomorphisms of abelian groups, $f\colon A \to B$ and $g\colon B \to C$, give a composed homomorphism $gf\colon A \to C$. This partial composition law is associative (whenever legitimate), and any identity homomorphism $\mathrm{id}\, A\colon A \to A$ acts as a unit for every legitimate composition.

An *isomorphism* $f\colon A \to B$ of abelian groups is a homomorphism that has an inverse homomorphism: there is a homomorphism $g\colon B \to A$ such that $gf = \mathrm{id}\, A$ and $fg = \mathrm{id}\, B$. This happens if and only if the homomorphism $f$ is a bijective mapping, and $g = f^{-1}$ is the inverse homomorphism. Then the abelian groups $A$ and $B$ are said to be *isomorphic*, and we write $A \cong B$, an equivalence relation between abelian groups.

$\mathrm{Hom}(A, B)$ of all homomorphisms from $A$ to $B$ is an abelian group, when equipped with the *pointwise sum* of $f, g \in \mathrm{Hom}(A, B)$

$$(f+g)(x) = f(x) + g(x) \qquad (\text{for } x \in A). \tag{1.57}$$

The identity of this operation is the *zero homomorphism* from $A$ to $B$

$$0_{AB} \colon A \to B, \qquad\qquad 0_{AB}(x) = 0_B, \tag{1.58}$$

and the opposite of $f \in \mathrm{Hom}(A, B)$ is the *opposite homomorphism*, also computed pointwise:

$$(-f)(x) = -f(x). \tag{1.59}$$

(f) For any abelian group $A$, the group $\mathrm{Hom}(\mathbb{Z}, A)$ is canonically isomorphic to $A$.

(g) (*The ring of endomorphisms*) For an abelian group $A$, the set $\mathrm{End}(A) = \mathrm{Hom}(A, A)$ of all *endomorphisms* of $A$ is a unital ring, when equipped with the previous sum and the composition law $(f, g) \mapsto gf$. This ring is not commutative, generally. It is a multiplicative subsemigroup of the semigroup $\mathrm{End}(|A|)$ of all endomappings of the underlying *set* $|A|$, and of course we should not confuse these items.

### *1.3.3 Multiples and linear combinations*

In an abelian group $A$ we can write any finite sum $x_1 + x_2 + ... + x_n$ of elements without parentheses. In particular, for every $x \in A$ and every integer $n \geqslant 0$ we have the *multiple element* $nx = x + x + ... + x$ (a sum of $n$ terms), inductively defined by:

$$0.x = 0_A, \qquad (n+1)x = nx + x \qquad\qquad (n \geqslant 0). \tag{1.60}$$

Moreover, for a negative integer $k = -n < 0$, we let

$$kx = n(-x). \tag{1.61}$$

Multiples have the following properties, for $x, y \in A$ and $h, k \in \mathbb{Z}$

$$\begin{array}{llll} (i) & hx + kx = (h+k)x, & 0_{\mathbb{Z}}.x = 0_A, & (-h)x = -(hx), \\ (ii) & h(kx) = (hk)x, & 1_{\mathbb{Z}}.x = x, & \\ (iii) & hx + hy = h(x+y), & h.0_A = 0_A, & h(-x) = -(hx). \end{array}$$

This will be proved in Section 1.5, working in multiplicative notation, where the multiple $kx$ becomes the power $x^k$. More precisely, we will see in Exercises 1.5.1(d) and 1.5.2(c) that these properties hold in a commutative semigroup for positive integers $h, k$; in a commutative unital semigroup for which is obviously associative, has identity $[0]$ and opposites $-[x] = [-x]$.

$A/E$ becomes thus an abelian group, called the *quotient* of the abelian group $A$ modulo the congruence $E$. The canonical projection on the quotient set

$$p\colon A \to A/E, \qquad p(x) = [x], \tag{1.74}$$

is a homomorphism, and the structure we have put on $A/E$ is the only one having this outcome.

For a fixed abelian group $A$, there is a natural bijection *between congruences and subgroups*

$$\begin{aligned} E &\mapsto \{x \in A \mid x\, E\, 0_A\} = \operatorname{Ker} p, \\ H &\mapsto \equiv_H, \qquad x \equiv_H x' \;\Leftrightarrow\; x - x' \in H. \end{aligned} \tag{1.75}$$

The reader can easily prove this fact (or see the solution of Exercise 1.3.9(a)).

The quotient of $A$ modulo the associated congruence $\equiv_H$ is denoted as $A/H$ and read as $X$ *modulo* $H$. In this quotient, the equivalence class of an element $x$ is determined as

$$[x] = x + H = \{x + h \mid h \in H\}, \tag{1.76}$$

and called a *coset* of $H$ (with respect to the element $x$).

The null subgroup $\{0\}$ determines the discrete congruence $x = y$, so that $A/\{0\}$ can (and will) be identified with $A$. The total subgroup $A$ determines the indiscrete congruence $x, y \in A$, so that $A/A$ is a null group, and can be written as $\{0\}$.

Since a subgroup is more elementary notion than a congruence, the quotient of abelian groups are often presented in the form $A/H$. Yet, the notion of congruence in an object $A$ makes sense for any equational algebraic structure, and in various cases cannot be expressed by means of a substructure of $A$ (see 1.5.7).

*Exercises and complements.* (a) For a homomorphism $f\colon A \to B$, the equivalence relation $R_f$ coincides with the congruence of $A$ associated to the subgroup $\operatorname{Ker} f$, defined (for $x, y \in A$) by

$$f(x) = f(y) \;\Leftrightarrow\; f(x - y) = 0 \;\Leftrightarrow\; (x - y) \in \operatorname{Ker} f. \tag{1.77}$$

(b) A congruence $E$ of $A$ is always a subgroup of $A \times A$.

### *1.3.6 Exercises and complements* (Modular arithmetic)

Everyone is familiar with adding integers *modulo 7*, when we want to know the day of the week in (say) 15 days; or *modulo 12*, when we want to know