جامعة سطيف 1 - فرحات عباس

Setif 1 University - Ferhat ABBAS

وزارة التعليم العالي والبحث العلمي

Sétif 1 University-Ferhat ABBAS
Faculty of Sciences
Department of Mathematics

FACULTY OF SCIENCES

Title

جامعة فرحات عباس سطيف 1
قسم الرياضيات
كلية العلوم

Mathematical logic:
Course and corrected exercises

Intended mainly for students in the 2nd year of the
"Licence in Mathematics"
and the 1st year of the
"State Engineer in Computer Science"

Presented by:

Dr. Ali KHALOUTA

Teacher at: Setif 1 University-Ferhat ABBAS

Academic Year: 2025/2026

بسم الله الرحمن الرحيم

Table of contents

Introduction

This course document is a work mainly intended for students of the 2^{nd} year of the "Licence in Mathematics" as well as the 1^{st} year of the "State Engineer in Computer Science" includes the Mathematical Logic module, it contains the essentials of the course with examples according to the program proposed by the Ministry of Higher Education and Scientific Research.

The particularity of this work is that it was designed to allow a student to acquire, understand, and dominate by himself all the concepts covered.

In this work, we will find three chapters of course, written in an easy-to-read style very detailed:

Chapter 1 is devoted to propositional calculus and predicate calculus, and in particular covers the rules of inference, the basic elements of mathematical reasoning.

Chapter 2 is devoted to set theory, after a reminder of naive set theory we approach Russell's paradox. This paradox allows a natural transition to Zermelo-Fraenkel's theory denoted ZF theory. If the handout addresses ZF theory it is nevertheless possible to move on to the following sections without prejudice.

Two important concepts in set theory are addressed at the end of the chapter, the continuum hypothesis and the axiom of choice.

Chapter 3 is devoted to well-ordered sets and the proof by the principle of good order. We approach the simplest version of the proof by the principle of good order which is the proof by recurrence. We generalize this principle at the beginning to sets where the relation of good order is easy to find.

The proof by the principle of good order is often used in theoretical computer science to demonstrate the finiteness of certain algorithms for example.

The last section concerns the proof of Zermelo's theorem on the existence of a good order relation for any set.

Exercises with solutions are provided at the end of each chapter to allow students to test their knowledge and prepare for tests and final exams.

Finally, I hope that this work can help students who want to master the various concepts that have been well developed.

Chapter 1

Basic notions of mathematical logic

In propositional logic, we study the relations between statements, which we call propositions or formulas. These relations can be expressed through logical connectives that, through composition, allow the construction of syntactically correct formulas. These include conjunction, disjunction, implication, equivalence, and negation. This chapter aims to introduce propositional calculus, predicate calculus, and the rules of deduction that form the basis of mathematical proofs.

1.1 Propositional calculus

1.1.1 Proposition (Assertion)

A proposition is a mathematical statement to which one assigns one of two logical values: true (1) or false (0).

Example 1.1.1 - *Proposition « $1 - 1 = 0$ » is true.*

- *Proposition « $3 + 2 = 1$ » is false.*

Propositions are generally denoted by the letters $P, Q, R, ...$

1.2 Logical connectors

There are five (5) logical connectors, the basis of all mathematical reasoning. Let P and Q be two propositions.

1.2.1 Negation « no » or « $\neg$ »

We call the negation of P, the proposition (no P) (not P) and we denote it : $\neg P$ or $\overline{P}$.

Truth table of negation

Consider proposition P (see Table 1.1). The negation of a proposition P (true) is a false proposition. If P (false) then $\neg P$ is true.

P	$\neg P$
1	0
0	1

Table 1.1: Truth table of negation

Negation of the negation

In general, a double negation often reinforces the negation such as : do you want to go out? no no.

In mathematics, a double negation is considered a proposition.

Example 1.2.1 *1- If P is proposition $x = 0$, $\neg P$ is proposition $x \neq 0$.*

2- The 03 is not even so 03 is odd.

Remark 1.2.1 *The meaning of the symbol $\Leftrightarrow$, which reads equivalent, and which means here that the two propositions always have the same value.*

1.2.2 Conjunction « and » or « $\wedge$ »

We call conjunction of P and Q, the proposition (P and Q) which is denoted $P \wedge Q$.

Example 1.2.2 *P : « The earth is round » (true) and Q : « The sky is blue » (true).*

*P and Q or $P \wedge Q$ therefore reads «The earth is round **AND** the sky is blue». $P \wedge Q$ is true. We will say that the proposition $P \wedge Q$ is false when at least one of the two propositions is false. So « The earth is round **AND** the sky is green » is a false proposition.*

Commutativity

$(P \wedge Q) \Leftrightarrow (Q \wedge P)$.

Truth table of conjunction

The result of the conjunction is proved by the truth table 1.2.

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

Table 1.2: Truth table of conjunction

1.2.3 Disjunction « or » or « $\vee$ »

We call disjunction of P and Q, the proposition (P or Q) which is denoted $P \vee Q$.

Remark 1.2.2 *In mathematics, the «or» is non-exclusive, i.e, it includes the possibility that both propositions are true. Thus the proposition « $xy = 0$ » is equivalent to the proposition « $x = 0$ or $y = 0$ », it is true when one of the two numbers is zero, it is also true when both are zero.*

Commutativity

$(P \vee Q) \Leftrightarrow (Q \vee P)$.

Truth table of disjunction

The result of the disjunction is proved by the truth table 1.3.

P	Q	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

Table 1.3: Truth table of disjunction

Remark 1.2.3 *Conjunction and disjunction are associative connectors. that is, we can write $P \wedge (Q \wedge R)$ or $(P \wedge Q) \wedge R$ or simply $P \wedge Q \wedge R$. Similarly $P \vee (Q \vee R)$ or $(P \vee Q) \vee R$ or simply $P \vee Q \vee R$.*

1.2.4 Exclusive disjunction (xor)

Let P and Q be two propositions, the compound proposition $(P \vee Q) \vee \neg(P \wedge Q)$ is written as $P \oplus Q$. The binary connector $\oplus$ is called exclusive disjunction, the proposition $P \oplus Q$ is true if one and only one of the propositions is true and the truth table is given by

P	Q	$P \oplus Q$
1	1	0
1	0	1
0	1	1
0	0	0

Table 1.4: Truth table of exclusive disjunction

Remark 1.2.4 *xor is an abbreviation for exclusive or.*

1.2.5 Implication « $\Longrightarrow$ »

The proposition denoted by « $P \Longrightarrow Q$ » corresponds to the proposition $\neg P \vee Q$. P is then called the hypothesis and Q the conclusion. $P \Longrightarrow Q$ is a proposition which is called implication and which we can read in different ways :

- If P then Q.
- For P we need Q.
- For Q it suffices P.
- P is a sufficient condition for Q
- Q is a necessary condition of P.

Truth table of implication

The result of the implication is proved by the truth table 1.4.

P	Q	$\neg P$	$P \Longrightarrow Q$	$\neg P \vee Q$
1	1	0	1	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

Table 1.5: Truth table of implication

The proposition is true whenever P is false (regardless of the truth of Q). If P is true and $P \Longrightarrow Q$ true then Q is true. Moreover the implication $Q \Longrightarrow P$ is called the reciprocal of the implication $P \Longrightarrow Q$.

Example 1.2.3 *- $P : 2 = 2$ and $Q : 4 = 4$ are two true assertions, so $P \Longrightarrow Q$ or $\neg P \vee Q$ is true,*

- If $x \in \{1, 3, 5, 6\}$ then $x \leq 6$ is a true assertion.

1.2.6 Equivalence « $\Longleftrightarrow$ »

We say that two propositions are logically equivalent if they have the same truth value and denoted by $P \Longleftrightarrow Q$. In other words $P \Longleftrightarrow Q$ is true if P and Q are both true or both are false. The proposition $P \Longleftrightarrow Q$ corresponds to the proposition $(P \Longrightarrow Q)$ and $(Q \Longrightarrow P)$. it can be expressed as follows:

- P is equivalent to Q.
- For P, it is necessary and sufficient Q.
- P is a necessary and sufficient condition for Q.
- P if and only if Q.

Truth table of equivalence

The result of the equivalence is proved by the truth table 1.5.

P	Q	$P \Longleftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Table 1.6: Truth table of equivalence

Example 1.2.4 *Take $(P \wedge Q)$ and $(\neg(\neg P \vee \neg Q))$. See the result in Table 1.6.*

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

Table 1.7: Example of equivalence

1.2.7 Distributivity and Morgan's Laws

Distribution of conjunction over disjunction

The propositions $P \wedge (Q \vee R)$ and $(P \wedge Q) \vee (P \wedge R)$ are equivalent (have the same truth table).

Distribution of disjunction over conjunction

The propositions $P \vee (Q \wedge R)$ and $(P \vee Q) \wedge (P \vee R)$ are equivalent (have the same truth table).4

Morgan's Laws

- The negation of the proposition $(P \wedge Q)$ is the proposition $\neg P \vee \neg Q$.

- The negation of the proposition $(P \vee Q)$ is the proposition $\neg P \wedge \neg Q$.

1.3 Tautology and antilogy

Assertions (dependent on P and Q) that are true regardless of the truth value of P and Q are said to be tautology. A tautology is actually a theorem of logic. Assertions (dependent on P and Q) that are false regardless of the truth value of P and Q are said to be antilogy.

Example 1.3.1 *Let P be a proposition, the formula $P \vee \neg P$ is a tautology.*

P	$\neg\ P$	$P \vee \neg P$
1	0	1
0	1	1

Table 1.8: Example of tautology

Example 1.3.2 *Let P be a proposition, the formula $P \wedge \neg P$ is a antilogy.*

P	$\neg\ P$	$P \wedge \neg P$
1	0	0
0	1	0

Table 1.9: Example of antilogy

1.4 Predicate Calculus

1.4.1 Universal and existential quantifier

Definition 1.4.1 *A predicate is a statement that depends on one or more variables. The truth value of the predicate thus depends on the variable(s) that compose it.*

Example 1.4.1 *$P(x) : x^2 + 1 = 2x$ is a predicate. We can only know its truth value by replacing the value of x.*

Thus the predicate is true for $x = 1$ and false for $x \neq 1$.

Definition 1.4.2 *Let $P(x)$ be a predicate dependent on the variable x. We introduce the propositions:*

1- $\forall x(P(x))$: By definition this proposition is true if any value of x makes the predicate $P(x)$ true.

2- $\exists x(P(x))$: By definition this proposition is true if there exists at least one value of x for which the predicate $P(x)$ is true.

The symbol $\forall$ which means (Whatever) or (For all) represents the universal quantifier. This symbol represents the reversed letter (A) which is the initial of the English word (All). The symbol $\exists$ which means (There exists at least one ... such that) represents the existential quantifier. This symbol represents the reversed letter (E) which is the initial from the English word (Exist).

Example 1.4.2 *1) "All students have a mobile phone" can be formalized in the following way:*

$\forall x$ (x is a student $\Longrightarrow$ x has a mobile phone).

2) " There is at least one African country at war " can be formalized as follows:

$\exists x$ *(x is a country in Africa $\wedge$ x is at war).*

In most cases the variables on which the quantifiers apply are taken from sets. We thus adopt the following notations:

- $\forall x \in A : P(x)$ is used to denote the formula $\forall x(x \in A \Longrightarrow P(x))$.
- $\exists x \in A : P(x)$ is used to denote the formula $\exists x(x \in A \wedge P(x))$.

1.4.2 Multiple quantifiers

When a multivariate predicate is quantified universally and existentially, the order in which the quantifiers appear is important. Thus for a predicate $p(x, y)$ the formulas $\forall x, \exists y, p(x, y)$ and $\exists x, \forall y, p(x, y)$ do not have the same meaning.

Example 1.4.3 $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y > x$, *which means « Whatever the real x, it exists at least one real y such that y is greater than x ». We can always find a number greater than a given real number because the set $\mathbb{R}$ is not bounded. The proposition is true.*

Let us now invert the quantifiers $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y > x$ « There exists at least one real x such that for any real y, y is greater than x ». This proposition this time is false because we cannot find a real number lower than all the others. Indeed the set $\mathbb{R}$ has no lower bound.

Remark 1.4.1 *It is possible to exchange quantifiers when they are of the same nature and consecutive.*

Example 1.4.4 *The two formulas below are equivalent:*

$$\begin{aligned} \forall x &\in \mathbb{R}, \forall y \in \mathbb{R} : x^2 + y^2 \geq 0, \\ \forall y &\in \mathbb{R}, \forall x \in \mathbb{R} : x^2 + y^2 \geq 0. \end{aligned}$$

1.4.3 Negation of a quantifier

The fundamental rules of negation of formulas are given by

$$\neg \ (\forall x : P(x)) \Leftrightarrow \exists x : \neg \ P(x) \text{ and } \neg \ (\exists x : P(x)) \Leftrightarrow \forall x : \neg \ P(x)$$

These rules are applied successively to several quantifiers.

1.4.4 Quantifiers and connectors

In formulas that use simultaneously quantifiers and conjunctions and disjunction connectors, attention must be paid to the meaning of the formulas.

Thus the formulas: $\forall x : (P(x) \wedge Q(x))$ and $(\forall x : P(x)) \wedge (\forall x : Q(x))$ are equivalent.

On the other hand the formulas $\forall x : (P(x) \vee q(x))$ and $(\forall x : P(x)) \vee (\forall x : Q(x))$ are not equivalent, the second implies the first.

Similarly $\exists x : (P(x) \vee Q(x))$ and $(\exists x : P(x)) \vee (\exists x : Q(x))$ are equivalent, while $\exists x : (P(x) \wedge Q(x))$ implies $(\exists x : P(x)) \wedge (\exists x : Q(x))$.

1.4.5 The quantifier of unique existence

The quantifier $\exists!$ means "there exists one and only one", the formula $\exists! x : p(x)$ asserts that there is a unique value of the variable x that makes the predicate $p(x)$ true, and this assertion can be expressed by the quantifiers $\forall$ and $\exists$:

$$(\exists x : P(x)) \wedge (\forall y, \forall z : P(y) \wedge P(z)) \Longrightarrow y = z.$$

1.4.6 Closure of a predicate

Definition 1.4.3 *A variable that appears after a quantifier is said to be bound. A variable that is not bound is said to be free.*

Example 1.4.5 $\exists x \in \mathbb{R} : x^2 = \alpha$. *Here the variable x is bound and the variable α is free.*

Definition 1.4.4 *A formula that does not contain any free variables is said to be closed. A closed formula is a proposition.*

Example 1.4.6 *The formula $\forall \alpha \in \mathbb{R}^+, \exists x \in \mathbb{R} : x^2 = \alpha$ is a closed formula (all variables are bound). It is a true proposition.*

Definition 1.4.5 *The universal closure (resp. existential closure) of a formula is the formula obtained by adding at the beginning of this formula the quantifiers $\forall$ (resp. $\exists$) to all the free variables of the formula.*

Example 1.4.7 *Let the predicate* $P(x,y) : x^2 = -y^2 - 1$.

The universal closure of this predicate is given by $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x^2 = -y^2 - 1$.

The existential closure of this predicate is given by $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x^2 = -y^2 - 1$.

1.5 Rules of deduction (inferences)

Rules of inference are rules based on tautology, and they form the basis of mathematical proofs.

1.5.1 Modus Ponens (Direct Proof)

We say that a proposition Q logically follows from a true proposition P if the implication $P \Rightarrow Q$ is true we write in this case

$$\begin{array}{rl} & P \\ & \underline{P \Longrightarrow Q} \\ \therefore & Q \end{array}$$

where the sign $\therefore$ reads "Therefore or Consequently".

The proposition P is called hypothesis and Q is called conclusion.

The Modus Ponens rule is based on the tautology $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$. Indeed we have

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q$	$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

Redaction

The redaction of a direct proof often takes the following form:

Proposition: If P then Q.

Proof: Suppose P

...

Therefore (Consequently, Hence...) Q.

Example 1.5.1 *Show that for any odd natural number n, the integer $3n + 7$ is even.*

Suppose that n is an odd integer so we have

$$\begin{aligned}
\underbrace{\forall n \text{ odd integer}}_{P} &\Longrightarrow \underbrace{\exists k \in \mathbb{N} : n = 2k + 1}_{P_1} \\
\underbrace{\exists k \in \mathbb{N} : n = 2k + 1}_{P_1} &\Longrightarrow \underbrace{\exists k \in \mathbb{N} : 3n + 7 = 3\,(2k + 1) + 7}_{P_2} \\
\underbrace{\exists k \in \mathbb{N} : 3n + 7 = 6k + 10 = 2(3k + 5)}_{P_3} &\Longrightarrow \underbrace{3n + 7 \text{ is even}}_{Q}
\end{aligned}$$

By transitivity of the logical implication we obtain: $P \Rightarrow P1 \Rightarrow P2 \Rightarrow P3 \Rightarrow Q$ therefore the proposition $P \Rightarrow Q$ is also true.

So we have

$$\begin{aligned}
&\underbrace{\forall n \text{ odd integer}}_{P} \\
&\underbrace{\forall n \text{ odd integer } \Longrightarrow 3n + 7 \text{ is even}}_{P \Rightarrow Q} \\
\therefore\ & Q
\end{aligned}$$

Remark 1.5.1 *In a direct proof we never start with a false proposition otherwise we cannot conclude anything. Indeed if the proposition P is false the proposition $P \Rightarrow Q$ is true. We cannot obtain any conclusion on the nature of Q which can be true or false.*

1.5.2 Proof by contrapositive

The proof by contrapositive is based on the following tautological equivalence

$$(P \Rightarrow Q) \Longleftrightarrow (\neg\, Q \Rightarrow \neg\, P)\,.$$

In some cases, it allows a demonstration to be simplified.

Remark 1.5.2 *The classical example of the use of proof by contrapositive concerns the injectivity of an application.*

So to show that a function $f : E \to F$ is injective we can show the logical implication

$$\forall x_1, x_1 \in E : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

But often it is simpler to show the contrapositive

$$\forall x_1, x_1 \in E : f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

1.5.3 Proof by the absurd

The proof by the absurd is based on the following tautology

$$(\neg\ P \Rightarrow F) \Longleftrightarrow\ P\ (F : \text{false proposition (contradiction)}$$

P	$\neg\ P$	F	$\neg\ P \Rightarrow F$	$(\neg\ P \Rightarrow F) \Longleftrightarrow\ P$
1	0	0	1	1
0	1	0	0	1

It consists in demonstrating that a logical implication having as antecedent $\neg\ P$ and as consequent a contradiction is true.

Thus the only possibility is that the proposition $\neg\ P$ is false which implies that the proposition P is true.

This demonstration generally begins with: "let us suppose $\neg\ P$ and look for a contradiction". The contradiction appears in the form of a proposition and its opposite true at the same time.

Example 1.5.2 *If $a, b \in \mathbb{Z}$ then $a^2 - 4b \neq 2$*

Suppose that the proposition is false.

Therefore, there exist two integers a and b such that $a^2 - 4b = 2$ $(*)$.

From this equation we obtain $a^2 = 4b + 2 = 2(2b + 1)$, so a^2 is even.

Since a^2 is even we deduce that a is also even, there exists an integer c such that $a = 2c$.

By replacing in the terms of the equation $(*)$ we obtain $(2c)^2 - 4b = 2$.

By dividing by 2 we obtain $2c^2 - 2b = 1$ from which $2(c^2 - b) = 1$.

We deduce that the integer 1 is even which constitutes a contradiction.

1.5.4 Proof by counterexample

The proof by counterexample is based on the following tautology

$$\neg\ (\forall x : P(x)) \Longleftrightarrow\ \exists x : \neg\ P(x).$$

To demonstrate that the proposition $\forall x : P(x)$ is false we find x_0 such that $\neg\ P(x_0)$ is true.

1.5.5 Proof by separation of cases

Let $P_1, P_2, ...P_n$ be propositions. We want to prove proposition Q given that proposition $P_1 \vee P_2 \vee ... \vee P_n$ is true.

It is then sufficient to prove separately that $\forall 1 \leq i \leq n$ if P_i is true then Q is true.

Example 1.5.3 *Show that if $n \in \mathbb{N}$ then $1 + (-1)^n(2n - 1)$ is a multiple of 4.*

Suppose $n \in \mathbb{N}$, then n is either even or odd.

Considering each case separately.

Case No 1: *Suppose n is even then there exists an integer k such that $n = 2k$. Then we obtain*

$$1 + (-1)^n(2n - 1) = 1 + 1.(2.2k - 1) = 4k.$$

Case No 2: *Suppose n is odd then there exists an integer k such that $n = 2k + 1$. Then we obtain*

$$1 + (-1)^n(2n - 1) = 1 - 1.(2.\,(2k + 1) - 1) = -4k.$$

1.5.6 Other rules of inference

The following rules of inference are less used in mathematical proofs in their direct forms but often allow conclusions to be drawn

$$\begin{array}{rlcl} & P \Longrightarrow Q & & P \vee Q \\ & \underline{\neg Q} & , & \underline{\neg P} \\ \therefore & \neg P & & \therefore Q \end{array}$$

1.6 Constructive and non-constructive proofs

1.6.1 Non-constructive proofs (Existential proofs)

Proposition 1.6.1 *There exist two irrational numbers x and y such that x^y is rational.*

Proof. We know that $\sqrt{2}$ is irrational. We then consider the number $\sqrt{2}^{\sqrt{2}}$ which is either rational or irrational.

If $\sqrt{2}^{\sqrt{2}}$ is rational, the proposition is proved by considering $x = y = \sqrt{2}$.

If $\sqrt{2}^{\sqrt{2}}$ is irrational then by setting $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ we obtain $xy = 2$ and the proposition is proven.

The proof of the existence of two irrational numbers x and y such that xy is rational is made without being able to give an example of two irrational numbers that verify $xy \in \mathbb{Q}$.

This type of proof is called "non-constructive proof" in mathematical language. ■

1.6.2 Constructive Proofs

Proposition 1.6.2 *There exist two irrational numbers x and y such that x^y is rational.*

Proof. Let $x = \sqrt{3}$ and $y = \log_3(4)$.

x and y are irrational and we have

$$x^y = \sqrt{3}^{\log_3(4)} = 3^{\frac{1}{2}\log_3(4)} = 3^{\log_3(4)^{\frac{1}{2}}} = 3^{\log_3(2)} = 2.$$

■

1.7 Corrected exercises

Exercise 1.7.1 *1) Let P denote the preposition « The child knows how to read » and Q denote the preposition « The child knows how to write ».*

Give the translation into everyday language of the following propositions :

(1) $P \wedge Q$, (2) $P \wedge \neg Q$, (3) $Q \Longrightarrow P$, (4) $\neg P \vee \neg Q$, (5) $\neg P \wedge \neg Q$.

2) Same question with P is the proposition « Man is mortal » and Q is the proposition « Man is eternal » and the propositions:

(1) $P \vee Q$, (2) $\neg P \vee \neg Q$, (3) $\neg (P \wedge Q)$, (4) $P \wedge \neg Q$, (5) $P \Longrightarrow \neg Q$.

Solution:

1) We have

P : The child knows how to read.

Q : The child knows how to write.

(1) $P \wedge Q$: The child knows how to read and write.

(2) $P \wedge \neg Q$: The child knows how to read but he doesn't know how to write.

(3) $Q \Longrightarrow P$: If the child knows how to write, then he knows how to read.

(4) $\neg P \vee \neg Q$: The child does not know how to read or he does not know how to write.

(5) $\neg P \wedge \neg Q$: The child does not know how to read and he does not know how to write.

2) We have

$$\begin{aligned} P &: \text{ Man is mortal.} \\ Q &: \text{ Man is eternal.} \end{aligned}$$

(1) $P \vee Q$: Man is mortal or eternal.

(2) $\neg P \vee \neg Q$: Man is not mortal or he is not eternal.

(3) $\neg\,(P \wedge Q)$: It is false that man is mortal and eternal.

(4) $P \wedge \neg Q$: Man is mortal buit not eternal.

(5) $P \Longrightarrow \neg Q$: If man is mortal then he is not eternal.

Exercise 1.7.2 ***(This exercise contributed by the author)***

Let P, Q and R be three propositions. For each of the following propositions:

(1) $P \wedge (\neg Q \vee R)$, (2) $(P \wedge Q) \Longrightarrow R$, (3) $P \wedge \neg Q$, (4) $P \vee \neg Q$, (5) $P \vee (Q \wedge R)$,

(6) $P \wedge (Q \wedge R)$, (7) $P \Longrightarrow \neg Q$, (8) $\neg P \Longrightarrow Q$, (9) $\neg (P \vee Q) \Longrightarrow R$, (10) $(P \wedge Q) \Longrightarrow \neg R$.

Write its negation.

Solution:

We write the negation of the following propositions:

(1) $P \wedge (\neg Q \vee R)$

$$\begin{aligned} \neg\,(P \wedge (\neg Q \vee R)) &\Longleftrightarrow \neg P \vee \neg(\neg Q \vee R) \\ &\Longleftrightarrow \neg P \vee (\neg\neg Q \wedge \neg R) \\ &\Longleftrightarrow \neg P \vee (Q \wedge \neg R) \\ &\Longleftrightarrow (\neg P \vee Q) \wedge (\neg P \vee \neg R)\,. \end{aligned}$$

(2) $(P \wedge Q) \Longrightarrow R$

$$\begin{aligned} \neg\left((P \wedge Q) \Longrightarrow R\right) &\iff \neg\left(\neg(P \wedge Q) \vee R\right) \\ &\iff \neg\neg(P \wedge Q) \wedge \neg R \\ &\iff P \wedge Q \wedge \neg R. \end{aligned}$$

(3) $P \wedge \neg Q$

$$\begin{aligned} \neg\left(P \wedge \neg Q\right) &\iff \neg P \vee \neg\neg Q \\ &\iff \neg P \vee Q. \end{aligned}$$

4) $P \vee \neg Q$

$$\begin{aligned} \neg\left(P \vee \neg Q\right) &\iff \neg P \wedge \neg\neg Q \\ &\iff \neg P \wedge Q. \end{aligned}$$

(5) $P \vee (Q \wedge R)$

$$\begin{aligned} \neg\left(P \vee (Q \wedge R)\right) &\iff \neg P \wedge \neg(Q \wedge R) \\ &\iff \neg P \wedge (\neg Q \vee \neg R) \\ &\iff \left(\neg P \wedge \neg Q\right) \vee \left(\neg P \wedge \neg R\right). \end{aligned}$$

(6) $P \wedge (Q \wedge R)$

$$\begin{aligned} \neg\left(P \wedge (Q \wedge R)\right) &\iff \neg P \vee \neg(Q \wedge R) \\ &\iff \neg P \vee (\neg Q \vee \neg R) \\ &\iff \neg P \vee \neg Q \vee \neg R. \end{aligned}$$

(7) $P \Longrightarrow \neg Q$

$$\begin{aligned} \neg\left(P \Longrightarrow \neg Q\right) &\iff \neg\left(\neg P \vee \neg Q\right) \\ &\iff \neg\neg P \wedge \neg\neg Q \\ &\iff P \wedge Q. \end{aligned}$$

(8) $\neg P \Longrightarrow Q$

$$\begin{aligned}\neg\left(\neg P \Longrightarrow Q\right) &\iff \neg\left(\neg\neg P \vee Q\right)\\ &\iff \neg\left(P \vee Q\right)\\ &\iff \neg P \wedge \neg Q.\end{aligned}$$

(9) $\neg(P \vee Q) \Longrightarrow R$

$$\begin{aligned}\neg\left(\neg(P \vee Q) \Longrightarrow R\right) &\iff \neg\left(\neg\neg(P \vee Q) \vee R\right)\\ &\iff \neg\left(P \vee Q \vee R\right)\\ &\iff \neg P \wedge \neg Q \wedge \neg R.\end{aligned}$$

(10) $(P \wedge Q) \Longrightarrow \neg R$

$$\begin{aligned}\neg\left((P \wedge Q) \Longrightarrow \neg R\right) &\iff \neg\left(\neg\left(P \wedge Q\right) \vee \neg R\right)\\ &\iff \neg\neg\left(P \wedge Q\right) \wedge \neg\neg R\\ &\iff P \wedge Q \wedge R.\end{aligned}$$

Exercise 1.7.3 *For each of the following formulas:*

(1) $\neg(P \vee Q) \vee \neg(P \wedge Q)$.

(2) $(P \Rightarrow Q) \iff (\neg\, Q \Rightarrow \neg\, P)$.

(3) $(\neg P \vee Q) \wedge\ (P \wedge \neg Q)$.

1) Create their own truth tables.

2) Indicate whether it is a tautology, an antilogy, or neither.

Solution:

1) Wer create the truth tables of

(1) $\neg(P \vee Q) \vee \neg(P \wedge Q)$

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \vee Q)$	$\neg(P \wedge Q)$	$\neg(P \vee Q) \vee \neg(P \wedge Q)$
1	1	1	1	0	0	0
1	0	1	0	0	1	1
0	1	1	0	0	1	1
0	0	0	0	1	1	1

Proposition (1) is neither a tautology nor an antilogy.

(2) $(P \Rightarrow Q) \Longleftrightarrow (\neg\, Q \Rightarrow \neg\, P)$

P	Q	$\neg\, P$	$\neg Q$	$P \Rightarrow Q$	$\neg\, Q \Rightarrow \neg\, P$	$(P \Rightarrow Q) \Longleftrightarrow (\neg\, Q \Rightarrow \neg\, P)$
1	1	0	0	1	1	1
1	0	0	1	0	0	1
0	1	1	0	1	1	1
0	0	1	1	1	1	1

Proposition (2) is neither a tautology.

(3) $(\neg P \vee Q) \wedge\ (P \wedge \neg Q)$.

P	Q	$\neg\, P$	$\neg Q$	$\neg P \vee Q$	$P \wedge \neg Q$	$(\neg P \vee Q) \wedge\ (P \wedge \neg Q)$
1	1	0	0	1	0	0
1	0	0	1	0	1	0
0	1	1	0	1	0	0
0	0	1	1	1	0	0

Proposition (3) is an antilogy.

Exercise 1.7.4 *Formalize the following propositions using only the indicated predicates, logical connectors and quantifiers.*

1) Nobody is perfect. $P(x) : x$ *is perfect.*

2) 0 *is a multiple of any integer.* $M(x, y) : x$ *divides* y, $E(x) : x$ *is an integer.*

3) Not all absentees are wrong. $A(x) : x$ *is absent,* $W(x) : x$ *is wrong.*

Solution:

1) Nobody is perfect.

$$P(x) : x \text{ is perfect.}$$

We denote by E the set of persons.

If $x \in E$, the proposition "$P(x) : x$ is perfect" is formally written as

$$\forall x \in E : \neg P(x).$$

2) 0 is a multiple of any integer.

$$\begin{aligned} M(x,y) &\ :\ x \text{ divides } y \text{ (or } y \text{ is a multiple of } x\text{)},\\ E(x) &\ :\ x \text{ is an integer.} \end{aligned}$$

This proposition is formally as

$$\forall x \left(E(x) \Longrightarrow M(x,0)\right).$$

3) Not all absentees are wrong.

$$\begin{aligned} A(x) &\ :\ x \text{ is absent},\\ W(x) &\ :\ x \text{ is wrong.} \end{aligned}$$

This proposition is formally as

$$\exists x \left(\neg \left(A(x) \Longrightarrow W(x)\right)\right).$$

Exercise 1.7.5 ***(This exercise contributed by the author)***

Write the negation of the following predicates:

(1) $\exists x \in E,\ P(x) \wedge Q(x)$, (4) $\forall x \in E, \forall y \in F,\ (P(x,y) \wedge Q(x,y)) \Longrightarrow R(x,y)$.

(2) $\forall x \in E,\ P(x) \Longrightarrow Q(x)$, (5) $\exists x \in E, \forall y \in F,\ Q(x,y) \Longrightarrow (P(x,y) \vee R(x,y))$.

(3) $\forall x \in E,\ P(x) \Longleftrightarrow Q(x)$.

Solution:

We write the negation of the following predicate:

(1) $\exists x \in E,\ P(x) \wedge Q(x)$

$$\begin{aligned} \neg \left(\exists x \in E, P(x) \wedge Q(x)\right) &\Longleftrightarrow \forall x \in E, \neg(P(x) \wedge Q(x))\\ &\Longleftrightarrow \forall x \in E, \neg P(x) \vee \neg Q(x). \end{aligned}$$

(2) $\forall x \in E,\ P(x) \Longrightarrow Q(x)$

$$\begin{aligned} \neg \left(\forall x \in E, P(x) \Longrightarrow Q(x)\right) &\Longleftrightarrow \exists x \in E, \neg(P(x) \Longrightarrow Q(x))\\ &\Longleftrightarrow \exists x \in E, \neg(\neg P(x) \vee Q(x))\\ &\Longleftrightarrow \exists x \in E, P(x) \wedge \neg Q(x). \end{aligned}$$

(3) $\forall x \in E,\ P(x) \Longleftrightarrow Q(x)$

$$\begin{aligned}
\neg\left(\forall x \in E, P(x) \Longleftrightarrow Q(x)\right) &\Longleftrightarrow \exists x \in E, \neg(P(x) \Longleftrightarrow Q(x)) \\
&\Longleftrightarrow \exists x \in E, \neg\left((P(x) \Longrightarrow Q(x)) \wedge (Q(x) \Longrightarrow P(x))\right) \\
&\Longleftrightarrow \exists x \in E, \neg(P(x) \Longrightarrow Q(x)) \vee \neg(Q(x) \Longrightarrow P(x)) \\
&\Longleftrightarrow \exists x \in E, , P(x) \wedge \neg Q(x) \vee Q(x) \wedge \neg P(x).
\end{aligned}$$

(4) $\forall x \in E, \forall y \in F,\ (P(x,y) \wedge Q(x,y)) \Longrightarrow R(x,y)$

$$\begin{aligned}
&\neg\left(\forall x \in E, \forall y \in F, (P(x,y) \wedge Q(x,y)) \Longrightarrow R(x,y)\right) \\
\Longleftrightarrow\ & \exists x \in E, \exists y \in F, \neg((P(x,y) \wedge Q(x,y)) \Longrightarrow R(x,y)) \\
\Longleftrightarrow\ & \exists x \in E, \exists y \in F, \neg(\neg\left(P(x,y) \wedge Q(x,y)\right) \vee R(x,y)) \\
\Longleftrightarrow\ & \exists x \in E, \exists y \in F, P(x,y) \wedge Q(x,y) \wedge \neg R(x,y).
\end{aligned}$$

(5) $\exists x \in E, \forall y \in F,\ Q(x,y) \Longrightarrow (P(x,y) \vee R(x,y))$

$$\begin{aligned}
&\neg\left(\exists x \in E, \forall y \in F, Q(x,y) \Longrightarrow (P(x,y) \vee R(x,y))\right) \\
\Longleftrightarrow\ & \forall x \in E, \exists y \in F, \neg(Q(x,y) \Longrightarrow (P(x,y) \vee R(x,y))) \\
\Longleftrightarrow\ & \forall x \in E, \exists y \in F, \neg(\neg Q(x,y) \vee (P(x,y) \vee R(x,y))) \\
\Longleftrightarrow\ & \forall x \in E, \exists y \in F, Q(x,y) \wedge \neg(P(x,y) \vee R(x,y)) \\
\Longleftrightarrow\ & \forall x \in E, \exists y \in F, Q(x,y) \wedge \neg P(x,y) \wedge \neg R(x,y).
\end{aligned}$$

Exercise 1.7.6 *1) Let $P(x)$ and $Q(x)$ be two predicates. Show that the following assertion is a tautology:*

$\neg(\forall x \in E,\ P(x) \Longrightarrow Q(x)) \Longleftrightarrow (\exists x \in E,\ P(x) \wedge \neg Q(x))$.

2) Let $P(x,y)$ be a two-variable predicate. Show that the following assertion is a tautology:

$\neg\left(\exists x \in E, (\forall y \in F, P(x,y))\right) \Longleftrightarrow (\forall x \in E,\ (\exists y \in F, \neg P(x,y)))$.

Solution:

1) Let $P(x)$ and $Q(x)$ be two predicates, we have

$\neg(\forall x \in E,\ P(x) \Longrightarrow Q(x)) \Longleftrightarrow \exists x \in E,\ \neg\left(P(x) \Longrightarrow Q(x)\right)$.

On the other hand we have

$\exists x \in E, \neg (P(x) \Longrightarrow Q(x)) \Longleftrightarrow \exists x \in E, P(x) \wedge \neg Q(x)$

So consequently we have

$\neg(\forall x \in E, P(x) \Longrightarrow Q(x)) \Longleftrightarrow (\exists x \in E, P(x) \wedge \neg Q(x))$ is a tautology.

2) Let $P(x,y)$ be two variables predicate, then

$\neg (\exists x \in E, (\forall y \in F, P(x,y))) \Longleftrightarrow \forall x \in E, \neg (\forall y \in F, P(x,y))\,.$

On the other hand we have

$\forall x \in E, \neg (\forall y \in F, P(x,y)) \Longleftrightarrow \forall x \in E, (\exists y \in F, \neg P(x,y))$

So therefore we have

$\neg (\exists x \in E, (\forall y \in F, P(x,y))) \Longleftrightarrow (\forall x \in E, (\exists y \in F, \neg P(x,y)))$ is a tautology

Exercise 1.7.7 *Translate the following sentences into the language of predicates.*

$$P(x) \ : \ x \textit{ is a plumber}$$

$$M(x) \ : \ x \textit{ is a man}$$

$$R(x) \ : \ x \textit{ is rich}$$

1) *All plumbers are men.*

2) *All men are plumbers or rich.*

3) *Some plumbers are rich.*

4) *Some plumbers are not rich.*

5) *There is no rich plumber.*

6) *All men are plumbers.*

7) *Not all men are plumbers.*

8) *There are men who are not plumbers.*

Solution:

We translate the following sentences into the language of predicates.

1) All plumbers are men.

$$\forall x \, (P(x) \Longrightarrow M(x))\,.$$

2) All men are plumbers or rich

$$\forall x \, (M(x) \Longrightarrow (P(x) \vee R(x)))\,.$$

3) Some plumbers are rich

$$\exists x\,(P(x)\wedge R(x))\,.$$

4) Some plumbers are not rich

$$\exists x\,(P(x)\wedge\neg R(x))\,.$$

5) There is no rich plumber

$$\neg\,(\exists x\,(P(x)\wedge R(x)))\,.$$

6) All men are plumbers

$$\forall x\,(M(x)\Longrightarrow P(x))\,.$$

7) Not all men are plumbers

$$\neg\,(\forall x\,(M(x)\Longrightarrow P(x)))\,.$$

8) There are men who are not plumbers

$$\exists x\,(M(x)\wedge\neg P(x))\,.$$

Exercise 1.7.8 ***(This exercise contributed by the author)***

Let n be a variable taking its values from the set of natural numbers and let the predicates

$$\begin{aligned} ev(n) &\ :\ n \textit{ is even,}\\ od(n) &\ :\ n \textit{ is odd.}\end{aligned}$$

Explain in each case the statement given by the following propositions

1.$\forall n\ (ev(n)\vee od(n))$. 2.$(\forall n\ ev(n))\vee(\forall n\ od(n))$.

3.$(\exists n\ ev(n))\wedge(\exists n\ od(n))$. 4.$\exists n\ (ev(n)\wedge od(n))$.

Solution:

et n be a variable taking its values from the set of natural numbers and let the predicates

$$\begin{aligned} ev(n) &\ :\ n \text{ is even,}\\ od(n) &\ :\ n \text{ is odd.}\end{aligned}$$

We explain in each case the statement given by the following propositions

1- The formula $\forall n\ (ev(n) \vee od(n))$ states that every natural number is even or odd

2- The formula $(\forall n\ ev(n)) \vee (\forall n\ od(n))$ states that all natural numbers are either all even or all odd.

3. The formula $(\exists n\ ev(n)) \wedge (\exists n\ od(n))$ states that there exists in the natural numbers at least one even and at least one odd.

4. The formula $\exists n\ (ev(n) \wedge od(n))$ states that there exists a natural number which is both even and odd.

Exercise 1.7.9 1) *Give the negation and the contrapositive of the following mathematical sentence.*

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \forall p \in \mathbb{N}, n \geq N \ \textit{and}\ p \geq 0 \Longrightarrow |u_{n+p} - u_n| \ < \varepsilon.$$

2) *Let x_0 and f be an application of $\mathbb{R}$ into $\mathbb{R}$.*

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in \mathbb{R}, |x - x_0| < \alpha \Longrightarrow |f(x) - f(x_0)| \ < \varepsilon.$$

Give the negation and the contrapositive of this logical sentence.

Solution:

1) We give the negation and the contrapositive of the following mathematical sentence.

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \forall p \in \mathbb{N}, n \geq N \text{ and } p \geq 0 \Longrightarrow |u_{n+p} - u_n| \ < \varepsilon.$$

The negation:

$$\exists \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \in \mathbb{N}, \exists p \in \mathbb{N}, n \geq N \text{ and } p \geq 0 \text{ and } |u_{n+p} - u_n| \ \geq \varepsilon.$$

The contrapositive:

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \forall p \in \mathbb{N}, |u_{n+p} - u_n| \ \geq \varepsilon \Longrightarrow n < N \text{ or } p < 0.$$

2) We give the negation and the contrapositive of the following logical sentence.

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in \mathbb{R}, |x - x_0| < \alpha \Longrightarrow |f(x) - f(x_0)| \ < \varepsilon.$$

The negation:

$$\exists\varepsilon > 0, \forall\alpha > 0, \exists x \in \mathbb{R}, |x - x_0| < \alpha \wedge |f(x) - f(x_0)| \ \ \geq \varepsilon.$$

The contrapositive:

$$\forall\varepsilon > 0, \exists\alpha > 0, \forall x \in \mathbb{R}, |f(x) - f(x_0)| \ \ \geq \varepsilon \Longrightarrow |x - x_0| \geq \alpha.$$

Exercise 1.7.10 ***(This exercise contributed by the author)***

Determine whether the formulas below are open or closed.

1) $P(x)$
2) $\exists x, Q(x)$
3) $\exists y, Q(x)$
4) $\forall x, P(x) \vee Q(x)$
5) $\exists y, (Q(y) \Longrightarrow P(y))$
6) $Q(y) \Longrightarrow \exists y, P(y)$
7) $\forall x, (P(x) \wedge Q(x))$
8) $P(x) \Longrightarrow \exists x, Q(x)$
9) $\forall x, (P(x) \wedge Q(y))$
10) $\forall x, (P(x) \Longrightarrow \exists y, (Q(y) \wedge R(x)))$

Solution:

We determine whether the formulas below are open or closed.

1) $P(x)$ is open, because the variable x is free.

2) $\exists x, Q(x)$ is closed, because the variable x is bound.

3) $\exists y, Q(x)$ is open, because the variable x is free.

4) $\forall x, P(x) \vee Q(x)$ is open, because the variable x is free.

5) $\exists y, (Q(y) \Longrightarrow P(y))$ is closed, because the two variables y are bound.

6) $Q(y) \Longrightarrow \exists y, \ P(y)$ is open, because the first variable y is free.

7) $\forall x, (P(x) \wedge Q(x))$ is closed, because the two variables x are bound.

8) $P(x) \Longrightarrow \exists x, Q(x)$ is open, because the second variable x is free.

9) $\forall x, (P(x) \wedge Q(y))$ is open, because the variable y is free.

10) $\forall x, (P(x) \Longrightarrow \exists y, (Q(y) \wedge R(x)))$ is closed, because all variables x and y are bound.

Exercise 1.7.11 ***"Modus Ponens"***

1) Let $f : \mathbb{R} \to \mathbb{R}$. Prove that f can be uniquely written as the sum of an even function and an odd function.

2) Show that

$$\forall\varepsilon > 0, \exists N \in \mathbb{N} \textit{ such as } \left(n \geq N \Longrightarrow 2 - \varepsilon < \frac{2n+1}{n+2} < 2 + \varepsilon\right).$$

Solution:

1) Let $f:\mathbb{R}\to\mathbb{R}$. We prove that f can be uniquely written as the sum of an even function and an odd function.

Suppose that f is written as $f=g+h$, with g an even function and h an odd function. Then, $\forall x\in\mathbb{R}$ we have

$$\begin{array}{rcl} f(x) & = & g(x)+h(x)......(1)\\ f(-x) & = & g(-x)+h(-x)\\ & = & g(x)-h(x)......(2) \end{array}$$

So we have necessarily

$$\begin{array}{rcl} (1)+(2) & \iff & g(x)=\dfrac{f(x)+f(-x)}{2}\\ (1)-(2) & \iff & h(x)=\dfrac{f(x)-f(-x)}{2} \end{array}$$

Thus, we have shown that if $f=g+h$, with g an even function and h an odd function are necessarily given by the above formulas and are therfore unique.

2) we show that

$$\forall\varepsilon>0,\exists N\in\mathbb{N}\text{ such as }\left(n\geq N\Longrightarrow 2-\varepsilon<\frac{2n+1}{n+2}<2+\varepsilon\right).$$

Let us first note that for $n\in\mathbb{N}$, we have $\frac{2n+1}{n+2}<2$, because $2n+1<2n+4<2(n+2)$. Given $\varepsilon>0$, therfore we have

$$\forall n\in\mathbb{N}:\frac{2n+1}{n+2}<2+\varepsilon.$$

Now, we look for a condition on n so that the inquality $2-\varepsilon<\frac{2n+1}{n+2}$ is true.

$$\begin{array}{rcl} 2-\varepsilon & < & \dfrac{2n+1}{n+2}\Leftrightarrow(2-\varepsilon)(n+2)<2n+1\\ & \iff & 3<\varepsilon(n+2)\iff n>\dfrac{3}{\varepsilon}-2. \end{array}$$

So we just take $N=\left[\frac{3}{\varepsilon}-2\right]+1\in\mathbb{N}$ as $N>\frac{3}{\varepsilon}-2$, then for all $n\geq N$, we have $n\geq N>\frac{3}{\varepsilon}-2$ and consequently we have $2-\varepsilon<\frac{2n+1}{n+2}$.

Conclusion, given $\varepsilon>0$, we found a $N=\left[\frac{3}{\varepsilon}-2\right]+1\in\mathbb{N}$ such taht for all $n\geq N$, we have

$$2-\varepsilon<\frac{2n+1}{n+2}<2+\varepsilon.$$

Exercise 1.7.12 ***"Proof by contrapositive"***

1) Show that for $n \in \mathbb{N}^*$:

$$\textit{If the integer } (n^2 - 1) \textit{ is not divisible by } 8, \textit{ then the integer } n \textit{ is even.}$$

2) Let a and b be two real numbers. Consider the following proposition:

$$\textit{If } a + b \textit{ is irrational, then } a \textit{ or } b \textit{ are irrational.}$$

i) Prove this proposition.

ii) Is the converse of this proposition always true?

Solution:

By the contrapositive, we show that $\forall n \in \mathbb{N}^*$, If the integer $(n^2 - 1)$ is not divisible by 8,then the integer n is even.

So it suffices to show that if n is odd, then the integer $(n^2 - 1)$ divisible by 8.

Let's take n an odd integer, so n is written as $n = 2k + 1$ where k is an integer.

- If k is even then we have $k = 2l$ and $n = 4l + 1$.

- If k is odd then we have $k = 2l + 1$ and $n = 4l + 3$.

In all cases, we have $n = 2k + r$ with $r \in \{1, 3\}$.

So we have

$$\begin{aligned} n^2 - 1 &= (4l + r)^2 - 1 \\ &= 16l^2 + 8lr + r^2 - 1 \\ &= 8\left(2l^2 + lr\right) + r^2 - 1. \end{aligned}$$

Then

- If $r = 1$, we get $n^2 - 1 = 8\left(2l^2 + lr\right)$ divisible by 8.

- If $r = 3$, we get $n^2 - 1 = 8\left(2l^2 + lr + 1\right)$ divisible by 8.

Therfore, by the principle of contrapositive, we have our proposition is true.

2) Let a and b two real numbers. We consider the proposition:

$$\text{If } a + b \text{ is irrational, then } a \text{ or } b \text{ are irrational.}$$

We demonstrate this proposition using the contrapositive.

The contrapositive of this proposition is:

If a and b are rational, then $a+b$ is rational.

Suppose that a and b are rational, then they are written as follows: $a=\frac{p}{q}$ and $b=\frac{p'}{q'}$ with p, p', q, q' are integers and q, q' non-zero.

We calculate $a+b$

$$a+b=\frac{p}{q}+\frac{p'}{q'}=\frac{pq'+qp'}{qq'}.$$

The number $a+b$ is the quontient of two integers, so it is rational.

c) The converse of the proposition is

If a or b are irrational, the $a+b$ is irrational.

This proposition is not allways true.

For example: if $a=\sqrt{2}$ and $b=-\sqrt{2}$, then a or b are irrational, but $a+b=0$ is not irrational.

Exercise 1.7.13 ***"Proof by the absurd"***

1) Show that $\sqrt{2}$ is an irrational number.

2) Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of applications of the set $\mathbb{N}$ into itself. We define an application f from $\mathbb{N}$ to $\mathbb{N}$ by setting $f(n)=f_n(n)+1$.

Prove that there exists no $p\in\mathbb{N}$ such that $f=f_p$.

Solution:

1) We show that $\sqrt{2}$ is an irrational number.

By the absurd, suppose that $\sqrt{2}$ be a rational number.

Therefore, there are two integers m and n prime numbers between them such that $\sqrt{2}=\frac{m}{n}$ with $n\neq 0$.

Squaring it, we get $2=\frac{m^2}{n^2}$, So we get $2n^2=m^2$ and conclude that m^2 is even and hence m is even.

Since 2 divides m then 4 divides m^2.

Since the result of dividing m^2 by n^2 is 2, then n is also even.

We conclude that m and n are both even which constitutes a contradiction with the fact that they are prime numbers between them.

2) Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of applications from $\mathbb{N}$ to $\mathbb{N}$.

We show that there exists no $p \in \mathbb{N}$ such that $f = f_p$.

By the absurd, suppose that there exists $p \in \mathbb{N}$ such that $f = f_p$.

Two applications are equal if and only if they take the same values $\forall n \in \mathbb{N} : f(n) = f_p(n)$.

In particular for $n = p$ we have $f(p) = f_p(p)$.

On the other hand the definition of f gives us $f(p) = f_n(p) + 1$,

We obtain a contradiction because $f(p)$ cannot take two distinct values, In conclusion, whatever $p \in \mathbb{N} : f \neq f_p$.

Exercise 1.7.14 ***"Proof by counterexample"***

1) Show that the assertion: "Every positive integer is the sum of three squares" is false.

2) Determine whether the following statement is true or false: "Every strictly increasing sequence tends to $+\infty$".

Solution:

1) We show that the assertion: "Every positive integer is the sum of three squares" is false.

The number 7 is not the sum of three squares, because there are only two non-zero squares less than or equal to 7 which are 1 and 4.

This proves that the assertion is false.

2) We determine whether the following statement is true or false: "Every strictly increasing sequence tends to $+\infty$"

Let n be a strictly positive natural integer.

We put

$$u_n = 1 - \frac{1}{n}.$$

Let us show that the sequence $(u_n)_{n\in\mathbb{N}}$ is strictly increasing-

For any integer $n > 0$, we have

$$\begin{aligned} u_{n+1} - u_n &= \left(1 - \frac{1}{n+1}\right) - \left(1 - \frac{1}{n}\right) \\ &= \frac{1}{n\,(n+1)} > 0. \end{aligned}$$

So the sequence $(u_n)_{n\in\mathbb{N}}$ is strictly increasing.

Now the limit of this sequence is equal to 1, so the statement is false.

Exercise 1.7.15 ***"Proof by separation of cases"***

1) Let E and F be two sets and let $x \in E$ and $y \in F$. Then we define the ordered pair (x, y) by

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Show that: $(x, y) = (x', y')$ if and only if $x = x'$ and $y = y'$.

2) Show that, for all $x \in \mathbb{R} : |x - 1| \leq x^2 - x + 1$.

Solution:

1) Let E and F be two sets and let $x \in E$ and $y \in F$, then we define the ordered pair (x, y) by

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Show that: $(x, y) = (x', y')$ if and only if $x = x'$ and $y = y'$.

We have

$$(x, y) = (x', y') = \{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}.$$

We have two situations

1- $\{x\} = \{x'\} \Longrightarrow x = x'$, hence $\{x, y\} = \{x', y'\}$, so we obtain $y = y'$.

2- $\{x\} = \{x', y'\} \Longrightarrow x = x' = y'$, as $\{x, y\} = \{x'\}$, we get $x = y = x' = y'$.

2) We show that for all $x \in \mathbb{R} : |x - 1| \leq x^2 - x + 1$.

As the absolute value has two distinct expressions following the sign of the quantity inside. This leads us to reason by disjunction of cases

$$|x - 1| = \begin{cases} x - 1 & \text{if } x \geq 1 \\ 1 - x & \text{if } x \leq 1 \end{cases}.$$

i) If $x \geq 1$, then $x - 1 \geq 0$ and $|x - 1| = x - 1$.

We must show that if $x \geq 1$ we have $x - 1 \leq x^2 - x + 1$. Let us study the sign of polynomial

$$\begin{aligned} p(x) &= x^2 - x + 1 - (x - 1) \\ &= x^2 - 2x + 2 \\ &= (x - 1)^2 + 1 \geq 0. \end{aligned}$$

The proposition is therefore true if $x \geq 1$.

ii) If $x \leq 1$, then $x - 1 \leq 0$ and $|x - 1| = 1 - x$.

We must show that if $x \leq 1$ we have $1 - x \leq x^2 - x + 1$. Let us study the sign of polynomial

$$\begin{aligned} q(x) &= x^2 - x + 1 - (1 - x) \\ &= x^2 \geq 0. \end{aligned}$$

The proposition is therefore true if $x \leq 1$.

In conclusion the proposition is true for all $x \in \mathbb{R}$.

1.8 Suggested exercises

Exercise 1.8.1 *Let P, Q, R be propositions, give the truth table of each of the following compound propositions*

$$P \Longrightarrow (P \Longrightarrow Q),\ Q \vee (\neg Q \wedge P),\ (P \vee Q) \Rightarrow R.$$

Exercise 1.8.2 *Rewrite each sentence using the logical implication notation "If... Then...".*

1- For a function to be continuous, it is sufficient that it be differentiable.

2- An integer is divisible by 8 only if it is divisible by 4.

Exercise 1.8.3 *Show that the proposition $(P \Longrightarrow (Q \Longrightarrow R)) \Longrightarrow ((P \Longrightarrow Q) \Longrightarrow (P \Longrightarrow R)))$ is a tautology.*

Exercise 1.8.4 *Give the values of the integers $n, m \in \mathbb{N}$ verifying*

$$\text{If } n^2 + m^2 = 25 \text{ then } n < m.$$

Exercise 1.8.5 *Let the predicates be:*

$$\begin{aligned} \textit{student}\ (x) &: \ x \textit{ is a student,} \\ \textit{bicycle}\ (y) &: \ y \textit{ is a bicycle,} \\ \textit{possesses}\ (x,y) &: \ x \textit{ possesses } y. \end{aligned}$$

Translate the following propositions into everyday language:

1. $\forall x(\textit{bicycle}\ (x) \Rightarrow \exists z(\textit{student}\ (z) \wedge \textit{ possesses}\ (z,x)))$.

2. $\forall x(\textit{student}\ (x) \Rightarrow \forall y \forall z(\textit{bicycle}\ (z) \wedge \textit{ bicycle}\ (y) \wedge (z = y) \Rightarrow \neg \textit{ possesses}\ (x,z) \vee \neg \textit{possesses}\ (x,y)))$.

3. $\exists x(\textit{student}\ (x) \wedge \forall y(\textit{bicycle}\ (y) \Rightarrow \neg \textit{ possesses}\ (x,y)))$.

Exercise 1.8.6 *Are the following two formulas equivalent?*

$$F1 : \exists m, n \in \mathbb{N} : m \wedge n = 1 \wedge \sqrt{2} = \frac{m}{n}$$

$$F2 : (\exists m, n \in N : m \wedge n = 1) \wedge \exists m, n \in N : \sqrt{2} = \frac{m}{n}$$

Exercise 1.8.7 *Let R be the proposition $\forall x(P(x) \vee Q(x))$ and S be the proposition $(\forall x P(x)) \vee (\forall x Q(x))$*

1. Show that $R \Rightarrow S$.

2. Do we have $S \Rightarrow R$? Justify your answer.

Exercise 1.8.8 *Show that the strict order relation $<$ on the set $\mathbb{R}$ is antisymmetric.*

Exercise 1.8.9 *Show that $\sqrt{3}$ is an irrational number.*

Exercise 1.8.10 *Show that if $\frac{2n}{1+n^2}$ is irrational then n is irrational.*

Exercise 1.8.11 *Show that for any real number a, if $a^2 > 0$ then $a = 0$.*

Exercise 1.8.12 *Show that if two integers have different parities then their sum is an odd integer.*

Exercise 1.8.13 *Show that any integer multiple of 4 can be written in the form $1+(-1)^n(2n-1)$.*

Exercise 1.8.14 *Show that for all real $x \in \left[0, \frac{\pi}{2}\right]$, we have $\sin(x) + \cos(x) \geq 1$.*

Chapter 2

Introduction to set theory

Set theory is a branch of mathematical logic that studies sets, which can be informally described as collections of objects. Although any type of object can be grouped into a set, set theory, as a branch of mathematics, is primarily concerned with objects relevant to mathematics as a whole. In this chapter, we present naive set theory, paradoxes related to naive set theory, and Zermelo-Fraenkel theory, which is based on axioms.

2.1 Naive set theory

In naive set theory, the notions of set and belonging considered intuitive are not precisely defined.

We denote by $x \in E$ the fact that x is an element of E. Two sets are equal when they have the same elements.

The empty set is denoted by $\{.\}$ or $\emptyset$.

In general, we describe a set or by giving the list of all its elements. For example, the set of students, 2nd year licence in Mathematics, promotion 2024-2025, or by characterizing its elements among those of a set already known.

For example, $E = \{n \in IN | (\exists m \in IN)(n = 2m)\}$.

We say that F is a subset of E or F is contained in E, and we denote $F \subset E$ if every element of F also belongs to E. We also say that F is a part of E.

The union of two sets denoted $E \cup F$ is the set of all elements of E and F. The intersection of two sets denoted $E \cap F$ is the set of all elements that belong to both E and F.

The difference of two sets denoted $E\backslash F$ is the set of all elements of E that do not belong to F. If $F \subset E$ then we denote $C_E F = E\backslash F$ the set complement of F in E.

Finally the symmetric difference $E\triangle F$ is the set defined by $E\triangle F = (E\backslash F) \cup (F\backslash E)$.

2.1.1 The Cartesian product

Definition 2.1.1 *Let E and F be two sets and let $x \in E$ and $y \in F$. Then we define the ordered pair (x, y) by*

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Lemma 2.1.1 *We have $(x, y) = (x', y')$ if and only if $x = x'$ and $y = y'$.*

Proof. We have

$$(x, y) = (x', y') \Longleftrightarrow \{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}.$$

We have two situations:

1- $\{x\} = \{x'\} \Rightarrow x = x'$ from which $\{x, y\} = \{x', y'\}$ so we get $y = y'$.

2- $\{x\} = \{x', y'\} \Rightarrow x = x' = y'$ as $\{x, y\} = \{x'\}$ we get $x = x' = y' = y$. ■

2.1.2 Sets of parts

Definition 2.1.2 *Let E be a set. We call the set of parts of E the set denoted $\mathcal{P}(E)$ consisting of all the subsets of E.*

Example 2.1.1 *Let $E = \{a, b, c\}$, then*

$$\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

2.1.3 Binary relation

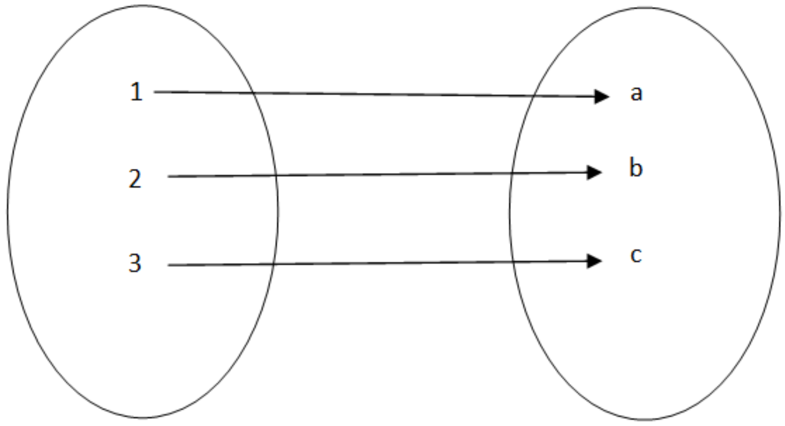
A binary relation $\mathcal{R}$ from a set E to a set F is defined by a part $G_{\mathcal{R}}$ of $E \times F$, where $G_{\mathcal{R}}$ denotes the graph of relation $\mathcal{R}$. The components of a pair belonging to the graph of a relation $\mathcal{R}$ are said to be related by $\mathcal{R}$.

If $(x, y) \in G$, we say that x is related to y and we denote $x\mathcal{R}y$.

When a binary relation is defined from a set E to itself, we call it an internal relation on E or simply a relation on E.

Example 2.1.2 *Let the sets* $E = \{1, 2, 3\}$ *and* $F = \{a, b, c\}$ *and the relation* $\mathcal{R}$ *defined by* $\{(1, a), (2, b), (3, c)\}$.

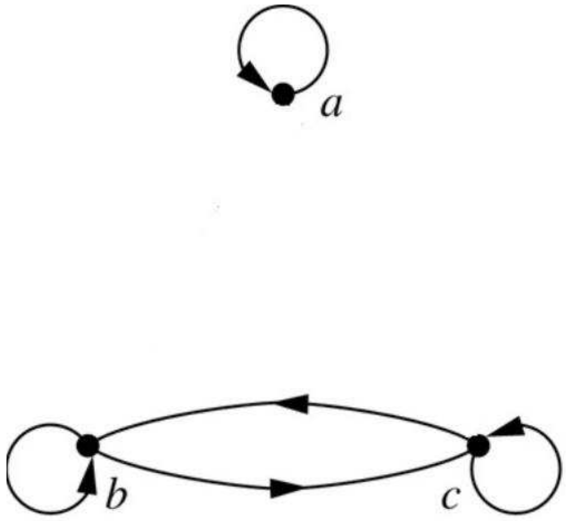
We can represent the relation $\mathcal{R}$ *by the following graph called sagittal representation*



The graph of relation $\mathcal{R}$.

Example 2.1.3 *Let the set* $E = \{a, b, c\}$ *and the relation* $\mathcal{R}$ *defined by* $\{(a, a), (b, b), (c, c), (b, c), (c, b)\}$.

As the starting and finishing sets are identical, we simply represent the relation by a directed graph



The graph of relation $\mathcal{R}$.

Definition 2.1.3 *1) Let $\mathcal{R}$ be a relation of E on F and $\mathcal{S}$ a relation of F in G. We define the composition relation $\mathcal{S} \circ \mathcal{R}$ of E on G by*

$$G_{\mathcal{S}\circ\mathcal{R}} = \{(x,y) \in E \times G : \exists z \in F, (x,z) \in G_{\mathcal{R}} \text{ and } (z,y) \in G_{\mathcal{S}}\}.$$

2) Let $\mathcal{R}$ be a relation of E on F. We can define a relation $\mathcal{R}^{-1}$ of F on E called an inverse or reciprocal relation by

$$G_{\mathcal{R}^{-1}} = \{(x,y) \in F \times E : (y,x) \in G_{\mathcal{R}} \}.$$

3) Let $\mathcal{R}$ be a relation of E on F. We can define a relation $\mathcal{R}$ of F on E called a complementary relation by

$$G_{\overline{\mathcal{R}}} = \{(x,y) \in F \times E : (x,y) \notin G_{\mathcal{R}} \}.$$

4) The diagonal Δ_E of a set E and the diagonal $\left|\overline{\mathcal{R}}\right|$ of an internal relation $\mathcal{R} \subset E \times E$ are defined by

$$\Delta_E = \{(x,x) : x \in E \} \text{ and } \left|\overline{\mathcal{R}}\right| = \{x \in E : (x,x) \in G_{\mathcal{R}} \}.$$

Definition 2.1.4 *Let $\mathcal{R}$ be a binary relation on E.*

- *$\mathcal{R}$ is reflexive if $\Delta_E \subset G_{\mathcal{R}}$.*
- *$\mathcal{R}$ is irreflexive if $\Delta_E \cap G_{\mathcal{R}} = \emptyset$.*
- *$\mathcal{R}$ is symmetric if $G_{\mathcal{R}} = G_{\mathcal{R}^{-1}}$.*
- *$\mathcal{R}$ is anti-symmetric if $G_{\mathcal{R}} \cap G_{\mathcal{R}^{-1}} = \Delta_E$.*
- *$\mathcal{R}$ is transitive if $G_{\mathcal{R}\circ\mathcal{R}} \subset G_{\mathcal{R}}$.*

The previous definition can be translated into the following form which is more practical for demonstrations.

Definition 2.1.5 *Let $\mathcal{R}$ be a binary relation on E.*

- *We say that $\mathcal{R}$ is reflexive when: $\forall x \in E, x\mathcal{R}x$.*
- *We say that $\mathcal{R}$ is irreflexive or antireflexive if no element of E is in relation with itself.*
- *We say that $\mathcal{R}$ is symmetric when: $\forall (x,y) \in E^2, x\mathcal{R}y \Longrightarrow y\mathcal{R}x$.*
- *We say that $\mathcal{R}$ is anti-symmetric when: $\forall (x,y) \in E^2, (x\mathcal{R}y \wedge y\mathcal{R}x) \Longrightarrow x = y$.*
- *We say that $\mathcal{R}$ is transitive when: $\forall (x,y,z) \in E^3, x\mathcal{R}y \wedge y\mathcal{R}z \Longrightarrow x\mathcal{R}z$.*

Example 2.1.4 *- The usual order relation on $\mathcal{R}$ is reflexive, antisymmetric and transitive.*

- The strict order relation on $\mathcal{R}$ is antireflexive, antisymmetric and transitive.

2.1.4 Applications

Definition 2.1.6 *A triple $f = (E, F, G)$ with a binary relation $G \subset E \times F$ is an application if it verifies*

$$\forall x \in E, \exists! y \in F : (x, y) \in G.$$

If $E = F = \emptyset$ then the function $f = (\emptyset, \emptyset, \emptyset)$ is called the empty function.

Definition 2.1.7 *Let E and F be two sets. We say that a function f from E to F is*

-injective if

$$\forall x, y \in E : f(x) = f(y) \Rightarrow x = y.$$

- surjective if

$$\forall y \in F, \exists x \in E : f(x) = y.$$

- A bijection is an application that is injective and surjective.

The definitions of relation and application that we have just seen call on the Cartesian product and consequently on the notion of set. In this case, we say that the definitions are set-theoretic.

Sets are of fundamental importance in mathematics. The inner mechanics of mathematics (numbers, relations, functions, etc.) can be defined in terms of sets.

In mathematics, a paradox (or antinomy) is a statement or reasoning that contains or appears to contain a logical contradiction.

2.2 Paradoxes related to naive set theory

A paradox, according to the etymology (from the Greek word paradoxos: *"contrary to common opinion"*, from para: *"against"* and doxa: *"opinion"*) is an idea or proposition which surprises or shocks at first sight, that is to say contrary to common sense.

In mathematics, a paradox (or antinomy) is a statement or reasoning that contains or appears to contain a logical contradiction.

Several paradoxes appear in naive set theory where precisely the notions of set and belonging are not clearly defined.

Russell described the paradox that bears his name in a 1902 letter to Gottlob Frege, in which he shows the latter that one of the rules introduced in his book "Grundgesetze der Arithmetik", the unrestricted comprehension, made Frege's theory contradictory.

Frege claims that any statement that depends on one or more variables allows us to define a set. This is called the unrestricted comprehension model.

2.2.1 Russell's paradox (1901)

Russell's paradox arises from the following question: *"The set of all sets that do not belong to itself belongs to itself ?"*

The set can be expressed by the following notation

$$E = \{x : x \notin x\} .$$

We then have two possibilities:

1. Suppose that the set E belongs to itself, therefore it verifies the predicate $x \notin x$ and consequently $E \notin E$.

2. Suppose now that the set E does not belong to itself, we then have: $E \notin E$ therefore it by definition $E \in E$.

2.2.2 Other versions of Russell's paradox

Russell's paradox can be stated in more playful forms, we propose here some of these forms.

The Barber Paradox

The village barber decides to shave all the men in the village who do not shave themselves, and only those.

The question then arises: who shaves the barber? In this case we have two possibilities:

1. If he shaves himself, then he shaves someone who does not shave himself.

2. If he does not shave himself, then he should shave himself, respecting his decision.

The Cretan Liar Paradox

The Cretan Epimenides (between 600 and 550 BC) wrote a verse at the origin of this paradox: *"The Cretans are always liars, wicked beasts, lazy bellies"*.

We then ask ourselves the following question: Is Epimenides telling the truth?

In this case we have two possibilities:

1. The statement: *"The Cretans are always liars"* is true in this case Epimenides is telling the truth or Epimenides is Cretan so he is lying.

2. The statement: *"The Cretans are always liars"* is false in this case Epimenides is telling the truth.

The Librarian Paradox

Should the catalog of all catalogs that do not mention themselves mention themselves?

1. If the catalog does not mention itself then it must therefore appear in the list of catalogs that do not mention themselves.

2. If the catalog mentions itself then it is a catalog that does not mention itself by definition.

2.2.3 Berry's Paradox

The initial idea is to describe natural numbers by statements (in French). For example:

1. Two is a one-word expression describing a natural number.
2. One plus two is a three-word expression describing a natural number.
3. One plus two plus three plus...plus nine is a 17-word expression describing a natural number.

Since the available vocabulary is finite, the most complete French dictionaries reach 90000 words, statements of N words can describe at most 90000^N natural integers.

Now let us consider the set of natural numbers that cannot be described by an expression of fifteen words or less. This set has a smallest element. This smallest element should therefore be expressed by sixteen words or more, but the statement: *"The smallest natural number that cannot be described by an expression of fifteen words or less"* contains precisely fifteen words, hence the paradox.

2.2.4 Well-defined set

Definition 2.2.1 *A set E is well-defined if for any object x the statement "$x \in E$ and $x \notin E$ " is false.*

2.3 Zermelo-Fraenkel Theory

We present a simplified version of Zermelo-Fraenkel theory. This theory is based on the following axioms:

2.3.1 Axiom of equality (or Extensionality)

Two sets A and B are equal if and only if they have the same elements.

$$\forall A, \forall B \quad [\forall z(z \in A \Leftrightarrow z \in B) \Longrightarrow A = B] .$$

2.3.2 Axiom of comprehension (or separation).

Given a set U and a predicate $P(x)$ there exists a set E whose elements are those, among the elements of U, which have the property $P(x)$.

$$E = \{x \in U : P(x)\}.$$

Remark 2.3.1 *This axiom is also called the restricted axiom of comprehension as opposed to the universal axiom of comprehension which leads to Russell's paradox.*

Proposition 2.3.1 *There is no set having all sets as elements.*

Proof. We reason absurdly and assume that there exists a set of all sets denoted E. In this case the following writing is correct

$$F = \{x \in E : x \notin x\}.$$

However, this writing leads to Russell's paradox and therefore to a contradiction. Thus there is no set containing all sets. ■

Remark 2.3.2 *In this case we speak of a collection of all sets.*

2.3.3 Axiom of pair

Given two elements a and b, there exists a set C which contains a and b and only them.

$$\forall a, \forall b, \exists C, \forall t \ [t \in C \Longleftrightarrow (t = a \vee t = b)].$$

The set C whose only elements are a and b is denoted $\{a, b\}$.

- If $a \neq b$ the set $\{a, b\}$ is called a pair.

- If $a = b$ the set $\{a, b\}$ is called a singleton, we denote it $\{a\}$.

2.3.4 Axiom of union (or sum)

For any set A there exists a set B whose elements are exactly the elements of the elements of A. The corresponding formula is

$$\forall A, \exists B \ (\forall x, x \in B \Leftrightarrow \exists y, y \in A \wedge x \in y).$$

This set is unique, we call it the union of the elements of x and we denote it $\cup_{x \in y} y$.

2.3.5 Axiom of the set of parts.

To any set we can associate a set which contains exactly the parts of the first set.

$$\forall A, \exists B \ (\forall x, x \in B \Longrightarrow x \subset A).$$

Remark 2.3.3 *The notation $x \subset A$ is an abbreviation for $\forall y, y \in x \Leftrightarrow y \in A$.*

Remark 2.3.4 *The set of subsets of the set a is denoted $\mathcal{P}(A)$.*

2.3.6 Axiom of infinity

There exists a set M of which $\emptyset$ is an element and such that for all x belonging to M the set $\{x\}$ also belongs to M.

Remark 2.3.5 *This axiom indirectly constructs the natural integers. Thus $\emptyset$ corresponds to 0 and for each integer n the integer $n + 1$ corresponds to $n \cup \{n\}$.*

Natural integer	*Set notation*
0	$\emptyset$
1	$\emptyset \cup \{\emptyset\} = \{\emptyset\}$
2	$\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$
3	$\{\emptyset \cup \{\emptyset\}\} \cup \{\{\emptyset \cup \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

2.3.7 Axiom of foundation

Every non-empty set contains an element with which it has no element in common.

$$\forall x \ (x = \ \emptyset \Longrightarrow \exists y \ (y \in x, x \cap y = \emptyset).$$

Corollary 2.3.1 *No set belongs to itself.*

2.4 Continuum Hypothesis

2.4.1 Equipotence

Definition 2.4.1 *Two sets E and F are equipotent if and only if there exists a bijective application between E and F.*

A set E is said to be subpotent to a set F if there exists an injection of E into F.

Proposition 2.4.1 *Equipotence is an equivalence relation denoted $\sim$.*

Example 2.4.1 *The application $f :]-1, 1[\to \mathbb{R}$ defined by*

$$f(x) = \frac{x}{1 - |x|},$$

is a bijection and we therefore have $]-1, 1[\sim \mathbb{R}$.

2.4.2 Finite/infinite sets

Definition 2.4.2 *For any natural integer n, we will denote by*

$$\mathbb{N}_n = \{x \in \mathbb{N} : x < n\} = \{0, ..., n-1\},$$

the set of the first n natural integers.

Definition 2.4.3 *We say that E is a finite set of cardinality n, when E is equipotent to $\mathbb{N}_n$. A set that is not finite is said to be finite.*

Remark 2.4.1 *The empty set is the unique finite set of cardinality* 0.

Proposition 2.4.2 *Any injection of a finite set into itself is a bijection.*

Proof. It suffices to show the result for the sets $\mathbb{N}_n$.

We reason by recurrence on $n \geq 1$.

For $n = 1$ the set $\mathbb{N}_n$ is reduced to the singleton $\{1\}$ and the only application of $\{1\}$ into itself is the identity which is a bijection.

Let $n \geq 2$ and f be an injection of $\mathbb{N}_n$ into itself. Let $m = f(n-1)$, we define the application g of $\mathbb{N}_{n-1}$ into itself by

$$g(i) = \begin{cases} f(i) & \text{if } f(i) < m \\ f(i) - 1 & \text{if } f(i) > m \end{cases}.$$

Then g is injective since $n-1$ does not belong to $\mathbb{N}_{n-1}$.

By hypothesis of recurrence g is surjective. By construction we have $Im(f) = Im(g) \cup \{n-1\}$ hence $Im(f) = \{0, 1, ..., n-1\}$. ■

Corollary 2.4.1 *Every finite set is in bijection with a unique interval $\{1, ..., n\}$ of $\mathbb{N}$.*

2.4.3 Countable set

Definition 2.4.4 *A set is said to be countable if and only if it belongs to the equivalence class of $\mathbb{N}$.*

Example 2.4.2 *Let $S = \{2k, k \in \mathbb{N}\}$ be the set of even integers. Let the application $f : \mathbb{N} \to S$ which has every integer k associates $2k$. The application f is bijective, the set S is countable.*

Example 2.4.3 *The set $\mathbb{Z}$ is countable as well as $\mathbb{Q}$.*

2.4.4 Power of the continuum

Definition 2.4.5 *A set has the power of the continuum if it belongs to the equivalence class of* $\mathbb{R}$.

Example 2.4.4 *The application* $f :]-1,1[\to \mathbb{R}$ *defined by*

$$f(x) = \frac{x}{1-|x|},$$

is a bijection and we therefore have $]-1,1[\sim \mathbb{R}$.

Theorem 2.4.1 *(Cantor) For any set* E *we have* $|E| < |P(E)|$.

Proof. Let f be an application of a set E to its set of subsets $P(E)$. Let D denote the subset of elements of E that do not belong to their image by

$$f : D = \{x \in E : x \notin f(x)\}.$$

We will show that the set D has no antecedent by the application f.

Let us suppose that there exists $y \in E$ such that $D = f(y)$ we then have two situations:

1- Let $y \in D$, but by construction of D we have $y \notin f(y) = D$ from which $y \notin D$.

2- Let $y \notin D = f(y)$, from which by definition we have $y \in D$.

Consequently, f is not surjective. ∎

Continuum Hypothesis: Every subset of the set of real numbers is either finite, countably infinite, or has the power of the continuum.

The following proposition is admitted without proof.

Proposition 2.4.3 ***(Paul Cohen 1963)*** *The continuum hypothesis is independent of the axiomatic set theory.*

Paul Cohen's proposal shows that one can accept or reject the continuum hypothesis without contradicting the axioms of set theory.

2.5 Axiom of choice

Axiom: For any set E, there exists a function which associates an element of this part with each non-empty part of E, in other words:

$$\begin{aligned} f \quad &: \quad \mathcal{P}(E)\backslash\{\emptyset\} \to \mathcal{P}(E)\backslash\{\emptyset\} \\ X \quad &\to \quad f(X) \in E. \end{aligned}$$

here are other equivalent formulations such as:

— For any equivalence relation $\mathcal{R}$, there exists a system of representatives of the classes of $\mathcal{R}$.

— The product of a family of non-empty sets is non-empty.

The axiom of choice is not part of the set of axioms of ZF set theory. We call ZFC theory, tthe ZF theory equipped in addition with the axiom of choice.

The two propositions below demonstrated in 1938 and 1963 affirm that we can accept or not the axiom of choice without being in contradiction with set theory.

Proposition 2.5.1 ***(Kurt Godel 1938)*** *ZF + AC is a coherent theory if ZF is.*

Proposition 2.5.2 ***(Paul Cohen 1963)*** *ZF +(not) AC is a coherent theory if ZF is.*

2.6 Corrected exercises

Exercise 2.6.1 ***(This exercise contributed by the author)***

Justify the following statements.

a) Let E be a set, A and B two subsets of E. If A is included in B, then the complement of B in E is included in the complement of A in E.

b) Let E be a set, A and B two subsets of E. If A and B are disjoint, then every element of E is either in the complement of A in E or in the complement of B in E.

c) Let E be a set, A a subset of E. Determine the following sets:

$$C_E\left(C_E A\right),\ A \cap C_E A,\ A \cup C_E A,\ C_E\emptyset,\ C_E E.$$

Solution:

a) Let $x \in \overline{B} = C_E B$ therefore $x \notin B$ and since $A \subset B$ therefore $x \notin A$ in other words $x \in \overline{A} = C_E A$, which shows that if $x \in \overline{B}$ then $x \in \overline{A}$.

b) If $x \in A$ then $x \notin B$ (Because $A \cap B = \emptyset$) so $x \in \overline{B} = C_E B$.

- If $x \notin A$ then $x \in \overline{A} = C_E A$.

c) We have

$$C_E \left(C_E A \right) = A, \ A \cap C_E A = \emptyset, \ A \cup C_E A = E, \ C_E \emptyset = E, \ C_E E = \emptyset.$$

Exercise 2.6.2 *Let E be a set and F and G two parts of E. Show that:*

$$1) \ F \ \subset \ G \Longleftrightarrow F \cup G = G.$$

$$2) \ F \ \subset \ G \Longleftrightarrow F \cap C_E G = \emptyset.$$

Solution:

Let E be a set and F and G two parts of E. We show that:

1) $F \subset G \Longleftrightarrow F \cup G = G$.

Suffice it to show

$$\begin{cases} F \subset G \Longrightarrow F \cup G = G ....(1) \\ F \cup G = G \Longrightarrow F \subset G ....(2) \end{cases}$$

- For (1), suppose $F \subset G$.

If $x \in F \cup G$, then $x \in F \subset G$ or $x \in G$ so in both cases $x \in G$. Consequently we have $F \cup G \subset G$.

If $x \in G$, then $x \in F \cup G$, therefore we have $G \subset F \cup G$.

Since $F \cup G \subset G$ and $G \subset F \cup G$, therefore we conclude that $F \cup G = G$.

We have shown that $F \subset G \Longrightarrow F \cup G = G$.

- Suppose $F \cup G = G$.

Let $x \in F$ then $x \in F \cup G$, so $x \in G$.

We have shown that $F \cup G = G \Longrightarrow F \subset G$.

Finally we have $F \subset G \Longleftrightarrow F \cup G = G$.

2) $F \subset G \Longleftrightarrow F \cap C_E G = \emptyset$.

Suffice it to show
$$\begin{cases} F \subset G \Longrightarrow F \cap C_E G = \emptyset ....(1) \\ F \cap C_E G = \emptyset \Longrightarrow F \subset G ....(2) \end{cases}$$

- Suppose $F \subset G$.

If $x \in F \cap C_E G$ then $x \in F$ and $x \notin G \supset F$ then $x \notin F$.

We have $x \in F$ and $x \notin F$ which is impossible, therefore $F \cap C_E G = \emptyset$.

We have shown that $F \subset G \Longrightarrow F \cap C_E G = \emptyset$.

Let's assume that $F \cap C_E G = \emptyset$.

Let $x \in F$

We assume that $x \notin G \Longleftrightarrow x \in C_E G$, which means that $x \in F \cap C_E G$ is impossible so hypothesis $x \notin G$ is false.

Consequently $x \in G$ and we have $F \subset G$.

We have shown that $F \cap C_E G = \emptyset \Longrightarrow F \subset G$.

Finally, wer have $F \subset G \Longleftrightarrow F \cap C_E G = \emptyset$.

Exercise 2.6.3 *We recall that for all parts A and B of a set E, we note:*

$$A \Delta B = (A \backslash B) \cup (B \backslash A) .$$

1) Show that for all parts A, B and C of a set E

- $(A \cap B) \cap \left(\overline{A \cap C}\right) = A \cap B \cap \overline{C}$.

- $(A \cap C) \cap \left(\overline{A \cap B}\right) = A \cap C \cap \overline{B}$.

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

Solution:

1) We show that $(A \cap B) \cap \left(\overline{A \cap C}\right) = A \cap B \cap \overline{C}$.

$$\begin{aligned} (A \cap B) \cap \left(\overline{A \cap C}\right) &= (A \cap B) \cap \left(\overline{A} \cup \overline{C}\right) \\ &= \left(A \cap B \cap \overline{A}\right) \cup \left(A \cap B \cap \overline{C}\right) \\ &= \emptyset \cup \left(A \cap B \cap \overline{C}\right) \\ &= A \cap B \cap \overline{C}. \end{aligned}$$

For the second one, just swap B and C.

2) We deduce that $(A\cap B)\,\Delta\,(A\cap C) = A\cap(B\Delta C)$.

By definition we have

$$\begin{aligned}(A\cap B)\,\Delta\,(A\cap C) &= A\cap(B\Delta C)\\ &= ((A\cap B)\setminus(A\cap C))\cup((A\cap C)\setminus(A\cap B))\\ &= \left((A\cap B)\cap\left(\overline{A\cap C}\right)\right)\cup\left((A\cap C)\cap\left(\overline{A\cap B}\right)\right)\\ &= \left(A\cap B\cap\overline{C}\right)\cup\left(A\cap C\cap\overline{B}\right)\\ &= A\cap\left(\left(B\cap\overline{C}\right)\cup\left(C\cap\overline{B}\right)\right)\\ &= A\cap((B\backslash C)\cup(C\backslash B))\\ &= A\cap(B\Delta C).\end{aligned}$$

Exercise 2.6.4 ***(This exercise contributed by the author)***

Let E be a set. By two different methods, show the following assertion:

$$\forall A, B\in\mathcal{P}(E)\ :(A\cap B = A\cup B)\Longrightarrow A = B.$$

Solution:

1) By "**Direct method**"

We suppose that A such that B are such that $A\cap B = A\cup B$. We must show that $A = B$.

For this given $x\in A$, let us show that it is also in B. As $x\in A$ then $x\in A\cup B$, therefore $x\in A\cap B$, because we have $A\cap B = A\cup B$. Consequently $x\in B$.

Now we assume $x\in B$, and the same reasoning implies $x\in A$.

So every element of A is in B and every element of B is in A, that means that $A = B$.

2) By "**Contrapositive method**"

We assume $A\neq B$ and we need to show that $A\cap B\neq A\cup B$.

If $A\neq B$ that means there is an element $x\in A\backslash B$ or then an element $x\in B\backslash A$.

Without losing generality, we suppose that there is $x\in A\backslash B$, then $x\in A\cup B$ but $x\notin A\cap B$, so we have $A\cap B\neq A\cup B$.

Exercise 2.6.5 *Let $f:\mathbb{N}^2\to\mathbb{N}$ be defined for all $(n,m)\in\mathbb{N}^2$ by $f(n,m) = n\times m$.*

Let $g:\mathbb{N}\to\mathbb{N}^2$ be defined for all $n\in\mathbb{N}$ by $g(n) = (n,(n+1)^2)$.

1) Is f injective?

2) Is f surjective?

3) Is g injective?

4) Is g surjective?

Solution:

Let

$$\begin{array}{rcl} f & : & \mathbb{N}^2 \to \mathbb{N} \\ (n,m) & \to & f(n,m) = n \times m \end{array}$$

and

$$\begin{array}{rcl} g & : & \mathbb{N} \to \mathbb{N}^2 \\ n & \to & g(n) = (n,(n+1)^2) \end{array}$$

1) Is f injective?

We have $f(1,2) = 1 \times 2 = 2 \times 1 = f(2,1)$, but $(1,2) \neq (2,1)$ so f is not injective.

2) Is f surjective?

We have $f(1,p) = 1 \times p = p$ so for all $p \in \mathbb{N}$, there exists $(n,m) = (1,p)$ such that $p = f(n,m)$, so f surjective.

3) Is g injective?

For all $n_1, n_2 \in \mathbb{N}$, we have

$$\begin{array}{rcl} g(n_1) & = & g(n_2) \Longrightarrow (n_1,(n_1+1)^2) = (n_2,(n_2+1)^2) \\ & \Longrightarrow & \left\{ \begin{array}{c} n_1 = n_2 \\ (n_1+1)^2 = (n_2+1)^2 \end{array} \right. \Longrightarrow n_1 = n_2. \end{array}$$

So g is injective.

4) Is g surjective?

We will show that $(1,1)$ does not admit an antecedent.

Suppose $(1,1) = (n,(n+1)^2)$, then we have

$$\left\{ \begin{array}{c} 1 = n \\ 1 = (n_2+1)^2 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{c} 1 = n \\ 1 = 2^2 \end{array} \right.$$

which is impossible so $(1,1)$ does not admit an antecedent, so g is not surjective.

Exercise 2.6.6 *Let $f:\mathbb{N}\to\mathbb{N}$ be defined for all $n\in\mathbb{N}$ by $f(n)=2n$.*

Let $g:\mathbb{N}\to\mathbb{N}$ be defined for all $n\in\mathbb{N}$ by $g(n)=E\left(\frac{n}{2}\right)$,where $E(x)$ denotes the integer part of $x\in\mathbb{R}$.

Are functions injective, surjective? Compare $f\circ g$ and $g\circ f$.

Solution:

Let

$$\begin{aligned} f &\;:\; \mathbb{N}\to\mathbb{N} \\ n &\;\to\; f(n)=2n \end{aligned}$$

and

$$\begin{aligned} g &\;:\; \mathbb{N}\to\mathbb{N} \\ n &\;\to\; g(n)=E\left(\frac{n}{2}\right) \end{aligned}$$

where $E(x)$ denotes the integer part of $x\in\mathbb{R}$.

1) Is f injective?

For all $n_1,n_2\in\mathbb{N}$, we have $f(n_1)=f(n_2)\Longrightarrow 2n_1=2n_2\Longrightarrow n_1=n_2$, then f is injective.

2) Is f surjective?

1 has no antecedent because there is no natural number n such that $1=2n$, so f is not surjective.

3) Is g injective?

We have $g(0)=E\left(\frac{0}{2}\right)=E\left(0\right)=0$ and $g(1)=E\left(\frac{1}{2}\right)=E\left(0\right)=0$ therefore $g(0)=g(1)$ but $0\neq 1$ which means that g is not injective.

4) Is g surjective?

For all $y=n\in\mathbb{N}$, there exists $x=2n\in\mathbb{N}$, such that $g(x)=E\left(\frac{x}{2}\right)=E\left(\frac{2n}{2}\right)=E\left(n\right)=n=y$, so g is surjective.

5) Comparison $f\circ g$ and $g\circ f$.

- If n is even, there exists $p\in\mathbb{N}$ such that $n=2p$, so we have

$$\begin{aligned} \left(f\circ g\right)(n) &= f(g(n))=f(g(2p)) \\ &= f\left(E\left(\frac{2p}{2}\right)\right)=f\left(E\left(p\right)\right) \\ &= f(p)=2p=n. \end{aligned}$$

- If n is odd, there exists $p \in \mathbb{N}$ such that $n = 2p+1$, so we have

$$\begin{aligned}
(f \circ g)(n) &= f(g(n)) = f(g(2p+1)) \\
&= f\left(E\left(\frac{2p+1}{2}\right)\right) = f\left(E\left(p+\frac{1}{2}\right)\right) \\
&= f(p) = 2p = n-1.
\end{aligned}$$

So

$$(f \circ g)(n) = \begin{cases} n & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}.$$

- Whether n is even or odd we have

$$\begin{aligned}
(g \circ f)(n) &= g(f(n)) = g(2n)) \\
&= E\left(\frac{2n}{2}\right) = E(n) \\
&= n.
\end{aligned}$$

So $(g \circ f)(n) = n = Id_{\mathbb{N}}$.

2.7 Suggested exercises

Exercise 2.7.1 *Check whether the following set definition can be adapted to the notion of couple:*

$$(a,b) = \{\{\emptyset, a\}, \{\emptyset, b\}\}.$$

Exercise 2.7.2 *Show that equipotence is an equivalence relation.*

Exercise 2.7.3 *Find an injective application from* $]0,1[$ *to* $]0,1[\times]0,1[$.

Exercise 2.7.4 *Find an injective application from* $]0,1[\times]0,1[[$ *to* $]0,1[$.

Exercise 2.7.5 *Find an injective application from* $\mathcal{P}(\mathbb{N})$ *to* $\mathbb{R}$.

Exercise 2.7.6 *Let* E *be a set and* $\mathbb{R}$ *be an equivalence relation on* E. *Let* $a, b \in E$, *show that we have either* $\widetilde{a} = \widetilde{b}$ *or* $\widetilde{a} \cap \widetilde{b} = \emptyset$, *where* $\widetilde{a}$ *designates the equivalence class of* a.

Exercise 2.7.7 *What do you think of the following reasoning:*

Let X be a set. The empty set is not included in X.

Exercise 2.7.8 *Let E, F be two sets and f be a map from E to F.*

Demonstrate that:

1) $\forall (A, B) \in \mathcal{P}(E)^2 : f(A \cup B) = f(A) \cup f(B)$.

2) $\forall (A, B) \in \mathcal{P}(E)^2 : f(A \cap B) \subset f(A) \cap f(B)$.

3) $\forall B \in \mathcal{P}(E) : f(f^{-1}(B)) \subset B$.

Exercise 2.7.9 *Let E, F be two sets and f an application of E in F. We put*

$$\begin{aligned} \overline{f} \quad &: \quad \mathcal{P}(E) \to \mathcal{P}(E) \\ X \quad &\to \quad \overline{f}(X) = f(X). \end{aligned}$$

1) $\overline{f}$ *injective* $\Leftrightarrow f$ *injective.*

2) $\overline{f}$ *surjective* $\Leftrightarrow f$ *surjective.*

Exercise 2.7.10 *Let E be a set, A and B two parts of E. Let the application*

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

1) Prove that: f *injective* $\Leftrightarrow A \cup B = E$.

2) Prove that: f *surjective* $\Leftrightarrow A \cap B = \emptyset$.

3) Under what condition is f bijective? Then explain f^{-1}.

Exercise 2.7.11 *Show that $\mathbb{R} \backslash \mathbb{Q}$ is not countable.*

Chapter 3

Good order and proof by recurrence

In mathematics, reasoning by recurrence (or by induction, or complete induction) is a form of reasoning aimed at proving a property relating to all natural numbers. The property of recurrence is deduced from that of good order. The objective of this chapter is to present in detail the principle of good order, which is the proof by recurrence.

3.1 Proof by recurrence

3.1.1 Proof by simple recurrence

Theorem 3.1.1 *Let $P(n)$ be a predicate depending on an element n of $\mathbb{N}$.*

Suppose that $P(0)$ is true. ***(Initialization)***

Suppose also that for all integers n the implication $P(n) \Rightarrow P(n+1)$ is true. ***(Heredity)***

Then the proposition $P(n)$ is true for all integers n.

Proof. We reason by the absurd.

Let $E = \{n \in \mathbb{N}, P(n) \text{ is false}\}$.

As a non-empty part of $\mathbb{N}$, the set E has a smallest element n_0.

n_0 is different from 0 because we have assumed $P(0)$ to be true as $0 < n_0$ we know that $n_0 - 1 \in \mathbb{N}$.

$P(n_0 - 1)$ is true because $n_0 - 1 \notin E$.

By hypothesis $P(n) \Longrightarrow P(n+1)$ from which $P(n_0)$ is true which contradicts the fact that $n_0 \in E$.

This method of demonstration uses the principle called: **"principle of good order".**

■

Example 3.1.1 *Let the sequence be defined by the recurrence relation*

$$\begin{cases} u_0 = \frac{1}{2} \\ u_{n+1} = \frac{1+u_n^2}{2}, \forall n \geq 0 \end{cases}.$$

We will show by recurrence that $(u_n)_{n\in\mathbb{N}}$ *is bounded above by* 1.

For $n = 0$ *we have* $u_0 = \frac{1}{2} \leq 1$.

We then assume that the proposition is true for n *and we demonstrate it for* $n+1$.

We will note that the terms of the sequence are positive.

$$0 \leq u_n \leq 1 \Longrightarrow u_n^2 \leq 1 \Rightarrow 1 + u_n^2 \leq 2 \Rightarrow \frac{1+u_n^2}{2} \leq \frac{2}{2} = 1.$$

3.1.2 Scheme of the proof by the principle of good order

1. Define the set $E = \{n \in \mathbb{N}, P(n) \text{ is false}\}$.

2. Assume that E is non-empty as a basis for a proof by contradiction.

3. Since N is well-ordered, there is a smallest element n_0 in E.

4. The smallest element cannot be that of the initial proposition. Using heredity to arrive at contradiction.

Example 3.1.2 *Let the sequence be defined by the recurrence relation*

$$\begin{cases} u_0 = \frac{1}{2} \\ u_{n+1} = \frac{1+u_n^2}{2}, \forall n \geq 0 \end{cases}.$$

We will show by the principle of good order that $(u_n)_{n\in\mathbb{N}}$ *is bounded above by* 1.

We reason by the absurd.

Let $E = \{n \in \mathbb{N}, u_n > 1\}$.

As a non-empty subset of $\mathbb{N}$, *the set* E *has a smallest element* n_0.

We have n_0 *different from* 0 *because we have* $u_0 = \frac{1}{2} \leq 1$.

Since $0 < n_0$ *we know that*$n_0 - 1 \in \mathbb{N}$ *and* $n_0 - 1 \notin E$.

$$0 \leq u_{n_0-1} \leq 1 \Longrightarrow u_{n_0-1}^2 \leq 1 \Rightarrow 1 + u_{n_0-1}^2 \leq 2 \Rightarrow \frac{1+u_{n_0-1}^2}{2} \leq \frac{2}{2} = 1 \Rightarrow u_{n_0} \leq 1 \Rightarrow u_{n_0} \notin E.$$

Which contradicts the fact that $n_0 \in E$.

3.1.3 Importance of initialization

Example 3.1.3 *Is* $3^{2n+4} - 2^n$ *a multiple of* 7*?*

Suppose that $3^{2n+4} - 2^n$ *is a multiple of* 7.

We will show that $3^{2(n+1)+4} - 2^{n+1}$ *is a multiple of* 7.

We have

$$\begin{aligned} 3^{2n+6} - 2^{n+1} &= 9 \times 3^{2n+4} - 2 \times 2^n \\ &= (7+2) \times 3^{2n+4} - 2 \times 2^n \\ &= 7 \times 3^{2n+4} + 2 \times 3^{2n+4} - 2 \times 2^n. \end{aligned}$$

We therefore have the sum of two multiples of 7 *which is therefore a multiple of* 7.

Here initialization is impossible for $n = 0$ *we have* $3^4 - 2^0 = 80$, *which is not divisible by* 7.

We can demonstrate using congruence calculus that $3^{2n+4} - 2^n$ *is not a multiple of* 7.

Indeed we have:

$3^2 \equiv 2[7] \Rightarrow 3^{2n} \equiv 2^n[7]$, *moreover we have* $3^4 \equiv 4[7]$ *hence* $3^{2n+4} \equiv 4.2^n[7]$.

We also have $2^n \equiv 2^n[7]$ *hence* $3^{2n+4} - 2^n \equiv 3.2^n[7]$.

As 7 *does not divide* 3 *nor* 2, *then* 7 *does not divide* $3^{2n+4} - 2^n$.

Remark 3.1.1 *To show that a proposition* $P(n)$ *is true for any integer* $n \geq n_0$, *we replace the initialization hypothesis by* $P(n_0)$ *is true.*

Example 3.1.4 *Proof by simple recurrence (with a step greater than* 1*)*

The Fibonacci sequence is given by

$$\begin{cases} F_0 = 0, \\ F_1 = 1, \\ \forall n \in \mathbb{N} : F_{n+2} = F_{n+1} + F_n. \end{cases}$$

Let

$$\varphi = \frac{1+\sqrt{5}}{2} \text{ and } \varphi' = \frac{1-\sqrt{5}}{2}$$

where φ is called the golden ratio.

We have φ and φ' are solution of the equation $x^2 - x - 1 = 0$.

Question: *Show that for all $n \geq 1$ we have $F_n \leq \varphi^{n-1}$.*

Answer: *For $n = 1$ we have*

$$F_1 = 1 \leq 1 = \varphi^0.$$

For $n = 2$ we have

$$F_2 = F_1 + F_0 = 1 \leq \frac{1+\sqrt{5}}{2} = \varphi^1.$$

We must then demonstrate that:

$$\forall n \geq 1 : P(n) \wedge P(n+1) \Rightarrow P(n+2).$$

We have by definition

$$\forall n \in \mathbb{N} : F_{n+2} = F_{n+1} + F_n \Rightarrow \forall n \in \mathbb{N} : F_{n+2} \leq \varphi^n + \varphi^{n-1} \text{ (By recurrence hypotheses),}$$

$$\forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n-1}(\varphi + 1) \Rightarrow n \in \mathbb{N} : F_{n+2} \leq \varphi^{n-1}(\varphi^2) \text{ (Because } \varphi^2 - \varphi - 1 = 0).$$

So $\forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n+1}$.

3.1.4 Proof by generalized recurrence

Theorem 3.1.2 *Let $P(n)$ be a proposition depending on an element n of $\mathbb{N}$.*

Assume that $P(0)$ is true. ***(Initialization).***

Also assume that for any integer n that the implication $(P(0) \wedge P(1) \wedge .... \wedge P(n)) \Rightarrow P(n+1)$ is true. ***(Heredity).***

Then the proposition $P(n)$ is true for all integers n.

Proof. Let the proposition $P(0) \wedge P(1) \wedge .... \wedge P(n) = Q(n)$.

We will show that $Q(n)$ is true for any value of $\mathbb{N}$ if and only if $P(n)$ is true for any value of $\mathbb{N}$.

Here we are showing an equivalence, so we must show two implications.

Implication N°1

We will show that if $Q(n)$ is true for any value of $\mathbb{N}$ then $P(n)$ is true for any value of $\mathbb{N}$.

We have $P(0) \wedge P(1) \wedge .... \wedge P(n)$ true, consequently $P(0)$ true and $P(1)$ true...and $P(n)$ true therefore $P(n)$ is true.

Implication N°2

We will show that if $P(n)$ is true for any value of $\mathbb{N}$ then $Q(n)$ is true for any value of $\mathbb{N}$.

Since $P(n)$ is true for any value of $\mathbb{N}$, hence $P(0) \wedge P(1) \wedge .... \wedge P(n)$ is also true and therefore $Q(n)$ is true for any value of $\mathbb{N}$. ■

Example 3.1.5 *Demonstrate that any integer n greater than or equal to 2 can be uniquely decomposed into a product of prime factors.*

Demonstration:

Let us denote by $P(n)$ the property: any integer k of $\{2, 3, 4....., n-1, n\}$ can be decomposed into a product of prime factors.

i) We have $P(2)$ is true because $2 = 2$.

ii) Suppose that $P(k)$ is true for all natural numbers $2 \leq k \leq n$. We must prove that $P(n+1)$ is true.

- If $n+1$ is prime we can write $n+1 = n+1$.

- If $n+1$ is not prime it therefore admits a prime divisor p and we have: $n+1 = q.p$.

We necessarily have $q \leq n$ and therefore according to (ii) q decomposes into a product of prime factors.

Consequently, $P(n+1)$ is true.

3.1.5 Proof by strong recurrence

Theorem 3.1.3 *Let P be a proposition depending on an element n of $\mathbb{N}$.*

If for all n we have: $\forall k < n : P(k) \Rightarrow P(n)$, then the proposition $P(n)$ is true for all integers n.

Proof. We perform the proof by generalized recurrence on n.

We have for $n = 0$.

$\forall k < 0 : P(k)$ This proposition is true because k belongs to the empty set.

We assume that the proposition $P(0) \wedge P(1) \wedge .... \wedge P(n)$ is true and we demonstrate that $P(n+1)$.

Since $P(0) \wedge P(1) \wedge .... \wedge P(n)$ is true then $\forall k < n+1 : P(k)$ is true.

From which we obtain $P(n+1)$ is true. ■

3.1.6 Special case of proof by recurrence (Cauchy recurrence)

Proposition 3.1.1 *Let $P(n)$ be a predicate that verifies:*

(i): $P(1)$ is true.

(ii): $\forall n \in \mathbb{N} : P(n) \Rightarrow P(2n)$.

(iii): $\forall n \in \mathbb{N} : P(n+1) \Rightarrow P(n)$.

Then P (n) is true for any value of n.

3.1.7 Proof of the Cauchy Scwhartz inequality by recurrence

Theorem 3.1.4 *Harmonic, geometric and arithmetic mean.*

Let $a_1, a_2, ..., a_n$ be positive real numbers, then

$$\frac{n}{\frac{1}{a_1} + .\frac{1}{a_2} + .. + \frac{1}{a_n}} \leq \sqrt[n]{a_1.a_2...a_n} \leq \frac{a_1 + a_2... + a_n}{n}.$$

Equality holds if and only if all a_i are equal

Proof. For $n = 2$, it must be established that $a_1 a_2 \leq \left(\frac{a_1+a_2}{2}\right)^2$, i.e. $(a_1 - a_2)^2 \geq 0$ which is true.

We will show $P(n) \Rightarrow P(n-1)$.

We put

$$A = \sum_{k=-}^{n-1} \frac{a_k}{n-1},$$

then

$$\left(\prod_{k=1}^{n-1} a_k\right) A \overset{P(n)}{\leq} \left(\sum_{k=1}^{n-1} \frac{a_k + A}{n}\right)^n = \left(\frac{(n-1)A + A}{n}\right)^n = A^n.$$

So

$$\prod_{k=1}^{n-1} a_k \leq A^{n-1} = \left(\sum_{k=1}^{n-1} \frac{a_k}{n-1}\right)^{n-1}.$$

We now demonstrate that $P(n) \Rightarrow P(2n)$.

$$\begin{aligned}
\prod_{k=1}^{2n} a_k &\leq \left(\prod_{k=1}^{n} a_k\right)\left(\prod_{k=n+1}^{2n} a_k\right) \\
&\overset{P(n)}{\leq} \left(\sum_{k=1}^{n} \frac{a_k}{n}\right)^n \left(\sum_{k=n+1}^{2n} \frac{a_k}{n}\right)^n \\
&\overset{P(2n)}{\leq} \left(\frac{\sum_{k=1}^{2n} \frac{a_k}{n}}{2}\right)^{2n} \\
&= \left(\frac{\sum_{k=1}^{2n} \frac{a_k}{n}}{2n}\right)^{2n}.
\end{aligned}$$

Left inequality deduces from the previous one considering $\frac{1}{a_1}, \frac{1}{a_2}, ..., \frac{1}{a_n}$. ■

3.2 Well-founded order

3.2.1 Order and strict order

Definition 3.2.1 *Let $\mathcal{R}$ be a binary relation on E.*

- *We say that $\mathcal{R}$ is reflexive when: $\forall x \in E, x\mathcal{R}x$.*
- *We say that $\mathcal{R}$ is symmetric when: $\forall (x,y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$.*
- *We say that $\mathcal{R}$ is anti-symmetric when: $\forall (x,y) \in E^2, x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y$.*
- *We say that $\mathcal{R}$ is transitive when: $\forall (x,y,z) \in E^3, x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$.*

Definition 3.2.2 *A binary relation is an order relation if it is reflexive, anti-symmetric and transitive.*

Example 3.2.1 *The set $\mathbb{R}$ provided with the usual order relation $\leq$.*

Example 3.2.2 *Over all the parts of a set, the relation $\subset$ is a relation of order.*

Definition 3.2.3 *A binary relation is a strict order relation if it is transitive and anti-reflexive.*

$$\mathcal{R} \text{ anti-reflexive} : \forall x \in E : x \not\mathcal{R} x.$$

Example 3.2.3 *The set $\mathbb{R}$ equipped with the strict order relation $<$.*

Proposition 3.2.1 *A strict order relation is anti-symmetric.*

Proof. $\mathcal{R}$ is by definition transitive and anti-reflexive.

A relation is anti-symmetric if it satisfies

$$\forall(x,y) \in E^2, (x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y.$$

We will show that in a strict order, relation the proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ is always false.

We reason by the absurd.

We suppose that it exists $(x,y) \in E^2$ such that the proposition $x\mathcal{R}y \wedge y\mathcal{R}$ is true. So by transitivity we obtain $x\mathcal{R}x$ is true which contradicts the fact that $\mathcal{R}$ is anti-reflexive.

Consequently, the proposition $x\mathcal{R}y \wedge y\mathcal{R}$ is always false and therefore the logical involvement $(x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$ is always true. ■

Definition 3.2.4 *Let $(E,\mathcal{R})$ be an ordered set. Two elements x and y are said to be comparable if we have $x\mathcal{R}y$ or $y\mathcal{R}x$. Otherwise we say that x and y are incomparable.*

Example 3.2.4 *Let the set $\mathcal{P}(\{a,b,c\})$ be the set of parts of $\{a,b,c\}$ equipped with the order relation $\subset$.*

The elements $\{a,b\},\{b,c\}$ are incomparable.

Definition 3.2.5 *An order $\mathcal{R}$ on E is said to be total if two elements are always comparable*

$$\forall(x,y) \in E, x\mathcal{R}y \text{ or } y\mathcal{R}x.$$

An order that is not total is said to be partial.

Definition 3.2.6 *A strict order is said to be strict total if two distinct elements are always comparable*

$$\forall(x,y) \in E, x \neq y \Rightarrow x\mathcal{R}y \text{ or } y\mathcal{R}x.$$

Remark 3.2.1 *In what follows we will note an order relation by $\preceq$ a strict order relation by $\prec$.*

3.3 Majorants, Minorants, Minimums and Maximums

Definition 3.3.1 *Let $(E, \preceq)$ be an ordered set and F a non-empty subset of E.*

We say that $x \in E$ is a ***minorant*** *of F if we have*

$$\forall y \in F, x \preceq y.$$

If the minorant of F is an element of F we say that it is the smallest element or the ***minimum*** *of F.*

Definition 3.3.2 *We say that $x \in E$ is a* ***majorant*** *of F if we have*

$$\forall y \in F, y \preceq x.$$

If the majorant of F is an element of F we say that it is the largest element or the ***maximum*** *of F.*

Definition 3.3.3 *Let $(E, \preceq)$ be an ordered set and F be a non-empty part of E.*

- An element x is a minimal element of F when no element of F is strictly smaller than x

$$\forall y \in F, y \preceq x \Longrightarrow x = y.$$

- An element x is a maximal element in F when no element of F is strictly greater than x

$$\forall y \in F, x \preceq y \Longrightarrow x = y.$$

Remark 3.3.1 *If the relation is of total order then the notions of minimal element and minimum coincide. (Same remark for the notion of maximal element and maximum).*

Example 3.3.1 0 *is a minimal element of $(\mathbb{N}, \leq)$ it is also its minimum.*

Example 3.3.2 *Let the set $P(\{a, b, c\})\backslash\{\emptyset\}$ be equipped with the partial order relation $\subset$.*

The elements $\{a\}, \{b\}, \{c\}$ are minimal elements but there is no minimum.

3.3.1 Order product (lexicographic order)

Let $(E, \preceq_E)$ and $(F, \preceq_F)$ be two ordered sets. Consider the product set $E \times F$ and define the lexicographic order $\preceq_{lex}$ by

$$\forall (x,y) \in E \times F, \forall (x',y') \in E \times F, (x,y) \preceq_{lex} (x',y') \Leftrightarrow \begin{cases} x \preceq_E x' \\ \text{or} \\ x = x' \text{ and } y \preceq_E y' \end{cases}.$$

If $\preceq_E$ and $\preceq_F$ are total order relations then the lexicographic order is also.

Example 3.3.3 *The lexicographic order on the set $\mathbb{N}^2$ is defined by*

$$\forall (x,y) \in \mathbb{N}^2, \forall (x',y') \in \mathbb{N}^2, (x,y) \preceq_{lex} (x',y') \Leftrightarrow \begin{cases} x \leq_{\mathbb{N}} x' \\ or \\ x = x' \textit{ and } y \leq_{\mathbb{N}} y' \end{cases}.$$

3.3.2 Well-founded order

Definition 3.3.4 *Let $(E, \preceq)$ be a set ordered by a total order relation.*

We say that $\preceq$ is well-founded when there is no strictly decreasing infinite sequence of elements of E.

Remark 3.3.2 *We also say that the set E is well ordered.*

Example 3.3.4 *The usual order on $\mathbb{N}$ is well-founded but not on $\mathbb{Z}$ nor $\mathbb{R}^+$.*

Example 3.3.5 *The lexicographic order on $\mathbb{N}^2$ is well-founded.*

Theorem 3.3.1 *Let $(E, \preceq)$ be an ordered set. The order $\preceq$ is well-founded if and only if every non-empty part $F \subset E$ admits a minimum.*

Remark 3.3.3 *Let $(E, \preceq)$ we can associate with the order relation $\preceq$ a strict order relation by the following definition*

$$x \prec y \textit{ if and only if } x \preceq y \textit{ and } x \neq y.$$

Remark 3.3.4 *Let $(E, \prec)$ we can associate with the order relation $\prec$ an order relation by the following definition*

$$x \preceq y \textit{ if and only if } x \prec y \textit{ or } x = y.$$

3.4 Proof by induction

The proof by induction allows us to generalize the proof by recurrence to any well-ordered set. The principle of the proof is as follows.

Theorem 3.4.1 *Let $(E, \preceq)$ be a well-ordered set. Let e denote the minimal element of E.*

Let $P(x)$ be a proposition depending on the elements $x \in E$.

(i) Assume that $P(e)$ is true. ***(Initialization)***

(ii) Assume also that $\forall y \prec x : P(y) \Rightarrow P(x)$ is true. ***(Heredity)***

Then the proposition $P(x)$ is true for all $x \in E$.

Theorem 3.4.2 *Let $(E, \preceq)$ be an ordered set. Order $\preceq$ is well-founded if and only if the principle of induction is correct.*

Proof. We will only demonstrate that if the order is well-founded then the principle of induction is correct.

We reason by the absurd, we assume that $P(x)$ verifies properties (i) and (ii) and that there exist elements of E which do not verify $P(x)$.

Let $A = \{x \in E, P(x) \text{ is false}\}$.

A is therefore a non-empty subset of E.

As the order is well founded, the set A has a minimal element x_0.

Consequently for any element $y \prec x_0$ we have $P(y)$ true by definition.

By applying the principle of heredity we obtain $P(x_0)$ true which constitutes a contradiction. ■

Example 3.4.1 *We consider the sequence $S_{m,n}$ defined on $\mathbb{N}^2$ by $S_{0,0} = 0$ and the following relation:*

$$S_{m,n} = \begin{cases} S_{m-1,n} + 1 \text{ if } n = 0, \\ S_{m,n-1} + 1 \text{ otherwise.} \end{cases}$$

We will show that for any pair $(m, n) \in \mathbb{N}^2, S_{m,n} = m + n$.

Initialization: *We start by proving the property for the element $(0, 0)$*

We have $S_{0,0} = 0 = 0 + 0$ verified.

Heredity: *We show that if the property is true for any pair $(m', n') \prec (m, n)$ then it is true for (m, n).*

We therefore assume that we have

$$\forall (m', n') \prec (m, n) : S_{m',n'} = m' + n'.$$

We distinguish two cases:

Case 1: *If $n = 0$*

In this case we have by definition $S_{m,0} = S_{m-1,0} + 1 \overset{Hypothesis}{=} m - 1 + 1 = m + 0$.

Case 2: *If $n \neq 0$*

In this case we have by definition $S_{m,n} = S_{m,n-1} + 1$. We also have $(m, n-1) \prec (m, n)$ so by hypothesis we have $S_{m,n-1} = m + n - 1$. Hence

$$S_{m,n} = S_{m,n-1} + 1 = m + n - 1 + 1 = m + n.$$

3.5 Zermelo's general good order theorem

3.5.1 Preorder

Definition 3.5.1 *A preordered set is a set E equipped with a binary relation $\mathcal{R}$ whicht is reflexive and transitive. We say that the relation $\mathcal{R}$ is a preorder relation.*

- A preordered set is totally proordinate if we have $x\mathcal{R}y$ or $y\mathcal{R}x$ for all x and y in E.

Example 3.5.1 *The set of relative integers $\mathbb{Z}$ equipped with the relation of divisibility between integers:*

$$x\mathcal{R}y \Leftrightarrow x \text{ divides } y.$$

The relation $\mathcal{R}$ is a preorder relation but is not an order relation.

Example 3.5.2 *Between real functions of a real variable, domination is a preorder.*

We will use the notation $\preceq$ for the preorder relation.

Definition 3.5.2 *Two elements x and y of a preordered set E which are such that $x \preceq y$ and $y \preceq x$ are said to be equivalent.*

The notion of equivalence defined previously is in fact an equivalence relation on E. Thus, each preorder relation is associated with an equivalence relation.

Definition 3.5.3 *Let A be a part of a preordered set E.*

The closure of A denoted A^+ is the set defined by

$$A^+ = \{x \in E : \exists y \in A, x \preceq y \wedge y \preceq x\}.$$

The set A is said to be closed if $A = A^+$.

Definition 3.5.4 *Let x and y be two elements of the preordered set E. We say that x is strictly smaller than y if $x \preceq y$ and if x is not equivalent to y.*

Definition 3.5.5 *Let $(E, \preceq)$ be a preordered set and A a non-empty subset of E.*

Definition 3.5.6 *We say that $m \in E$ is a **minorant** of A if every element of A is greater than x.*

$$\forall y \in F, m \preceq y.$$

*If the **minorant** of A is an element of A we say that it is the smallest element or minimum of F.*

*We say that $M \in E$ is a **majorant** of A if every element of A is smaller than M.*

$$\forall y \in F, y \preceq M.$$

*If the **majorant** of A is an element of A we say that it is the largest element or maximum of F.*

Remark 3.5.1 *If the maximum (resp. the minimum) when it exists is unique in the case of an order relation, this is not the case for a preorder relation. Indeed, there can be several equivalent minimums.*

Example 3.5.3 *Let the preorder relation of divisibility between relative integers and the set $A = \{-2, 2, 4, 8, -8\}$.*

We have two minimums 2 and -2 and two maximums 8 and -8.

Definition 3.5.7 *An "upper bound" (resp. "lower bound") (if it exists) of a part A of E is a smallest element of the set of upper bounds of A (resp. a largest element of the set of lower bounds of A).*

Remark 3.5.2 *Several equivalent upper (resp. lower) bounds may exist.*

Lemma 3.5.1 *Let E be a finite preordered set. Then there exists an increasing injective application $f : E \to \mathbb{N}$.*

Proof. We proceed by recurrence on the number of elements of E.

For $n = 1$ the proposition is verified.

Suppose that the proposition is verified for $n - 1$ and we prove for n.

Since E is finite and non-empty there necessarily exists a minimal element a of E. We put $F = E - \{a\}$.

By recurrence hypothesis, there exists an increasing injective application $\varphi : E \to \mathbb{N}$.

We define $f : E \to \mathbb{N}$. by setting $f(a) = 0$ and $f(y) = \varphi(y) + 1$ for all $y \in Y$. This application is injective and increasing. ■

Definition 3.5.8 *A preordered set E is well-preordered if every non-empty subset of E admits a smaller element.*

Note that a well-preordered set is totally preordered, and that any subset of a well-preordered set is well-preordered. A fundamental example well-preordered set (in fact well-ordered) is the set $\mathbb{N}$ of natural integers (ordered in the usual way).

Definition 3.5.9 *A preordered set is said to be "inductive" if every well-ordered part of E admits an upper bound.*

Remark 3.5.3 *An inductive preordered set cannot be empty, since the empty part of this set, which is well-ordered, must have an upper bound.*

Definition 3.5.10 *A sieve on a preordered set E is a part A of E such that $x \in A$ and $y \preceq x$ result in $y \in A$ (for all x and y in E). The fact that A is a sieve on E will be denoted by $A \lhd E$.*

It is immediate that the intersection of any family of sieves on E is still a sieve on E. Similarly, the union of any family of sieves on E is a sieve on E. Moreover, it is clear that every sieve is closed.

Lemma 3.5.2 *Let A, B be two sieves on a totally preordered set E, then either $A \lhd B$ or $B \lhd A$.*

Proof. Indeed, let us suppose for example that there exists $x \in A$ such that $x \notin B$. Let $y \in B$, we cannot have $x \preceq y$ otherwise we would have $x \in B$. We therefore have $y \leq x$ therefore $y \in A$ and $B \subset A$. We have therefore shown $A \subset B$ or $B \subset A$ but since these are sieves, then either $A \lhd B$ or $B \lhd A$. ■

Definition 3.5.11 *Let A be a subset of a preordered set E and let $a \in A$. We denote $a \prec_A$ as the smallest sieve on A containing a.*

It is clear that $a \prec_A$ is none other than the set $\{x \in A : x \prec a\}$ of elements of A strictly smaller than a.

3.6 Zorn's Lemma and the theorem of general good order

Lemma 3.6.1 *Let E be a preordered set, A and B two parts of E. If $A \lhd B \lhd E$, then for all $a \in A$ we have $a \prec_A = a \prec_B$.*

Theorem 3.6.1 ***(Zorn's lemma)*** *Every inductive preordered set has an element maximum.*

Theorem 3.6.2 ***(Zermelo)*** *On every set there exists a good order.*

Proof. Let E be a set. Let E denote the set of pairs (A, R) where A is a subset of E and R a good order relation on A. Let $(A, R) \preceq (B, R')$ denote the fact that $A \subset B$ and R' extends R. E is then an inductive ordered set (for any good-ordered subset of E, take the union of its elements). It therefore follows from Zorn's lemma that E has a maximal element (A, R). Such an element must necessarily verify $A = E$ (otherwise, add an element to A and decide that it is greater than all those of A). ■

Remark 3.6.1 *This good order is difficult to explain in most sets. For example, the set of rational numbers can be well-ordered by the lexicographic order. For the reals, no well-ordering relation has been established.*

3.7 Corrected exercises

Exercise 3.7.1 *Let X be a set. For $f \in \mathcal{F}(X,X)$, we define $f^0 = Id_X$ and by recurrence for $n \in \mathbb{N}$, $f^{n+1} = f \circ f^n$.*

1. *Show that: $\forall n \in \mathbb{N}$, $f^{n+1} = f \circ f^n$.*
2. *Show that if f is bijective then $\forall n \in \mathbb{N}$, $\left(f^{-1}\right)^n = \left(f^n\right)^{-1}$.*

Solution:

Let X be a set and

$$\begin{cases} f^0 = Id_X \\ f^{n+1} = f \circ f^n, \forall n \in \mathbb{N} \end{cases}.$$

1) We show that: $\forall n \in \mathbb{N}, \left(f^{-1}\right)^n = \left(f^n\right)^{-1}$

Let the proposition

$$P(n) : \forall n \in \mathbb{N}, f^{n+1} = f^n \circ f.$$

By proof byrecurrence we show that proposition $P(n)$ is true.

This proposition is true for $n = 0$ and we have

$$f = f \circ f^0 = f \circ Id_X = f.$$

For $n \in \mathbb{N}$, suppose $P(n)$ is true, then

$$\begin{aligned} f^{n+2} &= f^{n+1} \circ f \\ &= \left(f \circ f^n\right) \circ f \\ &= f \circ \left(f^n \circ f\right) \\ &= f \circ f^{n+1}. \end{aligned}$$

We used the definition of f^{n+2}, then proposition $P(n)$, then the associativity of composition, then the definition of f^{n+1}.

So $P(n+1)$ is true.

By the principle of recurrence we have $\forall n \in \mathbb{N}$, $f^{n+1} = f \circ f^n$.

2) We show that if f is bijective then $\forall n \in \mathbb{N}$, $\left(f^{-1}\right)^n = \left(f^n\right)^{-1}$.

We proceed in the same way by recurrence.

Let $P(n)$ be proposition $\forall n \in \mathbb{N}, \left(f^{-1}\right)^n = \left(f^n\right)^{-1}$.

This proposition is true for $n = 0$.

For $n \in \mathbb{N}$, suppose $P(n)$ is true, then

$$\begin{aligned} \left(f^{-1}\right)^{n+1} &= \left(f^{-1}\right)^n \circ f^{-1} \\ &= \left(f^n\right)^{-1} \circ f^{-1} \\ &= \left(f \circ f^n\right)^{-1} \\ &= \left(f^n \circ f\right)^{-1} \\ &= \left(f^{n+1}\right)^{-1}. \end{aligned}$$

So $P(n+1)$ is true.

By the principle of recurrence we have $\forall n \in \mathbb{N}, \left(f^{-1}\right)^n = \left(f^n\right)^{-1}$.

Exercise 3.7.2 *Let the sequence $(x_n)_{n\in\mathbb{N}}$ be defined by $x_0 = 4$ and $x_{n+1} = \dfrac{2x_n^2 - 3}{x_n + 2}$.*

1. *Show that: $\forall n \in \mathbb{N}$, $x_n > 3$.*
2. *Show that: $\forall n \in \mathbb{N}$, $x_{n+1} - 3 > \dfrac{3}{2}(x_n - 3)$.*
3. *Show that: $\forall n \in \mathbb{N}$, $x_n \geq \left(\dfrac{3}{2}\right)^n + 3$.*
4. *Is the sequence $(x_n)_{n\in\mathbb{N}}$ convergent?*

Solution:

Let the sequence $(x_n)_{n\in\mathbb{N}}$ be defined by

$$\begin{cases} x_0 = 4 \\ x_{n+1} = \dfrac{2x_n^2 - 3}{x_n + 2} \end{cases}.$$

1) We show by recurrence that : $\forall n \in \mathbb{N}$, $x_n > 3$.

Let the recurrence hypothesis be $H(n) : \forall n \in \mathbb{N}$, $x_n > 3$.

- Proposition $H(0)$ is true because $x_0 = 4 > 3$.

- Let $n \geq 0$, suppose $H(n)$ is true and show that $H(n+1)$ is then true

$$x_{n+1} - 3 = \frac{2x_n^2 - 3}{x_n + 2} - 3 = \frac{2x_n^2 - 3x_n - 9}{x_n + 2}.$$

By the recurrence hypothesis $x_n > 3$ therefore $x_n + 2 > 0$ and $2x_n^2 - 3x_n - 9 > 0$ (This by studying the function $x \mapsto 2x^2 - 3x - 9$ for $x > 3$). Therefore $x_{n+1} > 3$ and $H(n+1)$ is true.

We have shown that $\forall n \in \mathbb{N} : H(n) \implies H(n+1)$ and as $H(0)$ is true then $H(n)$ is varied whatever n.

2) Let us show that $x_{n+1} - 3 - \frac{3}{2}(x_n - 3)$ is positive.

$$\begin{aligned} x_{n+1} - 3 - \frac{3}{2}(x_n - 3) &= \frac{2x_n^2 - 3}{x_n + 2} - 3 - \frac{3}{2}(x_n - 3) \\ &= \frac{1}{2}\left(\frac{x_n\,(x_n - 3)}{x_n + 2}\right), \end{aligned}$$

this last term is positive because $x_n > 3$ therefore $x_{n+1} - 3 > \frac{3}{2}(x_n - 3)$.

3) Let us show by recurrence $\forall n \in \mathbb{N}$, $x_n \geq \left(\frac{3}{2}\right)^n + 3$.

Let the recurrence hypothesis be $G(n) : \forall n \in \mathbb{N}$, $x_n \geq \left(\frac{3}{2}\right)^n + 3$.

- Proposition $G(0)$ is true.

- Let $n \geq 0$, suppose $G(n)$ is true and show that $G(n+1)$ is true.

According to the previous question $x_{n+1} - 3 > \frac{3}{2}(x_n - 3)$ and by recurrence hypothesis $x_n \geq \left(\frac{3}{2}\right)^n + 3$, by combining these two inequalities we have

$$x_{n+1} - 3 > \frac{3}{2}\left(\frac{3}{2}\right)^n = \left(\frac{3}{2}\right)^{n+1}.$$

We conclude by summarizing the situation: $G(0)$ is true and $G(n) \implies G(n+1)$ whatever n, so $G(n)$ is always true.

4) The sequence $(x_n)_{n\in\mathbb{N}}$ tends towards $+\infty$ and is therefore not convergent.

Exercise 3.7.3 *Show using the principle of good order that*

$$\forall n \in \mathbb{N}^* : \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Solution:

Let the proposition be

$$P(n) : \forall n \in \mathbb{N}^* : \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

We reason by the absurd.

We assume that the proposition $P(n)$ is false for all values of $n \in \mathbb{N}^*$.

Let A denote the set of values of n for which the proposition $P(n)$ is false.

$$A = \left\{ n \in \mathbb{N}^* : \sum_{i=1}^{n} i \neq \frac{n(n+1)}{2} \right\}.$$

As $A \subset \mathbb{N}^*$ then it has a minimum noted n_0.

We know that $n_0 \neq 1$ because the proposition $P(n)$ is true for 1 in fact we have

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}.$$

So as $n_0 > 1$, we know that $n_0 - 1 \in \mathbb{N}^*$ and $P(n_0 - 1)$ is true because $n_0 - 1 \notin A$.

We then have

$$\begin{aligned} \sum_{i=1}^{n_0-1} i &= \frac{(n_0-1)(n_0-1+1)}{2} = \frac{(n_0-1)\,n_0}{2} \\ &\Longrightarrow \sum_{i=1}^{n_0-1} i + n_0 = \frac{(n_0-1)\,n_0}{2} + n_0 \\ &\Longrightarrow \sum_{i=1}^{n_0} i = \frac{n_0\,(n_0+1)}{2}. \end{aligned}$$

Hence $P(n_0)$ is true.

Which is a contradiction with the fact that $n_0 \in A$.

Exercise 3.7.4 *We consider the sequence S defined on $\mathbb{N}^2$ par $S_{1,1} = 5$ and the following relation:*

$$S_{m,n} = \begin{cases} S_{m-1,n} + 2 \text{ if } n = 1 \\ S_{m,n-1} + 2 \text{ Otherwise} \end{cases}$$

Show that for any pair $(m,n) \in \mathbb{N}^2, S_{m,n} = 2(m+n)+1$.

Solution

We use proof by induction

Let the proposition be defined by

$$P(m,n) : \forall (m,n) \in \mathbb{N}^2, S_{m,n} = 2(m+n)+1$$

We start by showing that the proposition is true for the minimum, that is to say $(1,1)$.

We have indeed: $S_{1,1} = 5 = 2(1+1)+1$, so the proposition $P(1,1)$ is true.

We now assume that the proposition is true for any value $(m', n') \prec (m,n)$ and we show that it is true for (m,n).

According to the definition of $S_{m,n}$ we have two cases:

Case No 1: if $n = 1$.

$$S_{m,n} \overset{definition}{=} S_{m-1,n} + 2 \overset{Hypothesis}{=} = 2(m-1+n)+1+2 = 2m+2n+1 \text{ (Verified).}$$

Case No 2: if $n \neq 1$.

$$S_{m,n} \overset{definition}{=} S_{m,n-1} + 2 \overset{Hypothesis}{=} = 2(m+n-1)+1+2 = 2m+2n+1 \text{ (Verified).}$$

3.8 Suggested exercises

Exercise 3.8.1 *Consider the sequence defined by:*

$$\begin{cases} u_0 = 2 \\ u_{n+1} = 1 + \dfrac{1}{1+u_n} \end{cases} .$$

Using two different methods, show that for any natural integer we have: $1 \leq u_n \leq 2$.

Exercise 3.8.2 *1. Let* $(E, \prec)$ *be a set with a strict order relation.*

Show that we can define an order relation on E.

2. Let $(E, \preceq)$ *be a set with an order relation.*

Show that we can define a strict order relation on E.

Exercise 3.8.3 *Suppose that* R *is a partial order on a set* E. *Show that every finite subset* $E \subset A$ *has a minimal element.*

Exercise 3.8.4 *Let $(E, \prec)$ be a set equipped with a strict order relation. Show that the lexicographic order relation induced by $\prec$ on the set E^n is a strict order relation.*

Exercise 3.8.5 *Using the principle of good order show that*

$$\forall n \in \mathbb{N} : 3/\left(n^3 - n\right), (3 \textit{ is a divisor of } \left(n^3 - n\right)).$$

Exercise 3.8.6 *Is there an order relation for which the following sets are well-ordered?*

$$1)\ \mathbb{N}^3$$
$$2)\ \mathbb{Q}$$

Exercise 3.8.7 *Let the predicates below take their values in $\mathbb{Z}$ and which verify:*

$$\begin{cases} P_1(0) \textit{ true} \\ \forall n \in \mathbb{Z} : P_1(n) \Longrightarrow P_1(-n) \end{cases}, \begin{cases} P_2(0) \textit{ true} \\ \forall n \in \mathbb{Z} : P_2(n) \Longrightarrow P_2(n-1) \end{cases},$$

$$\begin{cases} P_3(0) \textit{ true} \\ \forall n \in \mathbb{Z} : P_3(n) \Longrightarrow P_3(n+2) \\ \forall n \in \mathbb{Z} : P_3(n+1) \Longrightarrow P_3(n) \end{cases}, \begin{cases} P_4(0) \textit{ true} \\ \forall n \in \mathbb{Z} : P_4(n) \Longrightarrow P_4(n+1) \\ \forall n \in \mathbb{Z} : P_4(n+2) \Longrightarrow P_4(n) \end{cases}.$$

Say in each case if the predicate is true for all values of $\mathbb{Z}$? Demonstrate your assertion.

Exercise 3.8.8 *In each case give an order relation for which the following sets are well-ordered.*

$$\left\{\frac{n}{n+1} n \in \mathbb{N}\right\}, \mathbb{N} \times \mathbb{Z}, \left\{\frac{1}{n}, n \in \mathbb{Z}^*\right\}, \{2n, n \in \mathbb{N}\} \cup \{-2n-1, n \in \mathbb{N}\}.$$

Exercise 3.8.9 *Let A be a finite set with an order relation and f be a monotone function from A to A.*

1. Show that the function f admits at least one fixed point, i.e. a point $r \in A$ that satisfies $f(r) = r$.

2. Show that if there are several fixed points then there is a smallest fixed point that can be written in the form $f^k(x)$ where $x \in A$ and $k \leq Card(A)$.

Exercise 3.8.10 *Show that a preorder is an order if and only if the associated equivalence relation is equivalence.*

Bibliography

[1] **J. Champavère**, Logique des propositions et logique des prédicats. Note de cours, 2007.

[2] **R. David, K. Nour, and C. Raffalli,** *Introduction à la logique: Théorie de la démonstration*, 2ème édition, Dunod, 2019.

[3] **H.B. Enderton**, *Introduction to Logic,* Harcourt academic press, New York, 2013.

[4] **P. Halmos**, *Introduction à la théorie des ensembles*, Gauthier-Villars, Paris 1970.

[5] **R.E. Hodel,** *An Introduction to Mathematical Logic,* Duke University, 2013.

[6] **T. Lucas, I. Berlanger, and V. Degauquier,** *Initiation à la logique formelle avec exercices et corrigés,* 2014.

[7] **S. Mathieu-Soucy,** *Logique formelle et démonstrations au niveau universitaire,* Université du Québec à Montréal, Mai 2015.

[8] **P.P. Petkov,** *Mathematical Logic,* Sofia University, Bulgaria, 1990.