Université Paris 1 Panthéon-Sorbonne

Lecture notes

Master Mathematical Models in Economics and Finance (MMEF)

LOGIC AND SETS

Michel Grabisch

Source:

- Lecture notes of Stéphane Gonzalez
  `http://www.stephane.gonzalez.com/Logic-and-set/lecture _ notes.pdf`
  and Xavier Venel `https://sites.google.com/site/xaviervenelsite/course-materials`
- A first Course in Mathematical Logic and Set Theory, Michael L. O'Leary.
- Schaum's Outline of Set Theory and Related Topics, Seymour Lipschutz

Contents

Chapter 1

Classical logic

1.1 Symbolic logic

Definition 1. A *proposition* is a statement which is either true or false.

Example 1.

- "Paris is in France" or "2+2=4" (are true).
- "2+2=5" (is false).
- "What time is it?" is not a proposition.

Logic is all about propositions and relationships between them.

Definition 2. Let p and q be two propositions:

(i) $p \wedge q$, called the *conjunction* of p and q, is the proposition which is true if and only if p is true and q is true.

(ii) $p \vee q$, called the *disjunction* of p and q, is the proposition which is true if p is true or q is true.

(iii) $\neg p$, called the *negation* of p, is the proposition which is true if and only if p is false.

(iv) The *material implication* $p \to q$, "if p then q", is the abbreviation of the proposition $\neg p \vee q$ (which is true unless p is true and q is false).

(v) The *material equivalence* $p \leftrightarrow q$, "p if and only if q", is the abbreviation of the proposition $(p \to q) \wedge (q \to p)$.

We can use a truth value tabular to evaluate if a "complex" proposition is true or false. For example :

p	q	$p \wedge q$	$p \vee q$	$\neg p$	$\neg q$	$p \to q$	$q \to p$	$p \leftrightarrow q$	$p \vee \neg p$	$p \wedge \neg p$
T	T	T	T	F	F	T	T	T	T	F
T	F	F	T	F	T	F	T	F	T	F
F	T	F	T	T	F	T	F	F	T	F
F	F	F	F	T	T	T	T	T	T	F

Definition 3. A *tautology* is a proposition which is always true regardless of which valuation is used for the propositional variables.

Definition 4. The sentence "if p then q" or "p implies q" or "p is a sufficient condition for q" or "q is a necessary condition for p" or "p only if q" is denoted by the abbreviation: "$p \Rightarrow q$" which means:

$$\text{“}p \rightarrow q\text{” is true.}$$

Example 2. Let p and q be the two following propositions:

- p: "1=2" (false)
- q: "2=3" (false)

$p \rightarrow q$ is true (see truth table). Hence we can write $p \Rightarrow q$.

Definition 5. The sentence "p if and only if q" or "p is equivalent to q" or "p is a necessary and sufficient condition for q" is denoted by the abbreviation: "$p \Leftrightarrow q$" which means:

$$\text{“}p \leftrightarrow q\text{” is true.}$$

Theorem 1. Let p, q and r be three propositions. The following propositions are tautologies:

(i) $p \vee (\neg p)$

(ii) $p \leftrightarrow (\neg(\neg p))$

(iii) $(p \vee q) \leftrightarrow (q \vee p)$

(iv) $(p \wedge q) \leftrightarrow (q \wedge p)$

(v) $((p \vee q) \vee r) \leftrightarrow (p \vee (q \vee r))$

(vi) $((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r))$

(vii) $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$

(viii) $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$

(ix) $(p \vee q) \wedge r) \leftrightarrow (p \wedge r) \vee (q \wedge r)$

(x) $(p \wedge q) \vee r) \leftrightarrow (p \vee r) \wedge (q \vee r)$

Exercice : Find the negation of the proposition

"If there is a problem then there is a solution".

Solution :

"There is a problem and there is no solution"

hint: use Theorem 1(vii) and (ii) with the propositions p:"there is a problem", and q:"there is a solution".

1.2 First-order logic

We gave a mathematical formalism for the sentence: "Tuesday is a nice day". We would like now to construct from this sentence "Every day of the week is a nice day".

Definition 6 (Naive definition of a set)**.** A *set* is a well-defined collection of objects. The objects in a set are called its elements. If A is a set,

(i) $a \in A$ means that a belongs to the set A, or that a is an element of A, or that A contains a.

(ii) $a \notin A$ means that a does not belong to A or that a is not an element of A, or that A does not contain a.

Example 3. The easiest way to define a set is to list all elements. For example, $\{\alpha, \beta, \gamma\}$ is the set which contains the elements called α, β and γ.

Definition 7. A *predicate* on a set A is an expression which associates to every element $x \in A$ a proposition $p(x)$.

Definition 8 (Universal Quantifier)**.** Given the predicate $p(x)$ on A, "$\forall x \in A, p(x)$" is the proposition which is true if and only if $p(x)$ is true for every element $x \in A$.

Example 4.

- $\forall x \in \mathbb{R},\ x^2 \geq 0,$
- $\forall x \in \mathbb{R},\ x + 1 = 2.$

Definition 9 (Existential Quantifier)**.** Given the predicate $p(x)$ on A, "$\exists x \in A, p(x)$" is the proposition which is true if and only if $p(a)$ is true for at least one element $a \in A$.

Example 5. Let $p(\alpha), p(\beta)$ and $p(\gamma)$ be three propositions which define a predicate on the set $\{\alpha, \beta, \gamma\}$. We have "$\exists x \in \{\alpha, \beta, \gamma\}, p(x)$" if and only if $p(\alpha) \vee p(\beta) \vee p(\gamma)$.

Definition 10 (Negation of quantified statements)**.** The *negation* of quantified statements is based on the following rule:

(i) $\neg(\forall x \in A, p(x)) \Leftrightarrow (\exists x \in A, \neg p(x))$

(ii) $\neg(\exists x \in A, p(x)) \Leftrightarrow (\forall x \in A, \neg p(x))$

Example 6. Let $A = \{\text{Lucy, Matthew, Lisa}\}$ and $P(x)$ the predicate on A, "x wears a red shirt". Let us denote by $p =$"Lucy wears a red shirt", $q =$"Matthew wears a red shirt", $r =$"Lisa wears a red shirt", then we have

p	q	r	$\forall x \in A, P(x)$	$\neg(\forall x \in A, p(x))$	$\neg p$	$\neg q$	$\neg r$	$\exists x \in A, (\neg p(x))$
T	T	T	T	F	F	F	F	F
T	T	F	F	T	F	F	T	T
T	F	T	F	T	F	T	F	T
T	F	F	F	T	F	T	T	T
F	T	T	F	T	T	F	F	T
F	T	F	F	T	T	F	T	T
F	F	T	F	T	T	T	F	T
F	F	F	F	T	T	T	T	T

Definition 11. A predicate can concern several variables. Let p be a predicate on $A \times B$ and Q_A and Q_B be two quantifiers then

- $Q_A\ x \in A,\ p(x, y)$ is a predicate on B,
- $Q_B\ y \in B,\ Q_A x \in A,\ p(x, y)$ is a proposition.

Example 7.

- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x \leq y$,
- $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x \leq y$.

Proposition 1. Let p be a predicate on $A \times B$ then

$$\exists y \in B,\ \forall x \in A, p(x, y) \Rightarrow \forall x \in A, \exists y \in B,\ p(x, y).$$

Remark 1. The order of quantifiers (if of different types) is important. If they are all of the same type the order is not important.

Remark 2. (Negation of complex quantifiers) Let p be a predicate on $A \times B$, then

$$\begin{aligned} \neg\left(\forall x \in A,\ \exists y \in B, p(x, y)\right) &\Leftrightarrow \exists x \in A,\ \neg(\exists y \in B,\ p(x, y)), \\ &\Leftrightarrow \exists x \in A,\ \forall y \in B,\ \neg(p(x, y)). \end{aligned}$$

Example 8. Let f be a function on an interval I, the function is said to be continuous on I if

$$\forall x \in I, \forall \varepsilon > 0, \exists \delta > 0,\ \text{s.t. } \forall y \in]x - \delta, x + \delta[, |f(x) - f(y)| \leq \varepsilon.$$

By taking the negation and applying successively the rules of inference on the negations: f is not continuous on I if

$$\exists x \in I, \exists \varepsilon > 0, \forall \delta > 0,\ \text{s.t. } \exists y \in]x - \delta, x + \delta[, |f(x) - f(y)| > \varepsilon.$$

Chapter

2 Reasoning in mathematics

In this chapter, we will highlight several typical ways to prove a mathematical statement. The type of proof will depend on the statement.

The main statements that you can find are of the following form:

- Universal statement: For every .....,... (is true).
- Conditional statement: If ....(is true) then .... (is true).
- Existential statement: There exists ... such that ... (is true).
- Equivalence statement: ...(is true) if and only if ... (is true).

Remark 3. Universal statements and conditional statements are in fact very similar: "Every even number is followed by an odd number" is equivalent to "If n is an even number then it is followed by an odd number" (the quantifier is omitted in this last formulation).

Remark 4. In the process of writing a proof there are several levels of formalism: the intuition (where anything is allowed), a sketch of the proof with the order of the arguments, a detailed formal proof where each step is written properly.

2.1 Existential/Conditional statements and direct proof

We start by introducing direct proofs. The intuition is to follow the direction of the statement. The precise way will depend on the type of statements (conditional, existential or equivalence).

Our example will concern integers (denoted by $\mathbb{N}$), real numbers and divisibility. We first introduce the definitions that we will use.

Definition 12. Let p and n be two integers. We say that p is *dividing* n or that p is *a divisor of* n if there exists an integer k such that $n = kp$.

$$\exists k \in \mathbb{N},\ n = kp.$$

Definition 13. An integer n is *even* if 2 is a divisor of n. Otherwise, the integer is said to be *odd*.

Remark 5. Combining the two definitions, we obtain that the set of even numbers is

$$\{n, \text{ such that } n \in \mathbb{N} \text{ and } 2 \text{ is dividing } n\} = \{n, \text{ s.t. there exists } k \in \mathbb{N} \text{ and } n = 2k\}$$
$$= \{2k, k \in \mathbb{N}\}.$$

We will now look at two examples and give *direct proof* of the results.

Example 9. (Universal statement) For every number n divisible by 3, 9 is a divisor of n^2.

Example 10. (Conditional statement) Let n be an integer. If n is divisible by 3, then 9 is a divisor of n^2.

Since it is a conditional statement, the proof goes as follows: assume the hypothesis, deduce consequences logically until conclusion.

Proof. Let n be a number divisible by 3. We want to show that 9 is dividing n^2. By assumption, there exists $k \in \mathbb{N}$ such that

$$n = 3k.$$

It follows that $n^2 = (3k)^2 = 9k^2$. Since k^2 is an integer, 9 is dividing n^2. □

Example 11. (Existential statement) There exists a number divisible by 9 and 10.

Since it is an existential statement, the direct proof goes as follows: introduce a candidate, check that this candidate is indeed satisfying the conclusion.

Proof. Let us consider $x = 900$. We know that $x = 9 * 100$ so 9 is indeed a divisor of x. On the other hand $x = 90 * 10$, hence 10 is also a divisor of x.

Therefore there exists a number divisible by 9 and 10. □

Example 12. (Equivalence statement) Let n be an integer. n is divisible by 3 if and only if $n + 6$ is also divisible by 3.

There are two different ways to write a direct proof. The first one is to decompose the statement into two implications and prove each of them.

The second one is to assume one of the two assumptions and follow a chain of known equivalence. We will see such a proof in the next chapter.

2.2 More involved direct proofs

We now describe two reasonings that are often used in proofs. They are based on the following logic tautologies.

Theorem 2. Let p, q and r be three propositions, then

(i) Disjunction of case : $[(p \vee q) \wedge (p \to r) \wedge (q \to r)] \Rightarrow r$

(ii) Transitivity: $[(p \to q) \wedge (q \to r)] \Rightarrow (p \to r)$

Example 13. (Disjunction) Let a and b two real numbers. If $ab = 0$ then $a = 0$ or $b = 0$.

Proof. Let a and b be two real numbers such that $ab = 0$. Let us consider two cases:

- if $a = 0$ then the conclusion is true $a = 0$ or $b = 0$ and the implication is true.
- if $a \neq 0$ then $c = \frac{1}{a}$ is well defined and we can multiply the equality $ab = 0$ on both sides by c. We obtain

$$\begin{aligned} c(ab) &= c0 = 0 \\ \frac{1}{a}(ab) &= 0 \\ b &= 0 \end{aligned}$$

so the conclusion is true.

By disjunction of cases, we proved the result. □

Example 14. (Transitivity) For every integer n, if n is divisible by 3 then $(n+6)^2$ is divisible by 9.

Proof. We proved previously that

- for every integer n divisible by 3, n^2 is divisible by 9.
- for every integer n divisible by 3, $n + 6$ is divisible by 3.

Let n be an integer divisible by 3, then by the second statement (left to right implication), we know that $n + 6$ is also divisible by 3.

Applying now the first statement to $m = n + 6$, we know that $m^2 = (n + 6)^2$ is divisible by 9. It concludes the proof. □

2.3 Indirect proof

We now present two methods that are called indirect and that are linked to the two following logic formulae.

Theorem 3. Let p, q and r be three propositions, then

(i) Contrapositive: $(p \to q) \Leftrightarrow (\neg q \to \neg p)$,

(ii) Contradiction: $(p \to q) \wedge \neg q \Rightarrow \neg p$,

Remark 6. "$\neg q \to \neg p$" is called the contrapositive of "$p \to q$"

Proof. Let us prove the contrapositive formula. It suffices to prove that for all propositions p and q, the proposition $(p \to q) \leftrightarrow (\neg q \to \neg p)$ is true... use a truth table!!

p	q	$p \to q$	$\neg q$	$\neg p$	$\neg q \to \neg p$	$(p \to q) \to (\neg q \to \neg p)$	$(\neg q \to \neg p) \to (p \to q)$	$(p \to q) \leftrightarrow (\neg q \to \neg p)$
T	T	T	F	F	T	T	T	T
T	F	F	T	F	F	T	T	T
F	T	T	F	T	T	T	T	T
F	F	T	T	T	T	T	T	T

The proposition $(p \to q) \leftrightarrow (\neg q \to \neg p)$ is always true, hence $(p \to q) \Leftrightarrow (\neg q \to \neg p)$. □

Exercice : Find the contrapositive of the proposition

"If there is a problem then there is a solution".

Solution :

"If there is no solution then there is no problem" (Shadock's motto).

Example 15. (Contrapositive) Let n be an integer. If n^2 is odd then n is odd.

The proof by contrapositive goes as follows: assume that the conclusion is false and prove that the assumption is false.

Proof. Let us describe first what would happen with a direct proof: let $n \in \mathbb{N}$. Assume that there exists $k \in \mathbb{N}$ such that

$$n^2 = 2k + 1,$$

and we are stuck since we can not exploit the fact that n^2 is a square.

Let us prove this result by the contrapositive. The contrapositive of the formula is "if n is not odd then n^2 is not odd" or equivalently " if n is even then n^2 is even".

Let n be an even number. There exists $k \in \mathbb{N}$ such that $n = 2k$. Hence $n^2 = 4k^2 = 2*(2k^2)$ and n^2 is indeed even. □

Example 16. (Contradiction) Consider a right-angle triangle. We denote by c the length of the hypotenuse and by a and b the length of the two other sides. Then $c \leq a + b$.

The proof by contradiction goes as follows: assume that the statement is false and deduce a contradiction (that some other statement is both false and true).

Proof. We assume that

$$a + b < c.$$

Then by taking the square, we obtain that

$$a^2 + 2ab + b^2 < c^2$$

By Pythagoras' theorem, we know that $a^2 + b^2 = c^2$, hence $0 \leq 2ab < 0$. This is impossible, hence the contradiction. □

2.4 Induction

We denote by $\mathbb{N} = \{0, 1, \ldots\}$ the set of natural numbers. Elementary facts about the ordered set of natural numbers:

- (F1) Every $n \in \mathbb{N}$ has a successor $n+1$ s.t.

$$\forall m \in \mathbb{N}, n < m \Leftrightarrow n + 1 \leq m.$$

- (F2) 0 is the least number.
- (F3) For all $m \in \mathbb{N} \setminus \{0\}$, there exists $n \in \mathbb{N}$, such that $m = n + 1$.

Remark 7. There are different ways to construct the natural numbers:

- define real numbers and consider $\mathbb{N}$ as a subset of $\mathbb{R}$ and check that it satisfies the previous facts.
- define $\mathbb{N}$ by the previous facts and then define operations (addition, multiplication) on $\mathbb{N}$.

Weak principle of induction. Let $p(n)$ be a predicate on $\mathbb{N}$. Suppose the two following propositions hold

(i) $p(0)$ is true (basis)

(ii) $\forall\ n \in \mathbb{N},\ p(n) \Rightarrow\ p(n+1)$ (induction step).

Then for all $n \in \mathbb{N}$, $p(n)$ is true.

Remark 8. The weak principle of induction becomes a theorem if one admits the following property of $\mathbb{N}$: For all $A \subseteq \mathbb{N}$, if $0 \in A$ and for all $n \in A$, then $n + 1 \in A$ then $A = \mathbb{N}$.

Indeed, let $p(n)$ be a predicate on $\mathbb{N}$ such that $p(0)$ is true and $\forall\ n \in \mathbb{N},\ p(n) \Rightarrow\ p(n+1)$. Let

$$A = \{n \in \mathbb{N}, p(n) \text{ is true}\}.$$

By assumption $0 \in A$ and if $n \in A$ then $n + 1 \in A$. Therefore $A = \mathbb{N}$.

Example 17. Prove that $p(n) : 0 + 1 + \cdots + n = \sum_{t=0}^{n} t = \frac{n(n+1)}{2}$.

- Basis: $p(0)$ is true since $0 = 0$,
- Induction step: let $n \in \mathbb{N}$ such that $p(n)$ is true. Then

$$\begin{aligned} 0 + 1 + \cdots + (n+1) = \sum_{t=1}^{n+1} t &= \frac{n(n+1)}{2} + (n+1), \text{ by the induction assumption} \\ &= (n+1)\left(\frac{n}{2} + 1\right), \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Therefore, $p(n+1)$ is true.

- By the weak principle of induction, the formula is true for every $n \in \mathbb{N}$.

To be correct, the weak induction principle must be used with some precaution:

(i) The initialization step (basis) may start at some number $k \neq 0$.

Example 18. Prove that $n^2 \geq 3n$ for all $n \geq 3$.

- Basis: $p(3)$ is true since $9 \geq 9$,
- Induction step: let $n \geq 1$ such that $p(n)$ is true. Then

$$(n+1)^2 = n^2 + 2n + 1 \geq 3n + 2n + 1 \geq 3n + 3,$$

hence $p(n+1)$ is true.
- By the weak principle of induction, the formula is true for every $n \geq 3$. Observe that it is false for $n = 2$.

(ii) Be careful not to overlook the basis!

Example 19. Consider the property $p(n)$: n is greater than itself ($n > n$). From $p(n)$ it is easy to deduce $p(n+1)$: $n > n$ implies $n+1 > n+1$. However, $p(0)$ fails.

(iii) If the basis is $p(n_0)$, then do not forget to check that $p(n) \Rightarrow p(n+1)$ is shown for *every* $n \geq n_0$. The next example is Polya's proof that there is no horse of a different color. Find the mistake in the proof!

Example 20. For every $n \geq 1$, in a set of n horses, all horses have the same color.

Polya's proof:

- Basis $p(1)$: if there is only one horse, there is only one color.
- Induction step: assume that for any set of n horses, there is only one color. Take a set of $n+1$ horses, numbered $1, 2, \ldots, n+1$. Consider the sets $\{1, \ldots, n\}$, $\{2, \ldots, n+1\}$. Each set is of one color and since they overlap, $\{1, \ldots, n+1\}$ is of one color. Hence $p(n+1)$ holds.

The mistake is that the proof that $p(n) \Rightarrow p(n+1)$ is valid only for $n > 1$. Hence the step $p(1) \Rightarrow p(2)$ is missing.

Strong principle of induction. Let $p(n)$ be a predicate on $\mathbb{N}$. Suppose the two following propositions hold

(i) $p(0)$ is true (basis)

(ii) for all $n \in \mathbb{N}$, $(\forall m \leq n, p(m)) \Rightarrow p(n+1)$ (induction step).

Then for all $n \in \mathbb{N}$, $p(n)$ is true.

Example 21. Prove that any number $n \geq 2$ has a prime divisor.

- basis: $p(2)$ is true.
- Let $n \geq 2$ and assume that $p(2), \ldots, p(n)$ are true. Then, either $n+1$ is prime, in which case it has a prime divisor (itself). Or it is not, then there exist $2 \leq d < n+1$ which divides $n+1$. By induction hypothesis, d has a prime divisor, which is also a prime divisor of $n+1$.

Theorem 4. The strong principle of induction follows from the weak principle of induction.

Proof. Consider $p(n)$ and assume that (i) and (ii) hold in the strong induction principle. We denote by $q(n)$ the predicate ($\forall m \in \mathbb{N}$ s.t. $m \leq n,\ p(m)$). Let us show by using the weak induction principle that for every $n \in \mathbb{N}$ $q(n)$ is true.

- Basis: $q(0) = p(0)$, and therefore is true by (i).
- Induction step: let $n \in \mathbb{N}$, such that $q(n)$ is true. Then
  - for every $m \leq n$, $p(m)$ is true (by definition of $q(n)$)
  - $p(n+1)$ is true (by (ii)).

  Therefore $q(n+1)$ is true
- By the weak principle of induction, for every $n \in \mathbb{N}$, $q(n)$ is true, hence $p(n)$ is true.

$\square$

Least Number Principle (infinite descent of Fermat). The LNP states: If $M \subseteq \mathbb{N}$ and $M \neq \emptyset$, then M has a least element.

Example 22. (proof that $\sqrt{2}$ is irrational (discovered by the ancient Greeks))

By contradiction, suppose that $\sqrt{2}$ were rational: $\sqrt{2} = \frac{p}{q}$ with $p, q \in \mathbb{N}$. Then $2q^2 = p^2$. It follows that p^2 is even, and so is p. Hence, there exists $r \in \mathbb{N}$ such that $p = 2r$. Then

$$2q^2 = 4r^2$$

i.e., $q^2 = 2r^2$, and so q is even, i.e., $q = 2s$ for some integer s. We have obtained

$$\frac{p}{q} = \frac{r}{s}, \text{ with } r < p,\ s < q.$$

The same reasoning can be pursued on r, s, and so *ad infinitum*:

$$\begin{aligned} p > r > r' > r'' > \cdots \\ q > s > s' > s'' > \cdots \end{aligned}$$

which is not possible by the LNP.

Theorem 5. The Least Number Principle follows from the strong principle of induction.

Proof. We prove the result by contradiction. Assume that $M \subseteq \mathbb{N}$, $M \neq \emptyset$ and M has no least element.

Let $p(n)$ be the predicate defined on $\mathbb{N}$ by $p(n)$: "$n \notin M''$. We prove by the strong induction principle that $p(n)$ is true for all $n \in N$, which contradicts the assumption $M \neq \emptyset$.

- Basis: $p(0)$ holds, otherwise 0 would be the least element.
- Induction step: assume that $p(m)$ holds for every $m \leq n$. This means that $m \notin M$ for every $m \leq n$. Then $n < x$ for all $x \in M$, which by Fact F1 is equivalent to $n + 1 \leq x$ for all $x \in M$. It follows that $n + 1 \notin M$, otherwise it would be the least element of M, a contradiction. Hence, $p(n + 1)$ holds.

□

Theorem 6. The weak induction principle follows from the LNP.

Proof. Let $p(n)$ be a property such that $p(0)$ is true and $\forall n \in \mathbb{N}$, $p(n) \Rightarrow p(n+1)$. We prove that $\forall n \in \mathbb{N}$, $p(n)$, which amounts to showing that the class

$$M := \{n \in \mathbb{N} \text{ s.t } p(n) \text{ does not hold}\}$$

is empty. By the LNP, it is enough to show that M has no least element.

Suppose M has a least element, say m. Since $p(0)$ holds, $0 \notin M$, hence $m \neq 0$. Therefore, by (F3), there exists $n \in \mathbb{N}$ s.t. $m = n + 1$, hence $n < m$. Since m is a least element of M, $n \notin M$, i.e., $p(n)$ holds.

From our assumption, we have then $p(n + 1)$ holds, i.e., $p(m)$ holds, which means that $m \notin M$, a contradiction. □

As a consequence of Theorems 4, 5 and 6, all three principles are equivalent.

Chapter

3 Basic set theory

3.1 Basic definitions

Definition 14 (Naive definition of a set; this is Def. 6)**.** A *set* is a well-defined collection of objects. The objects in a set are called its *elements*. If A is a set,

(i) $a \in A$ means that a belongs to the set A, or that a is an element of A. Equivalently, we write $A \ni a$ (A contains a).

(ii) $a \notin A$ means that a does not belong to A or that a is not an element of A. Equivalently, we write $A \not\ni a$ (A does not contain a).

Example 23. Example of sets

- $A = \{1, 2, 4, 6\}$,
- $B = [a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$,
- $C = \{1, 2, 4, 2, 6, 2\} = \{2, 1, 4, 6\}$.
- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.
- $D = \{\{1, 2\}, 3, a, \{a, b\}\}$

Definition 15. A set A is a *subset* of a set B if every element of A is an element of B; one writes $A \subseteq B$ (A is included in B). Equivalently, we write $B \supseteq A$ (B includes A). Formally:

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \to x \in B).$$

Example 24.

- $\{1, 2\} \subset \{1, 2, Marc\}$,
- $\{1, 2, John\}$ is not a subset of $\{1, 2\}$.

Definition 16. Two sets A and B are *equal*, denoted by $A = B$, if $A \subseteq B$ and $B \subseteq A$.

Two sets which are equal contain the same elements. Whenever two sets are not equal we denote it by $A \neq B$. If $A \subseteq B$ and $A \neq B$, we have *strict inclusion*, denoted by $A \subset B$.[1]

In order to prove that two sets A and B are equal, we have two methods:

[1]Many textbooks write $\subset$ for inclusion and $\subsetneq$ for strict inclusion.

(i) Prove that $A \subseteq B$ and $B \subseteq A$: fix $a \in A$ and show that it is in B, then fix $b \in B$ and show that it is in A.

(ii) Fix an element x and show that $x \in A$ if and only if $x \in B$.

A set can be defined via a property (this is called *specification*). Let A be a set and P be a predicate on A. There exists a set denoted $\{x \in A, P(x)\}$ or $\{x \in A \mid P(x)\}$ or $\{x \in A \ : \ P(x)\}$ or $\{x \in A \text{ s.t. } P(x)\}$ whose elements are the elements of $x \in A$ such that $P(x)$ is true.

Example 25. Let X be the set of animals.

- $P(x)$: "the animal x has feathers", $\{x \in X, P(x)\}$ is the set of animals with feathers.
- $Q(x)$: "the animal x has 3 legs", $\{x \in X, P(x)\}$ is the set of animals with 3 legs.

By taking the predicate $P(x) : x \neq x$, we obtain the *empty set*, denoted by $\emptyset$:

$$\emptyset = \{x \in A, x \neq x\}.$$

This set contains no element, since the predicate is always false.

Theorem 7. If X is a set, then $\emptyset \subseteq X$.

Proof. Recall that $\emptyset \subseteq X$ is the proposition

$$\forall x, (x \in \emptyset \to x \in X).$$

Therefore its negation is $\exists x, x \in \emptyset \wedge x \notin X$. This proposition is false since the empty set has no elements. Hence the initial proposition is true. □

Remark 9. If the above naive approach to set theory is sufficient most of the time, it cannot be used as a basis for the foundations of mathematics, as many paradoxes can be built with this loose definition of a set. The most famous one was proposed by Bertrand Russel: consider the set defined by the property that it contains only sets which do not belong to themselves:

$$S = \{x \mid x \text{ is a set such that } x \notin x\}$$

Then if $S \notin S$, it should belong to S (i.e., $S \in S$), and if $S \in S$, then it should not belong to S (i.e., $S \notin S$). This is why a rigorous axiomatic approach to set theory was constructed by Zermelo, and completed by Fraenkel, referred usually as the Zermelo-Fraenkel (ZF) axiomatic set theory.

3.2 Constructing new sets from operations on sets

We will now list different operations that can be used on sets and define new sets.

Definition 17. Let A and B be two sets. One can define

(i) (Pairing)[2] The set $\{A, B\}$ is the set with 2 elements A and B:

$$x \in \{A, B\} \text{ if and only if } (x = A \text{ or } x = B).$$

(ii) (Union) The set $A \cup B$ is the set containing both the elements of A and the elements of B:

$$x \in A \cup B \text{ if and only if } (x \in A \text{ or } x \in B).$$

(iii) (Intersection) The set $A \cap B$ is the set containing the elements that are both in A and in B:

$$x \in A \cap B \text{ if and only if } (x \in A \text{ and } x \in B).$$

(iv) (Relative complement) The set $A \setminus B$ (or $A - B$) is the set containing the elements that are in A and not in B:

$$x \in A \setminus B \text{ if and only if } (x \in A \text{ and } x \notin B).$$

(v) (Complement) Suppose U is some universal set. If $A \subseteq U$,

$$A^c := U \setminus A.$$

(vi) (Symmetric difference) The set $A \Delta B$ is the set containing the elements in $A \cup B$ and not in $A \cap B$.

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

Example 26. Union, intersection and relative complement are quite straightforward. One must be careful with the pairing, especially when pairing a set with itself: a set A and the singleton $\{A\} = \{A, A\}$ are two different sets. For example,

- If $A = \emptyset$, the set $\emptyset$ does not contain any element, while the set $\{\emptyset\}$ contains exactly one element: the element $\emptyset$!
- $A = \emptyset$, $B = \{\emptyset\}$, $C = \{B\} = \{\{\emptyset\}\}$, are three different sets.
- $A = \{1, 2\}$, $B = \{2, 3\}$ and $\{A, B\} = \{\{1, 2\}, \{2, 3\}\}$.

With the previous propositions and the results that we have shown in the chapter on logic, we can show the following rules of computation. They are theorems, hence have to be "proved" from definitions and previous results.

Theorem 8. The union $\cup$ satisfies the following properties:

(i) $A \cup \emptyset = A$;

(ii) $A \cup B = B \cup A$;

(iii) $(A \cup B) \cup C = A \cup (B \cup C)$.

[2]In ZF, pairing is an axiom permitting to construct a new set from two sets.

Theorem 9. The intersection $\cap$ satisfies the following properties:

(i) $A \cap \emptyset = \emptyset$;

(ii) $A \cap B = B \cap A$;

(iii) $(A \cap B) \cap C = A \cap (B \cap C)$.

(iv) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(v) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Theorem 10 (De Morgan's laws)**.** Let A, B and C be three sets:

(i) $A \setminus \emptyset = A$

(ii) $\emptyset \setminus A = \emptyset$

(iii) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$ in particular $(A \cup B)^c = A^c \cap B^c$.

(iv) $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$ in particular $(A \cap B)^c = A^c \cup B^c$

Proof. As exercice. □

Theorem 11. The symmetric difference Δ satisfies the following properties:

(i) $A \Delta \emptyset = A$;

(ii) $A \Delta B = B \Delta A$;

(iii) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

(iv) $A \Delta A = \emptyset$

3.3 Family of sets

We have already seen with the pairing axiom that one can consider sets whose elements are also sets. These are "sets of sets", usually called "collections of sets" or "family of sets".

Example 27. Let $A = \{a, b\}$. We have:

- $\{\{a, b\}\}$ is a set with one element which is A.
- $\{\{a\}, \{a, b\}\}$ is a set with two elements.
- $\{\emptyset, \{a\}, \{b\}\}$ is a set with three elements.

In particular the following set, called the power set, is very important

$$\{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

It is the set of all subsets of A.

Definition 18. Given any set A, the set denoted by 2^A (or $\mathcal{P}(A)$) and called *power set of* A is defined[3] by:

$$B \text{ is a member of } 2^A \text{ if and only if } B \subseteq A.$$

Formally:

$$\mathcal{P}(A) = \{B, B \subseteq A\}$$

Note that we have always $\emptyset \in 2^A$ and $A \in 2^A$.

Example 28.

- $2^{\emptyset} = \{\emptyset\}$.
- $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.
- $2^{\{a,b,c\}} = \{\emptyset, \{a\}, \{b\}, \{a,b\}, \{c\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
- $\mathcal{P}(\mathbb{R})$ is the set of all subsets of $\mathbb{R}$.

We can now extend the notion of union and intersection to family of sets.

Definition 19. Let $\mathcal{F}$ be a family of sets. The union and intersection of all sets in the family is defined as follows:

$$\bigcup \mathcal{F} = \{x,\ \exists A(A \in \mathcal{F} \wedge x \in A)\}$$

and

$$\bigcap \mathcal{F} = \{x,\ \forall A(A \in \mathcal{F} \rightarrow x \in A)\}$$

Definition 20. Let $\mathcal{F}$ be a family of sets such that $\mathcal{F} = \{A_i, i \in I\}$. The union and intersection of all sets in the family is defined as follows:

$$\bigcup_{i \in I} A_i = \{x,\ \exists i(i \in I \wedge x \in A_i)\}$$

and

$$\bigcap_{i \in I} A_i = \{x,\ \forall i(i \in I \rightarrow x \in A_i)\}$$

Remark 10. When $\mathcal{F}$ can be indexed by some set I, both definitions are available and are equivalent (union and intersection).

With these two new definitions, we can extend De Morgan's Law and the distributivity formulas.

Theorem 12. Let $(A_i)_{i \in I}$ a family of sets and B a set:

- $(\bigcup_{i \in I} A_i)^c = \bigcap_{i \in I} A_i^c$,
- $(\bigcap_{i \in I} A_i)^c = \bigcup_{i \in I} A_i^c$,
- $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I}(B \cap A_i)$,
- $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I}(B \cup A_i)$.

[3]In ZF, this is an axiom saying that if A is a set, then 2^A is also a set.

3.4 Cartesian product

Definition 21 (Naive definition of an ordered pair)**.** An *ordered pair* (x, y), or simply a pair, is a list of two objects x and y given in a definite order; x is said to be the first (or left) coordinate of the pair, while y is the second (or right) coordinate.

A formal definition due to Kuratowski and using only sets is as follows: An ordered pair (x, y) is the set which contains the singleton $\{x\}$, and the pair $\{x, y\}$:

$$(x, y) = \{\{x\}, \{x, y\}\} \in 2^{2^{A\cup B}}.$$

As pairs are ordered, equality of pairs means equality of their components "coordinate-wise":

$$(a, b) = (c, d) \Leftrightarrow (a = c) \wedge (b = d).$$

In the Kuratowski's definition, this statement has to be proved[4].

Definition 22. The *Cartesian product* of two sets A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$, that is:

$$A \times B = \{x, (\exists a \in A)(\exists b \in B), x = (a, b)\}.$$

- If $A = B$ we simply denote $A \times A$ by A^2.
- The Cartesian product of three sets A, B and C, denoted $A\times B\times C$, is the abbreviation of the set $(A \times B) \times C$. The elements of $A \times B \times C$ are called the ordered triplets of A, B and C.

[4]Here is a proof:

- " $\Leftarrow$ " If $a = c$ and $b = d$, then $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Thus $(a, b) = (c, d)$.
- " $\Rightarrow$ ": Two cases:
  (i) If $a = b$:
  $$(a, b) = \{\{a\}, \{a, b\}\} = \{\{a\}, \{a, a\}\} = \{\{a\}\},$$
  $$(c, d) = \{\{c\}, \{c, d\}\} = \{\{a\}\}.$$
  Thus $\{c\} = \{c, d\} = \{a\}$, which implies $a = c$ and $a = d$. By hypothesis, $a = b$. Hence $b = d$.
  (ii) If $a \neq b$, then $(a, b) = (c, d)$ implies
  $$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}.$$
  – Suppose $\{a\} = \{c, d\}$. Then $c = d = a$, and so
  $$\{\{c\}, \{c, d\}\} = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}.$$
  But then $\{\{a\}, \{a, b\}\}$ would also equal $\{\{a\}\}$, so that $b = a$ which contradicts $a \neq b$.
  – Suppose $\{a\} = \{c\}$. Then $a = c$ and we have
  $$\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}\}$$
  Since $a \neq b$, we have $\{a, b\} = \{a, d\}$ and therefore $b = d$.

Proposition 2. (i) $A \times B = \emptyset$ is equivalent to $(A = \emptyset \vee B = \emptyset)$.

(ii) If $A \neq \emptyset$ and $B \neq \emptyset$ then

(a) $A \times B \subseteq A' \times B'$ is equivalent to $(A \subseteq A' \wedge B \subseteq B')$.

(b) $(A \times B) \cup (A' \times B) = (A \cup A') \times B$.

(c) $(A \times B) \cap (A' \times B) = (A \cap A') \times B$.

Proof. (i) $\neg(A = \emptyset \vee B = \emptyset) \Leftrightarrow (A \neq \emptyset \wedge B \neq \emptyset) \Leftrightarrow ((\exists a \in A) \wedge (\exists b \in B)) \Leftrightarrow ((a, b) \in A \times B) \Leftrightarrow \neg(A \times B = \emptyset)$

(ii) Let $A \neq \emptyset$ and $B \neq \emptyset$:

(a) "$\Rightarrow$": Suppose $A \times B \subseteq A' \times B'$. Let $a \in A$ and $b \in B$. By hypothesis $(a, b) \in A \times B$ implies $(a, b) \in A' \times B'$ which implies by definition of the cartesian product that: $(a \in A') \wedge (b \in B')$.

"$\Leftarrow$": Suppose $(A \subseteq A') \wedge (B \subseteq B')$. Let $x \in A \times B$, then $(\exists a \in A) \wedge (\exists b \in B)$ such that $x = (a, b)$, but $(A \subseteq A') \wedge (B \subseteq B')$ implies $(a \in A') \wedge (b \in B')$. Hence $x = (a, b) \in A' \times B'$.

□

Chapter 4

Functions

4.1 Definition of a function

Definition 23. • A *mapping* or *function* from the set A to the set B, denoted by $f : A \to B$, is a triplet $(A, B, graph(f))$ where A and B are two sets and $graph(f)$ is a subset of $A \times B$ such that for every $a \in A$, there is one and only one $b \in B$ such that $(a, b) \in graph(f)$:

$$[\forall x \in A, \exists y \in B, (x, y) \in graph(f)] \quad \wedge \quad [((a, b) \in graph(f) \wedge (a, c) \in graph(f)) \Rightarrow (b = c)].$$

In other words, for every $a \in A$ there is exactly one element denoted $f(a) \in B$ such that the ordered pair $(a, f(a)) \in graph(f)$.

- The set A is called the *domain* of f;
- The set B is called the *codomain* of f;
- The set $graph(f)$ is called the *graph* of f;
- The unique element $f(a)$ such that $(a, f(a)) \in graph(f)$ is called the *image* of a by f;
- If $C \subseteq A$, the set $f(C) := \{b \in B \mid \exists a \in C, (a, b) \in graph(f)\} = \{b \in B \mid \exists a \in C, b = f(a)\}$ is called the image of C by f.
- The set $f(A) := \{b \in B \mid (a, b) \in graph(f)\} = \{b \in B \mid \exists a \in A, b = f(a)\}$ [1] is called the image of f.

• We denote by B^A (or $\mathcal{F}(A, B)$) the set of functions from A to B.

Observe that:

$$graph(f) = \{(a, b) \in A \times B \mid b = f(a)\}.$$

Note that

- $C = \emptyset$ is equivalent to $f(C) = \emptyset$.
- If $f : A \to B$, $f(\{x\}) = \{f(x)\}$ for every $x \in A$.

[1] Observe that $f(A) \subseteq B$

Definition 24. Two mappings f and g from A to B are said to be *equal* if for every element $a \in A$ one has $f(a) = g(a)$.

Example 29. Here are some examples of mappings:

- The identity mapping on A, denoted by id_A, is the mapping from A to A defined by $id_A(a) = a$ for every $a \in A$.
- A mapping $f : A \to B$ is said to be constant if for every a and a' in A, one has
$$f(a) = f(a').$$
In other words, there exist an element $b \in B$ such that for every $a \in A$, $f(a) = b$.
- The mapping $proj_1 : A \times B \to A$ (resp. $proj_2 : A \times B \to B$) which associates to the pair (a, b) the element a (resp. b) is called the canonical projection of $A \times B$ on A (resp., B).
- Let $C \subseteq A$. The restriction of the mapping $f : A \to B$ to C is the mapping $f_{|C} : C \to B$ defined by $f_{|C}(x) := f(x)$ for every $x \in C$.
- Let $B \subseteq A$. The characteristic function of the set B is the function $\chi_B : A \longrightarrow \{0, 1\}$ defined by
$$\chi_B(a) = \begin{cases} 1, & \text{if } a \in B \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 3. Let $f : A \to B$ and let A_1, A_2 be two subsets of A. Then

(i) $A_1 \subseteq A_2$ implies $f(A_1) \subseteq f(A_2)$,

(ii) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$,

(iii) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

Note that the above inclusion may not be an equality. Find a counter-example.

Definition 25. The inverse image of $C \subseteq B$ by $f : A \to B$ is the set
$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}.$$

Proposition 4. Let $f : A \to B$ and let B_1, B_2 be two subsets of B. Then

(i) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$,

(ii) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

4.2 Injection, Surjection, Bijection.

Given a function f from A to B that associates to a an element $f(a)$, one could want to define an inverse function from B to A that associates to $f(a)$ the element a. Unfortunately, two problems may arise when trying to define such a function

- an element of B may not be in relation with any element in A.
- an element of B may be in relation with several elements in A.

It is interesting to focus on functions where at least one of these problems do not occur. This yields the two following definitions.

Definition 26. A mapping $f : A \to B$ is said to be *surjective (or onto)* if every point in B is the image of a point in A, that is

- $B = f(A)$,

  or equivalently

- for all $b \in B$, there exists $a \in A$, such that $f(a) = b$.

Informally, if f is surjective every element of B has at least one “pre-image” by f.

Example 30.

- $f : \mathbb{R} \to \mathbb{R}_+$ defined by $f(x) = x^2$ is surjective,
- $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not surjective.

Definition 27. A mapping $f : A \to B$ is said to be *injective (or one-to-one)* if two distinct elements of A have different images by f. That is,

- if $a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$,

  or equivalently

- if $f(a_1) = f(a_2)$ then $a_1 = a_2$ (by using the contrapositive).

Informally, if f is injective, every element of B has at most one “pre-image” by f.

Example 31.

- $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not injective,
- $f : \mathbb{R}_+ \to \mathbb{R}$ defined by $f(x) = x^2$ is injective.

Avoid the confusion between the definition of injectivity and the fact that every mapping has the property that $a_1 = a_2$ implies that $f(a_1) = f(a_2)$, which simply means that every element has a unique image.

Definition 28. A mapping $f : A \to B$ is said to be *bijective* if it is both surjective and injective.

Definition 29. Let $f : A \to B$ and $g : B \to C$. The *composition* of f by g is the mapping $g \circ f : A \to C$ defined by

$$g \circ f(a) = g(f(a)), \qquad \forall a \in A.$$

Proposition 5. Given $f : A \to B$, $g : B \to C$ and $h : C \to D$ then

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

Indeed let $a \in A$,

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

whereas

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

Recall the identity mapping id_A we defined in Example 29.

Definition 30. A mapping $f : A \to B$ is *invertible* if there exists a mapping $g : B \to A$ such that:

- $g \circ f = id_A$,
- $f \circ g = id_B$.

When the mapping g exists, it is unique. One denotes it by f^{-1}, and calls it the *inverse mapping* of f.

Proof. (Proof of uniqueness) Let us assume that f is invertible and there exists a least two mappings satisfying the assumptions:

- $g_1 : B \to A$ such that $g_1 \circ f = id_A$ and $f \circ g_1 = id_B$.
- $g_2 : B \to A$ such that $g_2 \circ f = id_A$ and $f \circ g_2 = id_B$.

We now prove that $g_1 = g_2$. Since $g_1 \circ f = g_2 \circ f$ we have, by composition by f,

$$(g_1 \circ f) \circ g_1 = (g_2 \circ f) \circ g_1.$$

Hence

$$g_1 \circ (f \circ g_1) = g_2 \circ (f \circ g_1),$$

which implies

$$g_1 \circ (id_B) = g_2 \circ (id_B).$$

Hence $g_1 = g_2$. □

Note that the notation f^{-1} may have two different meanings:

- **if $C \subseteq B$, $f^{-1}(C)$ is the inverse image of a set C and is always defined.**
- **if $y \in B$, then $f^{-1}(y)$ is the image of $y \in B$ by the inverse mapping and is only defined if f is invertible.**

Proposition 6. Let $f : A \to B$ be a function. Then f is injective if and only if for every $A_1, A_2 \subseteq A$, we have

$$f(A_1 \cap A_2) = f(A_1) \cap f(A_2).$$

Proof. $\Rightarrow$) the inclusion $\subseteq$ is always true. We show the inclusion $\supseteq$: let $y \in f(A_1) \cap f(A_2)$ and let us show that $y \in f(A_1 \cap A_2)$.

We have in particular that $y \in f(A_1)$, hence there exists $x_1 \in A_1$ such that $f(x_1) = y$. Similarly, we have $y \in f(A_2)$, hence there exists $x_2 \in A_2$ such that $f(x_2) = y$.

Since f is injective and $f(x_1) = f(x_2)$, we obtain $x_1 = x_2 =: x$ and x is both in A_1 and in A_2, therefore $x \in A_1 \cap A_2$. Hence there exists $x \in A_1 \cap A_2$ such that $f(x) = y$, which means $y \in f(A_1 \cap A_2)$.

$\Leftarrow$) Let $x \neq y$. We have immediately

$$\emptyset = f(\emptyset) = f(\{x\} \cap \{y\}) = f(\{x\}) \cap f(\{y\}),$$

which implies $f(x) \neq f(y)$. □

Proposition 7. Let $f : A \to B$ and $g : B \to C$.

- f and g injective $\Rightarrow$ $g \circ f$ injective
- f and g surjective $\Rightarrow$ $g \circ f$ surjective
- $g \circ f$ injective $\Rightarrow$ f injective
- $g \circ f$ surjective $\Rightarrow$ g surjective

Proof. As exercice. □

Proposition 8. A mapping $f : A \to B$ is bijective if and only if it is invertible.

Proof. $\Rightarrow$): For every $b \in B$, we consider the set

$$f^{-1}(\{b\}) = \{a \in A \text{ such that } f(a) = b\}.$$

Since f is surjective, we know that this set is non-empty. Since f is injective it is a singleton. We denote by $g(b)$ its unique element. By construction, for every $b \in B$, $g(b) \in f^{-1}(\{b\})$ so $f(g(b)) = b$. Moreover, for every $a \in A$, $f(a) \in \{f(a)\}$ so $a \in f^{-1}(\{f(a)\}) = \{g(f(a))\}$. Hence $g(f(a)) = a$.

$\Leftarrow$): Let $g : B \to A$ be a mapping which satisfies $f \circ g = id_B$ and $g \circ f = id_A$.

- id_A is bijective therefore it is injective. By Proposition 7, $g \circ f$ injective implies f injective.
- id_B is bijective therefore it is surjective. By Proposition 7, $f \circ g$ surjective implies f surjective. We conclude that f is bijective.

$\square$

Chapter 5

Relations

5.1 Definition of a binary relation

Definition 31. A *binary relation* $\mathcal{R}$ on a set A is a subset of the Cartesian product $A^2 = A \times A$.

If $(x, y) \in \mathcal{R}$, it is common to write $x\mathcal{R}y$, which is read "x is in relation with y (by $\mathcal{R}$)".

Example 32.

- Let E be a set. The *equality relation* on E, denoted by $=_E$, is the binary relation defined by

$$=_E := \{(x, x) \in E^2, x \in E\}$$

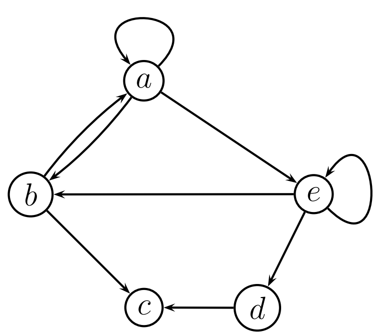
(diagonal of E^2). We write $x =_E y$ if $(x, y) \in =_E$, or more commonly $x = y$.

- $<$ on the set of real numbers is a relation.
- If X is the set of human beings, $x\mathcal{R}y$ if and only if x is a friend of y defines a relation on X.
- Consider $\mathbb{N}$ the set of natural numbers. We define the relation $\mathcal{R}$ "divide" by $a\mathcal{R}b$ if a divides b.
- Consider a set A. The the inclusion of sets, $\subseteq$, is a binary relation defined on 2^A.

One can represent a relation as a graph or a table. For example : the relation $\mathcal{R}$ on $\{a, b, c, d, e\}$ defined by

$$\mathcal{R} := \{(a, a), (e, e), (a, b), (b, a), (a, e), (b, c), (d, c), (e, b), (e, d)\},$$

can be represented as follows:



	a	b	c	d	e
a	1	1	0	0	1
b	1	0	1	0	0
c	0	0	0	0	0
d	0	0	1	0	0
e	0	1	0	1	0

Definition 32. Given a binary relation $\mathcal{R}$, we define the *dual relation* denoted by $\mathcal{R}^d$ as follows

$$\mathcal{R}^d = \{(x, y) \in A^2 \mid (y, x) \in \mathcal{R}\}$$

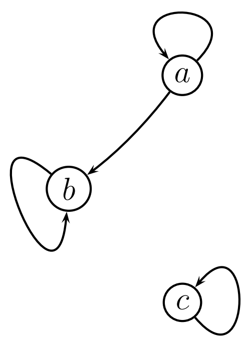
or equivalently $x\mathcal{R}^d y$ if and only if $y\mathcal{R}x$.

Definition 33. A relation $\mathcal{R}$ on A is said to be:

- *reflexive* if:

$$\forall x \in A, x\mathcal{R}x$$

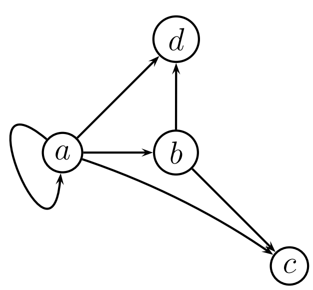
Example:



- *transitive* if:

$$\forall (x, y, z) \in A^3, (x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow (x\mathcal{R}z)$$

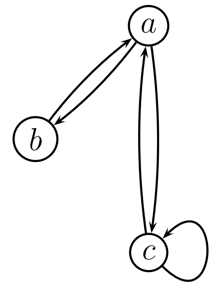
Example:



- *symmetric* if:

$$\forall (x, y) \in A^2, x\mathcal{R}y \Leftrightarrow y\mathcal{R}x.$$

Example:

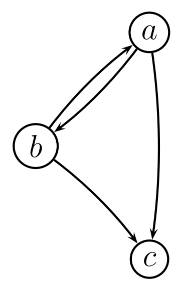


- *antisymmetric* if
$$\forall (x,y) \in A^2, x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y.$$

  Example: Let X be a set, one can see $\subseteq$ as an antisymmetric relation on 2^X.

- *complete* if
$$\forall (x,y) \in A^2, x\mathcal{R}y \vee y\mathcal{R}x \text{ is true.}$$

  Example:



5.2 Equivalence relation

Definition 34. An *equivalence relation* on E is a binary relation on E which is reflexive, symmetric, and transitive.

Example 33. Here are some standard examples of equivalence relations:

- The equality relation $=_E$.
- The equality between subsets of E, that is, the equality $=_{2^E}$.
- Given a set E and a mapping $u : E \to \mathbb{R}$ (think of a utility function), the relation $\mathcal{R}$ on E defined by $u(x) = u(y)$.

Definition 35. Let $\mathcal{R}$ be an equivalence relation on E and $x \in E$. The *equivalence class* of x for $\mathcal{R}$ is the subset of E:
$$\mathcal{R}(x) = \{y \in E \mid x\mathcal{R}y\}$$

If there is no ambiguity, the equivalence class of x if usually denoted by $[x]$.

Definition 36. We say that $\Pi \subseteq 2^E$ is a *partition* of a set E if it satisfies:

(i) Two distinct elements of Π are disjoint, that is:

$$\forall P \in \Pi,\ \forall Q \in \Pi,\ (P \neq Q) \Rightarrow (P \cap Q = \emptyset).$$

(ii) Every element x of E belongs to some $P \in \Pi$, that is

$$\bigcup_{P \in \Pi} P = E$$

Remark 11. In order to prove that some $\Pi \subset 2^E$ is not a partition, one has to prove one of the two following results:

- there exists $x \in E$ such that $x \notin \cup_{P \in \Pi} P$
- there exists $P \in \Pi$ and $Q \in \Pi$ such that $P \neq Q$ and $P \cap Q \neq \emptyset$.

Example 34. Let $E = \{1, 2, 3, 4, 5\}$. Then

- $\Pi = \{\{1, 2\}, \{3, 4\}, \{5\}\}$ is a partition.
- $\Pi = \{\{1, 2\}, \{3, 4\}\}$ is not a partition.
- $\Pi = \{\{1, 2\}, \{3, 4, 5\}, \{5\}\}$ is not a partition.

Proposition 9. Let $x, y \in E$ such that $x\mathcal{R}y$. Then $\mathcal{R}(x) = \mathcal{R}(y)$.

Proof. Let $x, y \in E$ such that $x\mathcal{R}y$. We show the equality by double inclusion. Let $z \in \mathcal{R}(x)$. By definition, we have

$$x\mathcal{R}z$$

Since $\mathcal{R}$ is symmetric, we know that $y\mathcal{R}x$. By transitivity, we deduce that $y\mathcal{R}z$ and thus $z \in \mathcal{R}(y)$. We prove similarly that if $z \in \mathcal{R}(y)$ the $z \in \mathcal{R}(x)$ and therefore the two sets are equal. □

Theorem 13. Let E be a set. The two following propositions are equivalent:

(i) Π is a partition of E.

(ii) There exists an equivalence relation $\mathcal{R}$ on E such that $\Pi = \{\mathcal{R}(x), x \in E\}$.

Proof. See Exercise. □

Definition 37. Let $\mathcal{R}$ be an equivalence relation on E. The *quotient set* of E by $\mathcal{R}$ is the set $E_{/\mathcal{R}}$ of equivalence classes[1] of $\mathcal{R}$, that is, the set:

$$E_{/\mathcal{R}} := \{\mathcal{R}(x), x \in E\} \subseteq 2^E.$$

[1]It is a partition of E.

5.3 Order relations

Definition 38.
- A *preorder* on E is a transitive and reflexive binary relation;
- An *order* on E is a reflexive, transitive and antisymmetric binary relation;
- A *total (or complete) preorder* on E is a reflexive, transitive and complete binary relation (and similarly for a complete or total order).

Instead of using the general notation $\mathcal{R}$, it is common to use the notation $\succcurlyeq$ (or similar) for orders and preorders. $x \succcurlyeq y$ reads "x is larger/greater than y", however, be careful that x, y are not necessarily numbers, and that $\succcurlyeq$ is not always the natural ordering of numbers (see examples below). We use the notation $x \succ y$ when $x \succcurlyeq y$ and $y \not\succcurlyeq x$.

An order is often called "partial order" to emphasize the fact that it may be not complete. Considering a partial order $\succcurlyeq$, if neither $x \succcurlyeq y$ nor $y \succcurlyeq x$ are true, then x, y are said to be *incomparable*.

Example 35.
- If E is a set, $\subseteq$ is an order relation on 2^E but not a total preorder: assume $E = \{1, 2\}$ then $\{1\}$ and $\{2\}$ are incomparable. It is a typical example of partial order.
- $=_E$ is the unique preorder on E which is an order relation and an equivalence relation.
- Taking $E = \mathbb{R}$, the natural ordering of numbers $\leq$ is a total order, defined by $x \geq y$ if $x - y \in \mathbb{R}_+$.
- Given a mapping $u : E \to \mathbb{R}$ (utility function), the relation $\mathcal{R}$ defined by $x \succcurlyeq y$ if $u(x) \geq u(y)$ is a complete preorder.
- Supposing E is finite and $\succcurlyeq$ is a partial order, it is convenient to represent E together with its order (denoted by $(E, \succcurlyeq)$) in a diagram, called *Hasse diagram*, with the following convention: 1) the nodes are the elements of E; 2) a link exists between x and y if $x \succcurlyeq y$, putting x above y; 3) Unnecessary links (reflexive, or which can be deduced by transitivity) are not represented.

  Example: $E = \{a, b, c, d, e\}$, with $\succcurlyeq$ defined by the matrix

	a	b	c	d	e
a	1	0	1	1	1
b	0	1	0	1	1
c	0	0	1	0	1
d	0	0	0	1	1
e	0	0	0	0	1

  It is easy to check that it is a (partial) order, and its Hasse diagram is given below.

Definition 39. Let $\succcurlyeq$ be an order on E, and $X \subseteq E$ a nonempty subset of E.

(i) $m \in E$ is a *lower bound* of X for $\succcurlyeq$ if for every element $x \in X$, we have $x \succcurlyeq m$. When X has a lower bound, it is said to be *bounded from below*.

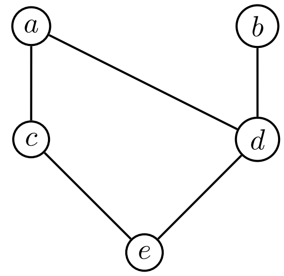


Figure 5.1: Hasse diagram of $(E, \succcurlyeq)$

(ii) $M \in E$ is an *upper bound* of X for $\succcurlyeq$ if for every element $x \in X$, we have $M \succcurlyeq x$. When X has an upper bound, it is said to be *bounded from above*.

Definition 40. Let $\succcurlyeq$ be an order on E, and $X \subseteq E$ a nonempty subset of E.

(i) $m \in X$ is a *minimal element* of X if no $x \in X$ satisfies $m \succ x$.

(ii) $M \in X$ is a *maximal element* of X if no $x \in X$ satisfies $x \succ M$.

Definition 41. Let $\succcurlyeq$ be an order on E, and $X \subseteq E$ a nonempty subset of E.

(i) $m \in X$ is a *least element* of X if for every $x \in X$ we have $x \succcurlyeq m$.

(ii) $M \in X$ is a *greatest element* of X if for every $x \in X$ we have $M \succcurlyeq x$.

Minimal, maximal elements, as well as least and greatest elements may not exist. However, if a least element (resp., a greatest element) exists, it is unique.

Definition 42. Let $\succcurlyeq$ be an order on E, and $X \subseteq E$ a nonempty subset of E.

(i) The *infimum* of X, denoted by $\inf X$ or $\bigwedge X$, is the greatest element of the set of lower bounds of X (greatest lower bound).

(ii) The *supremum* of X, denoted by $\sup X$ or $\bigvee X$, is the least element of the set of upper bounds of X (least upper bound).

Even if X is bounded from below (resp., from above), the infimum (resp, the supremum) may not exist.

Example 36.

- Taking $(E, \succcurlyeq)$ of Fig. 5.1, we have:
  - Taking $X = \{c, d\}$, e is the unique lower bound and hence the infimum, while a is the unique upper bound, hence its supremum. Observe that c, d are both minimal elements, and both maximal elements, and there is neither least nor greatest element.
  - Taking $X = \{a, b, d\}$, there is no upper bound (hence no supremum), but a unique lower bound (infimum) which is d (observe that it is also the least element of X). a, b are maximal, but there is no greatest element.

- Consider $\mathbb{N}$ with the natural ordering. Take X to be the set of prime numbers. It has no upper bound, no maximal element, its unique lower bound is 1, which is the infimum and the least element.

- Consider the power set 2^E with the inclusion relation. Take $A, B \in 2^E$ and consider $X = \{A, B\}$. Then the supremum of X is $A \cup B$ and the infimum of X is $A \cap B$.

The existence of infimum and supremum on $(\mathbb{R}, \geq)$ is a fundamental axiom of the real numbers (and not a theorem!).

Axiom 1 (Existence of supremum and infimum)**.** Consider $E = \mathbb{R}$, the natural ordering $\geq$, and $X \subseteq \mathbb{R}$ a nonempty subset of $\mathbb{R}$.

(i) If X is bounded from below, it has an infimum.

(ii) If X is bounded from above, it has a supremum.

Note that $\mathbb{Q}$ does not satisfy the supremum and infimum axiom (see exercises). An important property of supremum and infimum on $(\mathbb{R}, \geq)$ is the following.

Theorem 14 (Characterization of supremum and infimum)**.** Let $A \subseteq \mathbb{R}$ be nonempty and bounded from above. Then $L = \sup A$ if and only if L is an upper bound of A and

$$\forall \epsilon > 0, \exists a \in A, L - \epsilon < a \leq L.$$

Similarly, if $A \subseteq \mathbb{R}$ is nonempty and bounded from below, $L = \inf A$ if and only if L is a lower bound of A and

$$\forall \epsilon > 0, \exists a \in A, L + \epsilon > a \geq L.$$

Example 37. Consider $E = \mathbb{R}$ and the natural ordering.

- If $X = [a, b]$, a and b are the infimum and supremum respectively, and they are also least and greatest elements.

- If $X =]a, b[$, a, b are still infimum and supremum respectively, but there is no least and no greatest element.

Chapter

6 Cardinality

We recall that $\mathbb{N} = \{0, 1, \ldots\}$ is the set of natural numbers.

6.1 Cardinality of a set

We start with a simple observation.

Proposition 10. If $f : E \to \{1, \ldots, n\}$ and $g : E \to \{1, \ldots, p\}$ are two bijections, then $n = p$.

Proof.

(i) Suppose $p \geq n$. f is a bijection, then f^{-1} is a bijection, therefore $h_1 = g \circ f^{-1} : \{1, \ldots, n\} \to \{1, \ldots, p\}$ is a bijection. Hence h_1 is a surjection, therefore $\forall j \in \{1, \ldots, p\}, \exists i \in \{1, \ldots, n\}$ such that $h_1(i) = j$ which implies $n \geq p$. $\Rightarrow n = p$.

(ii) Suppose $n \geq p$, then applying the previous reasonning to $g^{-1} \circ f$ yields the same result.

□

Definition 43. A set E is *finite* if $E = \emptyset$ or if there exists $n \in \mathbb{N} \setminus \{0\}$ and a bijection $f : E \to \{1, \ldots, n\}$. Otherwise, E is said to be *infinite*.

By the previous Proposition, such an n is unambiguously defined. It is called the *cardinality* of E and is denoted by $|E|$. We put by convention $|\emptyset| = 0$. Observe that a subset of a finite set is also finite.

The next proposition gives elementary properties of the cardinality of finite sets.

Proposition 11. Suppose E to be finite, and consider A, B subsets of E. The following holds:

(i) $|A \cup B| = |A| + |B| - |A \cap B|$

(ii) $|A \setminus B| = |A| - |A \cap B|$

(iii) $|A^c| = |E| - |A|$

(iv) $|A \times B| = |A| \cdot |B|$

(v) $|2^A| = 2^{|A|}$.

So far, cardinality is not defined for infinite sets. The key point here is to proceed by comparison.

Definition 44. Two sets A and B *have the same cardinality (or same power) (or are equipotent)* if there is a bijection between A and B.

Remark 12. For two finite sets, the existence of a bijection between A and B implies that $|A| = |B|$, hence indeed they have same cardinality in both sense.

Example 38.

- $\mathbb{Z}^+, \mathbb{Z}^-$ have same cardinality by the bijection $f : \mathbb{Z}^+ \to \mathbb{Z}^-$, $z \mapsto -z$.
- The set $\mathbb{N}_o$ of odd natural numbers and the set $\mathbb{N}_e$ of even natural numbers have same cardinality by $f : \mathbb{N}_o \to \mathbb{N}_e$, $n \mapsto n - 1$ (assuming 0 is odd).
- More curiously, $\mathbb{N}_o$ (or $\mathbb{N}_e$) and $\mathbb{N}$ have same cardinality by $f : \mathbb{N} \to \mathbb{N}_o$, $n \mapsto 2n + 1$.

Definition 45. A set A has a *cardinality at least as large as* a set B if there is a bijection from B to a subset of A (equivalently, an injection from B to A).

Theorem 15. (Cantor-Schröder-Bernstein) If A has cardinality at least as large as B, and B has cardinality at least as large as A, then A and B have the same cardinality (are equipotent).

Definition 46. A set equipotent with $\mathbb{N}$ is said to be *countably infinite*. Sets being finite or countably infinite are called *countable*, otherwise they are *uncountable*.

The cardinality of $\mathbb{N}$ (and therefore of every countably infinite set) is denoted by $\aleph_0$ (aleph 0).

We give two elementary properties:

(i) Subsets of countable sets are countable.

(ii) If a set contains an uncountable subset, it is uncountable.

6.2 Generalized union and intersection

We consider a family of subsets $(A_i)_{i \in I}$ of X, where I is the index set.

(i) The union of the A_i's, denoted by $\bigcup_{i \in I} A_i$, is the set of all x belonging at least to one A_j, $j \in I$:

$$\bigcup_{i \in I} A_i = \{x \in X \mid \exists i \in I, x \in A_i\}.$$

(ii) The intersection of the A_i's, denoted by $\bigcap_{i \in I} A_i$, is the set of all x belonging to all A_j, $j \in I$:

$$\bigcap_{i \in I} A_i = \{x \in X \mid \forall i \in I, x \in A_i\}.$$

If I is finite (resp., countable, uncountable), we speak of finite (resp., countable, arbitrary) union or intersection.

By convention, we put $\cap_{i \in \emptyset} A_i = X$ and $\cup_{i \in \emptyset} A_i = \emptyset$ (reason: $\bigcap_{i \in I \cup J} A_i = \bigcap_{i \in I} A_i \cap \bigcap_{i \in J} A_i$).

6.3 Advanced properties of cardinality

Property 1. Countable unions of countable sets are countable.

Property 2. Finite Cartesian products of countable sets are countable.

In particular, the set of rational numbers $\mathbb{Q}$ is countable. Here is a direct proof, using the Cantor-Schröder-Bernstein theorem: write $q \in \mathbb{Q}$ as $q = \frac{n}{p}$ in irreducible form. Then consider the injection $f : \mathbb{Q} \to \mathbb{N}$ defined by

$$q = \frac{n}{p} \mapsto 2^n + 3^p$$

Since no 3^p can be a multiple of 2^n, this is an injection. Conversely, consider the injection $\mathbb{N} \to \mathbb{Q}$ given by $n \mapsto n$. Therefore, $\mathbb{Q}$ and $\mathbb{N}$ are equipotent.

Property 3. The set of all finite subsets of a countable set is countable.

Sketch of the proof: the argument is similar as with $\mathbb{Q}$. Given a finite subset of A, it can be coded by elements of $\mathbb{N}$, say $i_1, \ldots, i_n$. Then it suffices to consider the injection f mapping $\{i_1, \ldots, i_n\}$ to $2^{i_1} + \cdots + 2^{i_n}$.

Theorem 16. Let $I \subseteq \mathbb{R}$, and $f : I \to \mathbb{R}$ a nondecreasing function. Then f has at most countably many points of discontinuity.

Proof. For every $x \in I$, since f is nondecreasing:

$$\sup\{f(y) \mid y < x\} =: f(x_-) \leq f(x) \leq f(x_+) := \inf\{f(y) \mid y > x\},$$

f is continuous at x if $f(x_-) = f(x) = f(x_+)$. So, if x is a point of discontinuity, there exists $q_x \in \mathbb{Q}$ s.t. $f(x_-) < q_x < f(x_+)$ (as $\mathbb{Q}$ is dense in $\mathbb{R}$). Furthermore, if x, y are points of discontinuity with $x < y$, we have $q_x < q_y$. As $\mathbb{Q}$ is countable, so is the set of points of discontinuity. □

6.4 The cardinality of the continuum

G. Cantor showed that the real interval $[0, 1]$ is not countable by the *argument of the diagonal*:

> Suppose $[0, 1]$ were countable. Then we could list the decimal expansion (infinite decimal expansion without infinitely many zeroes at the end) of the real numbers in order:

$\mathbb{N}$	$[0,1]$
1	$0.a_{11}a_{12}a_{13}\cdots$
2	$0.a_{21}a_{22}a_{23}\cdots$
3	$0.a_{31}a_{32}a_{33}\cdots$
4	$0.a_{41}a_{42}a_{43}\cdots$
$\vdots$	$\vdots$

We now construct a real number in $[0,1]$ that does not appear in the list. For every n, choose $b_n \neq a_{nn}$, with $b_n \in \{1, \ldots, 8\}$. Then $b = 0.b_1 b_2 b_3 \cdots$ belongs to $[0,1]$ and so must have an index in the list, say k. But this cannot be as by construction $b_k \neq a_{kk}$.

The same kind of argument shows that $\mathbb{N}^{\mathbb{N}}$ (all sequences of natural numbers) is uncountable.

The cardinality of $\mathbb{R}$ is equal to the cardinality of $[0,1]$, and is called the *cardinality of the continuum*, denoted by c. The *continuum hypothesis* says that there is no uncountable set with a smaller cardinality, and therefore $\aleph_1 = c$.

Example 39. The following sets have the cardinality of the continuum:

(i) any interval of $\mathbb{R}$, open or closed

(ii) $\mathbb{R}^n$ (and therefore $\mathbb{C}$)[1]

(iii) the set of irrational numbers in any nontrivial interval of $\mathbb{R}$

(iv) 2^A when A is countably infinite, e.g., $2^{\mathbb{N}}$. For this reason on can write $c = 2^{\aleph_0}$, so that the continuum hypothesis can be written as: $\aleph_1 = 2^{\aleph_0}$.

(v) $\mathbb{N}^{\mathbb{N}}$.

[1]This result needs the axiom of choice.

A Appendix A: More on real numbers

There are different ways to construct real numbers. One way is by using axioms. There are three groups of axioms:

(i) Algebraic axioms: $(\mathbb{R}, +, \cdot, 0, 1,)$ is a *field*, which means:

  (a) addition $(+)$ is commutative, associative, has neutral element 0, and any $x \in \mathbb{R}$ has an (additive) inverse $-x$, i.e., $x + (-x) = 0$.
  (b) multiplication $(\cdot)$ is commutative, associative, has neutral element 1, and each nonzero $x \in \mathbb{R}$ has an inverse $x^{-1} = 1/x$, i.e., $x^{-1} \cdot x = 1$.
  (c) multiplication is distributive over addition: $x \cdot (y + z) = x \cdot y + x \cdot z$.
  (d) $1 \neq 0$.

(ii) Order axioms: There exists a subset $\mathbb{R}_+ \subset \mathbb{R}$ such that

  (a) The binary relation $\leq$ defined by $x \leq y$ iff $y - x \in \mathbb{R}_+$ is a total order.
  (b) $x \leq y$ and $z \leq w$ implies $x + z \leq y + w$
  (c) $x \leq y$ and $z \geq 0$ implies $x \cdot z \leq y \cdot z$.

(iii) The supremum axiom: every subset of $\mathbb{R}$ bounded from above has a supremum.

Remarks:

(i) The supremum axiom is nothing else than Axiom 1 in Chapter 5.

(ii) Recall that a *group* is a triple $(G, *, e)$, where $e \in G$ is the *neutral element*, $*$ is a binary operation on G which is associative, has neutral element e (i.e., $x * e = e * x = x$ for every $x \in G$), and each $x \in G$ has an inverse $-x$ (i.e., $x * (-x) = e$). An *ordered group* is a tuple $(G, *, e, \leq)$ where $(G, *, e)$ is a group, $\leq$ is a total order, and $x \leq y$ implies $x + w \leq y + w$ for every $w \in G$. The axioms above for $\mathbb{R}$ imply that $(\mathbb{R}, +, 0, \leq)$ is a commutative (or Abelian) ordered group.

The supremum axiom has important consequences. One of them is that $\mathbb{R}$ is Archimedean. Generally speaking, let $(G, +, 0, \leq)$ be an ordered group, and $x, y \in G$. Then $x > 0$ is *infinitesimal for y* if for every $n \in \mathbb{N}$,

$$nx := \underbrace{x + x + \cdots x}_{n \text{ times}} < y.$$

x is *infinitesimal* if it is infinitesimal for 1. We say that G is *Archimedean* if there is no pair $(x, y) \in G^2$ such that x is infinitesimal for y.

Theorem 17. $\mathbb{R}$ is Archimedean.

Proof. Denote by Z the set of infinitesimals of $\mathbb{R}$. Assume by contradiction that $Z \neq \emptyset$. Then Z is bounded above by 1. By the supremum axiom, it has a supremum, say c, which is positive. Therefore, $\frac{c}{2} < c < 2c$. As $2c > c$, $2c$ is not an infinitesimal, therefore there exists $n \in \mathbb{N}$ such that

$$\frac{1}{n} < 2c. \tag{A.1}$$

As $\frac{c}{2} < c$, it is an infinitesimal, so for every $m \in \mathbb{N}$, $\frac{1}{m} \geq \frac{c}{2}$. But taking $m = 4n$, this contradicts (A.1). $\square$

A consequence of the Archimedean property of $\mathbb{R}$ is that $\mathbb{Q}$ is dense in $\mathbb{R}$, which means that for every $a, b \in \mathbb{R}$ such that $a < b$, there exists $c \in \mathbb{Q}$ such that $a \leq c \leq b$.

Theorem 18. $\mathbb{Q}$ is dense in $\mathbb{R}$.

Proof. Take $x, y \in \mathbb{R}$, $x < y$. Then $y - x > 0$. By the Archimedean property, there exists $n \in \mathbb{N}$ such that $n(y - x) > 1$, i.e.,

$$1 + nx < ny. \tag{A.2}$$

As $nx \in \mathbb{R}$, there exists $z \in \mathbb{Z}$ such that $z - 1 \leq nx < z$. Therefore

$$nx < z \leq nx + 1. \tag{A.3}$$

Combining (A.2) and (A.3), we find

$$nx < z < ny.$$

Dividing by n yields

$$x < \underbrace{\frac{z}{n}}_{\in \mathbb{Q}} < y.$$

$\square$

B Appendix B: Sequence of sets; limits

B.1 Superior and inferior limits of a sequence of numbers

Consider $(u_n)_{n\in\mathbb{N}}$ a sequence of real numbers bounded from above. Then

$$v_n = \sup\{u_k \ : \ k \geq n\}, \quad w_n = \inf\{u_k \ : \ k \geq n\}$$

are respectively decreasing and increasing sequences. Moreover, these sequences converge since $w_n \leq u_n \leq v_n$. We define the *superior limit* and *inferior limit* of $(u_n)_{n\in\mathbb{N}}$ by

$$\limsup_{n\to\infty} u_n = \lim_{n\to\infty} v_n, \quad \liminf_{n\to\infty} u_n = \lim_{n\to\infty} w_n$$

B.2 Superior and inferior limits of a sequence of sets

Let $\{E_n\}_{n\in\mathbb{N}}$ be a sequence of sets in X.

(i) The *superior limit* of $\{E_n\}_{n\in\mathbb{N}}$ is the set of elements of X that belong to inifinitely many E_n. It is denoted by $\limsup_n E_n$ or $\overline{\lim}_n E_n$.

(ii) The *inferior limit* of $\{E_n\}_{n\in\mathbb{N}}$ is the set of element of X that belong to E_n for all $n \in \mathbb{N}$ but a finite number of them. It is denoted by $\liminf_n E_n$ or $\underline{\lim}_n E_n$.

We give some properties.

Theorem 19. Let $\{E_n\}_{n\in\mathbb{N}}$ be a sequence of sets in X.

$$\limsup_n E_n = \bigcap_{n=1}^{\infty} \bigcup_{i=n}^{\infty} E_i$$
$$\liminf_n E_n = \bigcup_{n=1}^{\infty} \bigcap_{i=n}^{\infty} E_i$$
$$\liminf_n E_n \subseteq \limsup_n E_n.$$

Example 40. Take $X = \{a, b\}$ and $E_n = \{a\}$ if n is even, $E_n = \{b\}$ is n is odd. Then

$$\limsup_n E_n = X, \quad \liminf_n E_n = \emptyset.$$

Example 41. Take $X = \left]-\infty, \infty\right[$ and the following sequence:

$$\begin{aligned} &E_1 = [0,1[\,, \\ &E_2 = \left[0, \frac{1}{2}\right[, \ E_3 = \left[\frac{1}{2}, 1\right[, \\ &E_4 = \left[0, \frac{1}{4}\right[, \ E_5 = \left[\frac{1}{4}, \frac{1}{2}\right[, \ E_6 = \left[\frac{1}{2}, \frac{3}{4}\right[, \ E_7 = \left[\frac{3}{4}, 1\right[, \\ &E_8 = \left[0, \frac{1}{8}\right[, \text{ etc.} \end{aligned}$$

Then

$$\limsup_n E_n = [0,1[\,, \quad \liminf_n E_n = \emptyset.$$

A sequence $\{E_n\}_{n\in\mathbb{N}}$ is *increasing* (resp., *decreasing*) if $E_n \subseteq E_{n+1}$ (resp., $E_n \supseteq E_{n+1}$), $\forall n \in \mathbb{N}$. A sequence is *monotone* if it is increasing or decreasing.

Theorem 20. If $\{E_n\}_{n\in\mathbb{N}}$ is monotone, $\lim_n E_n$ exists, and is equal to $\bigcup_{n\in\mathbb{N}} E_n$ (if increasing) or $\bigcap_{n\in\mathbb{N}} E_n$ (if decreasing).

(usual notation: $E_n \nearrow E$, $E_n \searrow E$)

Example 42. Take $X = \left]-\infty, \infty\right[$ and $E_n = [\frac{1}{n}, 1]$. Then $\{E_n\}_{n\in\mathbb{N}}$ is increasing and $E_n \nearrow \left]0,1\right]$. Consider now the sequence $F_n = \left]-1-\frac{1}{n}, 1+\frac{1}{n}\right[$. It is decreasing and $F_m \searrow [-1,1]$.