Chapter 1

Basic logic

The purpose of this chapter is to introduce the mathematical logic language used throughout the book, including the fundamentals of propositional logic and predicate logic. By studying this chapter, students will master the basic methods of mathematical reasoning, laying a solid foundation for learning algebra and analysis.

1.1 Mathematical statements

1.1.1 Definition. We call *statement* a declarative sentence without free variable in a given mathematical theory, whose truth value (that is, *true* or *false*) can in principle be determined. In a consistent mathematical theory, any statement is either true or false, but cannot be true and false in the same time.

1.1.2 Example. "2 is an even number", "$1 > 2$" are both statements. The former one is true, the latter is false.

1.1.3 Example. "$1 + 2$" is a computational formula, it is *not* a statement. The inequality "$2x + 1 > 0$" contains a free variable x, so judging its truth value is meaningless. Therefore, it is *not* a statement. In this book, we use the symbol $:=$ to interpret the notation on the left hand side of the symbol as the expression on the right hand side. For example, "$a := 3 + 5$" means that we denote by a the value of $3 + 5$. This expression is *not* a statement.

1.1.4 Definition. In a mathematical theory, statements admitted as true without justification are called the *axioms*. All statements that can be rigorously deduced from axioms are true. A statement that is confirmed to be true through rigorous mathematical proof is called a *theorem*. A statement that can be deduced from a theorem via straightforward reasoning is usually referred to as a *corollary* of that *theorem*.

In mathematical literature, a statement is often called a *proposition*. In this book, the term "*proposition*" is rather used to label theorems that are relatively simple or not repeatedly applied in the book.

1.1.5 Remark. Some mathematical conjectures have neither been proved nor disproved. However, these conjectures have similar forms with the statements the truth values of which have been determined. In principle the truth values of these conjectures could be determined in the future. They should be classified as statements. Furthermore, there exist declarative sentences that are neither provable nor disprovable within a certain mathematical theory. However, in an enriched axiomatic mathematical theory, their truth values can be in principle determined. Such declarative sentences should also be recognised as statements in the enriched mathematical theory.

1.2 Negation

Starting from given statements, compound statements can be constructed through the syntax of construction. This section introduces the negation of statements.

1.2.1 Definition. Let P be a statement. Then the sentence "*not* P" is also a statement, called the *negation* of P. It has the opposite true value of that of P. Sometimes we denote the statement "*not* P" as $\neg P$.

1.2.2 Notation. When a statement is expressed by a linking verb of judgement, its negation can be expressed by negating the linking verb. For example, the negation of the statement "2 *is an even number*" can be expressed as "2 *is not an even number*".

If a statement is expressed as a relation linked by a relation symbol, its negation could be expressed by overlaying the relation symbol with a diagonal line from the upper right to the lower left. For example, the negation of "$1 > 2$" can be expressed as "$1 \not> 2$".

1.2.3 Remark. The double negation of a statement P has the same truth value as that of the statement P. This point can be seen by the table of truth values as follows, where T stands for "true" and F stands for "false".

P	$\neg P$	$\neg\neg P$
T	F	T
F	T	F

1.3 Conjunction and disjunction

1.3.1 Definition. Let P and Q be statements. Then "P *and* Q" is a statement, called the *conjunction* of P and Q, often denoted as $P \wedge Q$. When both P and Q are true, the statement $P \wedge Q$ is true, otherwise it is false.

Similarly, the sentence "P *or* Q" is a statement, called the *disjunction* of P and Q, often denoted as $P \vee Q$. When both P and Q are false, the statement $P \vee Q$ is false, otherwise it is true.

1.3.2 Remark. We describe the truth values of conjunction and disjunction in the following table.

P	Q	$P \wedge Q$	$P \vee Q$	$Q \wedge P$	$Q \vee P$
T	T	T	T	T	T
T	F	F	T	F	T
F	T	F	T	F	T
F	F	F	F	F	F

We observe from the table that $P \wedge Q$ and $Q \wedge P$ have the same truth value, and $P \vee Q$ and $Q \vee P$ have the same truth value.

1.3.3 Proposition. *Let P and Q be statements. The statements $\neg(P \wedge Q)$ and $(\neg P) \vee (\neg Q)$ have the same truth value, and $\neg(P \vee Q)$ and $(\neg P) \wedge (\neg Q)$ have the same truth value.*

Proof. This can be observed from the following tables.

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$(\neg P) \wedge (\neg Q)$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

□

1.4 Conditional statement

1.4.1 Definition. Let P and Q be statements. The sentence "*if P, then Q*" is a statement, often denoted as $P \Rightarrow Q$. It has the same truth value as that of $(\neg P) \vee Q$. A statement of this form is called a *conditional statement*. We describe its true value in the following table.

P	Q	$\neg P$	$P \Rightarrow Q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

1.4.2 Remark. We observe from the table that, only in the case where P is true and Q is false, the statement $P \Rightarrow Q$ is false, otherwise it is true. Therefore, if one can prove Q under the assumption that P is true, then the statement $P \Rightarrow Q$ is true. However, the statement $P \Rightarrow Q$ itself does not signify that we are considering a proof of the statement Q from P.

We also observe from the table that, in the case where both P and $P \Rightarrow Q$ are true, the statement Q must be true. This type of reasonings often appear in a mathematical proof.

1.4.3 Proposition. *Let P, Q and R be statements. If both $P \Rightarrow Q$ and $Q \Rightarrow R$ are true, then $P \Rightarrow R$ is true.*

Proof. It suffices to treat the case where P is true, since otherwise $P \Rightarrow R$ is automatically true. In the case where P is true, since $P \Rightarrow Q$ is true, we deduce that Q is true. Furthermore, since $Q \Rightarrow R$ is true, we deduce that R is true. Therefore, $P \Rightarrow R$ is true. □

1.4.4 Proposition. *Let P and Q be statements. The statements $P \Rightarrow Q$ and $(\neg Q) \Rightarrow (\neg P)$ have the same truth value.*

Proof. We could conclude from the following table.

P	Q	$\neg P$	$\neg Q$	$(\neg Q) \Rightarrow (\neg P)$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

□

1.4.5 Definition. Let P and Q be two statements. The statement $(\neg Q) \Rightarrow (\neg P)$ is called the *contrapositive* of the statement $P \Rightarrow Q$. If one proves the contrapositive statement $(\neg Q) \Rightarrow (\neg P)$, then, by Proposition 1.4.4, we obtain that the statement $P \Rightarrow Q$ is also true. This method is called *proof by contraposition.*

1.4.6 Example. Let n be an integer. We prove by contraposition that, if n^2 is an even number, then n is an even number. Note that the contrapositive of this statement says that, if n is not an even number, then n^2 is not an even number. Since n is an integer, if n is not an even number, it must be an odd number, namely it is of the form $2k + 1$, with k being an integer. Therefore,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$

is an odd number. Thus we have proved the contrapositive statement. Hence the initial statement is also true.

1.5 Biconditional statement

1.5.1 Definition. Let P and Q be statements. Then "P *if and only if* Q" is also a statement, often denoted as $P \Leftrightarrow Q$. When P and Q have the same truth value, the statement $P \Leftrightarrow Q$ is true, otherwise $P \Leftrightarrow Q$ is false. By definition, the statements $P \Leftrightarrow Q$ and $Q \Leftrightarrow P$ have the same true value.

1.5.2 Proposition. *Let P and Q be statements. Then $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ and $P \Leftrightarrow Q$ have the same truth value.*

Proof. We could conclude from the following table.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

□

1.5.3 Remark. The above proposition shows that, given two statements P and Q, to prove that they have the same truth value, it suffices to prove conditional statements of both directions $P \Rightarrow Q$ and $Q \Rightarrow P$. The statement $Q \Rightarrow P$ is called the *converse* of $P \Rightarrow Q$. The contraposition of $Q \Rightarrow P$, namely $(\neg P) \Rightarrow (\neg Q)$, is called the *inverse* of $P \Rightarrow Q$. Proposition 1.4.4 shows that the converse and

the inverse of a conditional statement have the same truth value. Therefore, to justify the biconditional statement $P \Leftrightarrow Q$, it also suffices to prove the conditional statement $P \Rightarrow Q$ and its inverse $(\neg P) \Rightarrow (\neg Q)$.

1.5.4 Example. Let n be an integer. Then n^2 is an even number if and only if n is an even number. In fact, we have proved in Example 1.4.6 that, if n^2 is an even number, then n is an even number. It remains to check that, if n is an even number, then n^2 is also an even number. Assume that n is of the form $2k$, where k is an integer. Then $n^2 = 4k^2$ is divisible by 2. Hence n^2 is an even number.

1.6 Proof by contradiction

1.6.1 Definition. In a consistent mathematical theory, a statement cannot be true and false at the same time. Let P be a statement. If we assume that $\neg P$ is true and deduce that a certain statement is both true and false, then we say that a *contradiction* happens and the assumption $\neg P$ is false. Thus the statement P is true. Such a reasoning is called *proof by contradiction*.

1.6.2 Example. We prove by contradiction that the equation $x^2 = 2$ does not have any rational solution. Suppose by contradiction that p/q is a solution of the equation $x^2 = 2$, where p is an integer and q is a positive integer, which do not have common prime divisor. By definition, one has $p^2 = 2q^2$. Hence p^2 is an even number. By Example 1.5.4, we obtain that p is an even number. Hence there exists $p_1 \in \mathbb{Z}$ such that $p = 2p_1$. Hence we deduce from $p^2 = 2q^2$ that $2q_1^2 = q^2$. This shows that q^2 is an even number and hence q is an even number. Thus p and q has 2 as a common prime divisor, which leads to a contradiction.

Exercises

1. Let P and Q be statements. Use truth tables to determine the truth values of the following statements according to the truth values of P and Q:

$$P \wedge \neg P,\ P \vee \neg P,\ (P \vee Q) \Rightarrow (P \wedge Q),\ (P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$$

2. Let P and Q be statements.

(1) Show that $P \Rightarrow (Q \wedge \neg Q)$ has the same truth value as $\neg P$.

(2) Show that $(P \wedge \neg Q) \Rightarrow Q$ has the same truth value as $P \Rightarrow Q$.

3. Consider the following statements:

$P :=$ "Little Bear is happy",
$Q :=$ "Little Bear has done her math homework",
$R :=$ "Little Rabbit is happy".

Express the following statements using P, Q, and R, along with logical connectives:

(1) If Little Bear is happy and has done her math homework, then Little Rabbit is happy.

(2) If Little Bear has done her math homework, then she is happy.

(3) Little Bear is happy only if she has done her math homework.

4. Does the following reasoning hold? Justify your answer.

— It is known that Little Bear is both smart and lazy, or Little Bear is not smart.

— It is also known that Little Bear is smart.

— Therefore, Little Bear is lazy.

5. Does the following reasoning hold? Justify your answer.

— It is known that at least one of the lion or the tiger is guilty.

— It is also known that either the lion is lying or the tiger is innocent.

— Therefore, the lion is either lying or guilty.

6. An explorer arrives at a cave with three closed doors, numbered 1, 2, and 3. Exactly one door hides treasure, while the other two conceal deadly traps.

— Door 1 states: "*The treasure is not here*";

— Door 2 states: "*The treasure is not here*";

— Door 3 states: "*The treasure is behind Door 2*".

Only one of these statements is true. Which door should the explorer open to find the treasure?

7. The Kingdom of Truth sent an envoy to the capital of the Kingdom of Lies. Upon entering the border, the envoy encountered a fork with three paths: dirt, stone, and concrete. Each path had a signpost:

— The concrete path's sign: "*This path leads to the capital, and if the dirt path leads to the capital, then the stone path also does.*"

— The stone path's sign: "*Neither the concrete nor the dirt path leads to the capital.*"

— The dirt path's sign: "*The concrete path leads to the capital, but the stone path does not.*" All signposts lie. Which path should the envoy take?

8. Let a and b be real numbers. Prove that, if $a \neq -1$ and $b \neq -1$, then $ab + a + b \neq -1$.

9. Let a, b, and c be positive real numbers such that $abc > 1$ and

$$a + b + c < \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

Prove the following:

(1) None of a, b, or c equals 1.

(2) At least one of a, b, or c is greater than 1.

(3) At least one of a, b, or c is less than 1.

10. Let $a \neq 0$ and b be real numbers. For real numbers x and y, prove that if $x \neq y$, then $ax + b \neq ay + b$.

11. Let $n \geq 2$ be an integer. Prove that if n is composite, then there exists a prime number p dividing n such that $p \leq \sqrt{n}$.

12. Let n be an integer. Prove that either 4 divides n^2 or 4 divides $n^2 - 1$.

13. Let n be an integer. Prove that 12 divides $n^2(n^2 - 1)$.

14. Prove that any integer divisible by 4 can be written as the difference of two perfect squares.

15. Let x and y be non-zero integers. Prove that $x^2 - y^2 \neq 1$.

16. A plane has 300 seats and is fully booked. The first passenger ignores their assigned seat and chooses randomly. Subsequent passengers take their assigned seat if available; otherwise, they choose randomly. What is the probability that the last passenger sits in their assigned seat?

17. Little Bear, Little Goat, and Little Rabbit are all wearing hats. A parrot prepared four red feathers and four blue feathers to decorate their hats. The parrot selected two feathers for each hat-wearing animal to place on their hats. Each animal cannot see the feathers on their own hat but can see the feathers on the other animals' hats. Here is their conversation:

— Little Bear: *I don't know what color the feathers on my hat are, but I know the other animals also don't know what color the feathers on their hats are.*"

— Little Goat: *Haha, now even without looking at Little Bear's hat, I know what color the feathers on my hat are.*"

— Little Rabbit: *Now I know what color the feathers on my hat are.*"

— Little Bear: *Hmm, now I also know what color the feathers on my hat are.*"

Question: What color are the feathers on Little Goat's hat?

18. The Sphinx tells the truth on one fixed weekday and lies on the other six. Cleopatra visits The Sphinx for three consecutive days:

— Day 1: The Sphinx declared, "*I lie on Monday and Tuesday.*"

— Day 2: The Sphinx declared, "*Today is either Thursday, or Saturday, or Sunday.*"

— Day 3: The Sphinx declared, "*I lie on Wednesday and Friday.*"

On which day does the Sphinx tell the truth? On which days of the week did Cleopatra visit the Sphinx?

Chapter 2

Sets

This book presents the fundamentals of algebra and analysis based on set theory. Set theory, proposed initially by Cantor, is the cornerstone of modern mathematics. Before the emergence of set theory, the progress of mathematics was often built upon intuition and visual imagery. Moreover, due to the limitations of available tools, the scope of mathematical research was relatively narrow—for instance, analysis was often confined to studying functions with analytic expressions. Cantor's set theory introduced a new language and new tools to mathematics, greatly advancing the development of modern mathematics.

Naive set theory regards a set as a collection of distinct objects that are clearly defined. However, treating any such collection as a set without restriction leads to paradoxes. For example, Russell's paradox considers the collection of all sets that do not contain themselves. If this collection is treated as a set, one arrives at a contradiction regardless of whether the set contains itself or not. Determining which types of collections should be considered as sets is a subtle issue that lacks universal agreement. Axiomatic set theory treats set theory itself as a structure governed by a system of axioms. These axioms ensure the existence of constructions needed in mathematics while avoiding known paradoxes, thus providing a sound foundation for mathematics.

The goal of this chapter is to introduce some fundamental concepts of set theory and basic structures to prepare for the chapters that follow. Since our aim is not to give a systematic introduction to mathematical logic, we will explain ideas as much as possible using natural language rather than formal language.

2.1 Roster notation

2.1.1 Definition. In naive set theory, a set refers to a certain collection of *distinct* objects. The objects in a set are called *elements* of it. Two sets A and B are said

to be *equal* if they have the same elements. We denote by $A = B$ the statement "*A and B are equal*".

If A is a set and a is an object, we denote by $a \in A$ the statement

"a is an element of A";

we denote by $a \notin A$ the statement

"a is not an element of A".

If a is an element of A, we also say that *a belongs to A*.

2.1.2 Notation. The *roster method* of representing a set refers to a notation where all elements of the set are explicitly enumerated in a single row within a pair of curly braces. For example the set consisting of the elements 1, 2 and 3 can be denoted as $\{1, 2, 3\}$. The represented set is independent of the enumeration order or element repetition. For example, one has

$$\{1, 2, 3\} = \{3, 2, 1\} = \{1, 1, 2, 3\}.$$

When representing a set using the roster method, an ellipsis $(\ldots)$ may be used to indicate elements with an obvious pattern. For example, the set of positive integers less than 100 can be written as:

$$\{1, 2, \ldots, 100\}.$$

Similarly, if n is a natural number the set of natural numbers not exceeding n can be written as

$$\{0, 1, \ldots, n\}.$$

When no ambiguity arises, an ellipsis may also be used to omit infinitely many elements with a clear pattern. For example, the set of all even integers can be expressed in roster notation as:

$$\{..., -6, -4, -2, 0, 2, 4, 6, ...\}.$$

When representing sets using the roster method, if the elements are indexed, an ellipsis can be used to summarise elements corresponding to indices with obvious patterns. For example, if n is a positive integer and for each $i \in \{1, \ldots, n\}$, a mathematical object x_i is given, then the set of these objects can be written as:

$$\{x_1, \ldots, x_n\}.$$

Similarly, if, for every natural number n, a mathematical object y_n, then the set of these objects can be written as:

$$\{y_0, y_1, y_2, \ldots\}.$$

More generally, if I is a set and if, for any $i \in I$, a mathematical object x_i is given, then the set of these objects can be written as

$$\{x_i \,|\, i \in I\},$$

where I is called the *index set* of this roster writing. For example,

$$\{2n \,|\, n \in \mathbb{Z}\}$$

denotes the set of all even numbers,

$$\{2n + 1 \,|\, n \in \mathbb{Z}\}$$

denotes the set of all odd numbers.

2.1.3 Definition. Let A and B be sets. We denote by $A \times B$ the following set of ordered pairs

$$\{(x, y) \mid x \in A,\ y \in B\},$$

and call it the *Cartesian product* of sets A and B.

More generally, if n is a positive integer and $A_1, \ldots, A_n$ be sets, we denote by

$$A_1 \times \cdots \times A_n$$

the set of all n-tuples $(x_1, \ldots, x_n)$, where $x_1 \in A_1, \ldots, x_n \in A_n$.

2.2 Subsets and powersets

2.2.1 Definition. Let A and B be sets. If any element of A is an element of B, we say that A is a *subset* of B. We denote by $A \subseteq B$ or by $B \supseteq A$ the statement

"*A is a subset of B*".

If A is a subset of B and A is *not* equal to B, we say that A is a *proper subset* of B, denoted by $A \subset B$ or by $B \supset A$.

If A is a subset (resp. proper subset) of B, we also say that A is *contained* (resp. *strictly contained*) in B, or that B *contains* (resp. *contains strictly*) A.

2.2.2 Remark. By definition, any set A is a subset of itself. Moreover, for any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then the sets A and B have the same elements, namely $A = B$.

2.2.3 Definition. We denote by $\varnothing$ the set that does not contain any element, and we call it the *empty set*. By definition, the empty set is a subset of any set.

2.2.4 Proposition. *Let A, B and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Proof. Let x be an element of A. Since $A \subseteq B$, x is an element of B. Since $B \subseteq C$, x is an element of C. Therefore, one has $A \subseteq C$. □

2.2.5 Definition. Let X be a set. We denote by $\mathscr{P}(X)$ the set of all subsets of X, called the *power set* of X. Note that $\{\varnothing, X\} \subseteq \mathscr{P}(X)$.

2.2.6 Example. The only subset of the empty set is itself, namely $\mathscr{P}(\varnothing) = \{\varnothing\}$. Moreover, $\mathscr{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$.

2.3 Set-builder notation

2.3.1 Definition. Let A be a set. If for any $x \in A$, we fix a statement $P(x)$, then we say that $P(\cdot)$ is a *condition* on A. For example, "*x is an odd number*" is a condition on $\mathbb{Z}$. If $P(x)$ is true, then we say that x *satisfies* the condition $P(\cdot)$.

Let A be a set and $P(\cdot)$ be a condition on A. We denote by

$$\{x \in A \,|\, P(x)\}$$

the set of elements $x \in A$ such that $P(x)$ is true. This is a subset of A. Such representation of a new set by a condition on a given set is called *set-builder notation*.

2.3.2 Notation. Sometimes we combine the roster notation and the set-builder notation to describe a set. Let I be a set. For any $i \in I$, let x_i be a mathematical object. Let $P(\cdot)$ be a condition on I, and I_P be the set $\{i \in I \,|\, P(i)\}$. The we use the expression

$$\{x_i \,|\, i \in I,\ P(i)\}$$

to denote the set

$$\{x_i \,|\, i \in I_P\}.$$

2.3.3 Example. In the set-builder notation, it is important to fix an environmental set on which we consider a condition. If, for any set A, we consider a statement $P(A)$ (having a determined truth value), then the collection of all sets A such that $P(A)$ is true does not necessarily form a set.

For example, Russell's paradox considers the collection of all sets A such that $A \notin A$. If we consider this collection as a set, either it belongs to itself or not will lead to a contradiction.

Moreover, the collection of all sets should not be consider as a set. In fact, if the collection $\mathscr{S}$ of all sets is a set, then by the set-builder notation, the construction in Russell's paradox should also be a set, which would be expressed as

$$\{A \in \mathscr{S} \,|\, A \notin A\}.$$

This leads to a contradiction.

2.4 Set difference

2.4.1 Definition. Let A and B be sets. Then the set

$$\{x \in B \,|\, x \notin A\}$$

is called the *set difference* of B and A. In the case where A is a subset of B, we also call $B \setminus A$ as the *complement* of A in B.

2.4.2 Example. Let A be a set, $P(\cdot)$ be a condition on A. Then the following equality holds:

$$\{x \in A \,|\, \neg P(x)\} = A \setminus \{x \in A \,|\, P(x)\}. \tag{2.1}$$

2.4.3 Proposition. *Let A and B be sets. Then $B \setminus A = \varnothing$ if and only if $B \subseteq A$. In particular, in the case where A is a subset of B, the set $B \setminus A$ is empty if and only if $A = B$.*

Proof. Suppose that $B \setminus A = \varnothing$. For any element x of B, one has $x \in A$ since otherwise $x \in B \setminus A$, which leads to a contradiction. Hence $B \subseteq A$.

Suppose that $B \setminus A \neq \varnothing$. Let x be an arbitrary element of $B \setminus A$. It is hence an element of B that does not belong to A. Therefore B is not included in A.

Suppose that $A \subseteq B$. If $B \setminus A = \varnothing$, by the first conclusion we obtain $B \subseteq A$, hence we deduce $A = B$ by the condition $A \subseteq B$. Conversely, if $A = B$, by definition one has $B \setminus A = \varnothing$. □

2.4.4 Proposition. *Let A and B be sets. Then*

$$B \setminus (B \setminus A) = \{x \in B \,|\, x \in A\}.$$

When $A \subseteq B$, one has

$$B \setminus (B \setminus A) = A.$$

In particular, $B \setminus \varnothing = B$.

Proof. By definition,

$$B \setminus (B \setminus A) = \{x \in B \,|\, x \notin B \setminus A\}.$$

Let x be an element of $B \setminus (B \setminus A)$. By definition, $x \in B$ and $x \notin B \setminus A$. If x does not belong to A, then $x \in B \setminus A$, which leads to a contradiction. Hence we obtain $x \in A$.

Conversely, let x be a common element of A and B. By definition, $x \in B$, and x is not an element of $B \setminus A$ since $x \in A$. Hence x belongs to $B \setminus (B \setminus A)$.

In the case where $A \subseteq B$, by definition one has

$$\{x \in B \,|\, x \in A\} = A.$$

Hence

$$B \setminus (B \setminus A) = A.$$

Apply this equality to the case where $A = B$, by Proposition 2.4.3 we get

$$B \setminus \varnothing = B \setminus (B \setminus B) = B.$$

□

2.5 Quantifiers

2.5.1 Definition. Let A be a set and $P(\cdot)$ be a condition on A.

We use the expression

$$\forall\, x \in A,\ P(x)$$

to denote the statement

$$\{x \in A \,|\, P(x)\} = A.$$

We often read it as

"*for any $x \in A$, x satisfies the condition $P(\cdot)$*".

We use the expression

$$\exists\, x \in A,\ P(x)$$

to denote the statement

$$\{x \in A \,|\, P(x)\} \neq \varnothing.$$

We often read it as

"*there exists $x \in A$ which satisfies the condition $P(\cdot)$*".

2.5.2 Example. Let $P(\cdot)$ be any condition on the empty set $\varnothing$. Note that

$$\{x \in \varnothing \,|\, P(x)\}$$

is a subset of $\varnothing$. Hence it is equal to $\varnothing$. Therefore,

$$\forall\, x \in \varnothing,\ \mathbb{P}(x)$$

is true, and

$$\exists\, x \in \varnothing,\ \mathbb{P}(x)$$

is false.

2.5.3 Proposition. (1) *The statements*

$$\text{“}\exists\, x \in A,\ \neg P(x)\text{”} \text{ and } \text{“}\forall\, x \in A,\ P(x)\text{”}$$

have opposite truth values.

(2) *The statements*

$$\text{“}\forall\, x \in A,\ \neg P(x)\text{”} \text{ and } \text{“}\exists\, x \in A,\ P(x)\text{”}$$

have opposite truth values.

Proof. (1) Note that

$$\{x \in A \,|\, \neg P(x)\} = A \setminus \{x \in A \,|\, P(x)\}.$$

By Proposition 2.4.3, $\{x \in A \,|\, P(x)\} = A$ if and only if $\{x \in A \,|\, \neg P(x)\} = \varnothing$. Hence the statements

$$\text{“}\exists\, x \in A,\ \neg P(x)\text{”} \text{ and } \text{“}\forall\, x \in A,\ P(x)\text{”}$$

have opposite truth values.

(2) We apply (1) to the condition $\neg P(\cdot)$ to obtain that

$$\text{“}\forall\, x \in A,\ \neg P(x)\text{”} \text{ and } \text{“}\exists\, x \in A,\ \neg\neg P(x)\text{”}$$

have opposite truth values. Since, for any $x \in A$, $\neg\neg P(x)$ and $P(x)$ have the same truth value, we obtain that “$\exists\, x \in A$, $\neg\neg P(x)$” and “$\exists\, x \in A$, $P(x)$” have the same truth value. The statement is thus proved. □

2.6 Sufficient and necessary conditions

2.6.1 Definition. Let A be a set, $P(\cdot)$ and $Q(\cdot)$ be conditions on A. If

$$\{x \in A \,|\, P(x)\} \subseteq \{x \in A \,|\, Q(x)\},$$

we say that $P(\cdot)$ is a *sufficient condition* of $Q(\cdot)$, and $Q(\cdot)$ is a *necessary condition* of $P(\cdot)$. If

$$\{x \in A \,|\, P(x)\} = \{x \in A \,|\, Q(x)\},$$

we say that $P(\cdot)$ is a *necessary and sufficient condition* of $Q(\cdot)$, or that the conditions $P(\cdot)$ and $Q(\cdot)$ are *equivalent*.

2.6.2 Proposition. *Let A be a set, $P(\cdot)$ and $Q(\cdot)$ be conditions on A.*

(1) *$P(\cdot)$ is a sufficient condition of $Q(\cdot)$ if and only if*

$$\forall\, x \in A,\ P(x) \Rightarrow Q(x).$$

(2) *$P(\cdot)$ is a necessary condition of $Q(\cdot)$ if and only if*

$$\forall\, x \in A,\ Q(x) \Rightarrow P(x).$$

(3) *$P(\cdot)$ is a necessary and sufficient condition of $Q(\cdot)$ if and only if*

$$\forall\, x \in A,\ P(x) \Leftrightarrow Q(x).$$

Proof. (1) By 2.4.3, we obtain that $P(\cdot)$ is a sufficient condition of $Q(\cdot)$ if and only if

$$\{x \in A \,|\, P(x)\} \setminus \{x \in A \,|\, Q(x)\} = \varnothing.$$

Moreover,

$$\begin{aligned}\{x \in A \,|\, P(x)\} \setminus \{x \in A \,|\, Q(x)\} &= \{x \in A \,|\, P(x) \wedge (\neg Q(x))\} \\ = A \setminus \{x \in A \,|\, (\neg P(x)) \vee Q(x)\} &= A \setminus \{x \in A \,|\, P(x) \Rightarrow Q(x), \}\end{aligned}$$

where the second equality comes from (2.1) and Proposition 1.3.3. By Proposition 2.4.3 ,

$$\{x \in A \,|\, P(x)\} \setminus \{x \in A \,|\, Q(x)\} = \varnothing.$$

if and only if

$$\{x \in A \,|\, P(x) \Rightarrow Q(x)\} = A,$$

namely

$$\forall\, x \in A,\ P(x) \Rightarrow Q(x).$$

(2) follows from (1) by switching $P(\cdot)$ and $Q(\cdot)$.
(3) follows from (1), (2), and Proposition 1.5.2. □

2.7 Union

2.7.1 Definition. Let I be a set. For any $i \in I$, let A_i be a set. We say that $(A_i)_{i\in I}$ is a *family of sets* parametrised by I.

We denote by $\bigcup_{i\in I} A_i$ the set consisting of all elements of all A_i. It is called the *union* of the sets A_i, $i \in I$. By definition, a mathematical object x belongs to $\bigcup_{i\in I} A_i$ if and only if

$$\exists\, i \in I,\ x \in A_i.$$

In particular, $\bigcup_{i\in I} A_i$ is empty when $I = \varnothing$.

2.7.2 Notation. Let n be a positive integer, $A_1, \ldots, A_n$ be sets. We denote $\bigcup_{i\in\{1,\ldots,n\}} A_i$ as

$$A_1 \cup \ldots \cup A_n.$$

Note that it does not depend on the order of $A_1, \ldots, A_n$.

2.7.3 Proposition. *Let I be a set and $(A_i)_{i\in I}$ be a family of sets parametrised by I. Let B be a set. Then $\bigcup_{i\in I} A_i \subseteq B$ if and only if*

$$\forall\, i \in I,\ A_i \subseteq B.$$

Proof. Let $A := \bigcup_{i\in I} A_i$.

For any $i \in I$ one has $A_i \subseteq A$. If $A \subseteq B$, then by Proposition 2.2.4 we deduce that $A_i \subseteq B$.

Conversely, we suppose that, for any $i \in I$, one has $A_i \subseteq B$. Let x be an element of A. By definition, there exists $i \in I$ such that $x \in A_i$. Since $A_i \subseteq B$, one has $x \in B$. Therefore, $A \subseteq B$. □

2.7.4 Corollary. *Let B and I be sets. For any $i \in I$, let $P_i(\cdot)$ be a condition on B. Then*

$$\{x \in B \,|\, \exists\, i \in I,\ P_i(x)\} = \bigcup_{i\in I} \{x \in B \,|\, P_i(x)\}.$$

Proof. Let

$$A := \{x \in B \,|\, \exists\, i \in I,\ P_i(x)\}.$$

For any $i \in I$, let

$$A_i := \{x \in B \,|\, P_i(x)\}.$$

For any $x \in A$, there exists $i \in I$ such that $P_i(x)$ is true. Hence $x \in \bigcup_{i\in I} A_i$.

Conversely, by definition, for any $i \in I$, one has $A_i \subseteq A$. Hence, by Proposition 2.7.3, one has

$$\bigcup_{i\in I} A_i \subseteq A.$$

□

2.7.5 Proposition. *Let $(A_i)_{i\in I}$ be a family of sets, and B be a set. Then*

$$\left(\bigcup_{i\in I} A_i\right) \setminus B = \bigcup_{i\in I} (A_i \setminus B).$$

Proof. Let $A := \bigcup_{i\in I} A_i$.

For any $i \in I$, one has $A_i \subseteq A$. Hence $A_i \setminus B \subseteq A \setminus B$. By Proposition 2.7.3, we obtain $\bigcup_{i\in I}(A_i \setminus B) \subseteq A \setminus B$.

Conversely, if $x \in A \setminus B$, then $x \in A$ and $x \notin B$. By definition, there exists $i \in I$ such that $x \in A_i$, and hence $x \in A_i \setminus B$. This leads to $A \setminus B \subseteq \bigcup_{i\in I}(A_i \setminus B)$. □

2.8 Intersection

2.8.1 Definition. Let I be a non-empty set and $(A_i)_{i\in I}$ be a family of sets parametrised by I. We denote by $\bigcap_{i\in I} A_i$ the set of all common elements of A_i, $i \in I$. This set is called the *intersection* of A_i, $i \in I$. Note that, if i_0 is an arbitrary element of I, the set-builder notation ensures that

$$\{x \in A_{i_0} \,|\, \forall\, i \in I,\ x \in A_i\}$$

is a set. This set is the intersection of $(A_i)_{i\in I}$.

By definition, an mathematical object x belongs to $\bigcap_{i\in I} A_i$ if and only if

$$\forall\, i \in I,\ x \in A_i.$$

2.8.2 Notation. Let n be a positive integer, $A_1, \ldots, A_n$ be sets. We denote $\bigcap_{i\in\{1,\ldots,n\}} A_i$ as

$$A_1 \cap \ldots \cap A_n.$$

Note that it does not depend on the order of $A_1, \ldots, A_n$. In particular, if A and B are two sets, then

$$\{x \in B \,|\, x \in A\} = B \cap A.$$

Therefore, the first statement of Proposition 2.4.4 becomes

for any sets A and B, one has $B \setminus (B \setminus A) = B \cap A$.

2.8.3 Remark. In set theory, it does not make sense to consider the intersection of an empty family of sets. In fact, if such an intersection existed as a set, for any mathematical object x, since the statement

$$\forall\, i \in \varnothing,\ x \in A_i$$

is true (see Example 2.5.2), we would obtain that x belongs to $\bigcap_{i\in\varnothing} A_i$. By Russell's paradox, this is impossible.

2.8.4 Proposition. *Let I be a non-empty set and $(A_i)_{i\in I}$ be a set parametrised by I. Let B be a set. Then $B \subseteq \bigcap_{i\in I} A_i$ if and only if*

$$\forall\, i \in I,\ B \subseteq A_i.$$

Proof. Let $A = \bigcap_{i\in I} A_i$.

Suppose that $B \subseteq A$. For any $x \in B$, one has $x \in A$, and hence

$$\forall\, i \in I,\ x \in A_i.$$

Therefore, for any $i \in I$, B is contained in A_i.

Suppose that, for any $i \in I$, $B \subseteq A_i$. Then, for any $x \in B$ and any $i \in I$, one has $x \in A_i$. Hence, for any $x \in B$, one has $x \in A$. Therefore, $B \subseteq A$. □

2.8.5 Corollary. *Let B be a set, I be a non-empty set. For any $i \in I$, let $P_i(\cdot)$ be a condition on B. Then*

$$\{x \in B \,|\, \forall\, i \in I,\ P_i(x)\} = \bigcap_{i \in I} \{x \in B \,|\, P_i(x)\}.$$

Proof. Let

$$A := \{x \in B \,|\, \forall\, i \in I,\ P_i(x)\}.$$

For any $i \in I$, let

$$A_i := \{x \in B \,|\, P_i(x)\}.$$

For any $x \in A$ and any $i \in I$, $P_i(x)$ is true. Hence $A \subseteq A_i$. By Proposition 2.8.4, we obtain

$$A \subseteq \bigcap_{i \in I} A_i.$$

Conversely, if $x \in \bigcap_{i \in I} A_i$, then for any $i \in I$, one has $x \in A_i$. Hence $x \in B$, and for any $i \in I$, $P_i(x)$ is true. Thus $x \in A$. □

2.8.6 Proposition. *Let B be a set, $(A_i)_{i \in I}$ be a non-empty family of sets. The following equality holds*

$$\left(\bigcap_{i \in I} A_i\right) \setminus B = \bigcap_{i \in I} (A_i \setminus B).$$

Proof. Let $A := \bigcap_{i \in I} A_i$. For any $i \in I$, one has $A \subseteq A_i$. Hence

$$A \setminus B = \{x \in A \,|\, x \notin B\} \subseteq \{x \in A_i \,|\, x \notin B\}.$$

By Proposition 2.8.4, we get

$$A \setminus B \subseteq \bigcap_{i \in I} (A_i \setminus B).$$

Conversely, if $x \in \bigcap_{i \in I} (A_i \setminus B)$, then, for any $i \in I$, one has $x \in A_i \setminus B$, namely $x \in A_i$ and $x \notin B$. Thus $x \in \bigcap_{i \in I} A_i$ and $x \notin B$. Therefore $x \in A \setminus B$.

□

2.8.7 Proposition. *Let I be a set and $(A_i)_{i \in I}$ be a family of sets parametrised by I. For any set B, the following statements hold.*

(1) $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$.

(2) *If $I \neq \varnothing$,* $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i)$,

(3) *If* $I \neq \varnothing$, $B \setminus \bigcup_{i\in I} A_i = \bigcap_{i\in I}(B \setminus A_i)$,

(4) *If* $I \neq \varnothing$, $B \setminus \bigcap_{i\in I} A_i = \bigcup_{i\in I}(B \setminus A_i)$.

Proof. (1) By Corollary 2.7.4, we obtain

$$B \cap (\bigcup_{i\in I} A_i) = \{x \in B \mid \exists\, i \in I,\ x \in A_i\} = \bigcup_{i\in I}\{x \in B \mid x \in A_i\} = \bigcup_{i\in I}(B \cap A_i).$$

(2) Let $A := \bigcap_{i\in I} A_i$. By definition, for any $i \in I$, one has $A \subseteq A_i$ and hence $B \cup A \subseteq B \cup A_i$. Thus, by Proposition 2.8.4, we obtain

$$B \cup \left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I}(B \cup A_i).$$

Conversely, let $x \in \bigcap_{i\in I}(B \cup A_i)$. For any $i \in I$, one has $x \in B \cup A_i$. If $x \in B$, then $x \in B \cup (\bigcap_{i\in I} A_i)$; otherwise one has

$$\forall\, i \in I,\ x \in A_i,$$

and we still get $x \in B \cup (\bigcap_{i\in I} A_i)$.

(3) By Proposition 2.5.3,

$$B \setminus \bigcup_{i\in I} A_i = \{x \in B \mid \neg(\exists\, i \in I,\ x \in A_i)\} = \{x \in B \mid \forall\, i \in I,\ x \notin A_i\}.$$

By Corollary 2.8.5, this is equal to

$$\bigcap_{i\in I}\{x \in B \mid x \notin A_i\} = \bigcap_{i\in I}(B \setminus A_i).$$

(4) By Proposition 2.5.3,

$$B \setminus \bigcap_{i\in I} A_i = \{x \in B \mid \neg(\forall\, i \in I,\ x \in A_i)\} = \{x \in B \mid \exists\, i \in I,\ x \notin A_i\}.$$

By Corollary 2.7.4, this is equal to

$$\bigcup_{i\in I}\{x \in B \mid x \notin A_i\} = \bigcup_{i\in I}(B \setminus A_i).$$

□

Exercices

1. Let $A = \{1, 2, 3, \text{Pikachu}\}$, $B = \{a, b, c, \text{Pikachu}\}$. Determine $A \cup B$ and $A \cap B$.

2. For any $k \in \mathbb{N}$, let

$$k\mathbb{N} = \{kn \mid n \in \mathbb{N}\}.$$

(1) Determine $2\mathbb{N} \cap 3\mathbb{N}$.

(2) Does the equality $2\mathbb{N} \cup 3\mathbb{N} = \mathbb{N}$ hold?

(3) Determine

$$\bigcap_{k\in\mathbb{N}} k\mathbb{N}.$$

3. Are the following sets equal:

$$A = \{(x, y) \in \mathbb{R}^2 \mid 4x - y = 1\}, \quad B = \{(t + 1, 4t + 3) \mid t \in \mathbb{R}\}?$$

Prove your conclusion.

4. Is the statement $0 \in \{\{0\}\}$ true?

5. Let A and B be two sets such that $A \subseteq B$. Prove that $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

6. Let A, B and C be sets. Prove the following equalities:

$$A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C.$$

7. Let I and J be non-empty sets, $(A_{i,j})_{(i,j)\in I\times J}$ be a family of sets. The goal of this exercise is to compare the following sets:

$$M = \bigcup_{i\in I}\bigcap_{j\in J} A_{i,j}, \quad N = \bigcap_{j\in J}\bigcup_{i\in I} A_{i,j}.$$

For any $i \in I$, let

$$M_i = \bigcap_{j\in J} A_{i,j}.$$

For any $j \in J$, let

$$N_j = \bigcup_{i\in I} A_{i,j}.$$

Thus,

$$M = \bigcup_{i\in I} M_i, \quad N = \bigcap_{j\in J} N_j.$$

(1) Let $(i, j) \in I \times J$. Prove that $M_i \subseteq A_{i,j} \subseteq N_j$.

(2) Prove that $M \subseteq N$.

(3) Consider the case $I = J = \mathbb{N}$. For any $(i, j) \in \mathbb{N} \times \mathbb{N}$, let $A_{i,j} = \{|i-j|\}$. Determine the sets M and N. Are they equal?

8. Let X and Y be sets.

(1) Prove that $\mathscr{P}(X \cap Y) = \mathscr{P}(X) \cap \mathscr{P}(Y)$.

(2) Prove that $\mathscr{P}(X) \cup \mathscr{P}(Y) \subseteq \mathscr{P}(X \cup Y)$.

(3) Construct two sets X and Y such that the equality

$$\mathscr{P}(X) \cup \mathscr{P}(Y) = \mathscr{P}(X \cup Y)$$

does not hold.

9. Let A and B be sets. Prove that

$$B \setminus A = (B \cup A) \setminus A = B \setminus (A \cap B).$$

10. Let A, B and C be sets. Prove that

$$C \setminus (B \setminus A) = (C \cap A) \cup (C \setminus B).$$

11. If X and Y are two sets, we denote by $X \Delta Y$ the symmetric difference

$$(X \setminus Y) \cup (Y \setminus X).$$

(1) Prove that, for any sets X and Y,

$$X \Delta Y = (X \cup Y) \setminus (X \cap Y).$$

(2) Prove that, if $X \supseteq Y$, then $X \Delta Y = X \setminus Y$.

12. Let A, B and C be sets.

(1) Compute $A \Delta A$ and $A \Delta \varnothing$.

(2) Prove that $(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$.

13. For each of the following statements, determine a statement of the opposite truth value, where no quantifier is preceded by a negation symbol. Determine their truth values.

(1) $\exists\, x \in \mathbb{R},\ \forall\, y \in \mathbb{R},\ x + y \geq 0$;

(2) $\exists\, x \in \mathbb{R},\ \exists\, y \in \mathbb{R},\ x + y \geq 0$;

(3) $\forall\, x \in \mathbb{R},\ \forall\, y \in \mathbb{R},\ x + y \geq 0$;

(4) $\forall\, x \in \mathbb{R},\ \exists\, y \in \mathbb{R},\ x + y \geq 0$;

14. By using quantifiers, rewrite the following statements.

(1) Any natural number has a real square root.

(2) Any natural number is strictly smaller than a certain real number.

(3) There is a real number that is smaller or equal to any natural number.

15. Consider the condition on $\mathbb{R}$:

$$P(x) := \text{“}\forall\, y \in [0,1],\ x \geq y \Rightarrow x \geq 2y\text{”}, \quad x \in \mathbb{R}.$$

Determine all real numbers satisfying $P(\cdot)$.

16. For each of the following conditions on $\mathbb{R}$, describe the sets of $x \in \mathbb{R}$ that satisfy the condition.

(1) $((x > 0) \wedge (x < 1)) \vee (x = 0)$,

(2) $(x > 3) \wedge (x < 5) \wedge (x \neq 4)$,

(3) $((x \leq 0) \wedge (x > 1)) \vee (x = 4)$,

(4) $(x \geq 0) \Rightarrow (x \geq 2)$.

17. Consider the following statement:

$$\exists\, a \in \mathbb{R}_{<0},\ \forall\, x \in \mathbb{R}_{\geqslant 1},\ x > a \Rightarrow \Big((x^2 > \tfrac{a^2}{4}) \vee (x \leq 0)\Big).$$

Determine a statement of the opposite truth value, where no quantifier is preceded by a negation symbol. Is this statement true?

18. Recall that a prime number is by definition a natural number that is ≥ 2, the only divisors of which are 1 and itself. Let $\mathbb{P}$ be the set of all prime numbers. Express the following statements as formulas by using quantifiers.

(1) If a prime number divides the product of two integers, then it divides at least one between them.

(2) Any integer that is greater or equal to 2 is divisible by a prime number.

(3) The natural number 2 is the only prime number that is even.

(4) Any primer number that is ≥ 5 is congruent to 1 or -1 modulo 6.

(5) Any even number that is > 2 can be written as the sum of two prime numbers.

(6) Any prime number that is congruent to 1 modulo 4 can be written as the sum of two squares.

(7) For any natural number n such that $n \geqslant 2$, there is always a primer number that lies between n and $2n$.

(8) There exist infinitely many prime numbers.

(9) Let p be an integer such that $p \geq 2$. Then p is a prime number if and only if p divides $(p-1)! + 1$.

19. Let x, y, x', and y' be mathematical objects. Prove that

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$$

if and only if $x = x'$ and $y = y'$.

Chapter 3

Correspondences

3.1 Correspondence and its inverse

3.1.1 Definition. We call a *correspondence* any triplet of the form

$$f = \big(\mathscr{D}_f, \mathscr{A}_f, \Gamma_f\big),$$

where $\mathscr{D}_f$, $\mathscr{A}_f$ are two sets, called respectively the *departure set* and the *arrival set* of f, and Γ_f is a subset of $\mathscr{D}_f \times \mathscr{A}_f$, called the *graph* of f.

If X and Y are two sets and f is a correspondence of the form $\big(X, Y, \Gamma_f\big)$, we say that f is a correspondence *from* X *to* Y.

3.1.2 Definition. Let f be a correspondence. We denote by f^{-1} the correspondence defined as follows:

$$\mathscr{D}_{f^{-1}} := \mathscr{A}_f, \quad \mathscr{A}_{f^{-1}} := \mathscr{D}_f,$$
$$\Gamma_{f^{-1}} := \{(y, x) \in \mathscr{A}_f \times \mathscr{D}_f \,|\, (x, y) \in \Gamma_f\}.$$

The correspondence f^{-1} is called the *inverse correspondence* of f. Clearly one has

$$(f^{-1})^{-1} = f, \tag{3.1}$$

namely f is the inverse correspondence of f^{-1}.

3.1.3 Example. Let X be a set. Denote by Δ_X the following subset of $X \times X$:

$$\{(x, x) \,|\, x \in X\},$$

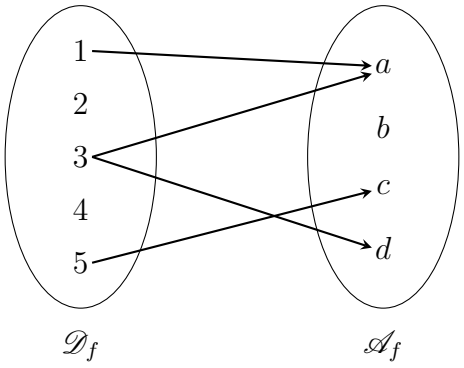
called the *diagonal subset* of $X \times X$. The correspondence (X, X, Δ_X) is called the *identity correspondence* of X, denoted as Id_X. By definition, one has $\mathrm{Id}_X^{-1} = \mathrm{Id}_X$.

3.1.4 Example. Let X and Y be two sets. There is a correspondence from X to Y whose graph is the empty set. This correspondence is called the *empty correspondence* from X to Y. Note that the inverse correspondence of the empty correspondence from X to Y is the empty correspondence from Y to X.

3.2 Illustration of a correspondence

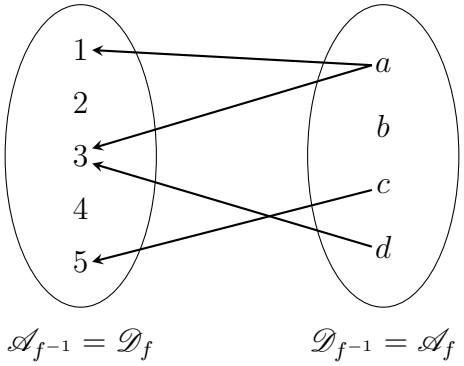
3.2.1 Remark. A correspondence can be viewed as a oriented graph. The elements of $\mathscr{D}_f$ and $\mathscr{A}_f$ are illustrated by two groups of vertices. For any ordered pair in the graph Γ_f, we link the corresponding vertices by an arrow. In the following figure, we illustrate a correspondence from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c, d\}$.

Figure 3.1: Visualization of a correspondance f



The inverse correspondence f^{-1} can be visualised by inverting the direction of the arrows in the above figure.

Figure 3.2: Visualization of the inverse correspondance f^{-1}



3.2.2 Remark. We can also represent a correspondence f by a table, whose rows are labelled by elements of $\mathscr{D}_f$ and whose columns are labelled by elements of $\mathscr{A}_f$. For each pair in Γ_f we mark the cell of corresponding coordinates by a ✓. For

example, the correspondence described by Figure 3.1 can be represented by the following table.

Table 3.1: Table representation of the correspondence f

	a	b	c	d
1	✓			
2				
3	✓			✓
4				
5			✓	

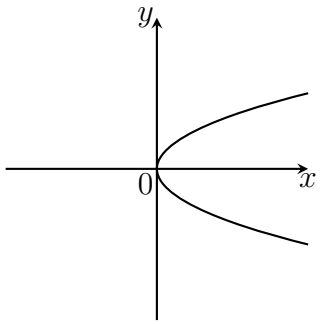
Its inverse correspondence can be represented by the transposed table.

Table 3.2: Table representation of the inverse correspondence f^{-1}

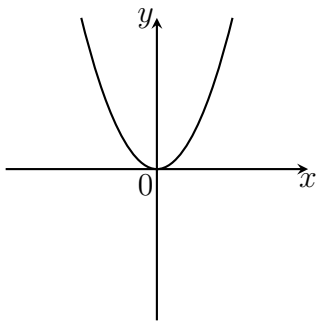
	1	2	3	4	5
a	✓		✓		
b					
c					✓
d			✓		

3.2.3 Remark. A correspondence from $\mathbb{R}$ to $\mathbb{R}$ can be illustrated by its graph in the coordinate plane. Consider for example such a correspondence f, with

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



The inverse correspondence is illustrated by a parabola that opens upward.



3.3 Image and preimage

3.3.1 Definition. Let X and Y be sets, and f be a correspondence from X to Y. If (x, y) is an element of Γ_f, we say that x is a *preimage* of y under f, and y is an *image* of x under f.

If A is a set, we denote by $f(A)$ the set

$$\{y \in \mathscr{A}_f \mid \exists\, x \in A,\, (x, y) \in \Gamma_f\},$$

called the *image* of A by the correspondence f.

If B is a set, the set $f^{-1}(B)$ is called the *preimage* of B by the correspondence f. Note that it is by definition the image of B by the inverse correspondence f^{-1}.

3.3.2 Definition. Let f be a correspondence. The set $f(\mathscr{D}_f)$ is called the *range* of f, denoted as $\mathrm{Im}(f)$. The set $f^{-1}(\mathscr{A}_f)$ is called the *domain of definition* of f, denoted as $\mathrm{Dom}(f)$. Note that the domain of definition of a correspondence f is the projection of the graph Γ_f to the departure set $\mathscr{D}_f$, and the range of a correspondence f is the projection of the graph Γ_f to the arrival set $\mathscr{A}_f$.

For any sets A and B,

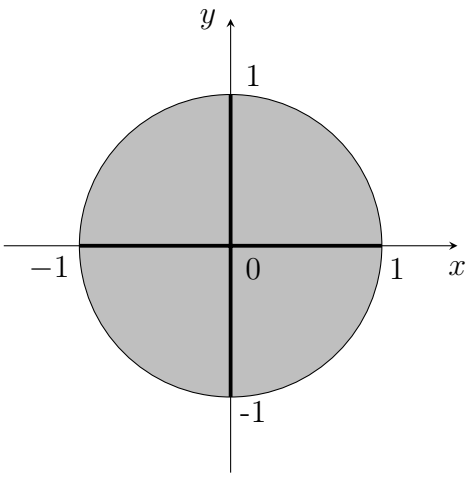
$$f(A) \subseteq \mathrm{Im}(f), \quad f^{-1}(B) \subseteq \mathrm{Dom}(f).$$

Moreover,

$$\mathrm{Dom}(f) = \mathrm{Im}(f^{-1}), \quad \mathrm{Im}(f) = \mathrm{Dom}(f^{-1}).$$

3.3.3 Example. The following figure illustrates a correspondence from $\mathbb{R}$ to $\mathbb{R}$, the image of which is

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}.$$



The domain of definition and the range of this correspondence are both $[-1, 1]$.

3.3.4 Proposition. *Let f be a correspondence.*

(1) *If A and A' are two sets such that $A' \subseteq A$, then one has $f(A') \subseteq f(A)$.*

(2) *If B and B' are two sets such that $B' \subseteq B$, then one has $f^{-1}(B') \subseteq f^{-1}(B)$.*

Proof. It suffices to prove the first statement. Let y be an element of $f(A')$. By definition there exists $x \in A'$ such that $(x, y) \in \Gamma_f$. Since $A' \subseteq A$, one has $x \in A$ and hence $y \in f(A)$. □

3.3.5 Proposition. *Let f be a correspondence. The following equalities hold:*

$$\mathrm{Im}(f) = f(\mathrm{Dom}(f)), \quad \mathrm{Dom}(f) = f^{-1}(\mathrm{Im}(f)).$$

Proof. Since $\mathrm{Dom}(f) \subseteq \mathscr{D}_f$, by Proposition 3.3.4, one has

$$f(\mathrm{Dom}(f)) \subseteq f(\mathscr{D}_f) = \mathrm{Im}(f).$$

Let y be an element of $\mathrm{Im}(f)$. There exists $x \in \mathscr{D}_f$ such that $(x, y) \in \Gamma_f$. By definition one has $x \in \mathrm{Dom}(f)$ and hence $y \in f(\mathrm{Dom}(f))$. Therefore the equality $\mathrm{Im}(f) = f(\mathrm{Dom}(f))$ is true. Applying this equality to f^{-1}, we obtain the second equality. □

3.3.6 Proposition. *Let f be a correspondence.*

(1) *Let A be a set and y be an mathematical object. Then y belongs to $f(A)$ if and only if $A \cap f^{-1}(\{y\}) \neq \varnothing$.*

(2) *Let B be a set and x be a mathematical object. Then x belongs to $f^{-1}(B)$ if and only if $B \cap f(\{x\}) \neq \varnothing$.*

Proof. (1) By definition, $y \in f(A)$ if and only if there exists $x \in A$ such that $(x, y) \in \Gamma_f$, or equivalently $x \in A \cap f^{-1}(\{y\})$

Applying (1) to f^{-1}, we obtain (2). □

3.3.7 Proposition. *Let f be a correspondence.*

(1) *Let I be a set and $(A_i)_{i\in I}$ be a family of sets parametrised by I. Then the equality*

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i)$$

holds. Moreover, if I is not empty, then

$$f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f(A_i)$$

(2) *Let I be a set and $(B_i)_{i\in I}$ be a family of sets parametrised by I. Then the equality*

$$f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i)$$

holds. Moreover, if I is not empty, then

$$f^{-1}\left(\bigcap_{i\in I} B_i\right) \subseteq \bigcap_{i\in I} f^{-1}(B_i).$$

Proof. (1) By Propositions 3.3.6 and 2.8.7, we obtain

$$\begin{aligned} f\left(\bigcup_{i\in I} A_i\right) &= \left\{ y \in Y \,\middle|\, \left(\bigcup_{i\in I} A_i\right) \cap f^{-1}(y) \neq \varnothing \right\} \\ &= \left\{ y \in Y \,\middle|\, \bigcup_{i\in I} \left(A_i \cap f^{-1}(\{y\})\right) \neq \varnothing \right\} \\ &= \left\{ y \in Y \,\middle|\, \exists\, i \in I,\ A_i \cap f^{-1}(\{y\}) \neq \varnothing \right\} = \bigcup_{i\in I} f(A_i), \end{aligned}$$

where the last equality comes from Corollary 2.7.4.

Let $A = \bigcap_{i\in I} A_i$. For any $i \in I$, one has $A \subseteq A_i$ and hence, by Proposition 3.3.4, one has $f(A) \subseteq f(A_i)$. By Proposition 2.8.4, we get

$$f(A) \subseteq \bigcap_{i\in I} f(A_i).$$

Applying (1) to f^{-1}, we obtain (2). □

3.4 Composition

3.4.1 Definition. Let f and g be correspondences. We define the *composite* of g and f as the correspondence $g \circ f$ from $\mathscr{D}_f$ to $\mathscr{A}_g$ whose graph $\Gamma_{g\circ f}$ is composed of the elements (x, z) of $\mathscr{D}_f \times \mathscr{A}_g$ such that there exists some object y satisfying $(x, y) \in \Gamma_f$ and $(y, z) \in \Gamma_g$ (note that the object y should be an element of $\mathscr{A}_f \cap \mathscr{D}_g$). In other words,

$$\Gamma_{g\circ f} = \{(x, z) \in \mathscr{D}_f \times \mathscr{A}_g \,|\, \exists\, y \in \mathscr{A}_f \cap \mathscr{D}_g,\ (x, y) \in \Gamma_f \text{ and } (y, z) \in \Gamma_g\}.$$

3.4.2 Proposition. *Let f and g be correspondences. The following equality holds:*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}. \tag{3.2}$$

Proof. Let $x \in \mathscr{A}_{f^{-1}} = \mathscr{D}_f$, $z \in \mathscr{D}_{g^{-1}} = \mathscr{A}_g$. Then $(z, x) \in \Gamma_{(g\circ f)^{-1}}$ if and only if $(x, z) \in \Gamma_{g\circ f}$, namely there exists y such that $(x, y) \in \Gamma_f$ and $(y, z) \in \Gamma_g$. This is also equivalent to the existence of y such that $(z, y) \in \Gamma_{g^{-1}}$ and $(y, x) \in \Gamma_{f^{-1}}$, namely $(z, x) \in \Gamma_{f^{-1}\circ g^{-1}}$. □

3.4.3 Proposition. *Let f, g and h be correspondences. The following equality holds:*

$$h \circ (g \circ f) = (h \circ g) \circ f. \tag{3.3}$$

Proof. It suffices to verify that $h \circ (g \circ f)$ and $(h \circ g) \circ f$ have the same graph. By definition, an element $(x, w) \in \mathscr{D}_f \times \mathscr{A}_h$ belongs to the graph of $h \circ (g \circ f)$ if and only if there exists z such that $(x, z) \in \Gamma_{g\circ f}$ and $(z, w) \in \Gamma_h$, which is equivalent to the existence of y and z such that $(x, y) \in \Gamma_f$, $(y, z) \in \Gamma_g$ and $(z, w) \in \Gamma_h$. A similar argument shows that this condition is also equivalent to $(x, w) \in \Gamma_{(h\circ g)\circ f}$. Hence the equality (3.3) holds. □

3.4.4 Proposition. *Let X and Y be sets, f be a correspondence from X to Y. Then the following equalities hold:*

$$f \circ \mathrm{Id}_X = f = \mathrm{Id}_Y \circ f.$$

Proof. Let $(x, y) \in X \times Y$. By definition, (x, y) belongs to the graph of $f \circ \mathrm{Id}_X$ if and only if there exists x' such that $(x, x') \in \Delta_X$ and $(x', y) \in \Gamma_f$, that is, $x = x'$ and $(x, y) \in \Gamma_f$. Therefore $f \circ \mathrm{Id}_X = f$. Applying this equality to f^{-1}, we obtain

$$f^{-1} \circ \mathrm{Id}_Y = f^{-1}.$$

Taking the inverse correspondences, by (3.1) and (3.2) we deduce

$$\mathrm{Id}_Y \circ f = f.$$

□

3.4.5 Proposition. *Let f and g be correspondences.*

(1) *For any set A, one has*

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

In particular,

$$\mathrm{Im}(g \circ f) = g(\mathrm{Im}(f)) \subseteq \mathrm{Im}(g).$$

If in addition $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$*, then the equality* $\mathrm{Im}(g \circ f) = \mathrm{Im}(g)$ *holds.*

(2) *For any set B, one has*

$$(g \circ f)^{-1}(B) = f^{-1}(g^{-1}(B)).$$

In particular,

$$\mathrm{Dom}(g \circ f) = f^{-1}(\mathrm{Dom}(g)) \subseteq \mathrm{Dom}(f).$$

If in addition $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$*, then the equality* $\mathrm{Dom}(g \circ f) = \mathrm{Dom}(f)$ *holds.*

Proof. (1) By definition

$$\begin{aligned}(g \circ f)(A) &= \{z \in \mathscr{A}_g \,|\, \exists\, x \in A,\ (x, z) \in \Gamma_{g \circ f}\} \\ &= \{z \in \mathscr{A}_g \,|\, \exists\, x \in A,\ \exists\, y \in \mathscr{A}_f,\ (x, y) \in \Gamma_f,\ (y, z) \in \Gamma_g\} \\ &= \{z \in \mathscr{A}_g \,|\, \exists\, y \in f(A),\ (y, z) \in \Gamma_g\} = g(f(A)).\end{aligned}$$

Applying this equality to the case where $A = \mathscr{D}_f$, we obtain

$$\mathrm{Im}(g \circ f) = (g \circ f)(\mathscr{D}_f) = g(f(\mathscr{D}_f)) = g(\mathrm{Im}(f)) \subseteq \mathrm{Im}(g).$$

In the case where $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$, by Propositions 3.3.5 and 3.3.4 we obtain

$$\mathrm{Im}(g) = g(\mathrm{Dom}(g)) \subseteq g(\mathrm{Im}(f)) = \mathrm{Im}(g \circ f).$$

Hence the equality $\mathrm{Im}(g \circ f) = \mathrm{Im}(g)$ holds.

Applying (1) to g^{-1} and f^{-1}, by (3.2) we obtain (2). □

3.5 Surjectivity

3.5.1 Definition. Let f be a correspondence. If $\mathscr{A}_f = \mathrm{Im}(f)$, we say that f is *surjective*. If f^{-1} is surjective, or equivalently $\mathrm{Dom}(f) = \mathscr{D}_f$, we say that f is a *multivalued mapping*.

3.5.2 Proposition. *Let f be a correspondence.*

(1) *Assume that f is surjective. Then, for any subset B of $\mathscr{A}_f$, one has $B \subseteq f(f^{-1}(B))$.*

(2) *Assume that f is a multivalued mapping. Then, for any subset A of $\mathscr{D}_f$, one has $A \subseteq f^{-1}(f(A))$.*

Proof. (1) Let y be an element of B. Since f is surjective, there exists $x \in \mathscr{D}_f$ such that $(x, y) \in \Gamma_f$. Therefore, $x \in f^{-1}(B)$ and hence $y \in f(f^{-1}(B))$.

Applying (1) to f^{-1}, we obtain (2). □

3.5.3 Proposition. *Let f and g be correspondences.*

(1) *If $g \circ f$ is surjective, so is g.*

(2) *If $g \circ f$ is a multivalued mapping, so is f.*

Proof. (1) By (1) of Proposition 3.4.5, one has

$$\mathrm{Im}(g \circ f) \subseteq \mathrm{Im}(g) \subseteq \mathscr{A}_g = \mathscr{A}_{g \circ f}. \tag{3.4}$$

If $g \circ f$ is surjective, namely $\mathrm{Im}(g \circ f) = \mathscr{A}_{g \circ f}$, then we deduce from (3.4) that $\mathrm{Im}(g) = \mathscr{A}_g$, namely g is surjective.

Applying (1) to g^{-1} and f^{-1}, we obtain (2). □

3.5.4 Proposition. *Let f and g be correspondences.*

(1) *If g is surjective and $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$, then $g \circ f$ is also surjective.*

(2) *If f is a multivalued mapping and $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$, then $g \circ f$ is a multivalued mapping.*

Proof. (1) Since $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$, by (1) of Proposition 3.4.5 we obtain

$$\mathrm{Im}(g \circ f) = \mathrm{Im}(g).$$

Since g is surjective,

$$\mathrm{Im}(g) = \mathscr{A}_g = \mathscr{A}_{g \circ f}.$$

Hence $g \circ f$ is also surjective.

Applying (1) to g^{-1} and f^{-1}, we obtain (2). □

3.6 Injectivity

3.6.1 Definition. Let f be a correspondence. If each element of $\mathscr{D}_f$ has at most one image under f, we say that f is a *function*. If f^{-1} is a function, or equivalently, each element of $\mathscr{A}_f$ has at most one preimage under f, we say that f is *injective*.

3.6.2 Notation. Functions form a special case of correspondences. The defining feature of functions is that corresponding to each element in the domain of definition, is a unique element in the arrival set of the function.

Let f be a function, and let $x \in \mathrm{Dom}(f)$. We denote the unique image of x under f as $f(x)$, and we say that f *sends* $x \in \mathrm{Dom}(f)$ to $f(x)$ or $f(x)$ is the *value* of f at x. We can also use the notation

$$x \longmapsto f(x)$$

to indicate the correspondence of x to its image under f.

3.6.3 Proposition. *Let f be a correspondence.*

(1) *Assume that f is injective. For any set A one has $f^{-1}(f(A)) \subseteq A$.*

(2) *Assume that f is a function. For any set B one has $f(f^{-1}(B)) \subseteq B$.*

Proof. (1) Let x be an element of $f^{-1}(f(A))$. By definition, there exists $y \in f(A)$ such that $(x, y) \in \Gamma_f$. Since $y \in f(A)$ there exist $x' \in A$ such that $(x', y) \in \Gamma_f$. Since y admits at most one preimage, we obtain $x = x'$. Hence $x \in A$.

Applying (1) to f^{-1}, we obtain (2). □

3.6.4 Proposition. *Let f and g be correspondences.*

(1) *If f and g are functions, so is $g \circ f$. Moreover, for any $x \in \mathrm{Dom}(g \circ f)$, one has $(g \circ f)(x) = g(f(x))$.*

(2) *If f and g are injective, so is $g \circ f$.*

Proof. Let x be an element of $\mathrm{Dom}(g \circ f)$. Assume that z and z' are images of x under $g \circ f$. Let y and y' be such that

$$(x, y) \in \Gamma_f, \quad (y, z) \in \Gamma_g, \quad (x, y') \in \Gamma_f, \quad (y', z') \in \Gamma_g.$$

Since f is a function, one has $y = y' = f(x)$. Since g is a function, we deduce that $z = z' = g(f(x))$. Therefore $g \circ f$ is a function, and the equality $(g \circ f)(x) = g(f(x))$ holds for any $x \in \mathrm{Dom}(g \circ f)$.

Applying (1) to g^{-1} and f^{-1}, we obtain (2). □

3.6.5 Proposition. *Let f and g be correspondences.*

(1) *If $g \circ f$ is injective and $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$, then f is also injective.*

(2) *If $g \circ f$ is a function and $\mathrm{Dom}(g) \subseteq \mathrm{Im}(f)$, then g is also a function.*

Proof. (1) Let y be an element of the image of f. Let x and x' be preimages of y under f. Since $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$, one has $y \in \mathrm{Dom}(g)$. Hence there exists $z \in \mathscr{A}_g$ such that $(y, z) \in \Gamma_g$. We then deduce that (x, z) and (x', z) are elements of $\Gamma_{g \circ f}$. Since $g \circ f$ is injective, we obtain $x = x'$. Therefore, f is injective.

Applying (1) to g^{-1} and f^{-1}, we obtain (2). □

3.6.6 Proposition. *Let f be a correspondence, and I be a non-empty set.*

(1) *Suppose that f is a function. For any family $(B_i)_{i \in I}$ of sets parametrised by I, one has*

$$f^{-1}\left(\bigcap_{i \in I} B_i\right) = \bigcap_{i \in I} f^{-1}(B_i).$$

(2) *Suppose that f is injective. For any family $(A_i)_{i \in I}$ of sets parametrised by I, one has*

$$f\left(\bigcap_{i \in I} A_i\right) = \bigcap_{i \in I} f(A_i).$$

Proof. (1) Let x be an element of $\bigcap_{i \in I} f^{-1}(B_i)$. For any $i \in I$, one has $f(x) \in B_i$. Hence $x \in f^{-1}\big(\bigcap_{i \in I} B_i\big)$. Therefore we obtain

$$f^{-1}\left(\bigcap_{i \in I} B_i\right) \supseteq \bigcap_{i \in I} f^{-1}(B_i).$$

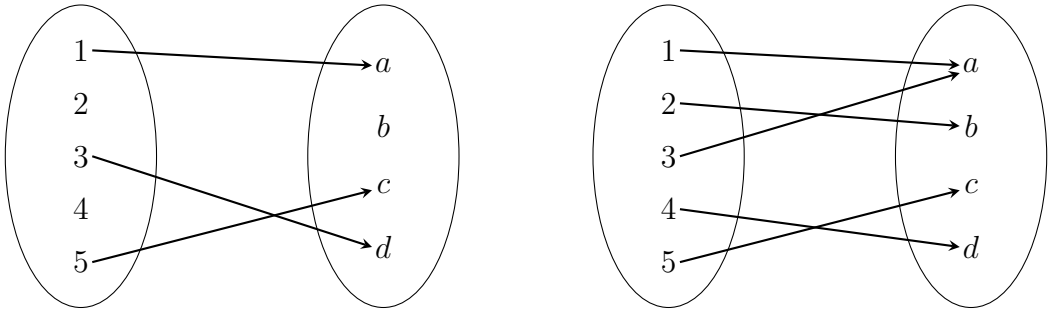
Combing with (2) of Proposition 3.3.7, we obtain the equality

$$f^{-1}\left(\bigcap_{i \in I} B_i\right) = \bigcap_{i \in I} f^{-1}(B_i).$$

Applying (1) to f^{-1}, we obtain (2). □

3.6.7 Example. In the following we illustrate two functions.

Figure 3.3: Visualization of two functions



The function illustrated on the left hand side of the figure is injective and not surjective, that illustrated on the right hand side is surjective and not injective.

3.7 Mappings

3.7.1 Definition. A correspondence f is said to be a *mapping* if any element of $\mathscr{D}_f$ has a unique image, or equivalently, f is a function and $\mathscr{D}_f = \mathrm{Dom}(f)$. Note that f is a mapping if and only if f^{-1} is both injective and surjective.

3.7.2 Notation. Let X and Y be sets. We denote by Y^X the set of all mappings from X to Y. An element $u \in Y^X$ is often written in the form of a family of elements of Y parametrised by X as follows

$$(u(x))_{x\in X}.$$

In the case where $X = \{1, \ldots, n\}$, where n is a positive integer, the set $Y^{\{1,\ldots,n\}}$ is also denoted as Y^n. An element u of Y^n is often written as an n-tuple

$$(u(1), \ldots, u(n)).$$

3.7.3 Example. (1) Let X be a set. The identity correspondence Id_X is a mapping. It is also called the *identity mapping* of X.

(2) Let X and Y be sets and y be an element of Y. The mapping from X to Y sending any $x \in X$ to y is called the *constant mapping with value* y.

3.7.4 Remark. Let $f : X \to Y$ be a mapping, I be a set.

(1) By (1) of Proposition 3.3.7, for any family of sets $(A_i)_{i\in I}$, one has

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i).$$

By (2) of Proposition 3.3.7, for any family of sets $(B_i)_{i\in I}$, one has

$$f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i).$$

(2) Assume that I is not empty. By (1) of Proposition 3.3.7, for any family of sets $(A_i)_{i\in I}$, one has

$$f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f(A_i).$$

By (1) of Proposition 3.6.6, for any family of sets $(B_i)_{i\in I}$, one has

$$f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i).$$

(3) By (2) of Proposition 3.6.3, for any set B, one has $f(f^{-1}(B)) \subseteq B$. Since $\mathrm{Dom}(f) = X$, by (2) of Proposition 3.5.2, for any subset A of X one has $A \subseteq f^{-1}(f(A))$. If moreover f is injective, by (1) of Proposition 3.6.3, one has $f^{-1}(f(A)) \subseteq A$ and hence the equality $f^{-1}(f(A)) = A$ holds.

3.7.5 Proposition. *Let f and g be mappings. Suppose that $\mathrm{Im}(f) \subseteq \mathscr{D}_g$. Then $g \circ f$ is also a mapping. Moreover, for any $x \in \mathscr{D}_f = \mathscr{D}_{g\circ f}$ one has*

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

Proof. Note that $\mathscr{D}_g = \mathrm{Dom}(g)$ since g is a mapping. Hence the statement is a direct consequence of Propositions 3.6.4 and 3.5.4. □

3.7.6 Remark. Let $f : X \to Y$ and $g : Y \to Z$ be mappings.

(1) By Proposition 3.5.4, if f and g are both surjective, so is $g\circ f$. By Proposition 3.5.3, if $g \circ f$ is surjective, so is g.

(2) By Proposition 3.6.4, if f and g are both injective, so is $g\circ f$. By Proposition 3.6.5, if $g \circ f$ is injective, so is f.

3.8 Bijection

3.8.1 Definition. Let f be a mapping, that is, a correspondence such that f^{-1} is injective and surjective. If f is injective and surjective, we say that f is a *bijection*, or a *one-to-one correspondence*. Note that a correspondence is a bijection if and only if its inverse is a bijection.

3.8.2 Proposition. *Let X and Y be sets, f be a correspondence from X to Y. If f is a bijection, then $f^{-1} \circ f = \mathrm{Id}_X$ and $f \circ f^{-1} = \mathrm{Id}_Y$. Conversely, if there exists a correspondence g such that $g \circ f = \mathrm{Id}_X$ and $f \circ g = \mathrm{Id}_Y$, then f is a bijection and $g = f^{-1}$.*

Proof. If f is a bijection, then f and f^{-1} are both mappings. By Proposition 3.7.5, one has

$$\begin{aligned} \forall\, x \in X, \quad & (f^{-1} \circ f)(x) = f^{-1}(f(x)) = x, \\ \forall\, y \in Y, \quad & (f \circ f^{-1})(y) = f(f^{-1}(y)) = y. \end{aligned}$$

Hence $f^{-1} \circ f = \mathrm{Id}_X$ and $f \circ f^{-1} = \mathrm{Id}_Y$.

Assume that g is a correspondence such that $g \circ f = \mathrm{Id}_X$ and $f \circ g = \mathrm{Id}_Y$. Since identity correspondences are surjective mappings, by Proposition 3.5.3, we deduce from the equality $g \circ f = \mathrm{Id}_X$ (which can also be written as $f^{-1} \circ g^{-1} = \mathrm{Id}_X$) that g and f^{-1} are surjective. In particular, $\mathrm{Dom}(f) = X = \mathrm{Im}(g)$.

Similarly, we deduce from the equality $f \circ g = \mathrm{Id}_Y$ (which can also be written as $g^{-1} \circ f^{-1} = \mathrm{Id}_Y$) that f and g^{-1} are surjective. In particular, $\mathrm{Dom}(g) = Y = \mathrm{Im}(f)$.

Since identity correspondences are injective, by Proposition 3.6.5, we deduce from $g \circ f = \mathrm{Id}_X$ that f is injective. Similarly, we deduce from $f \circ g = \mathrm{Id}_Y$ that f is a function. Therefore, f is a mapping which is injective and surjective, namely a bijection.

Finally, by Propositions 3.4.4 and 3.4.3, we obtain

$$g = g \circ \mathrm{Id}_Y = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{Id}_X \circ f^{-1} = f^{-1}.$$

□

3.8.3 Proposition. *Let $f : X \to Y$ and $g : Y \to Z$ be bijections. Then the composite correspondence $g \circ f$ is also a bijection.*

Proof. This is a direct consequence of Propositions 3.7.5, 3.6.4 and 3.5.4. □

3.8.4 Proposition. *Let X and Y be sets, f be a correspondence from X to Y, and g be a correspondence from Y to X. If $f \circ g$ and $g \circ f$ are bijections, then f and g are both bijections.*

Proof. By Proposition 3.5.3, f and g are surjective and are multivalued mappings. In particular,

$$\mathrm{Dom}(f) = X, \quad \mathrm{Im}(f) = Y, \quad \mathrm{Dom}(g) = Y, \quad \mathrm{Im}(g) = X.$$

Therefore, by Proposition 3.6.5, we deduce that f and g are injective and are functions. Hence f and g are both bijections. □

3.9 Direct product

3.9.1 Definition. Let I be a set and $(A_i)_{i\in I}$ be a family of sets parametrised by I. We denote by

$$\prod_{i\in I} A_i$$

the set of all mappings from I to $\bigcup_{i\in I} A_i$ which send any $i \in I$ to an element of A_i. This set is called the *direct product* of $(A_i)_{i\in I}$. Using Notation 3.7.2, we often write an element of the direct product in the form of a family $x := (x_i)_{i\in I}$ parametrised by I, where each x_i is an element of A_i, called the i-th *coordinate* of x. In the case where I is the empty set, the union $\bigcup_{i\in I} A_i$ is empty. Therefore, the direct product contains a unique element (identity mapping of $\varnothing$).

For each $j \in I$, we denote by

$$\mathrm{pr}_j : \prod_{i\in I} A_i \longrightarrow A_j$$

the mapping which sends each element $(a_i)_{i\in I}$ of the direct product to its j-th coordinate a_j. This mapping is called the *projection to the j-th coordinate.*

3.9.2 Notation. Let n be a non-zero natural number. If $(A_i)_{i\in\{1,\ldots,n\}}$ is a family of sets parametrised by $\{1,\ldots,n\}$, then the set

$$\prod_{i\in\{1,\ldots,n\}} A_i$$

is often denoted as

$$A_1 \times \cdots \times A_n.$$

3.9.3 Axioms (Axiom of choice)**.** In this book, we adopt the following axiom. If I is a non-empty set and if $(A_i)_{i\in I}$ is a family of non-empty sets, then the direct product $\prod_{i\in I} A_i$ is not empty.

3.9.4 Proposition. *Let I be a set and $(A_i)_{i\in I}$ be a family of sets parametrised by I. For any set X, the mapping*

$$\left(\prod_{i\in I} A_i\right)^X \longrightarrow \prod_{i\in I} A_i^X, \tag{3.5}$$

which sends f to $(\mathrm{pr}_i \circ f)_{i\in I}$, is a bijection.

In other words, for any family $(f_i : X \to A_i)_{i\in I}$ of mappings, there exists a unique mapping $f : X \to \prod_{i\in I} A_i$ such that

$$\forall\, i \in I,\ \mathrm{pr}_i \circ f = f_i$$

Proof. Let $(f_i)_{i\in I}$ be an element of

$$\prod_{i\in I} A_i^X,$$

where each f_i is a mapping from X to A_i. Let $f : X \to \prod_{i\in I} A_i$ be the mapping which sends $x \in X$ to $(f_i(x))_{i\in I}$. By definition, for any $i \in I$ one has

$$\forall\, x \in X, \quad \mathrm{pr}_i(f(x)) = f_i(x).$$

Therefore the mapping (3.5) is surjective.

If f and g are two mappings from X to $\prod_{i\in I} A_i$ such that $\mathrm{pr}_i \circ f = \mathrm{pr}_i \circ g$ for any $i \in I$, then, for any $x \in X$ one has

$$\forall\, i \in I, \quad \mathrm{pr}_i(f(x)) = \mathrm{pr}_i(g(x)).$$

Hence $f(x) = g(x)$ for any $x \in X$, namely $f = g$. Therefore the mapping (3.5) is injective. □

3.9.5 Notation. Let I be a set, $(A_i)_{i\in I}$ be a family of sets parametrised by I.

Let X be a set. For any $i \in I$, let $f_i : X \to A_i$ be a mapping from X to A_i. By Proposition 3.9.4, there exists a unique mapping $f : X \to \prod_{i\in I} A_i$ such that $\mathrm{pr}_i \circ f = f_i$ for any $i \in I$. By abuse of notation, we denote by $(f_i)_{i\in I}$ this mapping.

Let $(B_i)_{i\in I}$ be a family of sets parametrised by I. For any $i \in I$, let $g_i : B_i \to A_i$ be a mapping from B_i to A_i. We denote by

$$\prod_{i\in I} g_i : \prod_{i\in I} B_i \longrightarrow \prod_{i\in I} A_i$$

the mapping which sends $(b_i)_{i\in I}$ to $(g_i(b_i))_{i\in I}$. In the case where $I = \{1, \ldots, n\}$, where n is a non-zero natural number, the mapping $\prod_{i\in\{1,\ldots,n\}} g_i$ is also denoted as

$$g_1 \times \cdots \times g_n.$$

3.9.6 Proposition. *Let $f : X \to Y$ be a mapping.*

(1) *If f is surjective, then there exists an injective mapping $g : Y \to X$ such that $f \circ g = \mathrm{Id}_Y$.*

(2) *If f is injective and X is not empty, then there exists a surjective mapping $h : Y \to X$ such that $h \circ f = \mathrm{Id}_X$.*

Proof. (1) The case where $Y = \varnothing$ is trivial since in this case $X = \varnothing$ and f is the identity mapping of $\varnothing$. In the following, we assume that Y is not empty. Since f is surjective, for any $y \in Y$, the set $f^{-1}(\{y\})$ is not empty. Hence the direct product

$$\prod_{y \in Y} f^{-1}(\{y\})$$

is not empty. In other words, there exists a mapping g from Y to X such that $f(g(y)) = y$ for any $y \in Y$, that is $f \circ g = \mathrm{Id}_Y$. By (2) of Remark 3.7.6, g is injective.

(2) Let x_0 be an element of X. We define a mapping $h : Y \to X$ as follows:

$$h(y) := \begin{cases} f^{-1}(y), & \text{if } y \in \mathrm{Im}(f), \\ x_0, & \text{else.} \end{cases}$$

Then, by construction one has $h \circ f = \mathrm{Id}_X$. By (1) of Remark 3.7.6, h is surjective. □

3.10 Restriction and extension

3.10.1 Definition. Let f and g be correspondences. If $\Gamma_f \subseteq \Gamma_g$, we say that f is a *restriction* of g and that g is an *extension* of f. By definition, f is a restriction of g if and only if f^{-1} is a restriction of g^{-1}.

Let X and Y be sets, h be a correspondence from X to Y, and A be a subset of X. Denote by $h|_A$ the correspondence from A to Y such that

$$\Gamma_{h|_A} = \Gamma_h \cap (A \times Y).$$

We call it the *restriction of h to A*.

3.10.2 Proposition. *Let g be a correspondence.*

(1) *If g is a function, then all its restrictions are functions.*

(2) *If g is injective, the all its restrictions are injective.*

(3) *If g is a function and A is a subset of* $\mathrm{Dom}(g)$*, then $g|_A$ is a mapping.*

Proof. (1) Let f be a restriction of g. Then one has $\mathrm{Dom}(f) \subseteq \mathrm{Dom}(g)$. For any $x \in \mathrm{Dom}(f)$, if $(x, y) \in \Gamma_f$, then $(x, y) \in \Gamma_g$. Since g is a function, x admits at most one image under g. Therefore, it also admits at most one image under f. Hence f is a function.

Applying (1) to g^{-1}, we obtain (2).

(3) By (1), $g|_A$ is a function. Moreover, for any $x \in A$,

$$(x, g(x)) \in (A \times \mathscr{A}_g) \cap \Gamma_g = \Gamma_{g|_A},$$

which implies that $x \in \mathrm{Dom}(g|_A)$. Hence $g|_A$ is a mapping. □

3.10.3 Definition. Let X be a set and A be a subset of X. The restriction of the identity mapping Id_X to A is called the *inclusion mapping* of A into X, denoted by $\jmath_A : A \to X$. Note that, if h is a correspondence from X to a set Y, then $h|_A$ identifies with $h \circ \jmath_A$, the composite correspondence of h with the inclusion mapping $\jmath_A : A \to X$.

3.11 Equivalence relation

3.11.1 Definition. Let X be a set. We call *binary relation* on X any correspondence from X to itself. If R is a binary relation on X, for any $(x, y) \in X \times X$, we denote by $x\,R\,y$ the statement "$(x, y) \in \Gamma_R$", and denote by $x \not R\, y$ the statement "$(x, y) \notin \Gamma_R$". If Y is a subset of X, then there is a unique binary relation on Y, the graph of which is $\Gamma_R \cap (Y \times Y)$. We call it the *restriction of R to Y* as a binary relation. We emphasise that it is different from the restriction of R to Y as a correspondence.

3.11.2 Notation. Let X be a set, n be a positive integer, $R_1, \ldots, R_n$ be binary relations on X. If $x_0, \ldots, x_n$ are elements of X, then

$$x_0\, R_1\, x_1 R_2 \ldots R_{n-1} x_{n-1}\, R_n\, x_n$$

denotes

$$\forall\, i \in \{0, \ldots, n-1\}, \quad x_i\, R_i\, x_{i+1}.$$

3.11.3 Definition. Let X be a set and R be a binary relation on X.

(a) If for any $x \in X$, one has $x\,R\,x$, then we say that the binary relation R is *reflexive*. Note that R is reflexive if and only if $\Delta_X \subseteq \Gamma_R$.

(b) If for any $(x, y) \in X \times X$, $x\,R\,y$ implies $y\,R\,x$, then we say that the binary relation R is *symmetric*. Note that R is symmetric if and only if $R = R^{-1}$.

(c) If for all elements x, y and z of X, $x\,R\,y$ and $y\,R\,z$ imply $x\,R\,z$, then we say that the binary relation R is *transitive*. Note that R is transitive if and only if $\Gamma_{R\circ R} \subseteq \Gamma_R$.

(d) If R is reflexive, symmetric and transitive, then we say that R is an *equivalence relation*.

3.11.4 Lemma. *Let X be a set and $\sim$ be a symmetric and transitive binary relation on X. For any $x \in X$, denote by $[x]$ the subset*

$$\{y \in X \,|\, y \sim x\}.$$

(1) *If x_1 and x_2 are elements of X such that $x_1 \sim x_2$, then one has $[x_1] = [x_2]$.*

(2) *If x_1 and x_2 are elements of X such that $x_1 \not\sim x_2$, then one has $[x_1] \cap [x_2] = \varnothing$.*

Proof. (1) Let y be an element of $[x_1]$. By definition, $y \sim x_1$. Since $x_1 \sim x_2$, by the transitivity we obtain $y \sim x_2$, namely $y \in [x_2]$. Therefore, we obtain $[x_1] \subseteq [x_2]$. Moreover, by the symmetry one has $x_2 \sim x_1$, and hence, by what has been proved above, we obtain $[x_2] \subseteq [x_1]$. Therefore $[x_1] = [x_2]$.

(2) We reason by contraposition. Assume that z is a common element of $[x_1]$ and $[x_2]$. By definition, one has $z \sim x_1$ and $z \sim x_2$. Hence, by the symmetry and the transitivity, we get $x_1 \sim x_2$. □

3.11.5 Definition. Let X be a set, $\sim$ be an equivalence relation on X. A subset of X of the form

$$[x] := \{y \in X \,|\, y \sim x\}, \text{ where } x \in X$$

is called an *equivalence class* under the equivalence relation $\sim$, and the element x is called a *representative* of the equivalence class. We denote by $X/_\sim$ the set of all equivalence classes under $\sim$, called the *quotient set* of X by the equivalence relation $\sim$. This is a subset of the power set $\mathscr{P}(X)$. The mapping from X to $X/_\sim$ which sends $x \in X$ to the equivalence class $[x]$ represented by x is called the *projection mapping*. Note that the projection mapping is surjective.

3.11.6 Proposition. *Let X be a set and $\sim$ be an equivalence relation on X. Then the elements of $X/_\sim$ are pairwise disjoint sets and one has*

$$X = \bigcup_{A \in X/_\sim} A. \tag{3.6}$$

In other words, X is the disjoint union of the equivalence classes under $\sim$.

Proof. By Lemma 3.11.4, two equivalence classes under $\sim$ are either disjoint or equal, which shows that the sets in $X/_\sim$ are pairwise disjoint. Moreover, by the reflexivity of $\sim$, for any $x \in X$, one has $x \in [x]$. Hence

$$X \subseteq \bigcup_{A \in X/_\sim} A.$$

Conversely, for any $A \in X/_\sim$, one has $A \subseteq X$. Hence, by Proposition 2.7.3, one has

$$\bigcup_{A \in X/_\sim} A \subseteq X.$$

Hence the equality (3.6) holds. □

3.11.7 Example. Let p be a natural number. Consider the binary relation $\sim_p$ on $\mathbb{Z}$ defined as follows:

$$x \sim_p y \text{ if and only if there exists } n \in \mathbb{Z} \text{ such that } x - y = pn.$$

One can check that $\sim_p$ is an equivalence relation on $\mathbb{Z}$. We call it the *relation of congruence* modulo p. For any $a \in \mathbb{Z}$, we denote by $a + p\mathbb{Z}$ the equivalence class of a under $\sim_p$.

3.11.8 Proposition. *Let X be a set, $\sim$ be an equivalence relation on X, and $f : X \to Y$ be a mapping. Denote by $\pi : X \to X/_\sim$ the projection mapping, Assume that, for any $(x, x') \in X \times X$ such that $x \sim x'$, one has $f(x) = f(x')$. There exists a unique mapping $\widetilde{f} : X/_\sim \to Y$ such that $\widetilde{f} \circ \pi = f$ (namely, such that $\widetilde{f}([x]) = f(x)$ for any $x \in X$). Moreover, the equality $\mathrm{Im}(f) = \mathrm{Im}(\widetilde{f})$ holds.*

Proof. By (1) of Proposition 3.9.6, since π is surjective, there exists an injective mapping $g : X/_\sim \to X$ such that $\pi \circ g = \mathrm{Id}_{X/_\sim}$. Therefore, if $\widetilde{f} : X/_\sim \to Y$ is a mapping such that $\widetilde{f} \circ \pi = f$, then one has

$$f \circ g = (\widetilde{f} \circ \pi) \circ g = \widetilde{f} \circ (\pi \circ g) = \widetilde{f} \circ \mathrm{Id}_{X/_\sim} = \widetilde{f}.$$

This shows the uniqueness of $\widetilde{f}$. Moreover, since $f = \widetilde{f} \circ \pi$ and since π is surjective, by (1) of Proposition 3.4.5, we obtain $\mathrm{Im}(\widetilde{f}) = \mathrm{Im}(f)$.

It remains to check that, if we define $\widetilde{f}$ as $f \circ g$, then the mapping $\widetilde{f}$ satisfies the equality $\widetilde{f} \circ \pi = f$. Note that, for any $\alpha \in X/_\sim$, one has $\pi(g(\alpha)) = \alpha$, namely $g(\alpha)$ is a representative of α. Therefore, for any $x \in X$, one has $g(\pi(x)) \sim x$ and hence

$$\widetilde{f}(\pi(x)) = f(g(\pi(x))) = f(x).$$

□

3.11.9 Definition. Let X be a set, $\sim$ be an equivalence relation on X, and $f : X \to Y$ be a mapping. If, for any $(x, x') \in X \times X$ such that $x \sim x'$, one has $f(x) = f(x')$, then we say that the mapping f is *compatible* with the equivalence relation $\sim$.

Assume that $f : X \to Y$ is a mapping compatible with the equivalence relation $\sim$. The mapping $\widetilde{f} : X/_\sim \to Y$ described in Proposition 3.11.8 is said to be *induced by f by passing to quotient.*

3.11.10 Corollary. *Let $f : X \to Y$ be a mapping of sets. The binary relation $\sim_f$ on X defined by*

$$x \sim_f x' \text{ if and only if } f(x) = f(x')$$

is an equivalence relation. Moreover, f induces by passing to quotient an injective mapping $\widetilde{f} : X/_{\sim_f} \to Y$, the rang of which is $f(X)$.

Proof. For any $x \in X$ one has $f(x) = f(x)$ and hence $x \sim_f x$. If x and x' are elements of X such that $x \sim_f x'$, then one has $f(x') = f(x)$ and hence $x' \sim_f x$. If x, x' and x'' are elements of X such that $x \sim_f x'$ and $x' \sim_f x''$, then the equalities $f(x) = f(x') = f(x'')$ hold, and hence $x \sim_f x''$.

By Proposition 3.11.8, the mapping f induces by passing to quotient a mapping $\widetilde{f} : X/_{\sim_f} \to Y$. If α and β are two elements of $X/_{\sim_f}$, which are represented by elements x and y of X respectively, and such that $\widetilde{f}(\alpha) = \widetilde{f}(\beta)$, then one has $f(x) = f(y)$ and hence $x \sim_f y$. This leads to $\alpha = \beta$. Therefore $\widetilde{f}$ is injective.

Finally, by Proposition 3.11.8, f and $\widetilde{f}$ have the same range, namely $\mathrm{Im}(\widetilde{f}) = \mathrm{Im}(f) = f(X)$. □

3.11.11 Corollary. *Let I be a set and $(X_i)_{i\in I}$ be a family of sets parametrised by I. For any $i \in I$, let R_i be an equivalence relation on X_i and $\pi_i : X_i \to X_i/R_i$ be the projection mapping. Let $X = \prod_{i\in I} X_i$ and let $\sim$ be the binary relation on X defined as follows*

$$(x_i)_{i\in I} \sim (y_i)_{i\in I} \text{ if and only if } \forall\, i \in I,\ x_i\, R_i\, y_i.$$

(1) *The binary relation $\sim$ is an equivalence relation on X.*

(2) *The mapping*

$$\prod_{i\in I} \pi_i : X \longrightarrow \prod_{i\in I} (X_i/R_i)$$

induces by passing to quotient a bijection from $X/_\sim$ to $\prod_{i\in I}(X_i/R_i)$.

Proof. Note that, for any elements $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ of X, $(x_i)_{i\in I} \sim (y_i)_{i\in I}$ if and only if $(\pi_i(x_i))_{i\in I} = (\pi_i(y_i))_{i\in I}$. Therefore, by Corollary 3.11.10, the binary relation $\sim$ is an equivalence relation, and the mapping $\prod_{i\in I} \pi_i$ induces by passing

to quotient an injective mapping from $X/_\sim$ to $\prod_{i\in I}(X_i/R_i)$. Moreover, by Proposition 3.11.8 this mapping have the same image as that of $\prod_{i\in I}\pi_i$. Since $\prod_{i\in I}\pi_i$ is surjective, we obtain that the induced mapping is also surjective. □

Exercises

1. Here is a table that shows courses chosen by 6 students, followed by a list of the assigned instructors.

	Analysis	Physics	Chemistry	Programming	Calculus	Phys. Lab	Chem. Lab
Charles	√	√		√			
Charlie		√		√	√		
Carlo			√		√		√
Karl	√	√				√	
Charuzu		√	√		√		
Charlot	√	√	√				

- Analysis: Maicon,
- Physics: Mikkel,
- Chemistry: Michelle,
- Programming: Mikhail,
- Calculus: Micheal,
- Physics Lab: Mitchell,
- Chemistry Lab: Mihai.

Let X denote the set that consists of these 6 students, Y denote the set of all the courses, Z denote the set of all the instructors, f denote the correspondence from X to Y based on the above table, g denote the correspondence from Y to Z based on the assignment of the course instructors.

(1) Draw a table of g.

(2) Is the correspondence f injective? surjective? a function? a multi-valued mapping? What about g?

(3) Draw a table of the composite $g \circ f$. What can we conclude from it?

(4) Draw a table of the composite $f^{-1} \circ f$. What can we conclude from it?

2. For each of the following mappings, determine if it is injective, surjective. Justify your answer.

(1) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 3x + 4$.

(2) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = 3x + 4$.

(3) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2x + 4$.

(4) $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (x + y, x - y)$.

3. For each of the following functions from $\mathbb{R}$ to $\mathbb{R}$, determine its domain of definition and its range.

(1) $\cos \circ \sin$.

(2) $\exp \circ \ln$.

(3) $\ln \circ \exp$.

(4) ι defined as $\iota(x) = x^{-1}$.

(5) $\iota \circ \iota$.

4. Consider the correspondence φ from $\mathbb{R}$ to $\mathbb{R}$ whose graph is given by

$$\{(x, y) \,:\, x^2 + y^2 \leq 1\}.$$

(1) Draw the graph of the correspondance φ.

(2) Determine the domain of definition and the range of φ.

(3) We view φ as a binary relation on $\mathbb{R}$. Is this binary relation reflexive, symmetric, transitive?

(4) Draw the graph of $\varphi \circ \varphi$.

5. Consider the mapping $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = x^2$. Let

$$A = \{x \in \mathbb{R} \,|\, -1 \leqslant x \leqslant 4\}.$$

Determine $f(A)$ and $f^{-1}(A)$.

6. Let f and g be functions from $\mathbb{R}$ to $\mathbb{R}$ defined as

$$f(x) = 3x + 1, \quad g(x) = x^2 - 1.$$

Determine the functions $f \circ g$ and $g \circ f$. Are they equal?

7. For each of the following function h from $\mathbb{R}$ to $\mathbb{R}$. Determine two functions f and g such that $h = f \circ g$.

(1) $h(x) = \sqrt{3x-1}$,
(2) $h(x) = \sin(x + \pi/2)$,
(3) $h(x) = 1/(x+1)$.

8. Let f and g be mappings from $\mathbb{N}$ to $\mathbb{N}$ defined as

$$f(n) = 2n, \quad g(n) = \begin{cases} n/2, & \text{if } n \text{ is even,} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

Determine $g \circ f$ and $f \circ g$. Is the mapping f injective, surjective, a bijection? Is the mapping g injective, surjective, a bijection?

9. Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the mapping sending $(n, p) \in \mathbb{N} \times \mathbb{N}$ to $2^n(2p+1)$.

(1) Show that f is injective.
(2) Determine the range of f.

10. Let $f : \mathbb{R} \to \mathbb{R}$ be a mapping. For each of the following statements, construct a statement of the opposite truth value, where no quantifier is preceded by a negation symbol.

(1) $\forall\, x \in \mathbb{R},\ f(x) \neq 0$,
(2) $\forall\, M \in \mathbb{R}_{>0},\ \exists\, A \in \mathbb{R}_{>0},\ \forall\, x \geq A,\ f(x) > M$.
(3) $\forall\, x \in \mathbb{R},\ f(x) > 0 \Rightarrow x \leq 0$.
(4) $\forall \varepsilon \in \mathbb{R}_{>0},\ \exists\, \eta \in \mathbb{R}_{>0},\ \forall\, (x, y) \in \mathbb{R} \times \mathbb{R},\ |x - y| < \eta \Rightarrow |f(x) - f(y)| < \varepsilon$.

11. Let $f : \mathbb{R} \to \mathbb{R}$ be a mapping. By using the quantifiers, express the following statements:

(1) f is constant.
(2) 0 lies in the range of f.
(3) f only takes non-negative values.

12. We consider the following condition $P(\cdot)$ on the set $\mathbb{R}^{\mathbb{R}}$ of mappings from $\mathbb{R}$ to $\mathbb{R}$

$$P(f) := \text{“}\exists\, M \in \mathbb{R},\ \forall\, x \in \mathbb{R},\ f(x) \leq M\text{”}.$$

(1) Construct a condition $Q(\cdot)$ on $\mathbb{R}^{\mathbb{R}}$ without quantifier proceeded by a negation symbol, such that, for any $f \in \mathbb{R}^{\mathbb{R}}$, $Q(f)$ and $\neg P(f)$ have the same truth value.

(2) Construct an example of mapping in $\mathbb{R}^{\mathbb{R}}$ that satisfies the condition $P(\cdot)$.

(3) Construct an example of mapping in $\mathbb{R}^{\mathbb{R}}$ that does not satisfies the condition $P(\cdot)$.

(4) For each of the following conditions, determine if it is satisfied by all mappings in $\mathbb{R}^{\mathbb{R}}$, if it is not satisfied by none of the mappings in $\mathbb{R}^{\mathbb{R}}$, or if it is satisfied by some but not all of the mappings in $\mathbb{R}^{\mathbb{R}}$.

a) $\exists\, x \in \mathbb{R}, \forall\, M \in \mathbb{R},\ f(M) \leq x$.
b) $\exists\, x \in \mathbb{R}, \forall\, M \in \mathbb{R},\ f(x) \leq M$.
c) $\forall\, M \in \mathbb{R}, \exists\, x \in \mathbb{R},\ f(x) \leq M$.
d) $\forall\, M \in \mathbb{R}, \exists\, x \in \mathbb{R},\ f(M) \leq x$.

13. Let n and p be two natural numbers, $X = \{1, \ldots, n\}$ and $Y = \{1, \ldots, p\}$.

(1) How many correspondences are there from X to Y?

(2) How many injective correspondences are there from X to Y?

(3) How many surjective correspondences are there from X to Y?

(4) How many functions are there from X to Y?

(5) How many mappings are there from X to Y?

(6) How many bijections are there from X to Y.

14. For any natural number n, let E_n be the set $\{1, \ldots, n\}$ (by convention E_0 denotes the empty set). For any $(n, p) \in \mathbb{N}^2$, let $S_{n,p}$ be the number of surjective mappings from E_n to E_p.

(1) Determine $S_{n,p}$ for $(n, p) \in \mathbb{N}^2$ such that $p > n$.

(2) For any $n \in \mathbb{N}$, determine $S_{n,0}$.

(3) Show that, for any non-zero natural number p, one has

$$\sum_{i=0}^{p} (-1)^i \binom{p}{i} = 0,$$

where

$$\binom{n}{p} := \frac{n!}{p!(n-p)!}$$

(4) Let i, q and p be natural numbers such that $i \leq q \leq p$. Show that

$$\binom{p}{q}\binom{q}{i} = \binom{p}{i}\binom{p-i}{q-i}.$$

(5) Show that, for any $(i,p) \in \mathbb{N}^2$ such that $i < p$, one has

$$\sum_{q=i}^{p} (-1)^q \binom{p}{q}\binom{q}{i} = 0.$$

(6) Let p and q be natural numbers such that $q \leq p$. Show that the number of mappings from E_n to E_p whose range has exactly q elements is equal to $S_{n,q}\binom{p}{q}$.

(7) Let p and n be natural numbers such that $p \leq n$ and $n \geq 1$. Show that

$$p^n = \sum_{q=1}^{p} \binom{p}{q} S_{n,q}.$$

(8) Let p and n be natural numbers such that $p \leq n$ and $n \geq 1$. Show that

$$(-1)^p S_{n,p} = \sum_{i=1}^{p} (-1)^i \binom{p}{i} i^n.$$

(9) Let p and n be natural numbers such that $1 \leq p < n$. Show that

$$S_{n,p} = p(S_{n-1,p} + S_{n-1,p-1}).$$

(10) Let $p \in \mathbb{N}$. Determine $S_{p,p}$ and $S_{p+1,p}$.

(11) Let p and n be natural numbers such that $p \leq n$. Show that the number of surjective functions from E_n to E_p is equal to

$$\sum_{j=p}^{n} \binom{n}{j} S_{j,p}.$$

(12) Prove the equality

$$\sum_{j=p}^{n} \binom{n}{j} S_{j,p} = \frac{1}{p+1} S_{n+1,p+1}.$$

15. For any natural number n, let E_n be the set $\{1, \ldots, n\}$ (by convention E_0 denotes the empty set).

(1) Let n and p be natural numbers such that $n \leq p$. Show that the number of injective mappings from E_n to E_p is equal to $p!/(p-n)!$.

(2) Show that the number of injective functions from E_n to E_p is

$$\sum_{k=0}^{\min\{n,p\}} \binom{n}{k}\binom{p}{k}k!.$$

16. Let X be a set and $\mathscr{P}(X)$ be the power set of X, namely $\mathscr{P}(X)$ is the set of all subsets of X. The purpose of this exercise is to prove that there does not exist any injective mapping from $\mathscr{P}(X)$ to X. We reason by contradiction assuming that $\Phi : \mathscr{P}(X) \to X$ is an injective mapping.

(1) Show that Φ^{-1} is a function from X to $\mathscr{P}(X)$.

(2) Let A be the set of $n \in \mathrm{Im}(\Phi)$ such that $n \notin \Phi^{-1}(n)$. Show that $\Phi^{-1}(\Phi(A)) = A$.

(3) Examine the truth value of the statement $\Phi(A) \in A$ and obtain a contradiction.

Chapter 4

Ordering

4.1 Partially ordered set

4.1.1 Definition. Let X be a set and $\underline{R}$ be a binary relation (see Definition 3.11.3) on X. If, for any $(x, y) \in X \times X$, $x \,\underline{R}\, y$ and $y \,\underline{R}\, x$ imply $x = y$, then we say that the binary relation $\underline{R}$ is *antisymmetric*. If the binary relation $\underline{R}$ is reflexive, transitive (see Definition 3.11.3) and antisymmetric, then we say that $\underline{R}$ is a *partial order* and that $(X, \underline{R})$ is a *partially ordered set*. Note that, if $\underline{R}$ is a partial order on X, then its inverse correspondence (see Definition 3.1.2) is also a partial order on X.

Let $\underline{R}$ be a partial order on X. If, for any $(x, y) \in X \times X$, $x \,\underline{R}\, y$ or $y \,\underline{R}\, x$ holds, then we say that $\underline{R}$ is a *total order* and that $(X, \underline{R})$ is a *totally ordered set*.

4.1.2 Notation. Given a binary relation represented by a certain symbol, we often use the mirror-symmetric symbol to represent the inverse of this binary relation. For instance, if we use the symbol $\leq$ to represent a partial order on a set, then the symbol $\geq$ represents the inverse of the partial order $\leq$, that is, $x \leq y$ if and only if $y \geq x$.

In the case where the partial order is denoted by $\leq$, it is common to refer to the partially ordered set by its underlying set, without explicitly mentioning the partial order.

4.1.3 Example. Let X be a set, $\mathscr{P}(X)$ be the power set of X. Then the inclusion relation $\subseteq$ is a partial order on $\mathscr{P}(X)$.

4.1.4 Example. Consider a partially ordered set $(X, \leq)$ and let A be a subset of X. The restriction of the binary relation $\leq$ to A defines a partial order on A, referred to as the *induced partial order* on A. We denote by $(A, \leq)$ the partially ordered set obtained by endowing A with this induced partial order.

4.1.5 Proposition. *Let $(X, \leq)$ be a partially ordered set. We denote by $<$ the binary relation on X such that*

$$\forall\,(x,y) \in X \times X, \quad x < y \text{ if and only if } (x \leq y \text{ and } x \neq y).$$

Then the binary relation $<$ has the following properties.

(1) Irreflexivity: *for any $x \in X$, $x < x$* does not *hold.*

(2) Asymmetry: *for any $(x, y) \in X \times X$, if $x < y$, then $y < x$* does not *hold.*

(3) Transitivity: *for any elements x, y and z of X, if $x < y$ and $y < z$, then $x < z$.*

Proof. (1) By definition, $x < x$ is equivalent to $x \leq x$ and $x \neq x$. Since $x \neq x$ is never true, the condition $x < x$ could not hold.

(2) If $x < y$ and $y < x$ hold at the same time, then $x \leq y$ and $y \leq x$ also hold at the same time, which leads to $x = y$ by the symmetry of $\leq$. Then by (1) $x < y$ could not be true, which is a contradiction.

(3) If $x < y$ and $y < z$ hold, then, by the transitivity of $\leq$ one obtains $x \leq z$. Note that, by (2), $x = z$ could not hold. Therefore, we get $x < z$. □

4.1.6 Notation. Let $(X, \leq)$ be a partially ordered set. For any $a \in X$, we denote by $X_{\leq a}$ the set

$$\{x \in X \,|\, x \leq a\}.$$

Similarly, we denote by $X_{<a}$ the set

$$\{x \in X \,|\, x < a\}.$$

4.1.7 Definition. We call *strict partial order* a binary relation which is irreflexive, asymmetric, and transitive. The binary relation $<$ in Proposition 4.1.5 is a strict partial order, which is called the *strict partial order associated with* $\leq$.

4.1.8 Notation. In this book, we always use underlined symbols to denote partial orders and use the corresponding ununderlined symbol to denote the associated strict partial order. For instance, if $\leq$ denotes a partial order on a set, then $<$ denotes the associated strict partial order on the same set.

4.2 Monotonic functions

4.2.1 Definition. Let I and X be partially ordered sets, f be a function from I to X.

(a) If, for any elements a and b of $\mathrm{Dom}(f)$ such that $a < b$, one has $f(a) \leq f(b)$, we say that f is *increasing*.

(b) If, for any elements a and b of $\mathrm{Dom}(f)$ such that $a < b$, one has $f(a) < f(b)$, we say that f is *strictly increasing*.

(c) If, for any elements a and b of $\mathrm{Dom}(f)$ such that $a < b$, one has $f(a) \geq f(b)$, we say that f is *decreasing*.

(d) If, for any elements a and b of $\mathrm{Dom}(f)$ such that $a < b$, one has $f(a) > f(b)$, we say that f is *strictly decreasing*.

A function f is said to be *monotonic* if it is either increasing or decreasing. If f is strictly increasing or strictly decreasing, then it is said to be *strictly monotonic*. A restriction of a monotonic (resp. strictly monotonic) function is also monotonic (resp. strictly monotonic) and has the same monotonicity direction.

4.2.2 Example. Let X be a partially ordered set, and let A be a subset of X equipped with the induced partial order. Then, the inclusion mapping $\iota_A : A \to X$ is strictly increasing.

4.2.3 Proposition. *Let f and g be functions between partially ordered sets.*

(1) *Assume that f and g are both increasing or are both decreasing, then $g \circ f$ is increasing.*

(2) *Assume that f and g are both strictly increasing or are strictly decreasing, then $g \circ f$ is strictly increasing.*

(3) *Assume that the one of g and f is increasing and the other is decreasing, then $g \circ f$ is decreasing.*

(4) *Assume that the one of g and f is strictly increasing and the other is strictly decreasing, then $g \circ f$ is strictly decreasing.*

Proof. Let x and y be elements of the domain of definition of $g \circ f$, such that $x < y$. If f is increasing, then $f(x) \leq f(y)$, if moreover g is increasing, then $g(f(x)) \leq g(f(y))$. Similarly, if both f and g are strictly increasing, then one deduces from $x < y$ the relation $f(x) < f(y)$ and furthermore $g(f(x)) < g(f(y))$. Therefore, if both f and g are increasing (resp. strictly increasing), then $g \circ f$ is increasing (resp. strictly increasing).

If one replaces one or both of the partial orders of $\mathrm{Dep}(f)$ and $\mathrm{Arr}(g)$ by the corresponding inverse partial order(s), we deduce from what we have proved above the other statements.

□

4.2.4 Proposition. *Let I and X be partially ordered set, and f be a function from I to X.*

(1) *If f is monotonic and is injective, then it is strictly monotonic.*

(2) *If I is a totally ordered set and f is strictly monotonic, then it is injective.*

Proof. (1) Let a and b be elements of $\mathrm{Dom}(f)$, such that $a < b$. Assume that f is increasing. Then one has $f(a) \leq f(b)$. Since f is injective, $f(a)$ and $f(b)$ are different. Hence one has $f(a) < f(b)$. Therefore, the function f is strictly increasing. The case where f is decreasing is similar.

(2) Let a and b be different elements of $\mathrm{Dom}(f)$. Since I is totally ordered, either $a < b$ or $b < a$. Since f is strictly monotone, one deduces that, either $f(a) < f(b)$, or $f(b) < f(a)$. Hence f is injective. □

4.2.5 Proposition. *Let X be a totally ordered set, Y be a partially ordered set, f be an injective function from X to Y (in this case f^{-1} is also an injective function). If f is monotonic, then so is f^{-1}. Moreover, f^{-1} and f have the same direction of monotonicity.*

Proof. Without loss of generality, we may assume that f is increasing. Let a and b be two elements of $\mathrm{Im}(f) = \mathrm{Dom}(f^{-1})$. Since X is totally ordered, either $f^{-1}(a) < f^{-1}(b)$, or $f^{-1}(b) < f^{-1}(a)$. Since f is increasing and injective, by (1) of Proposition 4.2.4, f is strictly increasing. If $f^{-1}(b) < f^{-1}(a)$, then

$$b = f(f^{-1}(b)) < f(f^{-1}(a)) = a,$$

which contradicts the hypothesis $a < b$. Therefore, one should have $f^{-1}(a) < f^{-1}(b)$. Hence f^{-1} is strictly increasing. □

4.3 Supremum and infimum

4.3.1 Definition. Let $(X, \leq)$ be a partially ordered set, A be a subset of X.

(a) Let M be an element of X. If for every $x \in A$, we have $x \leq M$, then we say that M is an *upper bound* of A with respect to $\leq$. If Y is a subset of X which contains A and if A admits an upper bound that belongs to Y, we say that A is *bounded from above in Y*. If A is bounded from above in A, then it has a unique upper bound in A (by the antisymmetry of $\leq$). We denote this unique upper bound by $\max_{\leq} A$ and call it the *greatest element*[1] of A.

[1] In some literature, it is also called the *maximum* of A, which explains the expression max.

(b) Let m be an element of X. If for every $x \in A$, we have $m \leq x$, then we say that m is a *lower bound* of A with respect to $\leq$. If Y is a subset of X which contains A and if A admits an lower bound that belongs to Y, we say that A is *bounded from below in* Y. If A is bounded from below in A, then it has a unique lower bound in A. We denote this unique lower bound by $\min_{\leq} A$ and call it the *least element*[2] of A.

(c) Let f be a function from a set I to X. If the image of f is bounded from above (resp. bounded from below) in X, we say that f is *bounded from above* (resp. *bounded from below*). If f is bounded from above and bounded from below at the same time, we say that f is *bounded*. Similarly, if a subset A of X is bounded from above and bounded from below at the same time, we say that A is *bounded*.

(d) Let Y be a subset of X such that $A \subseteq Y$. If the set of all upper bounds of A in Y admits a least element with respect to $\leq$, then we call this least element the *supremum* of A in Y with respect to $\leq$, denoted by $\sup_{(Y,\leq)} A$.

(e) Let Y be a subset of X such that $A \subseteq Y$. If the set of all lower bounds of A in Y admits a greatest element with respect to $\leq$, then we call this greatest element the *infimum* of A in Y with respect to $\leq$, denoted by $\inf_{(Y,\leq)} A$.

4.3.2 Notation. Let $(X, \leq)$ be a partially ordered set, A and Y be subsets of X such that $A \subseteq Y$. We denote by A^u_Y the set of all upper bounds of A in Y, and denote by A^ℓ_Y the set of all lower bounds of A in Y. In the case where $Y = X$, the sets A^u_X and A^ℓ_X are denoted as A^u and A^ℓ respectively.

The greatest element, least element, supremum, and infimum introduced in Definition 4.3.1 are specific to the choice of partial order on a set X. It is important to note that the greatest and least elements of a subset A of X only depend on the induced partial order of A. On the contrary, the supremum and infimum of a subset A of X depend on both the partial order and the choice of the ambient subset Y that contains A and the induced order relation on Y.

When there is no ambiguity about the partial order and ambient subset, we often omit the expressions "relatively to ..." and "in ..." when referring to these concepts, and omit the subscripts specifying the choices of the partial order and the ambient subset. For example, the expressions $\min_{\leq} A$, $\max_{\leq} A$, $\sup_{(X,\leq)} A$, and $\inf_{(X,\leq)} A$ are often abbreviated as $\min A$, $\max A$, $\sup A$, and $\inf A$, respectively.

4.3.3 Notation. Let $(X, \leq)$ be a partially ordered set and let I be a set.

[2]In some literature, it is also called the *minimum* of A, which explains the expression min.

(1) For a function f from I to X, we denote the greatest element, the least element, the supremum, and the infimum of the image of f by $\max f$, $\min f$, $\sup f$, and $\inf f$, respectively.

(2) For a family $(x_i)_{i\in I}$ of elements of X parametrised by I, we denote the greatest element, the least element, the supremum, and the infimum of the set

$$\{x_i \,|\, i \in I\}$$

as

$$\max_{i\in I} x_i, \quad \min_{i\in I} x_i, \quad \sup_{i\in I} x_i, \quad \inf_{i\in I} x_i,$$

respectively. We also refer to them as the greatest element, the least element, the supremum, and the infimum of the family $(x_i)_{i\in I}$.

(3) Let $(x_i)_{i\in I}$ be a family of elements of X parametrised by I and $\mathbb{P}$ be a statement depending on a parameter in I. we denote the greatest element, the least element, the supremum, and the infimum of the set

$$\{x_i \,|\, i \in I,\, \mathbb{P}(i)\}$$

as

$$\max_{i\in I,\, \mathbb{P}(i)} x_i, \quad \min_{i\in I,\, \mathbb{P}(i)} x_i, \quad \sup_{i\in I,\, \mathbb{P}(i)} x_i, \quad \inf_{i\in I,\, \mathbb{P}(i)} x_i,$$

respectively.

4.3.4 Example. Consider the set of natural numbers $\mathbb{N}$ equipped with the usual total order. Note that 0 is the least element of $\mathbb{N}$ but $\mathbb{N}$ does not have any greatest element. In fact, for any $n \in \mathbb{N}$ one has $n < n + 1$. Hence n could not be the greatest element of $\mathbb{N}$.

4.3.5 Proposition. *Let $(X, \leq)$ be a partially ordered set, and let A, Z and Y be subsets of X such that $A \subseteq Z \subseteq Y$.*

(1) *If A has a greatest element, then $\max A$ is also the supremum of A in Y.*

(2) *If A has a least element, then $\min A$ is also the infimum of A in Y.*

(3) *If A has a supremum in Y that belongs to Z, then $\sup_{(Y,\leq)} A$ is also the supremum of A in Z. In particular, if $\sup_{(Y,\leq)} A$ belongs to A, then it is the greatest element of A.*

(4) *If A has an infimum in Y that belongs to Z, then $\inf_{(X,\leq)} A$ is also the infimum of A in Z. In particular, if $\inf_{(Y,\leq)} A$ belongs to A, then it is the least element of A.*

Proof. (1) By definition, $\max A$ is an upper bound of A in Y. If M is an upper bound of A, since $(\max A) \in A$, one obtains $M \geq \max A$. So $\max A$ is the least upper bound of A in Y, namely $\max A = \sup_{(Y,\leq)} A$. By inverting the partial order of X, we deduce (2) from (1).

(3) Let $M \in Z$ be an upper bound of A. By definition one has $\sup_{(Y,\leq)} A \leq M$. If $\sup_{(Y,\leq)} A$ belongs to Z, then it is the least upper bound of A in Z, namely the following equality holds:

$$\sup_{(Y,\leq)} A = \sup_{(Z,\leq)} A.$$

By inverting the partial order of X, we deduce (4) from (3). □

4.3.6 Proposition. *Let $(X, \leq)$ be a partially ordered set, and let A, B and Y be subsets of X such that $A \subseteq B \subseteq Y$.*

(1) *If both A and B have suprema in Y, then $\sup_{(Y,\leq)} A \leq \sup_{(Y,\leq)} B$.*

(2) *If both A and B have infima in Y, then $\inf_{(Y,\leq)} A \geq \inf_{(Y,\leq)} B$.*

Proof. (1) Suppose that A and B have suprema in Y. By definition $\sup_{(Y,\leq)} B$ is an upper bound of B in Y, hence it is also an upper bound of A in Y since $A \subseteq B$. Therefore, $\sup_{(Y,\leq)} A \leq \sup_{(Y,\leq)} B$.

Inverting the partial order of X, we deduce (2) from (1). □

4.3.7 Proposition. *Let $(X, \leq)$ be a partially ordered set, I be a set, $f : I \to X$ and $g : I \to X$ be mappings. Assume that for any $t \in I$ one has $f(t) \leq g(t)$.*

(1) *If both $\inf_{t\in I} f(t)$ and $\inf_{t\in I} g(t)$ exist, then the following inequality holds:*

$$\inf_{t\in I} f(t) \leq \inf_{t\in I} g(t).$$

(2) *If both $\sup_{t\in I} f(t)$ and $\sup_{t\in I} g(t)$ exist, then the following inequality holds:*

$$\sup_{t\in I} f(t) \leq \sup_{t\in I} g(t).$$

Proof. (1) For any $s \in I$ one has

$$\inf_{t\in I} f(t) \leq f(s) \leq g(s).$$

Hence $\inf_{t\in I} f(t)$ is a lower bound of $g(I)$. Therefore

$$\inf_{t\in I} f(t) \leq \inf_{t\in I} g(t).$$

By inverting the partial order of X, we deduce (2) from (1). □

4.3.8 Proposition. *Let I be a totally ordered set, X be a partially ordered set, $f : I \to X$ be a mapping and J be a subset I. Assume that J* does not *have any upper bound in I.*

(1) *If f is increasing, then $f(I)^u = f(J)^u$.*

(2) *If f is decreasing, then $f(I)^\ell = f(J)^\ell$.*

Proof. (1) Since $f(J) \subseteq f(I)$, any upper bound of $f(I)$ is also an upper bound of $f(J)$. Conversely, suppose that M is an upper bound of $f(J)$. Let $x \in I$. Since I is totally ordered and J does not have any upper bound in I, there exists $y \in J$ such that $x < y$. Since f is increasing, one obtains $f(x) \leq f(y) \leq M$. Hence M is also an upper bound of $f(I)$.

By inverting the partial order of X, we deduce (2) from (1). □

4.3.9 Proposition. *Let $(X, \leq)$ be partially ordered set, Y be a subset of X, $(A_i)_{i\in I}$ be a family of subsets of Y, and A be the union of $(A_i)_{i\in I}$.*

(1) *Suppose that each A_i has a supremum y_i in Y. Then*

$$A^u = \{y_i \,|\, i \in I\}^u.$$

In particular, the set A has a supremum in Y if and only if $\{y_i \,|\, i \in I\}$ has a supremum in Y. Moreover, in the case where these suprema exist, the following equality holds:

$$\sup_{(Y,\leq)} A = \sup_{(Y,\leq)} \{y_i \,|\, i \in I\}.$$

(2) *Suppose that each A_i has a infimum z_i in Y. Then*

$$A^\ell = \{z_i \,|\, i \in I\}^\ell.$$

In particular, the set A has an infimum in Y if and only if $\{z_i \,|\, i \in I\}$ has an infimum in Y. Moreover, in the case where these infima exist, the following equality holds:

$$\inf_{(Y,\leq)} A = \inf_{(Y,\leq)} \{z_i \,|\, i \in I\}.$$

Proof. It suffices to treat the first statement. Let y be an element of Y. Note that the following statement are equivalent:

(a) y is an upper bound of A,

(b) for any $i \in I$, y is an upper bound of A_i,

(c) $\forall\, i \in I$, $y_i \leq y$.

Therefore, the sets A and $\{y_i \,|\, i \in I\}$ have the same upper bounds in Y. The statement is thus proved. □

4.4 Intervals

4.4.1 Notation. Let $(X, \leq)$ be a totally ordered set. For $(a, b) \in X \times X$, we denote the set

$$\{x \in X \mid a \leq x \leq b\}$$

as $[a, b]$. Note that $[a, b]$ is empty when $a \not\leq b$.

4.4.2 Definition. Let $(X, \leq)$ be a partially ordered sest, and I be a subset of X. If, for any $(x, y) \in I \times I$, one has $[x, y] \subseteq I$, then we say that I is an *interval* in X.

4.4.3 Example. Let $(X, \leq)$ be a partially ordered set. For $(a, b) \in I \times I$, we define the sets $]a, b[$, $[a, b[$, $]a, b]$ and $[a, b]$ as follows.

$$\begin{aligned}
]a, b[&:= \{x \in X \mid a < x < b\}, \\
[a, b[&:= \{x \in X \mid a \leq x < b\}, \\
]a, b] &:= \{x \in X \mid a < x \leq b\}, \\
[a, b] &:= \{x \in X \mid a \leq x \leq b\}.
\end{aligned}$$

These sets are all intervals in X.

Moreover, for any $x \in X$, the sets

$$\begin{aligned}
X_{<a} &:= \{x \in X \mid x < a\}, \\
X_{\leq a} &:= \{x \in X \mid x \leq a\}, \\
X_{>a} &:= \{x \in X \mid x > a\}, \\
X_{\geq a} &:= \{x \in X \mid x \geq a\}
\end{aligned}$$

are all intervals in X.

Finally the set X itself is also an interval in X.

4.4.4 Proposition. *Let $(X, \leq)$ be a partially ordered set and $(I_\alpha)_{\alpha \in \Lambda}$ be a family of intervals in X parametrised by a non-empty set Λ.*

(1) *The intersection $\bigcap_{\alpha \in \Lambda} I_\alpha$ is an interval.*

(2) *Suppose that $(X, \leq)$ is a totally ordered set. If $\bigcap_{\alpha \in \Lambda} I_\alpha$ is not empty, then $\bigcup_{\alpha \in \Lambda} I_\alpha$ is an interval.*

Proof. (1) Let a and b be elements of $\bigcap_{\alpha \in \Lambda} I_\alpha$. For any $\alpha \in \Lambda$, one has $\{a, b\} \subseteq I_\alpha$ and hence $[a, b] \subseteq I_\alpha$ since I_α is an interval. Therefore we obtain $[a, b] \subseteq \bigcap_{\alpha \in \Lambda} I_\alpha$, as required.

(2) Let x be an element of $\bigcap_{\alpha \in \Lambda} I_\alpha$. Let a and b be two elements of $\bigcup_{\alpha \in \Lambda} I_\alpha$ such that $a \leq b$. Let α and β be elements of Λ such that $a \in I_\alpha$ and $b \in I_\beta$. We will show that $[a, b] \subseteq I_\alpha \cup I_\beta$.

If $b \leq x$ then one has $[a, b] \subseteq [a, x] \subseteq I_\alpha$, where the second inclusion follows from the hypothesis that I_α is an interval and the condition $\{a, x\} \subseteq I_\alpha$. Similarly, if $x \leq a$, then one has $[a, b] \subseteq [x, b] \subseteq I_\beta$. If $a < x < b$, then $[a, b] = [a, x] \cup [x, b]$. Since $[a, x] \subseteq I_\alpha$ and $[x, b] \subseteq I_\beta$, we obtain $[a, b] \subseteq I_\alpha \cup I_\beta$. □

4.4.5 Definition. Let $(X, \leq)$ be a partially ordered set and I be a non-empty interval in X. If I has a supremum in X, then $\sup I$ is called the *right endpoint* of X. If I has an infimum in X, then $\inf I$ is called the *left endpoint* of X.

4.4.6 Proposition. *Let $(X, \leq)$ be a totally ordered set and I be an interval in X.*

(1) *Assume that I has a supremum b in X. For any $x \in I$, one has $[x, b[\subseteq I$.*

(2) *Assume that I has an infimum a in X. For any $x \in I$, one has $]a, x] \subseteq I$.*

Proof. (1) Let y be an element of X such that $x \leq y < b$. Since b is the supremum of I, y cannot be an upper bound of I, namely there exists $z \in I$ such that $y < z$. Since I is an interval, one has $[x, z] \subseteq I$. Hence $y \in I$.

If we apply (1) to $(X, \geq)$, then we obtain (2). □

4.4.7 Proposition. *Let $(X, \leq)$ be a totally ordered set and I be a non-empty interval in X. Assume that I has a supremum b and an infimum a in X. Then I is equal to one of the following intervals: $[a, b]$, $]a, b]$, $[a, b[$, $]a, b[$.*

Proof. Since I is non-empty, one has $a \leq b$. For any $x \in I$ one has $a \leq x \leq b$. Hence $I \subseteq [a, b]$. If $\{a, b\} \subseteq I$, then by the hypothesis that I is an interval, one has $[a, b] \subseteq I$. Therefore $I = [a, b]$.

If $a \in I$ but $b \notin I$, then $I \subseteq [a, b[$. Moreover, any element $t \in [a, b[$ is not an upper bound of I, otherwise b cannot be the least upper bound of I. Hence there exists $x \in I$ such that $x > t$. By the hypothesis of the proposition, one has $[a, x] \subseteq I$ and hence $t \in I$. Thus we obtain $[a, b[\subseteq I$. By the same method, one can prove that, if $b \in I$ and $a \notin I$, then $I =]a, b]$.

Suppose that $\{a, b\} \cap I = \varnothing$. Then $I \subseteq]a, b[$. For any $t \in]a, b[$, there exists elements x and y of I such that $x < t < y$. By the hypothesis of the proposition, one has $[x, y] \subseteq I$ and hence $t \in I$. Therefore $I =]a, b[$. □

4.4.8 Definition. Let $(X, \leq)$ be a totally ordered set. If for any couple (x, z) of elements of X such that $x < z$, there exists $y \in X$ such that $x < y < z$, we say that the totally ordered set $(X, \leq)$ is *dense*.

4.4.9 Example. The set $\mathbb{Q}$ equipped with the usual partial order $\leq$ is dense. However, the set $\mathbb{Z}$ equipped with the usual partial order $\leq$ is not dense.

4.4.10 Proposition. *Let $(X, \leq)$ be a dense totally ordered set, and $(a, b) \in X \times X$ such that $a \leq b$. If I is one of the intervals $[a, b]$, $]a, b]$, $[a, b[$ and $]a, b[$, then the following equalities hold:*

$$\inf I = a, \quad \sup I = b.$$

Proof. By definition b is an upper bound of I. Since $(X, \leq)$ is a totally ordered set, if b is not the supremum of I, then there exists an upper bound M of I such that $M < b$. Pick an element $x \in I$. By definition one has $x \leq M < b$. Hence by (1) of Proposition 4.4.6 one obtains $M \in I$. Therefore M is the greatest element of I. However, since X is dense, there exists M' such that $M < M' < b$. Still by (1) of Proposition 4.4.6 one has $M' \in I$, which leads to a contradiction. Hence b is the supremum of I in X. Applying the above argument to $(X, \geq)$, we obtain that a is the infimum of I in $(X, \leq)$. □

4.5 Order-completeness

4.5.1 Definition. Let $(X, \leq)$ be a partially ordered set. If any subset of X has a supremum in X, we say that $(X, \leq)$ is *order-complete*. Note that an order-complete partially ordered set is never empty.

4.5.2 Proposition. *Let $(X, \leq)$ be an order-complete partially ordered set. Then any subset of X has an infimum in X. Moreover, X has a greatest element and a least element.*

Proof. Let A be a subset of X and L_A be the set of all lower bounds of A in X. Since $(X, \leq)$ is an order-complete partially ordered set, L_A admits a supremum in X, which we denote by m. By definition, any element a of A is an upper bound of L_A. Hence $m \leq a$. This shows that m is a lower bound of A, namely $m \in L_A$. By (3) of Proposition 4.3.5, one obtains that m is actually the greatest element of L_A, namely $m = \inf A$. By definition, the infimum of $\varnothing$ is the greatest element of X, the supremum of $\varnothing$ is the least element of X. □

4.5.3 Example. Let A be a set. The power set $\mathscr{P}(A)$ equipped with the relation of inclusion forms a partially ordered set that is order-complete. Specifically, if $(A_i)_{i \in I}$ is a family of subsets of A, then the supremum of the family in $\mathscr{P}(A)$ is given by $\bigcup_{i \in I} A_i$. If I is non-empty, then the infimum of the family is $\inf_{i \in I} A_i = \bigcap_{i \in I} A_i$. If I is empty, then the infimum of the empty family in $\mathscr{P}(A)$ is A.

4.5.4 Definition. Let X be a set and f be a function from X to X. If x is an element of X such that $f(x) = x$, we say that x is a *fixed point* of f.

4.5.5 Theorem (Knaster-Tarski fixed point theorem)**.** *Let $(X, \leq)$ be an order-complete partially ordered set and $f : X \to X$ be an increasing mapping. Then the set of fixed points*

$$F = \{x \in X \mid f(x) = x\},$$

equipped with the induced partial order, forms an order-complete partially ordered set. In particular, f has at least one fixed point.

Proof. Let A be a subset of F. We consider the following subset of X:

$$S_A = \{y \in X \mid y \text{ is an upper bound of } A \text{ and } f(y) \leq y\}.$$

Let m be the infimum of S_A. Since S_A is a subset of the set of upper bounds of A, by (2) of Proposition 4.3.6, one obtains $\sup A \leq m$, namely m is an upper bound of A. Since f is increasing, for any $y \in S_A$, one has

$$f(m) \leq f(y) \leq y.$$

Therefore $f(m) \leq m$. Moreover, since f is increasing, for any $x \in A$ one has

$$x = f(x) \leq f(m),$$

and one has $f(f(m)) \leq f(m)$. Therefore, $f(m)$ belongs to S_A and hence $m \leq f(m)$. Thus m is a fixed point of f. Finally, if y is a fixed point of f and is an upper bound of A, then $y \in S_A$ and hence $m \leq y$. Therefore m is the least upper bound of A in F, namely the supremum of A in F. □

4.5.6 Theorem (Cantor-Bernstein)**.** *Let X and Y be sets. Assume that there exists an injective mapping from X to Y and an injective mapping from Y to X, then there exists a bijection from X to Y.*

Proof. Let $f : X \to Y$ and $g : Y \to X$ be injective mappings. We intend to find a subset C of X such that the restriction of g to $Y \setminus f(C)$ has $X \setminus C$ as its image. Then the mapping $h : X \to Y$ such that

$$\forall\, x \in X, \quad h(x) = \begin{cases} f(x), & \text{if } x \in C, \\ g^{-1}(x), & \text{if } x \in X \setminus C \end{cases}$$

is a bijection. By Example 4.5.3, the partially ordered set $(\mathscr{P}(X), \subseteq)$ is set-complete. We consider the mapping $\varphi : \mathscr{P}(X) \to \mathscr{P}(X)$ defined as follows:

$$\forall\, A \subseteq X, \quad \varphi(A) = X \setminus g(Y \setminus f(A)).$$

If A and B are two subsets of X such that $A \subseteq B$, then one has $f(A) \subseteq f(B)$ and furthermore

$$(Y \setminus f(B)) \subseteq (Y \setminus f(A)), \quad g(Y \setminus f(B)) \subseteq g(Y \setminus f(A)),$$

which leads to $\varphi(A) \subseteq \varphi(B)$. Thus φ is increasing. By Theorem 4.5.5, the mapping φ admits a fixed point C, as required. □

4.5.7 Lemma. *Let $(X, \leq)$ be a partially ordered set.*

(1) *Let A and B be subsets of X such that $A \subseteq B$. Then $B^u \subseteq A^u$, $B^\ell \subseteq A^\ell$.*

(2) *For any $A \in \mathscr{P}(X)$, we have $A \subseteq (A^u)^\ell \cap (A^\ell)^u$.*

Proof. (1) Since $A \subseteq B$, it follows that every upper bound of B is an upper bound of A, and every lower bound of B is a lower bound of A.

(2) Let $a \in A$. For any $x \in A^u$, we have $a \leq x$, so a is a lower bound of A^u. Similarly, for any $y \in A^\ell$, we have $y \leq a$, so a is an upper bound of A^ℓ. □

4.5.8 Theorem (MacNeille)**.** *Let $(X, \leq)$ be a partially ordered set. Define*

$$\widehat{X} := \{A \in \mathscr{P}(X) \,|\, (A^u)^\ell = A\}.$$

(1) *$(\widehat{X}, \subseteq)$ forms an order complete partially ordered set.*

(2) *For any $A \in \mathscr{P}(X)$, $A^\ell \in \widehat{X}$.*

(3) *The mapping*

$$X \longrightarrow \widehat{X}, \quad (x \in X) \longmapsto \widehat{x} := \{x\}^\ell$$

is strictly increasing.

(4) *For any $A \in \widehat{X}$, the following equality holds:*

$$A = \bigcup_{x \in A} \widehat{x}.$$

In particular, A is the supremum of $\{\widehat{x} \,|\, x \in A\}$ in $\widehat{X}$.

(5) *Let $A \in \widehat{X}$. If $A^u = \varnothing$, then $A = X$; if A^u is nonempty, then*

$$A = \bigcap_{x \in A^u} \widehat{x}.$$

In particular, A is the infimum of $\{\widehat{x} \,|\, x \in A^u\}$ in $\widehat{X}$.

Proof. (1) By Lemma 4.5.7 (1), the map

$$\varphi : \mathscr{P}(X) \longrightarrow \mathscr{P}(X), \quad A \longmapsto (A^u)^\ell$$

is increasing. By definition, $\widehat{X}$ is the set of all fixed points of φ. Since the poset $(\mathscr{P}(X), \subseteq)$ is order complete (Example 4.5.3), by Theorem 4.5.5 we obtain the order completeness of $(\widehat{X}, \subseteq)$.

(2) Apply the first inclusion of Lemma 4.5.7 (2) to A^ℓ to get $A^\ell \subseteq ((A^\ell)^u)^\ell$. Then apply the second inclusion of Lemma 4.5.7 (2) to A to get $A \subseteq (A^\ell)^u$. Finally, by Lemma 4.5.7 (1), we have $((A^\ell)^u)^\ell \subseteq A^\ell$.

(3) If $x < y$, then every lower bound of x is a lower bound of y, i.e., $\widehat{x} \subseteq \widehat{y}$. Moreover, y is a lower bound of itself but not of x, so $\widehat{x} \neq \widehat{y}$.

(4) First, for any $x \in A$, we have $x \in \widehat{x}$. Hence

$$A \subseteq \bigcup_{x \in A} \widehat{x}.$$

Conversely, for any $x \in A$, x is the least element of $\{x\}^u$, so

$$\{x\}^\ell = (\{x\}^u)^\ell \subseteq (A^u)^\ell = A,$$

where the inclusion follows from Lemma 4.5.7 (1). This yields

$$\bigcup_{x \in A} \widehat{x} \subseteq A,$$

and thus the equality $A = \bigcup_{x \in A} \widehat{x}$ holds. By Example 4.5.3, A is the supremum of $\{\widehat{x} \,|\, x \in A\}$ in $\mathscr{P}(X)$. By Proposition 4.3.5, we deduce that A is the supremum of $\{\widehat{x} \,|\, x \in A\}$ in $\widehat{X}$.

(5) If $A^u = \varnothing$, then

$$A = (A^u)^\ell = \varnothing^\ell = X.$$

Now assume A^u is nonempty. By definition,

$$\bigcap_{x \in A^u} \widehat{x} = \bigcap_{x \in A^u} \{a \in X \,|\, a \leq x\} = (A^u)^\ell = A.$$

By Example 4.5.3, A is the infimum of $\{\widehat{x} \,|\, x \in A^u\}$ in $\mathscr{P}(X)$. By Proposition 4.3.5, we deduce that A is the infimum of $\{\widehat{x} \,|\, x \in A^u\}$ in $\widehat{X}$. □

4.5.9 Remark. Let $(X, \leq)$ be a partially ordered set, $A \in \widehat{X}$, and x be an element of X. If $\widehat{x} \subseteq A$, then by $x \in \widehat{x}$ we obtain $x \in A$. Conversely, from the proof of Theorem 4.5.8 (4), we observe that, for any $x \in A$, we have $\widehat{x} \subseteq A$. Hence

$$A = \{x \in X \,|\, \widehat{x} \subseteq A\}.$$

Similarly, $x \in X$ is an upper bound of A if and only if $A \subseteq \widehat{x}$, namely

$$A^u = \{x \in X \,|\, A \subseteq \widehat{x}\}.$$

4.5.10 Definition. Let $(X, \leq)$ be a partially ordered set. Then the set

$$\widehat{X} = \{A \in \mathscr{P}(X) \,|\, (A^u)^\ell = A\}$$

under the inclusion relation $\subseteq$ forms an order complete partially ordered set, called the *Dedekind-MacNeille order completion* of X. Theorem 4.5.8 shows that the mapping $X \to \widehat{X}$, $x \mapsto \widehat{x}$ is strictly increasing. Via this mappng, we can identify X with a subset of $\widehat{X}$ and regard the inclusion relation on $\widehat{X}$ as an extension of the partial order $\leq$.

4.6 Mathematical induction

4.6.1 Definition. Let $(X, \leq)$ be a partially ordered set. If any non-empty subset of X has a least element, we say that $\leq$ is a *well-order* and that $(X, \leq)$ is a *well-ordered set.*

4.6.2 Proposition. *Let $(X, \leq)$ be a well-ordered set and Y be a subset of X. Then $(Y, \leq)$ is also a well-ordered set.*

Proof. Let A be a non-empty subset of Y. It is also a non-empty subset of X. Hence it has a least element. □

4.6.3 Proposition. *A well-ordered set is totally ordered.*

Proof. Let $(X, \leq)$ be a well-ordered set. If x and y are two elements of X, then $\{x, y\}$ has a least element. If this least element is x, then $x \leq y$, otherwise $y \leq x$. Hence $(X, \leq)$ is a totally ordered set. □

4.6.4 Axioms. We equip $\mathbb{N}$ with the usual partial order $\leq$ defined as follows:

$$a \leq b \text{ if and only if } \exists\, c \in \mathbb{N},\, b = a + c.$$

Then $(\mathbb{N}, \leq)$ forms a well-ordered set. Proposition 4.6.2 shows that any subset of $\mathbb{N}$ equipped with the restricted partial order is a well-ordered set.

4.6.5 Theorem (Induction)**.** *Let $(X, \leq)$ be a well-ordered set and $P(\cdot)$ be a condition on X. Suppose that*

$$\forall\, x \in X,\ \big(\forall\, y \in X_{<x},\ P(y)\big) \Rightarrow P(x). \tag{4.1}$$

Then the following statement holds:

$$\forall\, x \in X,\ P(x).$$

Proof. Let

$$A = \{x \in X \mid \neg P(x)\}.$$

If A is not empty, then it admits a least element α. For any $\beta \in X_{<\alpha}$, one has $\beta \notin A$ and hence $P(\beta)$ is true. By the hypothesis of the theorem, we obtain that $P(\alpha)$ is true, which leads to a contradiction. Therefore, for any $x \in X$, $P(x)$ is true.

□

4.6.6 Remark. We keep the notation and the assumptions of the previous theorem. The statement $\forall\, y \in X_{<x},\ P(y)$ in (4.1) is called *induction hypothesis* for x. If for any $x \in X$ we could deduce $P(x)$ from the induction hypothesis for x, then Theorem 4.6.5 proves that the condition $P(\cdot)$ is satisfied by any element of X. Let α be the least element of X. The statement

$$(\forall\, y \in X_{<\alpha},\ P(y)) \Rightarrow P(\alpha)$$

is true if and only if $P(\alpha)$ is true. Therefore, to check the condition (4.1), it is necessary to check that the statement $P(\alpha)$ is true.

4.6.7 Proposition. *Let $(X, \leq)$ be a totally ordered set and n be a non-zero natural number. For any family $(x_i)_{i\in\{1,\ldots,n\}}$ of elements of X, the set $\{x_1, \ldots, x_n\}$ admits a greatest element and a least element.*

Proof. We apply Theorem 4.6.5 to the well ordered set $\mathbb{N}_{>0}$.

In the case where $n = 1$, we observe that, for any $x_1 \in X$, the element x_1 is both greatest and least element of $\{x_1\}$.

Let n be a natural number such that $n \geq 2$. Assume that, for any $m \in \mathbb{N}_{>0}$ such that $m < n$, any family $(x_i)_{i\in\{1,\ldots,m\}}$ of elements of X admits a greatest element and a least element.

Let $(x_i)_{i\in\{1,\ldots,n\}}$ be a family of elements of X. By the induction hypothesis, the set $\{x_1, \ldots, x_{n-1}\}$ admits a least element a and a greatest element A. Since X is totally ordered, either $a \leq x_n$ or $x_n \leq a$. If $a \leq x_n$, then a is the least element of $\{x_1, \ldots, x_n\}$, otherwise x_n is the least element of $\{x_1, \ldots, x_n\}$. Therefore $\{x_1, \ldots, x_n\}$ admits a least element. A similar argument shows that either A or x_n is the greatest element of $\{x_1, \ldots, x_n\}$.

By Theorem 4.6.5, we deduce the current proposition. □

4.6.8 Proposition. *Let $(X, \leq)$ be a partially ordered set and $x_1, \ldots, x_n$ be elements of X where n is positive integer. Assume that $x_1 \leq \ldots \leq x_n$ (see Notation 3.11.2). Then $x_1 \leq x_n$.*

Proof. We reason by induction on n. The case where $n = 1$ is trivial. In the following, we consider the case where $n \geq 2$ in assume that the statement is true

for less than n elements. The induction hypothesis then leads to $x_1 \leq x_{n-1}$. Since $x_{n-1} \leq x_n$, by the transitivity of the partial order $\leq$, we obtain $x_1 \leq x_n$, as required. □

4.6.9 Corollary. *Let $(X, \leq)$ be a partially ordered set and $x_1, \ldots, x_n$ be elements of X where n is a natural number which is greater than or equal to 2. Assume that $x_1 \leq \ldots \leq x_n$ and $x_n \leq x_1$. Then all elements $x_1, \ldots, x_n$ are equal.*

Proof. By Proposition 4.6.8, for any $i \in \{2, \ldots, n\}$, from $x_1 \leq \ldots \leq x_i$, we deduce $x_1 \leq x_i$, and, from $x_i \leq \ldots \leq x_n \leq x_1$, we deduce $x_i \leq x_1$. Hence $x_1 = x_i$. □

4.6.10 Definition. Let $(X, \leq)$ be a partially ordered set. If a subset I of X satisfies

$$\forall\, a \in I,\ X_{<a} \subseteq I,$$

then we say that I is an *initial segment* of X.

4.6.11 Example. Let $(X, \leq)$ be a partially ordered set. For any $a \in X$, the sets $X_{<a}$ is an initial segment of X. In fact, if x is an element of $X_{<a}$ and if y is an element of X such that $y < x$, then the inequality $y < a$ holds. Similarly, the set $X_{\leq a}$ is an initial segment of X, too.

4.6.12 Proposition. *Let $(X, \leq)$ be a totally ordered set, and I and J are initial segments of X. Then, either $I \subseteq J$ or $J \subseteq I$.*

Proof. Suppose that x is an element of $I \setminus J$. We clame that, for any $y \in J$ one has $y \leq x$ and hence $y \in I$ since I is a initial segment. We reason by contradiction in assuming that $y \not\leq x$. Since $\leq$ is a total order, one has $x < y$. Since J is an initial segment, one has $x \in X_{<y} \subseteq J$, which leads to a contradiction. □

4.6.13 Proposition. *Let $(X, \leq)$ be a well-ordered set. If I is an initial segment of X such that $I \neq X$, then there exists a unique element $a \in X$ such that $I = X_{<a}$.*

Proof. Since $I \neq X$, the set $X \setminus I$ is not empty. Since $(X, \leq)$ is well ordered, $X \setminus I$ has a least element which we denote as a.

We claim that $I = X_{<a}$. In fact, for any $x \in I$ one has $x < a$ since otherwise by the hypothesis that I is an initial segment we obtain $a \in I$, which leads to a contradiction. Hence $I \subseteq X_{<a}$. Conversely, if y is an element of $X_{<a}$, then by the hypothesis that a is the least element of $X \setminus I$ we obtain $y \in I$.

Since a well-ordered set is totally ordered, for any $b \in X$ one has $X_{\geq b} = X \setminus X_{<b}$ and thus $b = \min(X \setminus X_{<b})$. Hence we obtain the uniqueness of $a \in X$ such that $I = X_{<a}$. □

4.6.14 Proposition. *Let $(X, \leq)$ be a partially ordered set. If $(I_\lambda)_{\lambda \in \Lambda}$ is a family of initial segments of X, then the union $I = \bigcup_{\lambda \in \Lambda} I_\lambda$ is an initial segment of X.*

Proof. Let x be an element of I. There exists $\lambda \in \Lambda$ such that $x \in I_\lambda$. Since I_λ is an initial segment, we obtain

$$X_{<x} \subseteq I_\lambda \subseteq I.$$

Hence I is also an initial segment. □

4.6.15 Theorem. *Let $(X, \leq)$ be a well-ordered set, and Y be a set. For any $x \in X$ and any mapping $h : X_{<x} \to Y$, we fix an element $\Phi(h)$ of Y. Then, there exists a unique mapping $f : X \to Y$ such that*

$$\forall\, x \in X, \quad f(x) = \Phi(f|_{X_{<x}}).$$

Proof. We first prove the uniqueness. Suppose that f and g are two mappings from X to Y such that

$$\forall\, x \in X,\ f(x) = \Phi(f|_{X_{<x}}),\ g(x) = \Phi(g|_{X_{<x}}).$$

Then, for any $x \in X$, one has

$$\big(\forall\, y \in X_{<x},\ f(y) = g(y)\big) \Longrightarrow f(x) = g(x).$$

By Theorem 4.6.5 we obtain

$$\forall\, x \in X,\ f(x) = g(x).$$

In the following, we prove the existence. Let $\mathscr{S}$ be the set of all initial segments S of X that satisfies the following condition:

$$\textit{there exists } f_S : S \to Y \textit{ such that } \forall\, x \in S,\ f_S(x) = \Phi(f_S|_{X_{<x}}).$$

Note that the uniqueness part applied to $(S, \leq)$ shows that $f_S : S \to Y$ is the unique mapping that satisfies

$$\forall\, x \in S,\ f_S(x) = \Phi(f_S|_{X_{<x}}).$$

Let $X_0 = \bigcup_{S \in \mathscr{S}} S$. By Proposition 4.6.14, X_0 is an initial segment of X.

For any $x \in X_0$, there exists $S \in \mathscr{S}$ such that $x \in S$. We claim that the value of $f_S(x)$ does not depend on the choice of S. In fact, if S and S' are two elements of $\mathscr{S}$ such that $x \in S \cap S'$. By Proposition 4.6.12, either $S \subseteq S'$ and $f_{S'}|_S = f_S$ (by the uniqueness of f_S), or $S' \subseteq S$ and $f_S|_{S'} = f_{S'}$. We denote by $f(x)$ the value $f_S(x)$. We thus obtain a mapping $f : X_0 \to Y$, that satisfies

$$\forall\, x \in X_0,\ f(x) = \Phi(f|_{X_{<x}}).$$

In particular, one has $X_0 \in \mathscr{S}$. Hence it is the greatest element of $\mathscr{S}$.

Suppose that $X_0 \neq X$. By Proposition 4.6.13, there exists $a \in X$ such that $X_0 = X_{<a}$. We extend f to a mapping from $X_{\leq a}$ to Y that sends a to $\Phi(f)$. This construction shows that $X_{\leq a} \in \mathscr{S}$, which contradicts the fact that X_0 is the greatest element of $\mathscr{S}$. Therefore, one has $X_0 = X$, which concludes the theorem. □

4.7 Finiteness and countability

4.7.1 Definition. Let A be a set. If there is an injective mapping from A to $\mathbb{N}$, we say that A is *countable*. If there is an injective mapping from A to $\mathbb{N}$ which is bounded from above (that is, the image of the mapping is bounded from above in $\mathbb{N}$, see (c) of Definition 4.3.1), we say that A is *finite*. By definition, if a subset I of $\mathbb{N}$ is bounded from above, then it is finite (one can consider the inclusion mapping from I to $\mathbb{N}$).

4.7.2 Lemma. (1) *Let n be a natural number and let $x_0, \ldots, x_n$ be elements of $\mathbb{N}$ such that $x_0 < \ldots < x_n$. Then, for any $i \in \{0, \ldots, n\}$, one has $i \leq x_i$.*

(2) *Let $(x_i)_{i\in\mathbb{N}}$ be a family of natural numbers. Assume that*

$$x_0 < x_1 < \ldots < x_i < x_{i+1} < \ldots.$$

Then, for any $i \in \mathbb{N}$, one has $i \leq x_i$.

Proof. We reason by induction on $i \in \{0, \ldots, n\}$ in (1), and on $i \in \mathbb{N}$ in (2).

Since $x_0 \in \mathbb{N}$, one has $0 \leq x_0$. Assume that

$$\forall\, j \in \{0, \ldots, i-1\},\ j \leq x_j.$$

By $x_i > x_{i-1}$, we obtain $x_i \geq x_{i-1} + 1$ since x_i and x_{i-1} are natural numbers. Hence $x_i \geq (i-1)+1 = i$. By Theorem 4.6.5, we obtain the statement announced in the lemma. □

4.7.3 Proposition. *Let $f : A \to B$ be a mapping.*

(1) *If f is injective and B is countable (resp. finite), then A is also countable (resp. finite). In particular, subsets of a countable (resp. finite) set are all countable (resp. finite).*

(2) *If f is surjective and A is countable (resp. finite), then B is also countable (resp. finite). In particular, the quotient set of a countable (resp. finite) set by an equivalence relation is a countable (resp. finite) set.*

Proof. (1) Assume that $\varphi : B \to \mathbb{N}$ is an injective mapping. Consider the composed mapping $\varphi \circ f : A \to \mathbb{N}$. By (2) of Proposition 3.6.4, $g \circ f$ is injective. Moreover, by Proposition 3.4.5 one has $\mathrm{Im}(g \circ f) \subseteq \mathrm{Im}(g)$. If $\mathrm{Im}(g)$ is bounded from above, then $\mathrm{Im}(g \circ f)$ is also bounded from above. Therefore the countability (resp. finiteness) of B implies that of A. By applying this statement to an inclusion mapping, we obtain the second statement.

(2) By (1) of Proposition 3.9.6 , there exists an injective mapping from B to A. Hence the first statement of (2) follows from the first statement of (1). By applying this statement to a quotient mapping, we obtain the second statement. □

4.7.4 Proposition. *Let X and Y be sets.*

(1) *If both X and Y are countable (resp. finite), then $X \cup Y$ is countable (resp. finite).*

(2) *If X is uncountable (resp. infinite) and Y is countable (resp. finite), then $X \setminus Y$ is uncountable (resp. infinite).*

Proof. (1) Let $f : X \to \mathbb{N}$ and $g : Y \to \mathbb{N}$ be injective mappings. We construct a mapping $h : X \cup Y \to \mathbb{N}$ as follows:

$$h(x) := \begin{cases} 2f(x), & \text{if } x \in X, \\ 2g(x) + 1, & \text{if } x \in Y \setminus X. \end{cases}$$

Let x and y be two different elements of $X \cup Y$. If $\{x, y\} \subseteq X$, then, by the injectivity of f we deduce that

$$h(x) = 2f(x) \neq 2f(y) = h(y).$$

If $\{x, y\} \subseteq Y \setminus X$, then by the injectivity of g we deduce that

$$h(x) = 2g(x) + 1 \neq 2g(y) + 1 = h(y).$$

If one of x and y belongs to X and the other belongs to $Y \setminus X$, then one of $h(x)$ and $h(y)$ is even and the other is odd, and hence $h(x) \neq h(y)$. Therefore h is injective. Moreover, if both f and g are bounded, then h is also bounded. Therefore the statement holds.

(2) Assume that $X \setminus Y$ is countable (resp. finite). By (1) of Proposition 4.7.3, $X \cap Y$ is countable (resp. finite) since Y is countable (resp. finite). Therefore, we deduce from (1) that

$$X = (X \setminus Y) \cup (X \cap Y),$$

is countable (resp. finite). □

4.7.5 Notation. Let X be a set and $f : X \to X$ be a mapping. We denote by f^0 the identity mapping Id_X. In a recursive way, for any non-zero natural number n, we denote by f^n the composite mapping $f \circ f^{n-1}$.

4.7.6 Proposition. *Let X be a subset of $\mathbb{N}$.*

(1) *The identity mapping Id_X is the only increasing bijection from X to itself.*

(2) *If X is bounded from above, then the identity mapping Id_X is the only strictly increasing mapping from X to itself. In particular, for any proper subset Y of X, there does not exist any strictly increasing mapping from X to Y.*

Proof. Let $f : X \to X$ be a strictly increasing mapping and let

$$A = \{n \in \mathbb{N} \,|\, f(n) \neq n\}.$$

Note that, by (2) of Proposition 4.2.4, the mapping f is injective. To show (1) and the first statement of (2), it suffices to prove that, if $f \neq \mathrm{Id}_X$, namely the set A is not empty, then f is not surjective and X is not bounded from above.

Assume that A is not empty. Since $(\mathbb{N}, \leq)$ is well-ordered, A admits a least element n_0. By definition one has $f(n_0) \neq n_0$. Since $\mathbb{N}$ is totally ordered, either $f(n_0) < n_0$ or $n_0 < f(n_0)$. If $f(n_0) < n_0$, then $f(n_0) \notin A$ and hence $f(f(n_0)) = f(n_0)$, this contradicts the injectivity of f. Thus we should have $n_0 < f(n_0)$. For any $n \in X$, if $n_0 \leq n$, then

$$n_0 < f(n_0) \leq f(n);$$

if $n < n_0$, then

$$f(n) = n < n_0.$$

Hence in both cases $f(n) \neq n_0$. In particular, f is not surjective. Moreover, since f is strictly increasing, from $n_0 < f(n_0)$ we deduces that

$$n_0 < f(n_0) < f(f(n_0)) < \ldots,$$

which implies that $f^k(n_0) \geq k$ for any $k \in \mathbb{N}$ by Lemma 4.7.2. Therefore X is not bounded from above.

It remains to prove the second statement of (2). Assume that there is a strictly increasing mapping $g : X \to Y$. Let $j_Y : Y \to X$ be the inclusion mapping. Then the composite mapping $j_Y \circ g$ is a strictly increasing mapping from X to X (see Example 4.2.2 and (2) of Proposition 4.2.3). However, the image of $j_Y \circ g$ is contained in Y and hence $j_Y \circ g$ can not be equal to Id_X. This contradicts the first statement of (2). □

4.7.7 Proposition. *Let I be a non-empty subset of $\mathbb{N}$.*

(1) *If I is bounded from above, then there exists a unique pair (N, f), where N is a natural number and $f : \{0, \ldots, N\} \to I$ is an increasing bijection.*

(2) *If I is not bounded from above, then there exists a unique increasing bijection from $\mathbb{N}$ to I.*

Proof. We construct in a recursive way a family of distinct elements of I as follows. Let x_0 be the least element of I. If $x_0, \ldots, x_n$ has been constructed and if $I \setminus \{x_0, \ldots, x_n\}$ is not empty, we choose x_{n+1} to be the least element of $I \setminus \{x_0, \ldots, x_n\}$.

By definition one has $x_n \neq x_{n+1}$. Moreover, since x_{n+1} belongs to $I \backslash \{x_0, \ldots, x_{n-1}\}$ (in the case where $n = 0$, by convention $\{x_0, \ldots, x_{n-1}\}$ denotes the empty set), one has $x_n \leq x_{n+1}$. Hence $x_n < x_{n+1}$. Therefore, by Lemma 4.7.2, we obtain that $n \leq x_n$ for any n. In particular, if I is bounded from above, then the recursive procedure terminates at a certain step, namely there exists $N \in \mathbb{N}$ such that $I = \{x_0, \ldots, x_N\}$. The mapping from $\{0, \ldots, N\}$ to I sending n to x_n is an increasing bijection. Suppose that M is another natural number and $g : \{0, \ldots, M\} \to I$ is an increasing bijection. Note that

$$f^{-1} \circ g : \{0, \ldots, M\} \longrightarrow \{0, \ldots, N\} \text{ and } g^{-1} \circ f : \{0, \ldots, N\} \longrightarrow \{0, \ldots, M\}$$

are both strictly increasing maps. By (2) of Proposition 4.7.6, we obtain that $M = N$ and $f = g$.

If I is not bounded from above, then $I \setminus \{x_0, \ldots, x_n\}$ is never bounded from above and the recursive procedure does not terminate. We then obtain a family $(x_n)_{n \in \mathbb{N}}$ of elements of I parametrised by $\mathbb{N}$, which corresponds to a strictly increasing mapping $f : \mathbb{N} \to I$ sending $n \in \mathbb{N}$ to x_n. If f is not surjective, the set $I \setminus f(\mathbb{N})$ admits a least element N. Then there exists $n \in \mathbb{N}$ such that $f(n) < N < f(n+1)$, this contradicts the way of construction of $f(n + 1)$.

Suppose that $g : \mathbb{N} \to I$ is another increasing bijection. By Propositions 3.8.3 and 4.2.3, $g^{-1} \circ f$ is an increasing bijection from $\mathbb{N}$ to $\mathbb{N}$. By Proposition 4.7.6, one has $g^{-1} \circ f = \mathrm{Id}_{\mathbb{N}}$ and hence $g = f$. □

4.7.8 Corollary. *A set X is finite if and only if there exist a natural number N and a family $(x_n)_{n \in \{0, \ldots, N\}}$ of elements of X such that $X = \{x_0, \ldots, x_N\}$. In particular, a subset of $\mathbb{N}$ is finite if and only if it is bounded from above.*

Proof. Assume that $X = \{x_0, \ldots, x_N\}$ where $N \in \mathbb{N}$. Then the mapping from $\{0, \ldots, N\}$ to X sending $n \in \{0, \ldots, N\}$ to x_n is surjective. Since $\{0, \ldots, N\}$ is finite, by (2) of Proposition 4.7.3, the set X is finite.

Conversely, assume that $f : X \to \mathbb{N}$ is an injective mapping such that $f(X)$ is bounded. By (1) of Proposition 4.7.7, there exists $N \in \mathbb{N}$ and a bijection

$$g : \{0, \ldots, N\} \to f(X).$$

Thus $f^{-1} \circ g : \{0, \ldots, N\} \to X$ is a bijection and hence

$$X = \big\{f^{-1}(g(0)), \ldots, f^{-1}(g(N))\big\}.$$

It remains to prove that a finite subset I of $\mathbb{N}$ is bounded from above (by definition a subset of $\mathbb{N}$ which is bounded from above is always finite). By the first statement, there exists a natural number N and a family $(x_n)_{n \in \{0, \ldots, N\}}$ of elements of I such that $I = \{x_0, \ldots, x_N\}$. By Proposition 4.6.7, I admits a greatest element, and hence is bounded from above. □

4.7.9 Proposition. *Let X be a set. The following statements are equivalent.*

(1) *X is infinite.*

(2) *There exists an injective mapping from $\mathbb{N}$ to X.*

(3) *There exists an injective mapping from X to X the image of which is a proper subset of X.*

Proof. "(1) $\Longrightarrow$ (2)": We construct in a recursive way a family of distinct elements $(x_n)_{n\in\mathbb{N}}$ as follows. Since X is infinite, it is not empty. We pick an arbitrary element x_0 of X. Suppose that $x_0, \ldots, x_n$ are chosen. By Corollary 4.7.8, $\{x_0, \ldots, x_n\}$ is finite. Therefore, by (2) of Proposition 4.7.4, the set $X \setminus \{x_0, \ldots, x_n\}$ is infinite, and hence is non-empty. We pick an arbitrary element x_{n+1} in $X \setminus \{x_0, \ldots, x_n\}$. Thus we obtain an injective mapping from $\mathbb{N}$ to X, sending $n \in \mathbb{N}$ to x_n.

"(2) $\Longrightarrow$ (3)": Let $f : \mathbb{N} \to X$ be an injective mapping. We define an injective mapping $g : X \to X$ as follows:

$$g(x) = \begin{cases} f(n+1), & \text{if } x = f(n), \\ x, & \text{if } x \notin f(\mathbb{N}). \end{cases}$$

Note that $g(X)$ is a proper subset of X since it does not contain $f(0)$.

"(3) $\Longrightarrow$ (2)": Let $g : X \to X$ be an injective mapping and x_0 be an element of $X \setminus g(X)$. For any $n \in \mathbb{N}$, let $x_n = g^n(x)$. Since g is injective, one has $x_n \in g^n(X) \setminus g^{n+1}(X)$. Hence the elements $(x_n)_{n\in\mathbb{N}}$ are distinct. Therefore one obtains an injective mapping from $\mathbb{N}$ to X.

"(2) $\Longrightarrow$ (1)" follows from Corollary 4.7.8 (which shows that $\mathbb{N}$ is infinite) and Proposition 4.7.3. □

4.7.10 Definition. Let X and Y be sets. If there exists a bijection from X to Y, we say that X and Y are *equipotent*.

4.7.11 Proposition. *Let X be an infinite set and Y a countable set. Then $X \cup Y$ is equipotent to X.*

Proof. Note that the equality $X \cup Y = X \cup (Y \setminus X)$ holds. Since $Y \setminus X$ is a countable set, we may assume without loss of generality that X and Y are disjoint. By Proposition 4.7.9, X has a subset A equipotent to $\mathbb{N}$. By Proposition 4.7.4, $A \cup Y$ is an infinite countable set, so there exists a bijection $\varphi : A \to A \cup Y$. Consider the map $\Phi : X \to X \cup Y$ defined by sending $x \in X \setminus A$ to x, and $a \in A$ to $\varphi(a)$. Since Φ is a bijection, the sets X and $X \cup Y$ are equipotent. □

4.7.12 Lemma. *The set $\mathbb{N} \times \mathbb{N}$ is equipotent to $\mathbb{N}$.*

Proof. Consider the map from $\mathbb{N}\times\mathbb{N}$ to $\mathbb{N}$ that sends (a,b) to $2^a(2b+1)-1$. First, we show this map is injective. Suppose (a,b) and (x,y) are two elements of $\mathbb{N}\times\mathbb{N}$ such that

$$2^a(2b+1)-1 = 2^x(2y+1)-1.$$

Assume without loss of generality that $a \leq x$. Then

$$2b+1 = 2^{x-a}(2y+1).$$

Hence $x = a$, otherwise $2b+1$ would be odd while $2^{x-a}(2y+1)$ would be even, a contradiction. This gives $2b+1 = 2y+1$ and thus $b = y$.

Let n be a natural number. Then $n+1$ is a positive integer, so it can be written as a power of 2 multiplied by an odd number. Therefore, the map is surjective. □

4.7.13 Proposition. *For any positive integer k, the set $\mathbb{N}^k$ is equipotent to $\mathbb{N}$.*

Proof. The case where $k = 1$ is trivial. Assume that $\mathbb{N}^k$ is equipotent to $\mathbb{N}$ and let $f : \mathbb{N}^k \to \mathbb{N}$ be a bijection. Then the mapping

$$\mathbb{N}^{k+1} \longrightarrow \mathbb{N}\times\mathbb{N}, \quad (x_1,\ldots,x_{k+1}) \longmapsto (f(x_1,\ldots,x_k),x_{k+1})$$

is also a bijection. Its inverse is given by $(a,b) \longmapsto (f^{-1}(a),b)$. Therefore, $\mathbb{N}^{k+1}$ is equipotent to $\mathbb{N}\times\mathbb{N}$, and hence is equipotent to $\mathbb{N}$, by Lemma 4.7.12. □

4.7.14 Proposition. *Let X be a set. There does not exist any surjective mapping from X to $\mathscr{P}(X)$. In particular, X and $\mathscr{P}(X)$ are not equipotent.*

Proof. We reason by contradiction that there exists a surjective mapping $f : X \to \mathscr{P}(X)$. Let

$$A = \{x \in X \mid x \notin f(x)\}.$$

Since f is surjective, there exists $y \in X$ such that $f(y) = A$. If $y \in A$, then by the definition of A one has $y \notin f(y) = A$, which leads to a contradiction; if $y \notin A$, then by the definition of A one has $y \in f(y) = A$, which is also contradictory. □

4.8 Zorn's lemma

4.8.1 Lemma. *Let $(X,\leq)$ be a partially ordered set, $\mathscr{S}$ be a subset of $\mathscr{P}(X)$ which satisfies the following conditions:*

(a) *For any $A \in \mathscr{S}$, $(A,\leq)$ is well ordered.*

(b) *For any $(A,B) \in \mathscr{S}\times\mathscr{S}$, either A is an initial segment of B, or B is an initial segment of A.*

Let Y be the union of sets in $\mathscr{S}$. Then the following assertion holds:

(1) *Any $A \in \mathscr{S}$ is an initial segment of Y.*

(2) *$(Y, \leq)$ is well ordered.*

Proof. (1) Let x be an element of A and y be an element of Y such that $y < x$. Let B be an element of $\mathscr{S}$ such that $y \in B$. Assume by contradiction that y does not belong to A. Then $B \not\subseteq A$ and hence B is not an initial segment of A. By the condition (b), A is an initial segment of B. Hence $y \in A$, which leads to a contradiction.

(2) Let Z be a non-empty subset of Y. There then exists $A \in \mathscr{S}$ such that $A \cap Z \neq \varnothing$. Let m be the least element of $A \cap Z$. We show that m is also the least element of Z. Let z be an element of Z and B be an element of $\mathscr{S}$ such that $z \in B$. If z belongs to A, then by definition $m \leq z$. Otherwise A is an initial segment of B. Since B is well-ordered, by Proposition 4.6.3 we obtain that B is totally ordered. If $m \not\leq z$, then $z < m$, which implies that $z \in A$. This leads to a contradiction. □

4.8.2 Definition. Let $(X, \leq)$ be a partially ordered set and A be a subset of X. We say that an element M of A is a *maximal element* of A if there does not exist any element $x \in A$ such that $M < x$. We say that an element m of A is a *minimal element* of A if there does not exist any element $x \in A$ such that $x < m$.

4.8.3 Remark. Let $(X, \leq)$ be a partially ordered set and A be a subset of X. If A has a greatest element (resp. least element), then its greatest element (resp. least element) is the unique maximal element (resp. minimal element) of A.

4.8.4 Theorem (Zorn's lemma)**.** *Let $(X, \leq)$ be a non-empty partially ordered set. If any well-ordered subset of X has an upper bound in X, then X admits a maximal element.*

Proof. Suppose by contradiction that X does not have any maximal element.

Let $\mathscr{W}$ be the set of all well-ordered subsets of X. By the axiom of choice, there exists a mapping $g : \mathscr{W} \to X$ which sends any $A \in \mathscr{W}$ to an upper bound of A in X which does not belong to A (in the case where A has a greatest element, we could take an element of X strictly greater than $\max A$ by the assumption that X does not have any maximal element). If A is an element of $\mathscr{W}$ such that

$$\forall\, a \in A, \quad a = g(A_{<a}), \tag{4.2}$$

we say that A is a g-set. Let $\mathscr{S}$ be the subset of $\mathscr{W}$ that is composed of all g-sets. It is a non-empty subset of $\mathscr{W}$ since $\varnothing \in \mathscr{S}$. Moreover, by definition, if $A \in \mathscr{S}$, then $A \cup \{g(A)\} \in \mathscr{S}$.

Let A and B be two g-sets. We claim that, either A is an initial segment of B, or B is an initial segment of A. Let I be the union of subsets of $A \cap B$ which are common initial segments of A and B. By Proposition 4.6.14, I is also a common initial segment of A and B, and hence is the greatest (with respect to the relation of inclusion) common initial segment. If $I \subset A$ and $I \subset B$, by Proposition 4.6.13 there exist $a \in A$ and $b \in B$ such that

$$A_{<a} = I = B_{<b}.$$

Since A and B are both g-sets, by (4.2) we obtain

$$a = g(I) = b.$$

Therefore $I \cup \{a\}$ is a common initial segment of A and B which contains strictly I. This contradicts the maximality of I. Therefore, either $I = A$ and A is an initial segment of B, or $I = B$ and B is an initial segment of A.

By Lemma 4.8.1, the union $Y = \bigcup_{A \in \mathscr{S}} A$ is well ordered, and any $A \in \mathscr{S}$ is an initial segment of Y. For any $a \in Y$, there exists $A \in \mathscr{S}$ such that $a \in A$. Since A is an initial segment of Y, one has $Y_{<a} = A_{<a}$ and hence $g(Y_{<a}) = g(A_{<a}) = a$. Therefore Y belongs to $\mathscr{S}$ and hence it is the greatest element of $\mathscr{S}$ with respect to $\subseteq$. However this is not possible since $Y \cup \{g(Y)\}$ is also an element of $\mathscr{S}$. This leads to a contradiction. □

4.8.5 Corollary. *Let $(X, \leq)$ be a non-empty partially ordered set. If any totally ordered subset of X has an upper bound in X, then X has a maximal element.*

Proof. This follows immediately from Theorem 4.8.4 and the fact that all well-ordered sets are totally ordered (see Proposition 4.6.3). □

4.8.6 Theorem (Well-ordering principle)**.** *Let X be a set. There exists a partial order $\leq$ on X such that $(X, \leq)$ is well-ordered.*

Proof. Let $\mathscr{S}$ be the set of all pairs $(A, \leq_A)$, where A is a subset of X and $\leq_A$ is a partial order on A such that $(A, \leq_A)$ is well-ordered. We consider the following binary relation $\preceq$ as follows: $(A, \leq_A) \preceq (B, \leq_B)$ if and only if $A \subseteq B$, $\leq_B$ extends $\leq_A$ and A is an initial segment of B. This is a partial order on $\mathscr{S}$. If $\mathscr{S}_0$ is a totally ordered subset of $\mathscr{S}$, by Lemma 4.8.1, the set $\mathscr{S}_0$ has an upper bound in $(\mathscr{S}, \preceq)$. Therefore, by Zorn's lemma the partially ordered set $(\mathscr{S}, \preceq)$ has a maximal element $(Y, \leq_Y)$. If $X \setminus Y$ is not empty and z is an element of $X \setminus Y$, we take $Z = Y \cup \{z\}$ and extends $\leq_Y$ to a partial order $\leq_Z$ on Z such that $y <_Z z$ for any $y \in Y$.

We claim that $(Z, \leq_Z)$ is well ordered. Let A be a non-empty subset of Z. If $A \cap Y \neq \varnothing$, then the least element of $A \cap Y = A \setminus \{z\}$ is also a least element of A.

If $A \cap Y = \varnothing$, then $A = \{z\}$ and z is the least element of A. Hence any non-empty subset of Z has a least element, namely $(Z, \leq_Z)$ is well ordered.

Note that Y is an initial segment of Z, which contradicts the maximality of Y. Therefore, one has $X = Y$ and $(X, \leq_Y)$ is well-ordered. □

Exercises

1. Compare $7/13$ and $6/11$.

2. Let a and b be real numbers. Compare $a^2 + b^2$ and ab.

3. Compare $a = 1\,000\,000\,002^2$ and

$$b = 999\,999\,996 \times 1\,000\,000\,008.$$

4. Compare

$$\frac{2+\sqrt{3}}{2-\sqrt{3}} \text{ and } 7 + 4\sqrt{3}$$

5. Resolve in $\mathbb{R}$ the following inequalities

$$|x+3| \leq 5, \quad |2x-4| \leq |x+2|, \quad |x+1| + |x-3| \leq 6.$$

6. Resolve in $\mathbb{R}$ the inequality $x - 1 \leqslant \sqrt{x+2}$.

7. Does each of the following subsets of $\mathbb{R}$ have the least element? If it is the case, determine it.

(a) The set of even natural numbers.

(b) $\{-1, 0, 1\}$.

(c) The image of the function $\exp : \mathbb{R} \to \mathbb{R}$.

8. Determine if each of the following set has an upper bound in $\mathbb{R}$, a lower bound in $\mathbb{R}$? Determine their supremum and infimum.

$$A = \{x \in \mathbb{R} \,|\, x^2 < 2\}, \quad B = \{\tfrac{1}{n} \,|\, n \in \mathbb{N},\ n \geqslant 1\}.$$

9. Determine the infimum of

$$\left\{ \frac{a}{b} + \frac{b}{a} \,\middle|\, (a,b) \in \mathbb{R}^2_{>0} \right\}$$

10. Let n be a positive integer. Determine

$$\inf\left\{(x_1+\cdots+x_n)(x_1^{-1}+\cdots+x_n^{-1}) \,\middle|\, (x_1,\ldots,x_n)\in\mathbb{R}_{>0}^n\right\}.$$

11. Let X be a set.

(1) Prove that the relation of inclusion $\subseteq$ is an order relation on $\mathscr{P}(X)$.

(2) Let I be a set and $(A_i)_{i\in I}$ be a family of elements of $\mathscr{P}(X)$. Prove that $\sup_{i\in I} A_i$ and $\inf_{i\in I} A_i$ exist.

12. In this exercise, we fix a partially ordered set $(X,\leq)$. We assume that X is *well-ordered*, namely, any non-empty subset of X has a least element. If a subset I of X satisfies

$$\forall\, a\in I,\quad X_{<a}:=\{x\in X\,|\,x<a\}\subseteq I,$$

then we say that I is an *initial segment* of X.

(1) Let a be an element of X. Prove that

$$X_{<a}=\{x\in X\,|\,x<a\}$$

is an initial segment of X.

(2) Let I be an initial segment of X. Assume that $I\neq X$. Prove that there exists a unique element $a\in X$ such that $I=X_{<a}$.

(3) Let Θ be a set and $(I_\lambda)_{\lambda\in\Theta}$ be a family of initial segments of X parametrised by Θ. Prove that $I=\bigcup_{\lambda\in\Theta} I_\lambda$ is an initial segment of X.

(4) Let $(\mathbb{P}(x))_{x\in X}$ be a family of mathematical statements. Let 0 be the least element of X. Assume that

(a) the statement $\mathbb{P}(0)$ is true.

(b) for any $a\in X$, if $\mathbb{P}(b)$ is true for any $b\in X_{<a}$, then $\mathbb{P}(a)$ is true.

Prove that, for any $x\in X$, $\mathbb{P}(x)$ is true.

13. Prove that, for any $n\in\mathbb{N}$, one has

$$\sum_{k=1}^{n} k^2=\frac{n(n+1)(2n+1)}{6}.$$

14. Prove that, for any positive integer n, one has

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}.$$

15. Let $(u_n)_{n\in\mathbb{N}}$ be the sequence in $\mathbb{R}$ defined as

$$u_0 = 1, \quad u_{n+1} = \sqrt{2 + u_n} \text{ for } n \in \mathbb{N}.$$

Prove that, for any $n \in \mathbb{N}$, $0 < u_n < 2$.

16. Let $(u_n)_{n\in\mathbb{N}}$ be the sequence in $\mathbb{R}$ defined as

$$u_0 = 1, \quad u_{n+1} = \sqrt{1 + u_n} \text{ for } n \in \mathbb{N}.$$

Prove that the sequence $(u_n)_{n\in\mathbb{N}}$ is increasing.

17. Prove that, for any positive integer n,

$$2^{n-1} \leq n! \leq n^n.$$

18. Let x be a real number such that $x \geqslant -1$. Prove that, for any positive integer n, one has $(1 + x)^n \geq 1 + nx$.

19. Let $(u_n)_{n\in\mathbb{N}}$ be the sequence in $\mathbb{R}$ defined as

$$u_0 = 2,\ u_1 = 3, \quad u_{n+2} = 3u_{n+1} - 2u_n \text{ for } n \in \mathbb{N}.$$

Prove that, for any $n \in \mathbb{N}$, $u = 2^n + 1$.

20. Consider the Fibonacci sequence $(u_n)_{n\in\mathbb{N}}$ defined as

$$u_0 = u_1 = 1, \quad u_{n+2} = u_n + u_{n+1} \text{ for } n \in \mathbb{N}.$$

(1) Prove that, for any $n \in \mathbb{N}$,

$$u_n u_{n+2} - u_{n+1}^2 = (-1)^n.$$

(2) Prove that the mapping

$$(n \in \mathbb{N}) \longrightarrow \frac{u_{2n+1}}{u_{2n}}$$

is increasing.

(3) Prove that the mapping

$$(n \in \mathbb{N}) \longrightarrow \frac{u_{2n+2}}{u_{2n+1}}$$

is decreasing.

(4) Let

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}.$$

Prove that, for any $n \in \mathbb{N}$,

$$\alpha^{n+2} = \alpha^{n+1} + \alpha^n, \quad \beta^{n+2} = \beta^{n+1} + \beta^n.$$

(5) Find real numbers λ and μ such that

$$\lambda + \mu = 1, \quad \lambda\alpha + \mu\beta = 1.$$

21. Recall that $\sqrt{2}$ is irrational. Deduce that $\cos(1^\circ)$ is irrational. We could assume by contradiction that $\cos(1^\circ)$ is rational and prove by induction that $\cos(n^\circ)$ is rational for any $n \in \mathbb{N}$.

22. We denote by $\mathbb{N}$ the set of all natural numbers. We define a binary relation $|$ on $\mathbb{N}$ as follows: for any $(d, n) \in \mathbb{N} \times \mathbb{N}$, $d \mid n$ if and only if there exists $m \in \mathbb{N}$ such that $n = dm$. For any $d \in \mathbb{Z}$, we denote by $d\mathbb{Z}$ the set

$$\{dn \,|\, n \in \mathbb{Z}\}.$$

In this exercise, we could use without justification the following Euclidean division principle: if $d \in \mathbb{N} \setminus \{0\}$ and $n \in \mathbb{Z}$, there exists a unique element $(m, r) \in \mathbb{Z} \times \{0, \ldots, d-1\}$ such that $n = dm + r$.

(1) Prove that $|$ is a partial order on $\mathbb{N}$.

(2) Let d and n be natural numbers such that $d \mid n$. Prove that, if $n \neq 0$, then $d \leq n$.

(3) Prove that the partially ordered set $(\mathbb{N}, |\,)$ has a least element. Determine this element.

(4) Prove that the partially ordered set $(\mathbb{N}, |\,)$ has a greatest element. Determine this element.

(5) Let A be an infinite subset of $\mathbb{N}$. Prove that A has a supremum. Determine $\sup_{(\mathbb{N}, |\,)} A$.

(6) Let A be a non-empty and finite subset of $\mathbb{N} \setminus \{0\}$. Let

$$M(A) := \{n \in \mathbb{N} \setminus \{0\} \,|\, \forall\, d \in A,\ d \mid n\}$$

(a) Prove that $M(A)$ is not empty.

(b) Let n_0 be the least element of $M(A)$ with respect to the usual partial order $\leq$. Prove that, for any $n \in M(A)$, one has $n_0 \mid n$.

(c) Deduce that A has a supremum in $(\mathbb{N}, |)$.

(7) Let A be a non-empty subset of $\mathbb{N} \setminus \{0\}$. We denote by $A\mathbb{Z}$ the set

$$\{a_1 n_1 + \ldots + a_k n_k \,|\, k \in \mathbb{N} \setminus \{0\},\ (a_1, \ldots, a_k) \in A^k,\ (n_1, \ldots, n_k) \in \mathbb{Z}^k\}.$$

(a) Let x and y be elements of $A\mathbb{Z}$. Prove that $x + y \in A\mathbb{Z}$.

(b) Let $x \in A\mathbb{Z}$ and $y \in \mathbb{Z}$. Prove that $xy \in A\mathbb{Z}$.

(c) Prove that $A \subseteq A\mathbb{Z}$ and deduce that $(A\mathbb{Z}) \cap (\mathbb{N} \setminus \{0\})$ is not empty.

(d) Let d be the least element of $(A\mathbb{Z}) \cap (\mathbb{N} \setminus \{0\})$ with respect to the usual partial order $\leq$. Prove that $A\mathbb{Z} = d\mathbb{Z}$.

(e) Deduce that d is the infimum of A in $(\mathbb{N}, |)$.

(8) Let A be a subset of $\mathbb{N}$. Prove that A has a supremum and an infimum in $(\mathbb{N}, |)$. We denote by

$$\gcd(A) := \inf_{(\mathbb{N},|)} A, \quad \operatorname{lcm}(A) := \sup_{(\mathbb{N},|)} A.$$

(9) Let a and b be positive integers, and $d = \gcd(\{a, b\})$. Prove that, there exists $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$d = an + bm.$$

(10) Let a and b be positive integers. Prove that

$$\gcd(\{a, b\}) \operatorname{lcm}(\{a, b\}) = ab.$$

23. If x and y are two sets, we denote by $x \subseteqq y$ the statement: "either $x = y$, or $x \in y$". We say that a set α is an ordinal if the elements of α are all subsets of α, and $(\alpha, \subseteqq)$ forms a well-ordered set.

(1) Let x and y be sets. Prove that $x \subseteqq y$ if and only if $x \in y \cup \{y\}$.

(2) Prove that $\varnothing$ is an ordinal.

(3) Let α be a set. Assume that its elements are all sets and

$$(\alpha \cup \{\alpha\}, \subseteqq)$$

forms a well ordered set, then α is an ordinal.

(4) Let α be an ordinal. Prove that $\alpha \cup \{\alpha\}$ is an ordinal and

$$\alpha = \bigcup_{x \in \alpha \cup \{\alpha\}} x.$$

In the following questions, if α is an ordinal, we denote by $\alpha + 1$ the ordinal $\alpha \cup \{\alpha\}$.

(5) Let α and β be ordinals. Prove that, if $\alpha + 1 = \beta + 1$, then $\alpha = \beta$.

(6) Let α be an ordinal, and x and y be two elements of $\alpha + 1$. Prove that one and only one of the following three conditions holds:

$$x \in y, \quad x = y, \quad y \in x.$$

(7) Let α be an ordinal. Prove that all elements of α are ordinals.

(8) Let α and β be ordinals. Prove that if $\beta \subseteq \alpha$, then β is an initial segment of α.

(9) Let α be an ordinal. Prove that $\alpha+1$ identifies with the set of all initial segments of α. Deduce that all initial segments of α are ordinals.

(10) Let α and β be ordinals. Prove that the following conditions are equivalent:

(a) $\beta \in \alpha$,

(b) β is an initial segment of α and $\beta \neq \alpha$

(c) $\beta \subsetneq \alpha$.

(11) Let I be a non-empty set and $(\alpha_i)_{i\in I}$ be a family of ordinals. Prove that

$$\bigcap_{i\in I} \alpha_i$$

is an ordinal.

(12) Let α and β be ordinals. Prove that, either $\alpha \subseteq \beta$, or $\beta \subsetneq \alpha$.

(13) Let A be a family of ordinals. Prove that $(A, \subseteq)$ is a well-ordered set and that the binary relations $\subseteq$ and $\leqq$ coincide on A.

(14) Let I be a set and $(\alpha_i)_{i\in I}$ be a family of ordinals. Prove that $\bigcup_{i\in I} \alpha_i$ is an ordinal.

24. Let α be an ordinal. The ordinal $\alpha + 1$ is called the *successor* of α. If an ordinal β is neither $\varnothing$ nor *successor* of any ordinal, we say that β is a limit ordinal. Let n be an ordinal, if none of the elements of $n+1$ is a limit ordinal, we say that n is a natural number.

(1) Let α be an ordinal. Prove that it is a successor of an ordinal if and only if

$$\bigcup_{x\in\alpha} x \subsetneq \alpha.$$

(2) Let α be an ordinal. Prove that the following conditions are equivalent:

(a) α is a limit ordinal.
(b) $\bigcup_{x\in\alpha} x = \alpha$.
(c) $\alpha \subseteq \bigcup_{x\in\alpha} x$.

(3) We denote by 0 the ordinal number $\varnothing$. Prove that 0 is a natural number.

(4) Prove that, if n is a natural number, then so is $n + 1$.

(5) Let α be an ordinal number. Prove that α is a natural number if and only if any non-empty subset of α has a greatest element.

(6) Prove that, if n is a natural number, then all of its elements are natural numbers.

(7) Suppose that that exists a set A consisting of some sets such that $\varnothing \in A$ and that

$$\forall\, x \in A, \quad x \cup \{x\} \in A.$$

Prove that the set $\mathbb{N}$ of all natural numbers forms an ordinal. Moreover, prove that, if an ordinal α is not a natural number, then $\mathbb{N} \subseteq \alpha$.

(8) Let $(\mathbb{P}(n))_{n\in\mathbb{N}}$ be a family of statements parametrized by natural numbers. We assume that $\mathbb{P}(0)$ holds and that $\mathbb{P}(n)$ implies $\mathbb{P}(n + 1)$ for any $n \in \mathbb{N}$. Prove that, for any $n \in \mathbb{N}$, $\mathbb{P}(n)$ holds.

(9) Let $f : \mathbb{N} \to \mathbb{N}$ is an increasing bijection. Prove that f is the identity mapping of $\mathbb{N}$.