CHAPTER 1

SETS AND FUNCTIONS

In this chapter we review the foundations and notations of naïve set theory. We will define sets and the notions of functions, relations and operations on sets that are required in this text. The reader who is well acquainted with basic mathematics can browse through the present chapter.

1.1 Sets

1.1.1 Set, element, inclusion

Let E be a *set* and e an *element*. $e \in E$ means that e is a member of the set E and is read 'e is in E'. The negation of this relation (i.e. e is not in E) is denoted by $e \notin E$. The empty set is a set containing no elements; it is denoted by $\emptyset$.

Let A, B be two sets. A is said to be a subset of B, or contained in B, if and only if any member of A is a member of B, and this is denoted by $A \subseteq B$. The negation of $A \subseteq B$ is denoted by $A \not\subseteq B$, and this does *not* mean that $B \subseteq A$. We notice that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$ (i.e. if and only if A and B have the same elements). If $A \subseteq B$, but $A \neq B$, we will write $A \subsetneq B$. Finally, the set of subsets of E is denoted by $\mathcal{P}(E)$; hence $A \subseteq E$ if and only if $A \in \mathcal{P}(E)$. Note that the sets $\emptyset$ and E are elements of $\mathcal{P}(E)$.

Example 1.1 Let $E = \{0, 1\}$. $\mathcal{P}(E) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

Remark 1.2 Some authors, mainly French, among them Bourbaki, denote inclusion by $\subset$; so, to avoid ambiguities, strict inclusion is denoted by $\subsetneqq$.

The *Cartesian product* of two sets E and F is the set of all ordered pairs consisting of an element of E and an element of F:

$$E \times F = \{(x, y) \,/\, x \in E \text{ and } y \in F\} .$$

The Cartesian product can be generalized to a finite family of sets:

$$E_1 \times \cdots \times E_n = \{(x_1, \dots, x_n) \,/\, x_1 \in E_1, \dots, x_n \in E_n\} \,.$$

Lastly, the Cartesian product of E by itself n times, for $n \geq 1$, is denoted by $E^n = E \times \cdots \times E$. E^n can be recursively defined by (see Chapter 3): $E^1 = E$ and $E^n = E \times E^{n-1}$.

1.1.2 Union, intersection, difference, complement, partition

Assume that a universal set E is given. Let A, B be two subsets of E. We define:

- the *intersection* of A and B: $A \cap B = \{e \in E \,/\, e \in A \text{ and } e \in B\}$,
- the *union* of A and B: $A \cup B = \{e \in E \,/\, e \in A \text{ or } e \in B\}$,
- the *difference* of A and B: $A \setminus B = \{e \in E \,/\, e \in A \text{ and } e \notin B\}$,
- the *complement* of A with respect to E, denoted by $\overline{A}$ or A^c:
$$\overline{A} = E \setminus A = \{e \in E \,/\, e \notin A\},$$
- the *symmetric difference* of A and B: $A \bigtriangleup B = (A \setminus B) \cup (B \setminus A)$.

Two subsets A and B of E are said to be *disjoint* if and only if $A \cap B = \emptyset$.

Example 1.3

- $\overline{E} = \emptyset$, and $\overline{\emptyset} = E$.
- $A \cap \emptyset = \emptyset, \quad A \cup E = E, \quad A \bigtriangleup E = \overline{A}$.
- $A \cap A = A \cup A = A \cup \emptyset = A \bigtriangleup \emptyset = A \cap E = \overline{\overline{A}} = A$.
- $A \setminus B = A \cap \overline{B}$.
- $A \setminus A = A \bigtriangleup A = \emptyset$.

De Morgan's laws enable us to compute the complement of a union and of an intersection: $\overline{A \cup B} = \overline{A} \cap \overline{B}$ and $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Union and intersection are associative and commutative operations (see Section 1.4.1). Moreover, they distribute over each other (see Section 1.4.1), i.e.

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \qquad \text{and} \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \,. \end{aligned}$$

These properties are to be found again in the study of lattices (see Chapter 2, Section 2.5) and in the study of Boolean algebras (see Chapter 4).

Notations

$\Longrightarrow$ (resp. $\Longleftrightarrow$) stands for 'implies' (resp. 'if and only if').

$\exists e \in E$ (resp. $\forall e \in E$) stands for 'there exists an e in E' (resp. 'for any e in E').

EXERCISE 1.1 Let A, B and C be three subsets of E. Show that

$$A \cap \overline{B} = A \cap \overline{C} \Longleftrightarrow A \cap B = A \cap C. \qquad \diamondsuit$$

EXERCISE 1.2 Let A, B and C be three subsets of E. Show that

$$\big(A \cup B \subseteq A \cup C \quad \text{and} \quad A \cap B \subseteq A \cap C\big) \Longrightarrow B \subseteq C.$$

When does the equality $B = C$ hold? $\diamondsuit$

EXERCISE 1.3 Let A, B and C be three subsets of E. What is the relationship between

(i) $A \bigtriangleup (B \cap C)$ and $(A \bigtriangleup B) \cap (A \bigtriangleup C)$ and
(ii) $A \bigtriangleup (B \cup C)$ and $(A \bigtriangleup B) \cup (A \bigtriangleup C)$?

When are they equal? $\diamondsuit$

Union and intersection can be generalized to any family of subsets of a set E. A family $(x_i)_{i\in I}$ of elements of a set X is a mapping from I to X (see Section 1.2). I is called the set of indices, and the image by this mapping of the element i of I is denoted by x_i. When we consider a family of subsets of a set E, it means that the elements of the family are subsets of E, i.e. $X = \mathcal{P}(E)$. Let $(A_i)_{i\in I}$ be a family of subsets of E. Recall that $\forall$ (resp. $\exists$) means 'for all' (resp. 'there exists'). We define:

$$\bigcup_{i\in I} A_i = \{e \in E \,/\, \exists i \in I, e \in A_i\} \,,$$

$$\bigcap_{i\in I} A_i = \{e \in E \,/\, \forall i \in I, e \in A_i\} \,.$$

Note that $\bigcup_{i\in\emptyset} A_i = \emptyset$ and $\bigcap_{i\in\emptyset} A_i = E$. On the other hand, if $I = \{1, \ldots, n\}$, the family $(A_i)_{i\in I}$ is finite, and these two operations are just the finite union and intersection, denoted by $A_1 \cup \cdots \cup A_n$ and $A_1 \cap \cdots \cap A_n$ respectively. This generalization enables us to define the notion of partition of a set E. A finite or infinite family $(A_i)_{i\in I}$ of subsets of E is a *partition* of E if it satisfies

(i) $A_i \neq \emptyset$ for any $i \in I$,
(ii) $A_i \cap A_j = \emptyset$ for all pairwise distinct i, j in I and
(iii) $E = \bigcup_{i\in I} A_i$.

EXAMPLE 1.4 The three sets

- $A_0 = \{n \in \mathbb{N} \,/\, n$ is a multiple of $3\}$,
- $A_1 = \{n + 1 \,/\, n \in A_0\} = \{$(multiples of 3)+1$\}$ and
- $A_2 = \{n + 2 \,/\, n \in A_0\} = \{$(multiples of 3)+2$\}$

form a partition of $\mathbb{N}$.

EXERCISE 1.4 Let A be a subset of E and $(B_i)_{i\in I}$ be a family of subsets of E. Show that

1. $A \bigcup \left(\bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} \left(A \cup B_i \right)$,
2. $A \bigcap \left(\bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} \left(A \cap B_i \right)$. ♢

1.2 Functions

1.2.1 Definitions

Intuitively, a mapping f from E to F assigns to each element x of E a unique element $f(x)$ of F. The slightly more general notions of correspondence and function will also be of use. Formally, the definitions are as follows.

Let E and F be two sets. A *correspondence* from E to F is a triple $f = (E, F, \Gamma)$, where Γ is a subset of $E \times F$. We say that E is the *pre-domain* of f, F is the *co-domain* of f and Γ is the *graph* of f. The set

$$Dom(f) = \{x \in E \,/\, \exists y \in F, (x, y) \in \Gamma\}$$

is the *domain* of f and the set

$$Im(f) = \{y \in F \,/\, \exists x \in E, (x, y) \in \Gamma\}$$

is the *range* of f. Let $x \in E$. Any element y of F such that $(x, y) \in \Gamma$ is an *image* of x by f. Let $X \subseteq E$. We denote by

$$f(X) = \{y \in F \,/\, \exists x \in X, (x, y) \in \Gamma\}$$

the set of images by f of the elements of X. Similarly, any element $x \in E$ such that $(x, y) \in \Gamma$ is called a *preimage* by f of $y \in F$. For $Y \subseteq F$, we denote by

$$f^{-1}(Y) = \{x \in E \,/\, \exists y \in Y, (x, y) \in \Gamma\}$$

the set of preimages by f of the elements of Y. We have $Dom(f) = f^{-1}(F)$ and $Im(f) = f(E)$.

A correspondence $f = (E, F, \Gamma)$ is said to be a *function* if it assigns at most one image to each element of E; for any element x of E this image is denoted by $f(x)$. The function f is denoted by $f\colon E \longrightarrow F$. A function $f\colon E \longrightarrow F$ is said to be a *mapping* if its domain is the whole set E: $Dom(f) = E$. The set of mappings from E to F is denoted by F^E.

Example 1.5

- The identity mapping on E defined by $f(x) = x$ for any x of E is denoted by $id_E \colon E \longrightarrow E$.
- The function $\chi_A \colon E \longrightarrow \{0, 1\}$ defined by:

$$\chi_A(e) = \begin{cases} 1 & \text{if } e \in A, \\ 0 & \text{if } e \notin A, \end{cases}$$

is called the *characteristic function* of the subset A of E.

A mapping $f \colon E \longrightarrow F$ is said to be *one-to-one* or *injective* (resp. *onto* or *surjective, bijective* or a *one-to-one correspondence*) if any element $y \in F$ has at most (resp. at least, exactly) one preimage by f. We thus have:

- f is injective if and only if $\forall x, y \in E$, $f(x) = f(y) \Longrightarrow x = y$.
- f is surjective if and only if $\forall y \in F$, $\exists x \in E, y = f(x)$.
- f is bijective if and only if $\forall y \in F$, $\exists! x \in E, y = f(x)$, i.e. if f is both injective and surjective. (The symbol $\exists!$ means 'there exists a unique'.)

Exercise 1.5 Let $f \colon E \longrightarrow F$ be a mapping and let $(A_i)_{i \in I}$ be a partition of F. Note: $f(E) = \{f(e) \,/\, e \in E\}$. Show that $\big(f^{-1}(A_i)\big)_{i \in I}$ is *almost* a partition of E, by which we mean that some $f^{-1}(A_i)$ may be empty, thus preventing $\big(f^{-1}(A_i)\big)_{i \in I}$ from being a partition of E. Give a sufficient condition for all the sets $f^{-1}(A_i)$ to be non-empty. ♢

Exercise 1.6 Let $f \colon E \longrightarrow F$ be a mapping. Find a necessary and sufficient condition for ensuring that the image by f of any partition of E is a partition of F. Assume that if f is injective, then $f(A \cap B) = f(A) \cap f(B)$ (see Exercise 1.8), and recall that the image of a partition $(A_i)_{i \in I}$ of E is defined by $f\big((A_i)_{i \in I}\big) = \big(f(A_i)_{i \in I}\big)$. ♢

Let $f \colon E \longrightarrow F$ and $g \colon F \longrightarrow G$ be two mappings. The composition of f and g is the mapping $g \circ f : E \longrightarrow G$ defined by $g \circ f(x) = g(f(x))$. For instance, if $f \colon E \longrightarrow F$ is a mapping, we have $f \circ id_E = id_F \circ f = f$. The composition of mappings is associative; hence, parentheses can be omitted and we can write $h \circ g \circ f$.

1.2.2 Properties

We present some useful properties of sets and mappings.

Let $f \colon E \longrightarrow F$ be a mapping, let A and B be two subsets of E and let C and D be two subsets of F. We have:

$$f(A \cup B) = f(A) \cup f(B) \quad \text{and} \quad f(A \cap B) \subseteq f(A) \cap f(B) \;,$$

$$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D) \quad \text{and} \quad f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D) \;.$$

If, moreover, f is injective, then $f(A \cap B) = f(A) \cap f(B)$. These properties are easily proved and can be generalized to arbitrary unions or intersections.

Exercise 1.7 Let $f: A \longrightarrow B$ be a mapping. Show that

1. f injective $\Longleftrightarrow \forall X \subseteq A,\ f^{-1}(f(X)) = X$,
2. f surjective $\Longleftrightarrow \forall Y \subseteq B,\ f(f^{-1}(Y)) = Y$. ♢

Exercise 1.8 Let $f: A \longrightarrow B$ be a mapping. Show that

$$f \text{ injective} \quad \Longleftrightarrow \quad \forall X, Y \subseteq A,\ f(X \cap Y) = f(X) \cap f(Y).$$ ♢

Exercise 1.9 Let E be a set and let A and B be two subsets of E. Consider the mapping

$$\begin{aligned} f: \mathcal{P}(E) &\longrightarrow \mathcal{P}(A) \times \mathcal{P}(B) \\ X &\longmapsto (X \cap A, X \cap B) , \end{aligned}$$

where $X \longmapsto (X \cap A, X \cap B)$ means that f assigns to each X in $\mathcal{P}(E)$ the pair $(X \cap A, X \cap B)$ in $\mathcal{P}(A) \times \mathcal{P}(B)$. Find necessary and sufficient conditions on A and B ensuring that f will be

1. injective,
2. surjective and
3. bijective. ♢

Proposition 1.6 *Let $f: E \longrightarrow F$ and $g: F \longrightarrow G$ be two mappings.*

(i) *f and g injective $\Longrightarrow g \circ f$ injective.*
(ii) *f and g surjective $\Longrightarrow g \circ f$ surjective.*
(iii) *f and g bijective $\Longrightarrow g \circ f$ bijective.*

Exercise 1.10 Prove these properties. ♢

Exercise 1.11 Consider two mappings $f: A \longrightarrow B$ and $g: B \longrightarrow C$.

1. Show that
   (i) $g \circ f$ injective $\Longrightarrow f$ injective,
   (ii) $g \circ f$ surjective $\Longrightarrow g$ surjective.
2. Find an example for which $g \circ f$ is bijective, f is non-surjective and g is non-injective.
3. Show that
   (i) $g \circ f$ injective and f surjective $\Longrightarrow g$ injective,
   (ii) $g \circ f$ surjective and g injective $\Longrightarrow f$ surjective. ♢

Exercise 1.12 Consider three mappings $f: A \longrightarrow B$, $g: B \longrightarrow C$ and $h: C \longrightarrow A$.

1. Show that if $h \circ g \circ f$ and $g \circ f \circ h$ are injective and if $f \circ h \circ g$ is surjective then f, g and h are bijective.
2. Show that if $h \circ g \circ f$ and $g \circ f \circ h$ are surjective and if $f \circ h \circ g$ is injective then f, g and h are bijective. ♢

Proposition 1.7 *Let $f: E \longrightarrow F$ be a mapping.*

(i) *If $E \neq \emptyset$ then f is injective if and only if f has a left inverse, i.e. if there exists a mapping $r: F \longrightarrow E$ such that $r \circ f = id_E$. The mapping r is surjective and is called a retraction of f.*
(ii) *f is surjective if and only if f has a right inverse, i.e. if there exists a mapping $s: F \longrightarrow E$ such that $f \circ s = id_F$. The mapping s is injective and is called a section of f.*
(iii) *f is bijective if and only if f has an inverse, i.e. if there exists a mapping $f^{-1}: F \longrightarrow E$ such that $f \circ f^{-1} = id_F$ and $f^{-1} \circ f = id_E$. The mapping f^{-1} is a bijection and is called the inverse bijection of f.*

EXERCISE 1.13 Prove these properties. ♢

1.3 Cardinals

1.3.1 Finite sets

For any integer n, let $[n]$ be the set $\{1, \ldots, n\}$ of integers between 1 and n.

Proposition 1.8 *If $n < m$, there is no injection from $[m]$ to $[n]$.*

EXERCISE 1.14 Prove this proposition by induction (see Chapter 3). ♢

We easily deduce from this proposition that two integers n and m are equal if and only if there exists a bijection from $[n]$ to $[m]$. A set E is *finite* if there exists an integer n and a bijection from E to $[n]$. This integer n is unique and is called the *cardinality* of E; it is denoted by $|E|$.

Let E and F be finite sets and $f: E \longrightarrow F$ be a mapping. With these notations, we have

$$\begin{array}{lcl} f \text{ injective} & \Longleftrightarrow & \forall y \in F,\ |f^{-1}(\{y\})| \leq 1 \ , \\ f \text{ surjective} & \Longleftrightarrow & \forall y \in F,\ |f^{-1}(\{y\})| \geq 1 \text{ and} \\ f \text{ bijective} & \Longleftrightarrow & \forall y \in F,\ |f^{-1}(\{y\})| = 1 \ . \end{array}$$

Moreover, if E is finite and $|E| = |F|$ then,

$$f \text{ injective} \Longleftrightarrow f \text{ surjective} \Longleftrightarrow f \text{ bijective}\,.$$

If E is not finite, these equivalences do not hold; for instance, $f: \mathbb{N} \Longrightarrow \mathbb{N}$ defined by $f(n) = 2n$ is injective, but not surjective.

Finally, the following properties are quite useful.

Proposition 1.9 *Let E and F be two finite sets.*

(i) *If E and F are disjoint then $|E \cup F| = |E| + |F|$.*
(ii) *If $(A_i)_{i \in [n]}$ is a partition of E then $|E| = |A_1| + \cdots + |A_n|$.*
(iii) $|E \times F| = |E| \times |F|$.
(iv) $|F^E| = |F|^{|E|}$, *where F^E denotes the set of mappings from E to F.*
(v) $|\mathcal{P}(E)| = 2^{|E|}$.

EXERCISE 1.15 Prove these properties. ♢

EXAMPLE 1.10 Let n be the number of strings that can be coded with sixteen bits. Each string is a sequence of 0s and 1s of length 16 and can be viewed as a mapping from [16] to $\mathbb{B} = \{0, 1\}$. Hence, $n = 2^{16} = 65\ 536$.

EXERCISE 1.16 A more picturesque way of stating Proposition 1.8 is the 'pigeonhole principle'. If $n < m$ and a flock of m pigeons flies into n pigeonholes then there must be at least one pigeonhole with two or more pigeons in it. More precisely, show that a pigeonhole will contain at least p pigeons, where p is an integer $p \geq m/n$. ♢

1.3.2 Countable sets

The notion of cardinality can be generalized to infinite sets in such a way that the following properties are verified for any two sets E and F:

(i) $|E| \leq |F| \iff$ there exists an injection from E to F.
(ii) $|E| \geq |F| \iff$ there exists a surjection from E to F.
(iii) $|E| = |F| \iff$ there exists a bijection from E to F.

EXERCISE 1.17 From the above relations, we deduce that if there exists both an injection and a surjection from E to F then there exists a bijection from E to F. Prove this result directly. ♢

A set E is *countable* if it is either finite or in a one-to-one correspondence with the set $\mathbb{N}$ of natural numbers. We denote by ω the cardinality of $\mathbb{N}$. A union $\bigcup_{i \in I} A_i$ is said to be countable if the set I of indices is countable.

The countable sets satisfy the following properties:

- Any subset of a countable set is countable.
- Any finite Cartesian product of countable sets is countable.
- Any countable union of countable sets is countable.

EXERCISE 1.18 Show that the set $\mathbb{N} \times \mathbb{N}$ is countable. ♢

Lastly, notice that there exist uncountable sets. This follows from the following result.

Proposition 1.11 *Let E be a set and let $\mathcal{P}(E)$ be the set of subsets of E. We have*

$$|E| < |\mathcal{P}(E)|\,.$$

Proof. We show by contradiction that there exists no bijection between E and $\mathcal{P}(E)$. Assume that $f\colon E \longrightarrow \mathcal{P}(E)$ is a bijective mapping, and let $A = \{x \in E \,/\, x \notin f(x)\}$. Assume that there exists an $a \in E$ such that $A = f(a)$:

- If $a \in A$, we deduce from the definition of A that $a \notin A$: contradiction.
- Similarly, the hypothesis $a \notin A$ leads to a contradiction.

Hence, A has no preimage by f, and this proves that f is not surjective and hence not bijective.

Hence, there exists no bijective mapping from E to $\mathcal{P}(E)$, and the sets E and $\mathcal{P}(E)$ thus have different cardinalities. The result is then deduced from the fact that the mapping $f\colon E \longrightarrow \mathcal{P}(E)$ defined by $f(x) = \{x\}$ is injective. □

We deduce that $\mathcal{P}(\mathbb{N})$ is uncountable.

Exercise 1.19 Consider the set U of sequences $(u_n)_{n\in\mathbb{N}}$ with values ranging over $\{0,1\}$, i.e. $\forall n \in \mathbb{N}$, $u_n \in \{0,1\}$. (Sequences are studied in Chapter 7.) Show that U is uncountable. ♢

1.4 Operations and relations

An *operation* Φ on a set E is a mapping $\Phi\colon E^n \longrightarrow E$. n is called the *arity*, or the *degree*, of Φ. We also say that Φ is an n-ary operation, and this is denoted by $a(\Phi) = n$. We will mainly study operations of arity two, or binary operations.

1.4.1 Binary operations

A *binary operation* or *binary relation* $*$ on a set E is a mapping $*\colon E \times E \longrightarrow E$. The image of a pair (x, y) by this operation is denoted by $x * y$ (infix notation). We define the following properties:

(i) $*$ is *associative* if $\forall a, b, c \in E$, $a * (b * c) = (a * b) * c$.
(ii) $*$ is *commutative* if $\forall a, b \in E$, $a * b = b * a$.
(iii) $*$ has the element $\mathbb{1}$ for *unit* if $\forall e \in E$, $e * \mathbb{1} = \mathbb{1} * e = e$.

If an operation $*$ is associative, we will denote by $a * b * c$ (without parentheses) the product of the three elements a, b and c that can be computed either as $(a * b) * c$ or as $a * (b * c)$. More generally, we will denote by $e_1 * e_2 * \cdots * e_n$ the product of n elements.

Exercise 1.20 Show that if $*$ has a unit, this unit is unique. ♢

Definition 1.12 *A set E together with an associative operation $*$ is a semi-group. If, moreover, E has a unit e for $*$, $(E, *, e)$ is said to be a monoid. If the operation $*$ is commutative, the semi-group (resp. the monoid) is said to be commutative.*

Example 1.13 The set $\mathbb{N}$ together with addition $+$ and its unit 0 is a commutative monoid. The set $\mathbb{N}$ together with multiplication $\times$ and its unit 1 is also a commutative monoid.

Example 1.14 The set $\mathcal{P}(E)$ equipped with intersection (or union) is a commutative monoid. The set of mappings from E to itself equipped with the composition of mappings is a non-commutative monoid if E has at least two elements. The set of square $n \times n$ matrices with real-valued entries in $\mathbb{R}$ is a monoid, non-commutative if $n > 1$, for the operation of multiplication of matrices.

A special case of monoids, discussed in more detail in Chapter 11 because of their importance in computer science, consists of the *free monoids*.

Definition 1.15 *Let A be a finite set called the alphabet, whose elements are called letters. The free monoid over A, denoted by A^*, is the set of strings written with letters of the alphabet A. A string u is just a finite sequence of letters.*

Given a string u, the number of elements of its sequence is called the length of u and is denoted by $|u|$. If the string u of length n is the sequence $(u_1, u_2, \ldots, u_n)$, it is simply denoted by $u = u_1u_2 \cdots u_n$. For instance, $aaba, acebdacebd, a, b, aa$ and aaa are strings over the alphabet $A = \{a, b, c, d, e\}$. The empty string, denoted by ε, is a special string of A^* containing no letters (the empty sequence). The operation of the monoid A^* is called *concatenation*. The concatenation of two strings $u = u_1u_2 \cdots u_n$ and $v = v_1v_2 \cdots v_m$ is the string $u \cdot v = u_1u_2 \cdots u_nv_1v_2 \cdots v_m$. For instance, $aaba \cdot cde = aabacde$. The unit for concatenation is of course the empty string ε.

Definition 1.16 *A set E equipped with an operation $*$ is a group if it is a monoid and every element has an inverse, i.e. $\forall e \in E, \exists e' \in E$ such that $e * e' = e' * e = \mathbb{1}$ (where $\mathbb{1}$ denotes the unit for $*$). If, moreover, $*$ is commutative, the group is said to be commutative.*

Example 1.17 The set $\mathbb{Z}$ of integers equipped with the addition operation is a commutative group. If E and operation $*$ form a monoid then the set of invertible elements of E is a group. In particular, the set of invertible $n \times n$ square matrices with real-valued entries in $\mathbb{R}$ is a group, non-commutative if $n > 1$, for the operation of multiplication of matrices.

Let $\top$ and $\perp$ be two operations on a set E. $\top$ is *distributive* over $\perp$ if $\forall a, b, c \in E$,

$$a \top (b \perp c) = (a \top b) \perp (a \top c)$$

and

$$(a \perp b) \top c = (a \top c) \perp (b \top c).$$

If the operation $\top$ is commutative, either of the above two conditions alone is of course enough.

EXAMPLE 1.18 In $\mathbb{R}$, multiplication is distributive over addition. In $\mathcal{P}(E)$, intersection and union are distributive over each other.

1.4.2 Relations

Definition 1.19 *A relation on a set E is a subset $\mathcal{R}$ of $E \times E$. To denote that a pair (e, e') of $E \times E$ is in this subset $\mathcal{R}$, we will use one of the following notations: $(e, e') \in \mathcal{R}$, $e \mathrel{\mathcal{R}} e'$, $\mathcal{R}(e, e')$.*

EXAMPLE 1.20

1. The following sets define relations on $E = \mathbb{N}$:
   - the set $\{(n, m) \,/\, n \le m\}$,
   - the set $\{(n, m) \,/\, n \le m \le 2n\}$,
   - the set $\{(n, m) \,/\, n \le m \text{ and } \exists k : n^2 + m^2 = k^2\}$.
2. For any set A, inclusion is a relation on $E = \mathcal{P}(A)$.

1.4.3 Set-theoretic operations on relations

Because a relation is a set, we can easily define:

- the *complement* $\overline{\mathcal{R}}$ of a relation $\mathcal{R}$; $\overline{\mathcal{R}}$ is the complement of $\mathcal{R}$ in $E \times E$:

$$(e, e') \in \overline{\mathcal{R}} \iff (e, e') \notin \mathcal{R} \ ,$$

- the *union* $\mathcal{R}_1 \cup \mathcal{R}_2$ of two relations $\mathcal{R}_1$ and $\mathcal{R}_2$:

$$(e, e') \in \mathcal{R}_1 \cup \mathcal{R}_2 \iff (e, e') \in \mathcal{R}_1 \text{ or } (e, e') \in \mathcal{R}_2 \ ,$$

- the *intersection* $\mathcal{R}_1 \cap \mathcal{R}_2$ of two relations $\mathcal{R}_1$ and $\mathcal{R}_2$:

$$(e, e') \in \mathcal{R}_1 \cap \mathcal{R}_2 \iff (e, e') \in \mathcal{R}_1 \text{ and } (e, e') \in \mathcal{R}_2 \ .$$

We can also define three special relations:

- the *empty relation*, denoted by $\emptyset_E$: $\forall e, e' \in E, \quad (e, e') \notin \emptyset_E$,

- the *full relation*, denoted by $\mathbf{\Pi}_E$: $\forall e, e' \in E, \quad (e, e') \in \mathbf{\Pi}_E$,
- the *identity relation*, denoted by Id_E: $\forall e, e' \in E, \ (e, e') \in Id_E \iff e = e'$.

Because $\mathcal{R}_1$ and $\mathcal{R}_2$ are sets, the property

$$\forall e, e' \in E, \ (e, e') \in \mathcal{R}_1 \quad \Longrightarrow \quad (e, e') \in \mathcal{R}_2$$

can be expressed by writing $\mathcal{R}_1 \subseteq \mathcal{R}_2$.

1.4.4 Other operations on relations

Let $\mathcal{R}$ be a binary relation on E. The *inverse relation*, denoted by $\mathcal{R}^{-1}$, is defined by

$$e \, \mathcal{R}^{-1} \, e' \quad \Longleftrightarrow \quad e' \, \mathcal{R} \, e \, .$$

Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be two binary relations on E. Their *product*, denoted by $\mathcal{R}_1.\mathcal{R}_2$, is the relation defined by

$$e \left(\mathcal{R}_1.\mathcal{R}_2\right) e' \quad \Longleftrightarrow \quad \exists e'' : e \, \mathcal{R}_1 \, e'' \text{ and } e'' \, \mathcal{R}_2 \, e'.$$

This product is associative; its unit is Id_E.

Let $\mathcal{R}$ be a binary relation. The relation $\mathcal{R}^*$ is equal to

$$Id_E \cup \mathcal{R} \cup (\mathcal{R}.\mathcal{R}) \cup (\mathcal{R}.\mathcal{R}.\mathcal{R}) \cup \cdots$$

or $\bigcup_{i \geq 0} \mathcal{R}^i$ with $\mathcal{R}^0 = Id_E$, $\mathcal{R}^{i+1} = \mathcal{R}.\mathcal{R}^i$, for $i \geq 0$. The relation $\mathcal{R}^+$ is defined by $\mathcal{R}^+ = \bigcup_{i>0} \mathcal{R}^i$, and hence $\mathcal{R}^* = Id_E \cup \mathcal{R}^+$.

We claim that $\forall i, j \leq 0, \mathcal{R}^{i+j} = \mathcal{R}^i.\mathcal{R}^j$. This result will be proved later (see Exercise 3.5).

Exercise 1.21 Let $\mathcal{R}$ be a binary relation on E. Show that

1. $(\mathcal{R}_1 \cup \mathcal{R}_2)^{-1} = \mathcal{R}_1^{-1} \cup \mathcal{R}_2^{-1}$.
2. $(\mathcal{R}_1 \cap \mathcal{R}_2)^{-1} = \mathcal{R}_1^{-1} \cap \mathcal{R}_2^{-1}$.
3. $\left(\overline{\mathcal{R}}\right)^{-1} = \overline{\mathcal{R}^{-1}}$.
4. $\mathcal{R}_1 \subseteq \mathcal{R}_2 \quad \Longleftrightarrow \quad \mathcal{R}_1^{-1} \subseteq \mathcal{R}_2^{-1}$.
5. $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$.
6. If $Id_E \subseteq \mathcal{R}$ then $\mathcal{R}^+ = \mathcal{R}^*$. Is the converse true? ♢

Exercise 1.22 Let $\mathcal{R}$ be a binary relation on E.

1. Show that
   (a) $(\mathcal{R}_1.\mathcal{R}_2)^{-1} = \mathcal{R}_2^{-1}.\mathcal{R}_1^{-1}$,
   (b) $(\mathcal{R}_1 \cup \mathcal{R}_2).\mathcal{R} = (\mathcal{R}_1.\mathcal{R}) \cup (\mathcal{R}_2.\mathcal{R})$,
   (c) $\mathcal{R}.(\mathcal{R}_1 \cup \mathcal{R}_2) = (\mathcal{R}.\mathcal{R}_1) \cup (\mathcal{R}.\mathcal{R}_2)$.
2. Show that $(\mathcal{R}_1 \cap \mathcal{R}_2).\mathcal{R} = (\mathcal{R}_1.\mathcal{R}) \cap (\mathcal{R}_2.\mathcal{R})$ does not necessarily hold, but that $(\mathcal{R}_1 \cap \mathcal{R}_2).\mathcal{R} \subsetneq (\mathcal{R}_1.\mathcal{R}) \cap (\mathcal{R}_2.\mathcal{R})$ holds. ♢

1.4.5 Some properties of binary relations

A relation $\mathcal{R}$ is said to be

- *left complete* if $\forall e \in E, \quad \exists e' \in E : e \,\mathcal{R}\, e'$,
- *right complete* if $\forall e' \in E, \quad \exists e \in E : e \,\mathcal{R}\, e'$.

The relation $\mathcal{R}$ is said to be

- *reflexive* if $\forall e \in E, \quad e \,\mathcal{R}\, e$,
- *irreflexive* if $\forall e, e' \in E, \quad e \,\mathcal{R}\, e' \implies e \neq e'$,
- *symmetric* if $\forall e, e' \in E, \quad e \,\mathcal{R}\, e' \implies e' \,\mathcal{R}\, e$,
- *antisymmetric* if $\forall e, e' \in E, \quad e \,\mathcal{R}\, e'$ and $e' \,\mathcal{R}\, e \implies e = e'$,
- *transitive* if $\forall e, e', e'' \in E, \quad e \,\mathcal{R}\, e'$ and $e' \,\mathcal{R}\, e'' \implies e \,\mathcal{R}\, e''$.

Exercise 1.23

1. Show that if $\mathcal{R}$ is left (resp. right) complete then $\mathcal{R}^{-1}$ is right (resp. left) complete.
2. Show that
   (i) $Id_E \subseteq \mathcal{R}.\mathcal{R}^{-1}$ if and only if $\mathcal{R}$ is left complete ,
   (ii) $Id_E \subseteq \mathcal{R}^{-1}.\mathcal{R}$ if and only if $\mathcal{R}$ is right complete .
3. Show that $\mathcal{R} \cap \mathcal{R}^{-1}$ and $\mathcal{R} \cup \mathcal{R}^{-1}$ are symmetric.
4. Show that if $\mathcal{R}$ and $\mathcal{R}'$ are transitive, then $\mathcal{R} \cap \mathcal{R}'$ is transitive, but $\mathcal{R} \cup \mathcal{R}'$ is not necessarily transitive.
5. Show that $\mathcal{R}^{+}$ is transitive.
6. Show that if $\mathcal{R}$ is transitive then $\mathcal{R} = \mathcal{R}^{+}$, and that if $\mathcal{R}$ is reflexive and transitive then $\mathcal{R} = \mathcal{R}^{*}$. $\diamondsuit$

Exercise 1.24 Is the relation $\mathcal{R}$ defined on $\mathbb{N}$ by $n \,\mathcal{R}\, m$ if and only if $m = n + 1$ symmetric? reflexive? transitive? What are the relations $\mathcal{R}^{+}$ and $\mathcal{R}^{*}$? $\diamondsuit$

Exercise 1.25 Is the relation '$n \,\mathcal{R}\, m$ if and only if n and m have a common divisor different from 1' transitive? $\diamondsuit$

Exercise 1.26 Let E be the finite set $\{e_1, ..., e_n\}$, and let $\mathcal{R}$ be a binary relation on E. We represent $\mathcal{R}$ by an $n \times n$ matrix, $M_{\mathcal{R}}$, with entries ranging over $\{0, 1\}$ as follows:

$$m_{i,j} = \begin{cases} 1 & \text{if } e_i \,\mathcal{R}\, e_j, \\ 0 & \text{otherwise.} \end{cases}$$

1. What property of $M_{\mathcal{R}}$ characterizes the fact that the relation $\mathcal{R}$ is symmetric? reflexive? irreflexive? antisymmetric?
2. Assuming $M_{\mathcal{R}}$ and $M_{\mathcal{R}'}$ are known, how can we compute $M_{\mathcal{R}^{-1}}$, $M_{\overline{\mathcal{R}}}$ and $M_{\mathcal{R}.\mathcal{R}'}$? $\diamondsuit$

1.4.6 Equivalence relations

Definition 1.21 *An equivalence relation is a reflexive, symmetric and transitive relation.*

EXAMPLE 1.22
(i) The equality on a set E is an equivalence relation, denoted by both $=$ and Id_E (see Section 1.4.3).
(ii) Let n be an integer greater than or equal to 2. The relation on $\mathbb{Z}$: 'x and y have the same remainder when divided by n' is an equivalence relation. It is denoted by both $x \equiv y[n]$ and $x \equiv y \bmod n$, and we say that 'x and y are *congruent modulo n*'.

The intersection $\mathcal{R} \cap \mathcal{R}'$ of two equivalence relations is also an equivalence relation, but the union $\mathcal{R} \cup \mathcal{R}'$ and the product $\mathcal{R}.\mathcal{R}'$ need not be equivalence relations.

Proposition 1.23 *If $\mathcal{R}$ is an arbitrary relation, $(\mathcal{R} \cup \mathcal{R}^{-1})^*$ is an equivalence relation, and it is the least equivalence relation containing $\mathcal{R}$.*

Proof. By definition, $(\mathcal{R} \cup \mathcal{R}^{-1})^*$ is reflexive and transitive. Since $\mathcal{R} \cup \mathcal{R}^{-1}$ is symmetric, $(\mathcal{R} \cup \mathcal{R}^{-1})^*$ also is symmetric.

Clearly, $(\mathcal{R} \cup \mathcal{R}^{-1})^*$ contains $\mathcal{R}$. Let $\mathcal{R}'$ be an equivalence relation containing $\mathcal{R}$. Since $\mathcal{R}'$ is symmetric, it also contains $\mathcal{R} \cup \mathcal{R}^{-1}$, and since it is reflexive and transitive, it contains $(\mathcal{R} \cup \mathcal{R}^{-1})^*$. □

EXERCISE 1.27 Show that if $\mathcal{R}$ and $\mathcal{R}'$ are two equivalence relations, the least equivalence relation containing $\mathcal{R}$ and $\mathcal{R}'$ is $(\mathcal{R} \cup \mathcal{R}')^+$. ♢

Definition 1.24 *Let $\mathcal{R}$ be an equivalence relation on E and e be an element of E. The set $\{e' \in E \,/\, e \,\mathcal{R}\, e'\}$, denoted by $[e]_{\mathcal{R}}$, is called the equivalence class of e.*

Proposition 1.25
1. $\forall e \in E \ , \ e \in [e]_{\mathcal{R}}$,
2. $\forall e, e' \in E, \ e \,\mathcal{R}\, e' \Longrightarrow [e]_{\mathcal{R}} = [e']_{\mathcal{R}}$,
3. *If* $[e]_{\mathcal{R}} \cap [e']_{\mathcal{R}} \neq \emptyset$, *then* $[e]_{\mathcal{R}} = [e']_{\mathcal{R}}$.

Proof. The first point is obvious because $e \,\mathcal{R}\, e$. To show the second point, consider $e'' \in [e']_{\mathcal{R}}$; then $e' \,\mathcal{R}\, e''$ and, as $e \,\mathcal{R}\, e'$, we also have $e \,\mathcal{R}\, e''$ and $e'' \in [e]_{\mathcal{R}}$. Hence, $[e']_{\mathcal{R}} \subseteq [e]_{\mathcal{R}}$. Conversely, $[e]_{\mathcal{R}} \subseteq [e']_{\mathcal{R}}$ for the same reasons. Lastly, if $e'' \in [e]_{\mathcal{R}} \cap [e']_{\mathcal{R}}$, then $e \,\mathcal{R}\, e''$ and $e'' \,\mathcal{R}\, e'$, and hence $e \,\mathcal{R}\, e'$ and $[e]_{\mathcal{R}} = [e']_{\mathcal{R}}$. □

The set $\{[e]_{\mathcal{R}} \,/\, e \in E\}$ of subsets of E, called the *factor set* of E by $\mathcal{R}$ and denoted by $E/\mathcal{R}$, is hence a *partition* of E. Conversely, if $A \subseteq \mathcal{P}(E)$ is a partition of E (i.e. $\forall E_1, E_2 \in A, E_1 \neq E_2 \Longrightarrow E_1 \cap E_2 = \emptyset$ and $\forall e \in E, \exists E_e \in A : e \in E_e$), we can define an equivalence relation $\mathcal{R}_A$ by $e \;\mathcal{R}_A\; e'$ if and only if e and e' are in the same subset of the partition. It is easy to see that this is indeed an equivalence relation.

Exercise 1.28 Let P and P' be two partitions of a set E. P is said to be a refinement of P' if $\forall p \in P$, $\exists p' \in P'$: $p \subseteq p'$.

Let $\mathcal{R}$ and $\mathcal{R}'$ be two equivalence relations on E. Show that $\mathcal{R} \subseteq \mathcal{R}'$ if and only if $E/\mathcal{R}$ is a refinement of $E/\mathcal{R}'$. $\diamondsuit$

Exercise 1.29 Let E be a set and let $\mathcal{F}$ be a set of subsets of E, i.e. $\mathcal{F} \subseteq \mathcal{P}(E)$. For $x \in E$, denote by $\mathcal{F}_x$ the set $\{X \in \mathcal{F} \,/\, x \in X\}$. Let $\mathcal{R}$ be the relation defined on E by

$$x \;\mathcal{R}\; y \Longleftrightarrow \mathcal{F}_x \subseteq \mathcal{F}_y \, .$$

1. Show that $\mathcal{F}$ is reflexive and transitive.
2. Show that $\mathcal{R}$ is antisymmetric if and only if: $\forall x, y \in E$, if $x \neq y$ then there exists $X \in \mathcal{F}$ such that $|X \cap \{x, y\}| = 1$.
3. Show that if $\forall X \in \mathcal{F}$, $\overline{X} \in \mathcal{F}$, then $\mathcal{R}$ is symmetric.
4. Assuming that the union and the intersection of any family of elements of $\mathcal{F}$ are elements of $\mathcal{F}$, prove the converse of 3. $\diamondsuit$

1.4.7 Congruences

Definition 1.26 *An equivalence relation $\mathcal{R}$ on a set endowed with an operation $*$ is said to be a congruence if it is compatible with the operation $*$, or, in other words if*

$$\forall e, e', d, d' \in E, \; (e \;\mathcal{R}\; e' \text{ and } d \;\mathcal{R}\; d') \quad \Longrightarrow \quad (e * d) \;\mathcal{R}\; (e' * d') \, .$$

Example 1.27 Let n be an integer greater than or equal to 2. The relation on $\mathbb{Z}$: '$x \equiv y[n]$' is a congruence for addition and for multiplication.

If $\mathcal{R}$ is a congruence on the set E equipped with the operation $*$, then the operation $*$ 'can be factored through' $\mathcal{R}$, i.e. the factor set $E/\mathcal{R}$ can be endowed with an operation $[*]$ defined by $[e][*][e'] = [e * e']$, and this operation $[*]$ is well defined. (It does not depend on the chosen representatives of the equivalence classes.) The operation $[*]$ will simply be denoted by $*$.

Proposition 1.28 *Let $\mathcal{R}$ be a congruence on a monoid (resp. group) $(E, *)$. The factor set $E/\mathcal{R}$ equipped with $*$ is a monoid (resp. group).*

EXAMPLE 1.29 Let n be an integer greater than or equal to 2. The factor of $\mathbb{Z}$ by the relation $x \equiv y[n]$ is denoted by $\mathbb{Z}/n\mathbb{Z}$. It is a group for addition and a monoid for multiplication.

EXERCISE 1.30 On the set $E = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ we define the operations + and × by

$$\begin{aligned}(a, b) + (c, d) &= (ad + bc, bd) \ , \\ (a, b) \times (c, d) &= (ac, bd) \ .\end{aligned}$$

1. Show that $(E, +)$ and $(E, \times)$ are commutative monoids.
We define on E a relation $\sim$ by: $(a, b) \sim (c, d) \Longleftrightarrow ad = bc$.
2. Show that $\sim$ is an equivalence relation on E and that it is a congruence for $+$ and $\times$.
3. Show that $(E/\sim, [+])$ is a group, show that $[\times]$ is distributive over $[+]$ and characterize the elements of $E/\sim$ having an inverse for $[\times]$.

Note: $(E/\sim, [+], [\times])$ is just the field $\mathbb{Q}$ of rational numbers. ♢