University of Paris 1 Year 2014 - 2015

Lecture notes

Master Mathematical Models in Economics and Finance (MMEF) and Erasmus Mundus Master : Models and Methods of Quantitative Economics (QEM)

Logic and sets.

Stéphane Gonzalez

Lesson 1: Classical 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 tabular to evaluate if a "complex" proposition is true or false. For example :

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

Definition 3. 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:

$$\text{“}p \to q\text{” is true.}$$

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

- p: "1=2" (false)

- q: “2=3” (false)

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

Definition 4. 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 and q be two propositions, we have the following equivalence:

$$(p \to q) \Leftrightarrow (\neg q \to \neg p).$$

Proof. 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 $(p \to q) \Leftrightarrow (\neg q \to \neg p)$. □

Definition 5. Let p and q be two propositions, “$\neg q \to \neg p$” is called the contrapositive of “$p \to q$”.

By Theorem 1, a proposition is equivalent to its contrapositive.

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).

Compare the accuracy of the mathematical language and the accuracy of the usual language...

Definition 6. A tautology is a proposition which is always true regardless of which valuation is used for the propositional variables.

Theorem 2. 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) $(p \wedge (p \rightarrow q)) \rightarrow q$

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

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

Note that:

- $p \Rightarrow q$ means $p \rightarrow q$ is a tautology;
- $q \Leftrightarrow q$ means $p \leftrightarrow q$ is a tautology.
- By Theorem 1, the proposition $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$ is a tautology.

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 not solution"

hint: use Theorem 2(iv) and (ii) to the propositions p:"there is a problem", and q:"there is a solution".

Theorem 3. Let p, q and r be three propositions. The following propositions are tautologies:

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

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

Definition 7 (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 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.

We can define a set in tabular form, listing all elements of the set.

Example 3. $\{\alpha, \beta, \gamma\}$ is the set which contains the elements called α, β and γ.

Definition 8. A predicate on a set A is an expression which associates to every element $x \in A$ a proposition $p(x)$.

Definition 9 (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. Let $p(\alpha), p(\beta)$ and $p(\gamma)$ three propositions which define a predicate on the set $\{\alpha, \beta, \gamma\}$. We have "$\forall x \in \{\alpha, \beta, \gamma\}, p(x)$" if and only if $p(\alpha) \wedge p(\beta) \wedge p(\gamma)$.

How to deal with the universal quantifier? In order to prove that a proposition of the form "$\forall x \in A, p(x)$" is true, you must consider an arbitrary element $x \in A$ and prove that $p(x)$ is true. By arbitrary we mean that in the course of the proof, one must only use the fact that $x \in A$.

Definition 10 (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 $p(\gamma)$ 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 $p(\alpha) \vee p(\beta) \vee p(\gamma)$.

How to deal with the existential quantifier? In order to prove that a proposition of the form "$\exists x \in A, p(x)$" is true, it suffices to find one element $a \in A$ such that $p(a)$ is true.

Definition 11 (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) $\neg(\exists x \in A, p(x)) \Leftrightarrow (\forall x \in A, \neg p(x))$

How to use this? Tells us that in order to prove a proposition of the form "$\forall x \in Ap(x)$" is false it suffices to find an element $a \in A$ such that $p(a)$ is false. Such an element is called a counter-example.

Lesson 2: Basic set theory.

All definitions are ultimately circular since they depend on concepts which must themselves have definitions, a dependence which can not be continued indefinitely without returning to the starting point. To avoid this vicious circle certain concepts must be taken as primitive concepts; terms which are given no definition. Although the concept of set provides a basis for all mathematics, we are not going to define the concept of set differently than the naive way of Definition 7. The concept of set and set memberships are taken as a primitive. However, even if both notions are not defined, we are going now to impose rules: what things we can do and what things we can not with these two mathematical tools. These required rules are called Axioms.

Definition 12. A set A is a subset of a set B if every element of A is an element of B; one writes $A \subseteq B$. We also say that A is contained in B or that B contains A. Formally:

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

Axiom 1 (Axiom of extensionality-Definition)**.** Two sets A and B are equal, denoted $A = B$, if $A \subseteq B$ and $B \subseteq A$.

$$(\forall A)(\forall B)[(A = B) \Leftrightarrow ((A \subseteq B) \wedge (B \subseteq A))].$$

We denote by $A \neq B$ the proposition $\neg(A = B)$.

How to deal with this definition? In order to prove that two set A and B are equal, we need to decompose the proof in two steps:

(i) Firstly prove $A \subseteq B$;

(ii) Secondly prove $B \subseteq A$.

Theorem 4. The following properties hold:

(i) All set contains itself.

$$\forall A, A \subseteq A.$$

(ii) Two sets A and B are equal if they have exactly the same elements[1]. Formally:

$$(\forall A)(\forall B)[(A = B) \leftrightarrow [(\forall x)(x \in A \leftrightarrow x \in B)]].$$

[1] Naive definition of the equality.

(iii) If a set A is contained in a set B and if B is contained in a set C, then the set A is contained in the set C. Formally:

$$(\forall A)(\forall B)(\forall C)([(A \subseteq B) \wedge (B \subseteq C)] \Rightarrow (A \subseteq C)).$$

Proof. (i) The definition,

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

is equivalent to:

$$\neg(A \subseteq A) \Leftrightarrow (\exists x)((x \in A) \wedge (x \notin A)).$$

The proposition $(\exists x)((x \in A) \wedge (x \notin A))$ is false. However, if $\neg(A \subseteq A)$ is true, then the proposition $(\exists x)((x \in A) \wedge (x \notin A))$ is true, a contradiction... We deduce that $\neg(A \subseteq A)$ is false, and since

$$A \subseteq A \Leftrightarrow \neg\neg(A \subseteq A),$$

we conclude that $A \subseteq A$ is true.

(ii) The Definition 1 is equivalent to :

$$(\forall A)(\forall B)[(A = B) \leftrightarrow ((\forall x)(x \in A \to x \in B) \wedge (\forall x)(x \in B \to x \in A))].$$

which is equivalent to

$$(\forall A)(\forall B)[(A = B) \leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)].$$

(iii) Suppose the proposition

$$(\forall A)(\forall B)(\forall C)([(A \subseteq B) \wedge (B \subseteq C)] \to (A \subseteq C)),$$

is false. Then the negation

$$(\exists A)(\exists B)(\exists C)([(A \subseteq B) \wedge (B \subseteq C)] \wedge \neg(A \subseteq C)),$$

is true, and it is equivalent to:

$$(\exists A)(\exists B)(\exists C)[(\forall x)(x \in A \to x \in B) \wedge (\forall x)(x \in B \to x \in C) \wedge (\exists x)(x \in A \wedge x \notin C)],$$

which is equivalent to:

$$(\exists A)(\exists B)(\exists C)[(\forall x)(x \notin A \vee x \in B) \wedge (\forall x)(x \notin B \vee x \in C) \wedge (\exists x)(x \in A \wedge x \notin C)],$$

which implies:

$$(\exists A)(\exists B)(\exists C)[(\exists x)[(x \notin A \vee x \in B) \wedge (x \notin B \vee x \in C) \wedge (x \in A \wedge x \notin C)].$$

If the expression is true, $(x \in A \wedge x \notin C)$ must be true. Then $x \notin C$ and $x \in A$. But in this case, $(x \notin B \vee x \in C)$ is true only if $x \notin B$ and $(x \notin A \vee x \in B)$ is true only if $x \in B$... Then at least one of the propositions $(\exists x)[(x \notin A \vee x \in B)$, $(\exists x)[(x \notin B \vee x \in C)$ and $(\exists x)[(x \in A \wedge x \notin C)$ is false. It follows that the proposition

$$(\exists A)(\exists B)(\exists C)[(\exists x)[(x \notin A \vee x \in B) \wedge (x \notin B \vee x \in C) \wedge (x \in A \wedge x \notin C)],$$

is false, which implies that

$$(\exists A)(\exists B)(\exists C)[(\forall x)(x \notin A \vee x \in B) \wedge (\forall x)(x \notin B \vee x \in C) \wedge (\exists x)(x \in A \wedge x \notin C)],$$

is false and we conclude that its negation

$$(\forall A)(\forall B)(\forall C)([(A \subseteq B) \wedge (B \subseteq C)] \rightarrow (A \subseteq C)),$$

is true.

□

We would like to characterize the elements of a set by a property.

Axiom 2 (Axiom of specification)**.** Let A be a set and P a predicate on A. There exists a set denoted $\{x \in A, P(x)\}$ such that the elements of $\{x \in A, P(x)\}$ are the elements of $x \in A$ such that $P(x)$ is true. Formally:

$$(\forall A)(\exists \{x \in A, P(x)\})(\forall x)[(x \in \{x \in A, P(x)\}) \Leftrightarrow ((x \in A) \wedge P(x))].$$

Example 6. Let X be the set of animals. $P(x)$: “the animal x has feathers”. The set $\{x \in X, P(x)\}$ is the set of animals with feathers.

Theorem 5. The set of all sets does not exist.

Proof. We suppose that the set A of all sets exists. We define the predicate P on A by:

$$P(x) : \, x \notin x.$$

Let B the set defined with the axiom of specification by:

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

If $B \in B$ then $P(B)$ is true which implies $B \notin B$; but if $B \notin B$ then $P(B)$ is true which implies $B \in B$... We have simultaneously $B \notin B$ and $B \in B$, a contradiction. Hence the set of all sets does not exist. □

Theorem 6. There exists a set having no elements. This set called emptyset and denoted $\emptyset$ is unique.

Proof. Let X be a set, and P the predicate on X defined by: $P(x)$: “$x \neq x$”. Using the Axiom of specification we define the set $\emptyset$ by:

$$\emptyset = \{x \in X, P(x)\}.$$

Suppose there exists $x \in \emptyset$, then $P(x)$ is true, but it is not possible according to the Axiom 1. Suppose there exists a set o without element such that $o \neq \emptyset$, then

$$(\exists x)[((x \in o) \wedge (x \notin \emptyset)) \vee ((x \in \emptyset) \wedge (x \notin o))],$$

that is not possible. Hence $o = \emptyset$, which proves the unicity. □

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

Proof. Let X be a set, suppose $\neg(\emptyset \subseteq X)$ is true. The proposition $\neg(\emptyset \subseteq X)$ is equivalent to $\neg((\forall y)(y \in \emptyset) \to (y \in X))$, which is equivalent to $((\exists y)((y \in \emptyset) \wedge (y \notin X)))$. the proposition $(\exists y)(y \in \emptyset)$ is always false, then $((\exists y)((y \in \emptyset) \wedge (y \notin X)))$ is false and we deduce that $\neg(\emptyset \subseteq X)$ is false. Hence $\emptyset \subseteq X$ is true. □

Axiom 3 (Axiom of pairing)**.** Given two sets A and B there exists a set denoted $\{A, B\}$ and called the pair of A and B whose members are exactly the two given sets. Formally:

$$(\forall A)(\forall B)(\exists\{A, B\})(\forall x)[x \in \{A, B\} \Leftrightarrow ((x = A) \vee (x = B))]$$

Definition 13. The pair $\{A, A\}$ is abbreviated $\{A\}$ and called the singleton containing A.

We should be vigilant in order to ensure that there was no confusion between a set A and the singleton $\{A\}$. The proposition $A \in \{A\}$ is always true. If $A = \emptyset$, the set $\emptyset$ does not contain element while the set $\{\emptyset\}$ contains exactly one element: the element $\emptyset$!

Similarly, do not make confusion between for example the set $\{\{1\}, \{2, 3\}\}$ and $\{1, 2, 3\}$: the first set contains two elements while the second contains three elements...

Note that If X is a set, the following is always true: x is an element of X if and only if the singleton $\{x\}$ is contained in X:

$$x \in X \Leftrightarrow \{x\} \subseteq X.$$

Axiom 4 (Axiom of union)**.** If A is a collection of sets, we can define a set $\bigcup\limits_{C \in A} C$ composed exactly with all the elements of the sets C, $C \in A$. Formally:

$$(\forall A)(\exists \bigcup_{C \in A} C)(\forall x)[(x \in \bigcup_{C \in A} C) \Leftrightarrow (\exists C)((C \in A) \wedge (x \in C))]$$

In order to prove that $x \in \bigcup\limits_{C \in A} C$, we must prove that x is an element of at least one of the sets which belong to A:

$$x \in \bigcup_{C \in A} C \leftrightarrow (\exists C \in A,\, x \in C).$$

Definition 14. Given two sets X and Y, we denote by $X \bigcup Y$ and we call union of X and Y the set defined by:

$$(x \in X \bigcup Y) \leftrightarrow ((x \in X) \vee (x \in Y))$$

Note that if we put $A = \{X, Y\}$, the previous definition becomes equivalent to:

$$(x \in X \bigcup Y) \leftrightarrow (\exists C)((C \in A) \wedge (x \in C)).$$

$(C \in A)$ means $C = X$ or $C = Y$

Hence the Axiom of union ensures the existence of $X \bigcup Y = \bigcup\limits_{C \in \{X,Y\}} C$ and allow us to define the union of a collection A of sets, larger than a simple pair $\{X, Y\}$.

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

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

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

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

Proof. (i), (ii), can be proved as exercice. (iii) comes from the tautology:

$$[(x \in A) \vee (x \in B)] \vee (x \in C) \Leftrightarrow (x \in A) \vee [(x \in B) \vee (x \in C)]$$

□

Example 7. Do not make confusion between elements of a set and the set itself:

- $$\{\alpha, \beta\} \cup \{\beta, \gamma\} = \bigcup_{C \in \{\{\alpha,\beta\},\{\beta,\gamma\}\}} C = \{\alpha, \beta, \gamma\}$$
- $$\bigcup_{C \in \emptyset} C = \emptyset$$
- $$\bigcup_{C \in \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}} C = (\emptyset \cup \{\emptyset\}) \cup (\{\emptyset, \{\emptyset\}\}\}) = \{\emptyset, \{\emptyset\}\}$$

Theorem 9. Let A be a nonempty collection of sets[2]. There exists a unique set denoted $\bigcap\limits_{C \in A} C$ such that each element of $\bigcap\limits_{C \in A} C$ is an element of each set which belongs to A.

$$(\forall A \neq \emptyset)(\exists \bigcap_{C \in A} C)(\forall x)[(x \in \bigcap_{C \in A} C) \leftrightarrow ((\forall C)(C \in A) \rightarrow (x \in C))]$$

Proof. A is nonempty, let $C \in A$ be an element (set) of A. We put:

$$B := \{x \in C, (\forall Z \in A)(x \in Z)\}$$

The Axiom 2 ensures that B is a set, while Axiom 1 ensures its uniqueness. We observe that the set B satisfies the properties required for $\bigcap\limits_{C \in A} C$. □

[2] A set which contains at least one set

Definition 15. Given two sets X and Y, we denote by $X\bigcap Y$ and we call union of X and Y the set defined by:

$$(x \in X\bigcap Y) \leftrightarrow ((x \in X) \wedge (x \in Y))$$

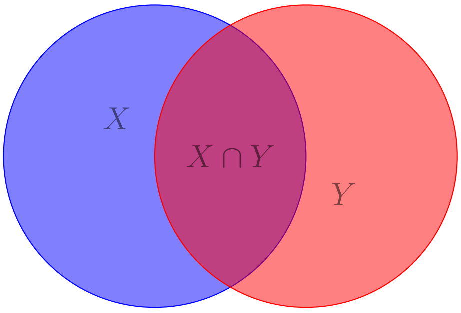
Note that if we put $A = \{X, Y\}$, the previous definition becomes equivalent to:

$$(x \in \bigcap_{C\in A} C) \leftrightarrow ((\forall C)(C \in A) \to (x \in C))].$$

$(C \in A)$ means $C = X$ or $C = Y$

Hence the Theorem 9 ensures the existence of $X\bigcap Y = \bigcap_{C\in\{X,Y\}} C$ and allow us to define the intersection of a collection A of sets, larger than a simple pair $\{X, Y\}$.

Venn diagrams of the intersection:



Theorem 10. The intersection $\bigcap$ satisfies the following properties:

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

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

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

(iv) $A\bigcap(B\bigcup C) = (A\bigcap B)\bigcup(A\bigcap C)$

(v) $A\bigcup(B\bigcap C) = (A\bigcup B)\bigcap(A\bigcup C)$

Proof. (i), (ii) and (iii) can be found as exercice. (iv) and (v) are direct consequence of Theorem 3 □

Theorem 11. Let A and B be two sets, there exists unique a set denoted $A \setminus B$ and called the relative complement of B in A whose elements are the elements of A which does not belong to B.

$$(\forall A)(\forall B)[(x \in A \setminus B) \Leftrightarrow (x \in A) \wedge (x \notin B)].$$

Proof. Use Axiom 2 for the existence and Axiom 1 for the uniqueness. □

Theorem 12 (Morgan's laws)**.** Let A, B and C be three sets:

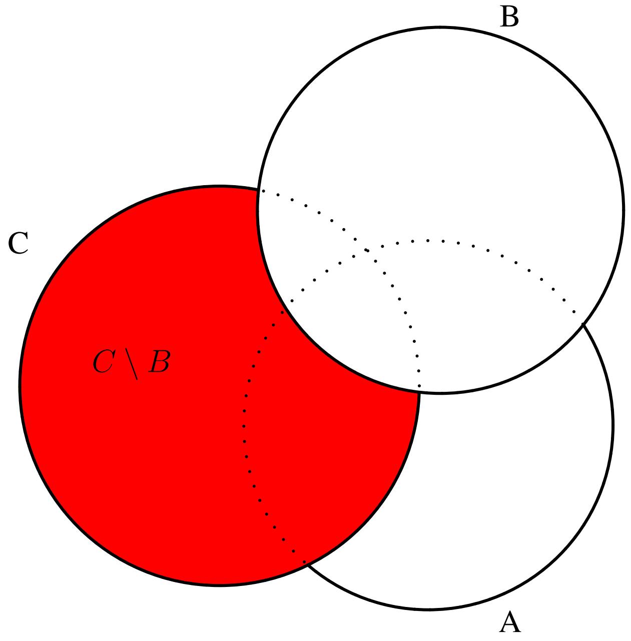
(i) $A \setminus \emptyset = A$

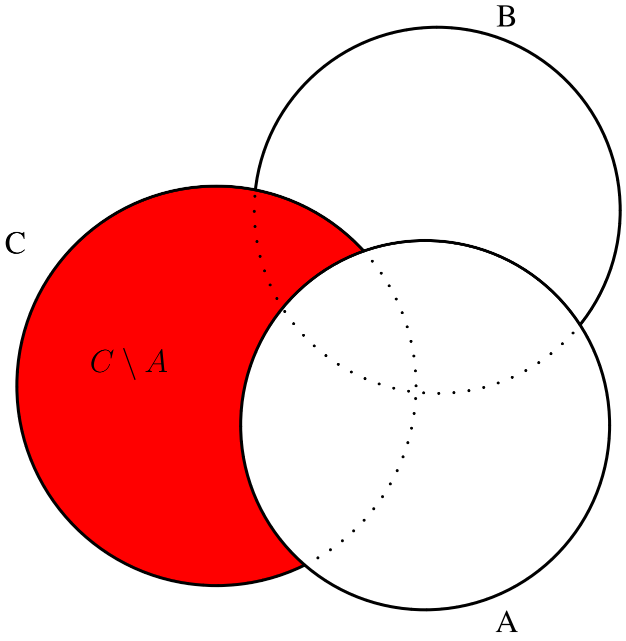
(ii) $\emptyset \setminus A = \emptyset$

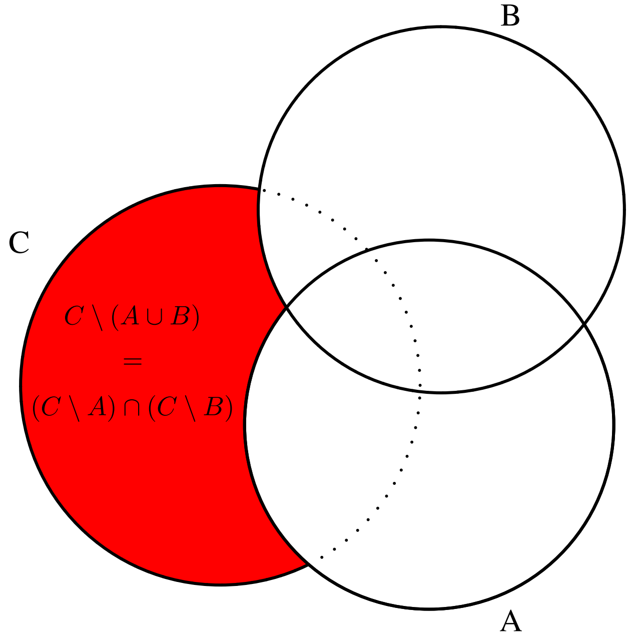
(iii) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$

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

Proof. As exercice. □


B
C
$C \setminus B$
A


B
C
$C \setminus A$
A


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

Definition 16. Let A and B be two sets. The symetric difference of A and B is the set:

$$A\Delta B := (A\bigcup B)\setminus(A\bigcap B)$$

Theorem 13. The symetric 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) $A\Delta A = \emptyset$

Lesson 3: Mappings, inverse image: definition and basic properties.

Axiom 5 (axiom of power set)**.** Given any set A, there is a set denoted 2^A (or $\mathcal{P}(A)$) and called power set of A such that, given any set B, B is a member of 2^A if and only if every element of B is also an element of A. Formally:

$$(\forall A)(\exists 2^A)(\forall x)(x \in 2^A \Leftrightarrow x \subseteq A)$$

If A is a set, the set 2^A is unique (consequence of Axiom 1).

Example 8.

- $2^\emptyset = \{\emptyset\}$.
- $2^{\{a\}} = \{\emptyset, \{a\}\}$.
- $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$
- $2^{\{a,b,c\}} = \{\emptyset, \{a\}, \{b\}, \{a,b\}, \{c\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
- ...

Definition 17.

- *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.
- *Kuratowski's definition:* An ordered pair (x, y) is the set which contains the singleton $\{x\}$, and the pair $\{x, y\}$:
$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Theorem 14.

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

Proof.

- " $\Rightarrow$ " If $a = c$ and $b = d$, then $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Thus $(a, b) = (c, d)$.
- " $\Leftarrow$ ": 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 $\{c,d\} = \{a\}$. 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 $\{c\} = \{a,b\}$. Then $a = b = c$, which also contradicts $a \neq b$.
  Therefore $\{c\} = \{a\}$, so that $c = a$ and $\{c,d\} = \{a,b\}$.
  If $d = a$ were true, then $\{c,d\} = \{a,a\} = \{a\} \neq \{a,b\}$, a contradiction. Thus $d = b$ is the case, so that $a = c$ and $b = d$.

□

Definition 18. 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:

$$A \times B = \{x \in 2^{2^{A\cup B}}, (\exists a \in A)(\exists b \in B), x = (a,b)\}.$$

- 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.

Proposition 1. (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) $\neg(A = \emptyset \vee B = \emptyset) \Leftrightarrow (A \neq \emptyset \wedge B \neq \emptyset) \Leftrightarrow ((\exists a \in A) \wedge (\exists b \in B) \Leftrightarrow (\exists x \in 2^{2^{A\cup B}}, (\exists a \in A)(\exists b \in B), x = \{\{a\},\{a,b\}\} = (a,b)) \Leftrightarrow A \times B \neq \emptyset \Leftrightarrow \neg(A \times B = \emptyset)$

(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 $x = (a, b) \in A' \times B'$.

□

Definition 19. • A mapping from the set A to the set B, denoted $f : A \to B$, 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 $f(C) := \{b \in B, \exists a \in C, (a, b) \in graph(f)\} = \{b \in B, \exists a \in C, b = f(a)\}$ is called the image of C by f.
- The set $f(A) := \{b \in B, (a, b) \in graph(f)\} = \{b \in B, \exists a \in A, b = f(a)\}$ [3] 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:

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

Note that

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

Definition 20. Two mappings f and g from A to B are said to be equal if for every element $a \in A$ one has $f(a) = g(a)$.

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

Example 9. Here are some examples of mappings:

- The identity mapping on A denoted 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 x and y in A, one has
$$f(x) = f(y).$$
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 $x \in C$.

Proposition 2. Let $f : A \to B$ and let A_1 , A_2 be two subsets of A:

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

Proposition 3. Let $f : A \to B$ and let B_1, B_2 be two subsets of B one has:

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

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

Lesson 4: Injection, Surjection, Bijection.

Definition 22. 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 if $B = f(A)$.

Definition 23. 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[4], if $f(a_1) = f(a_2)$ then $a_1 = a_2$.

Avoid the confusion between the definition of injectivity and the fact that every mappping as 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 24. A mapping $f : A \to B$ is said to be bijective if it is both surjective and injective.

Definition 25. let $f : A \to B$ and $g : C \to D$. The composition of f by g is the mapping $g \circ f : A \to D$ defined by

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

Definition 26. The inverse of a mapping $f : A \to B$ is a mapping $g : B \to A$ satisfying: $g \circ f = id_A$ and $f \circ g = id_B$. A mapping $f : A \to B$ is said to be invertible if it has an inverse mapping.

Proposition 4. The two following propositions are true:

(i) If $f : A \to B$ is injective, then $f^{-1}(f(A')) = A'$ for every $A' \subseteq A$.

(ii) If $f : A \to B$ is surjective, then $f(f^{-1}(B')) = B'$ for every $B' \subseteq B$.

Hence, in particular, if $f : A \to B$ is injective then $f^{-1}(f(a)) = \{a\}$ for every $a \in A$.; and if $f : A \to B$ is onto then $f(f^{-1}(\{b\})) = b$ for every $b \in B$

Proposition 5. The following propositions is true:

$$(f : E \to F \text{ injective}) \iff (\forall A \subseteq E)(\forall B \subseteq E)(f(A \cap B) = f(A) \cap f(B)).$$

[4] By using the contrapositive!!

Proof.

- " $\Rightarrow$ " the inclusion $\subseteq$ is always true. We show the inclusion $\supseteq$: Let $y \in f(A) \cap f(B)$, we have in particular $y \in f(A)$ and $y \in f(B)$, hence there exist $x_1 \in A$ and $x_2 \in B$ such that $f(x_1) = f(x_2) = y$. Since f is injective and $f(x_1) = f(x_2)$, we obtain $x_1 = x_2 =: x$. $x_1 \in A \Rightarrow x \in A$, $x_2 \in B \Rightarrow x \in B$. Hence there exists $x \in A \cap B$ such that $f(x) = y$. We conclude that $y \in f(A \cap B)$.

- " $\Leftarrow$ " Let $x \neq y$. we have immediatly

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

Which implies $f(x) \neq f(y)$.

□

Proposition 6. 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 7. A mapping $f : A \to B$ is bijective if and only if it is invertible.

Proof.

- "$\Rightarrow$": Since f is bijective, f is in particular surjective which implies $\forall b \in B, \exists a \in A$ such that $f(a) = b$ and since f is injective if there exists $a' \in A$ such that $f(a') = b$, we have $a = a'$. Hence $\forall b \in B$, there exists a unique a such that $f(a) = b$. Let $g : B \to A$ the mapping which associates to each element $b \in B$ the unique element $a \in A$ such that $f(a) = b$. We have immediatly:

$$\forall b \in B, \quad f \circ g(b) = f(g(b)) = f(a) = b;$$

and

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

Hence g is a well defined mapping which proves that f is invertible.

- "$\Leftarrow$": 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 6, $g \circ f$ injective implies f injective. Furthermore id_B is bijective therefore it is surjective. By Proposition 6, $f \circ g$ surjective implies f surjective. We conclude that f is bijective.

□

Proposition 8. Let $f : A \to B$ bijective: the inverse mapping of f is unique.

Proof. Let $g_1 : B \to A$ and $g_2 : B \to A$ such that $g_1 \circ f = id_A$ and $f \circ g_1 = id_B$ and $g_2 \circ f = id_A$ and $f \circ g_2 = id_B$. Since $g_1 \circ f = g_2 \circ f$ we have

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

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 $g_1 = g_2$.

□

If f is bijective[5], we denote by f^{-1} the unique inverse mapping of f.

Note that notation f^{-1} may have two different meanings, whether we consider $f^{-1}(C)$ the inverse image of a set C and $f^{-1}(y)$ the image of $y \in B$ by the inverse mapping $f^{-1} : B \to A$. In the latter case, the mapping f needs to be bijective to have an inverse, whereas no such assumption is made to talk about the inverse image of a set.

[5] Then it is invertible

Lesson 5: Relations.

Definition 27.
- A binary relation $\mathcal{R}$ on a set A is a subset of the Cartesian product $A^2 = A \times A$. More generally, a binary relation between two sets A and B is a subset of $A \times B$.
- Let $\mathcal{R}$ be a relation between A and B. The proposition $(x, y) \in \mathcal{R}$ is denoted by the abbreviation: $x\mathcal{R}y$.

Example 10.

Let E be a set. The diagonal $=_E$ (or $\Delta(E)$) of E is the subset of E^2 defined by

$$=_E := \{(x, x) \in E^2, x \in E\}^6.$$

$=_E$ can be see as a relation, and if $(x, y) \in =_E$ then we have $x =_E y$ or more commonly $x = y$.

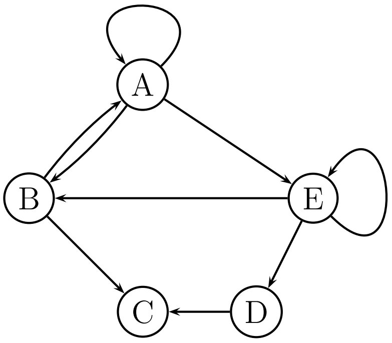
If $f : A \mapsto B$, then $graph(f)$ is a relation between A and B.

If X is the set of human being, $x\mathcal{R}y$ if and only if x is the friend of y define a relation on X.

One can represent a relation as a graph. 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 representing by



and vice versa.

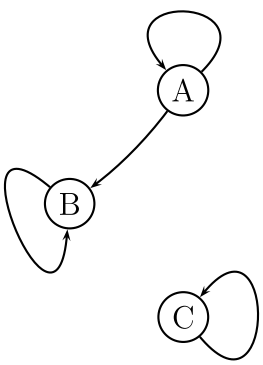
Definition 28. A relation $\mathcal{R}$ on $E \times E$ is said to be:

[6] Since $(x, x) = \{\{x\}\}$, we can define (x, x) without the definition of the equality between two elements.

- reflexive if:

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

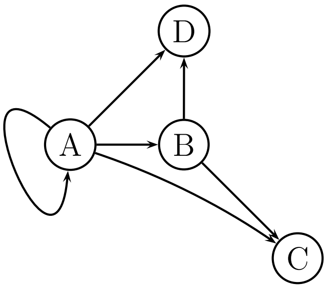
Example:



- transitive if:

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

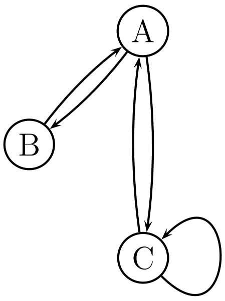
Example:



- symmetric if:

$$\forall (x,y,z) \in E^3, x\mathcal{R}y \Leftrightarrow y\mathcal{R}x.$$

Example:

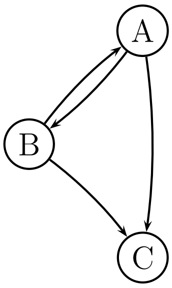


- anti-symmetric if
$$\forall (x,y,z) \in E^3, x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y.$$

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

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

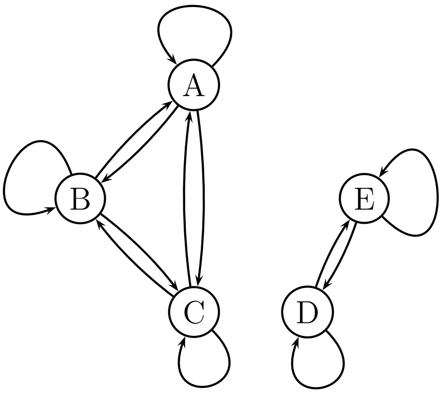
  Example:



Definition 29. An equivalence relation on E is a relation on $E \times E$ which is reflexive, symmetric, and transitive.

Example 11. 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, the relation in $2^E \times 2^E$ defined by "there exists a bijective mapping $f : A \mapsto B$."
-



Definition 30. 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:

$$\mathcal{R}(x) = \{y \in E | x\mathcal{R}y\}$$

Definition 31. 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:

$$((P \in \pi, Q \in \pi) \wedge (P \neq Q)) \Rightarrow (P \cap Q = \emptyset).$$

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

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

Theorem 15. 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 $\pi = \{\mathcal{R}(x), x \in E\}$.

Where $\mathcal{R}(x)$ is the equivalence class of x for $\mathcal{R}$.

Proof. □

Definition 32. 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[7] of $\mathcal{R}$, that is the set:

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

Lemma 1. If $\mathcal{R}$ is a relation on a set E, then the mapping $s : E \to E/\mathcal{R}$ which associates to each $x \in E$ the equivalence class $\mathcal{R}(x)$, is a surjection.

Lemma 2. Let E and F be two sets, and $f : E \to F$ a mapping from E to F. The relation $\mathcal{R}$ defined by

$$x\mathcal{R}y \Leftrightarrow f(x) = f(y),$$

is an equivalence relation. Furthermore, the following propositions hold:

(i) The mapping $b : E/\mathcal{R} \to f(E)$ which associates to each $\mathcal{R}(x) \in E/\mathcal{R}$ the unique element $f(x)$ of the singleton $f(\mathcal{R}(x))$, is a bijection.

(ii) The mapping $i : f(E) \to F$ which associates to each $y \in f(E)$ the element $y \in F$, is an injection.

Theorem 16. Every mapping $f : E \to F$ is the composition of an injection, a bijection and a surjection:

$$f = i \circ b \circ s$$

Where i, b and s are the injection, bijection and surjection defined

[7] It is a partition of E.

Definition 33.

- An order relation on E is a relation reflexive, transitive and antisymmetric;
- A total (or complete) preorder relation on E is a relation reflexive, transitive and total.

Example 12. If E is a set, $\subseteq$ is an order relation on 2^E but not a total preorder.

Definition 34. A preorder relation on E is a relation reflexive and transitive. A set together with a preorder relation is called a preordered set.

Hence:

- An equivalence relation is a preorder relation which is symmetric;
- An order relation is a preorder relation which is antisymmetric
- A total preorder is a preorder relation which is total.

$=_E$ is the unique preorder on E which is an order relation and an equivalence relation.

Definition 35. Let $\Subset$ be an order relation on E, and X a subset of E

- $m \in E$ is a lower bound of X for $\Subset$ if for every element $x \in X$ one has $m \Subset x$. When X has a lower bound, it is said to be bounded below.
- $M \in E$ is an upper bound of X for $\Subset$ if for every element $x \in X$ one has $x \Subset M$. When X has an upper bound, it is said to be bounded above.

Definition 36. Let $\Subset$ be a order relation on E, and X a subset of E.

- $m \in E$ is a minimum of X for $\Subset$ if:
  (i) $\forall x \in X$ one has $m \Subset x$ (m is a lower bound of X)
  (ii) $m \in X$.
- $M \in E$ is a maximum of X for $\Subset$ if:
  (i) $\forall x \in X$ one has $x \Subset M$ (M is a upper bound of X)
  (ii) $M \in X$.

Proposition 9. Let $\Subset$ be an order relation on E, and X a subset of E. When it exists, the minimum (resp. the maximum) is unique.

Proof. As exercice □

Let $\Subset$ be a total order relation on E, and X a subset of E. When it exists, we denote $\min(X)$ or $\min_{x\in X} x$ (resp. $\max(X)$ or $\max_{x\in X} x$) the minimum (resp. the maximum) of X.

Example 13. Let E be a set, for the order relation $\subseteq$ on 2^E we have:

$$\min(2^E) = \emptyset, \text{ and } \max(2^E) = E.$$

Definition 37. Let $\Subset$ be an order relation on E and X a subset of E. Then $m \in X$ is a minimal element of X if for all $x \in X$, $x \Subset m$ implies $m = x$.

Definition 38. Let $\Subset$ be an order relation on E and X a subset of E. Then $M \in X$ is a maximal element of X if for all $x \in X$, $M \Subset x$ implies $M = x$.

Example 14. Let E be a set, for the order relation $\subseteq$ on $2^E \setminus \{\emptyset\}$ the minimal elements are the singletons while the maximal element is E.

Definition 39. Let E be a set and A a subset of E. We put:

$$m(A) := \{\alpha \in E, \alpha \text{ lower bound of } E\},$$
$$M(A) := \{\alpha \in E, \alpha \text{ upper bound of } E\}.$$

(i) If $\max(m(A))$ exists, this maximum is called the infimum or the greatest lower bound of A and it is denoted $\inf(A)$ or $\inf_{x\in A} x$.

(ii) If $\min(M(A))$ exists, this minimum is called the supremum or the least upper bound of A and it is denoted $\sup(A)$ or $\sup_{x\in A} x$.

$$a = \inf(A) \Longleftrightarrow [(\forall x \in A, a \Subset x) \quad \wedge \quad (\forall \alpha,\ [\forall x \in A, \alpha \Subset x] \Rightarrow \alpha \Subset a)].$$

$$b = \sup(A) \Longleftrightarrow [(\forall x \in A, x \Subset b) \quad \wedge \quad (\forall \beta,\ [\forall x \in A, x \Subset \beta] \Rightarrow b \Subset \beta)].$$

Example 15. Let E be a set. We consider the order relation $\subseteq$ on 2^E. Let A and B be two subsets of E. We have:

$$\inf(\{A, B\}) = A \cap B$$
$$\inf(\{A, B\}) = A \cup B$$

Proposition 10. Let $\Subset$ be an order relation on E and X a subset of E.

$$\min(X) \text{ exists } \substack{\Rightarrow \\ \nLeftarrow} \inf(X) \text{ exists } \substack{\Rightarrow \\ \nLeftarrow} X \text{ has a lower bound.}$$

$$\max(X) \text{ exists } \substack{\Rightarrow \\ \nLeftarrow} \sup(X) \text{ exists } \substack{\Rightarrow \\ \nLeftarrow} X \text{ has an upper bound.}$$

Theorem 17. Let $\mathcal{A}$ be a family of sets. Let B the set defined by:

$$B := \bigcup_{A\in\mathcal{A}} A$$

The two following propositions hold:

(i) $\sup(B)$ exists if and only if $\forall A \in \mathcal{A}$, $\sup(A)$ exists.

(ii) If $\sup(B)$ exists, we have:

$$\sup(B) = \sup(\{\sup(A), A \in \mathcal{A}\}).$$

Lesson 6: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

Definition 40. A binary operation on a set S is a function $+ : S \times S \to S$

If $+$ is a binary operation on S and $(a,b) \in S \times S$ we denote $a+b$ the element $+(a,b)$.

Example 16. If E is a set, $\cup$ or $\cap$ are binary operation on 2^E.

Definition 41. - A group $(G,+)$ is a set G together with a binary operation $+$ (called the group law of G) wich satisfies:

  (i) If $a \in G$, $b \in G$, $c \in G$ then $(a+b)+c = a+(b+c)$; (associativity)

  (ii) There exists $0 \in G$, such that $\forall a \in G$, $0+a = a+0 = a$; (existence of the identity element)

  (iii) $\forall a \in G$, $\exists -a \in G$ such that $a+(-a) = (-a)+a = 0$, where 0 is the identity element; (existence of inverse).

- $(H,+)$ is a subgroup of $(G,+)$ if $\neq H \subseteq G$ and $\forall a,b \in H$, $a-b \in H$. Equivalently, $(H,+)$ is a subgroup of $(G,+)$ if $\emptyset \neq H \subseteq G$ and $(H, +_{|H\times H})$ is a group.

It is easy to prove that an identity element, that is an element which satisfies $\forall a \in G$, $0+a = a+0 = a$ is always unique. Similarly if an operation is associative and if $-a$ is such that $a+(-a) = (-a)+a = 0$ then $-a$ is unique.

Definition 42. A group $(G,+)$ is said to be abelian if furthermore

$$a+b = b+a \qquad \text{(Commutativity)}.$$

Example 17. - $\{0,1\}$ together with the commutative binary operation $+$ defined by $0+0=0$, $0+1=1+0=1$, $1+1=0$.

- If E is a set, the set 2^E together with the symetric difference Δ is a group.

Definition 43. - A ring $(A,+,\cdot)$ is a set A equipped with binary operations $+$ and $\cdot$ the eight following properties:

  1. $\forall a,b,c \in A$,
$$(a+b)+c = a+(b+c). \qquad \text{(+ is associative)}.$$

2. There is an element denoted 0 in A such that
$$a + 0 = a \textit{ and } 0 + a = a. \qquad \text{(0 is the additive identity)}$$
3. For each a in A there exists an element denoted $-a$ in A such that
$$a + (-a) = (-a) + a = 0 \qquad (-a \text{ is the additive inverse of } a).$$
4. $\forall a, b \in A$,
$$a + b = b + a \qquad (+ \text{ is commutative}).$$
5. $\forall a, b, c \in A$,
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \qquad (\cdot \text{ is associative}).$$
6. There is an element denoted 1 in A such that
$$a \cdot 1 = a \textit{ and } 1 \cdot a = a \qquad \text{(1 is the multiplicative identity)}.$$
7. $\forall a, b, c \in A$,
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad \text{(left distributivity)}.$$
8. $\forall a, b, c \in A$,
$$(b + c) \cdot a = (b \cdot a) + (c \cdot a) \qquad \text{(right distributivity)}.$$

- $(B, +, \cdot)$ is a subring of $(A, +, \cdot)$ if $\emptyset \neq B \subseteq A$ and $(B, +_{|B\times B}, \cdot_{|B\times B})$ is a ring.

1,2,3,4 means $(A, +)$ is an abelian group under addition, 5,6 means (for culture) $(A, \cdot)$ is a monoid under multiplication, while 7,8 means multiplication distributes over addition.

Example 18.
- $(\{0, 1\}, +, \times)$ with $+$ defined by $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $1 + 1 = 0$ and $\times$ defined by $0 \times 0 = 0$, $0 \times 1 = 1 \times 0 = 0$, $1 \times 1 = 1$
- If E is a set then $(2^E, \Delta, \cap)$ is a ring.

Lemma 3. Let $(A, +, \times)$ be a ring and $\mathcal{A} \subseteq 2^A$ such that $\forall B \in \mathcal{A}$, $(B, +, \times)$ is a subring of $(A, +, \times)$. Then
$$(\bigcap_{B\in\mathcal{A}} B, +, \times) \text{ is a subring of } (A, +, \times).$$

Proof. Let $x, y \in \bigcap_{B\in\mathcal{A}} B$ and $B' \in \mathcal{A}$. We have $x, y \in B'$ and since B' is a subring of $(A, +, \times)$, we have $x \times y \in B'$. Since B' is a subgroup of $(A, +)$ we have $x - y \in B$. Hence $\forall B \in \mathcal{A}$, $x \times y \in B$ and $x - y \in B$ which implies $x \times y \in \bigcap_{B\in\mathcal{A}} B$. Furthermore $\forall B \in \mathcal{A}$, we have $1 \in B$ which implies $1 \in \bigcap_{B\in\mathcal{A}} B$. □

Definition 44. - A field $(\mathbb{K}, +, \times)$ is a ring which contains at least the two distinct elements 0 (additive identity) and 1 (multiplicative identity), and such that:

  $$\forall x \in \mathbb{K}\backslash\{0\},\ \text{ there exists an element denoted } x^{-1} \in \mathbb{K} \text{ such that } x{\times}x^{-1} = x^{-1}{\times}x = 1$$

- A commutative field is a field $(\mathbb{K}, +, \times)$ such that $\forall x, y \in \mathbb{K},\ x \times y = y \times x$.
- $(K, +, \cdot)$ is a subfield of $(\mathbb{K}, +, \cdot)$ if $\{0, 1\} \subseteq K \subseteq \mathbb{K}$ and $(K, +_{|K\times K}, \cdot_{|K\times K})$ is a field.

Equivalently a commutative field can be defined as a ring such that $(\mathbb{K} \setminus \{0\}, \times)$ forms an abelian group.

Lemma 4. Let $(\mathbb{K}, +, \times)$ be a field and $\mathcal{K} \subseteq 2^{\mathbb{K}}$ such that $\forall K \in \mathcal{K}$, $(K, +, \times)$ is a subfield of $(\mathbb{K}, +, \times)$. Then

$$(\bigcap_{K\in\mathcal{K}} K, +, \times) \text{ is a subfield of } (\mathbb{K}, +, \times)$$

Proof. By Lemma 3, $\bigcap_{K\in\mathcal{K}} K$ is a ring. Let $x \in \bigcap_{K\in\mathcal{K}} K$, we have $\forall K \in \mathcal{K}, x \in K$. Since $\forall K \in \mathcal{K}$, K is a field, it follows that $\forall K \in \mathcal{K}$, $x^{-1} \in K$ which implies $x^{-1} \in \bigcap_{K\in\mathcal{K}} K$. □

Definition 45. Let X be a set and $\Subset$ an order relation on X. We say that X has the least-upper-bound property for $\Subset$ if $\forall A \in 2^X \setminus \{\emptyset\}$, if A has an upper bound for $\Subset$ then $\sup(A)$ exists for $\Subset$ and $\sup(A) \in X$.

Axiom 6. There exists a set denoted $\mathbb{R}$ such that:

(i) There exists two binary operations + and × such that $(\mathbb{R}, +, \times)$ is a commutative field.

(ii) There exists a total order relation denoted $\leq$ such that :

  (a) $\forall x, y, z \in \mathbb{R}, x \leq y \Rightarrow x + z \leq y + z$.

  (b) $\forall x, y \in \mathbb{R}$, $(0 \leq x \wedge 0 \leq y) \Rightarrow 0 \leq x \times y$.

  (c) $\mathbb{R}$ has the least-upper-bound property for $\leq$.

In the following the symbol + refers to the additive law of $(\mathbb{R}, +, \times)$ and × refers the multiplicative law of $(\mathbb{R}, +, \times)$. Furthermore 0 (resp 1) refers to the additive identity (resp the multiplicative identity) of the field $(\mathbb{R}, +, \times)$. The symbol $\leq$ will refer to the total order relation given in Axiom 6. The symbol $x < y$ means $x \leq y$ and $x \neq y$.

If $x, y \in \mathbb{R}$ and $y \neq 0$ we denote $\frac{1}{y}$ the real number y^{-1}, and $\frac{x}{y}$ the real number $x \times y^{-1}$.

If $x \in \mathbb{R}$, we denote x^2 the real number $x \times x$.

Proposition 11. The following propositions are true :

(i) If $x \in \mathbb{R}$ and $0 \leq x$ then $-x \leq 0$

(ii) $0 < 1$

(iii) If $x \in \mathbb{R}$ and $0 \leq x$ then $0 \leq x^{-1}$.

Proof. (i) Let $x \in \mathbb{R}$ by definition of $\mathbb{R}$, if $0 \leq x$ then $0 - x \leq x - x$ that is $-x \leq 0$.

(ii) Observe that if $x \times (-1) = 1$ then $-x = 1$ which implies $x = -1$. Suppose that $1 < 0$ hence $-1 > 0$ which implies by definition of $\mathbb{R}$ that $(-1) \times (-1) > 0$ but it is not possible because $(-1) \times (-1) = 1 < 0$. Absurd. Then $0 \leq 1$. Since 0 and 1 are distinct, we have $0 < 1$.

(iii) Suppose $x^{-1} < 0$ then $0 < -x^{-1}$ which implies by the definition of $\mathbb{R}$ that $0 < -x^{-1} \times x = -1$, which is not possible given that $0 < 1$

□

Definition 46. Let $\mathcal{K} \subseteq 2^{\mathbb{R}}$ the set of subsets $K \subseteq \mathbb{R}$ such that $\forall K \in \mathcal{K}$, $(K, +, \times)$ is a subfield of $(\mathbb{R}, +, \times)$. We define the set of rational number denoted $\mathbb{Q}$ as the set

$$\mathbb{Q} := \bigcap_{K \in \mathcal{K}} K.$$

Definition 47. Let $\mathcal{A} \subseteq 2^{\mathbb{Q}}$ the set of subsets $A \subseteq \mathbb{Q}$ such that $\forall A \in \mathcal{A}$, $(A, +, \times)$ is a subring of the ring[8] $(\mathbb{Q}, +, \times)$. We define the set of integers denoted $\mathbb{Z}$ as the set

$$\mathbb{Z} := \bigcap_{A \in \mathcal{A}} A.$$

Definition 48. We define the set of natural numbers denoted $\mathbb{N}$ as the set

$$\mathbb{N} := \{z \in \mathbb{Z},\ 0 \leq z\}.$$

observe that $0 \in \mathbb{N}$, $1 \in \mathbb{N}$, $1 + 1 = 2 \in \mathbb{N}$...

Theorem 18.

$$\mathbb{Q} = \{\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}\}.$$

Proof.

- For proving $\mathbb{Q} \subseteq \{\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}\}$, it suffices to prove that

$$(\{\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}\}, +, \times)$$

is a field contained in $\mathbb{R}$ because in this case

$$\mathbb{Q} = \bigcap_{K \in \mathcal{K}} K \subseteq \{\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}\}.$$

- Let $x \in \{\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}\}$, there exists $p \in \mathbb{Z}$, and $q \in \mathbb{N} \setminus 0$ such that $x = \frac{p}{q}$. $p \in \mathbb{Z}$ and $\mathbb{Z} \subseteq \mathbb{Q}$ implies $p \in \mathbb{Q}$; $q \in \mathbb{N} \setminus \{0\}$ and $\mathbb{N} \setminus \{0\} \subseteq \mathbb{Q} \setminus \{0\}$ implies $q \in \mathbb{Q} \setminus \{0\}$. Since $\mathbb{Q}$ is a field, $q^{-1} = \frac{1}{q} \in \mathbb{Q}$ and $p \times q^{-1} = \frac{p}{q} \in \mathbb{Q}$. Hence $\{\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}\} \subseteq \mathbb{Q}$.

□

[8] Since $(\mathbb{Q}, +, \times)$ is a field, it is in particular a ring.

Lesson 7: Properties of $\mathbb{N}$ and mathematical induction.

Theorem 19. The set $\mathbb{N}$ satisfies the following properties:

(i) $\forall A \subseteq \mathbb{N}$, if $0 \in A$ and $\forall n \in A, n+1 \in A$ then $A = \mathbb{N}$

(ii) $\forall n \in \mathbb{N} \setminus \{0\}$ there exists $p \in \mathbb{N}$ such that $n = p + 1$

(iii) $\forall n \in \mathbb{N}$ there is no element $m \in \mathbb{N}$ such that $n < m < n+1$. (in particular, there is no element between 0 and 1)

(iv) If $n \in \mathbb{N}$ and $m \in \mathbb{N}$ then $n + m \in \mathbb{N}$.

(v) If $n \in \mathbb{N}$ and $m \in \mathbb{N}$ then $n \times m \in \mathbb{N}$.

Proof. Let $\mathcal{P} = \{P \subseteq \mathbb{N} : (0 \in P) \wedge (\forall x \in P, x+1 \in P)\}$ and $\mathbb{N}_0 = \bigcap_{P \in \mathcal{P}} P$.

- First, we prove that $\mathbb{N}_0 \in \mathcal{P}$. Let $n \in \mathbb{N}_0$. $\forall P \in \mathcal{P}$, we have $n \in P$ but $n \in P \Rightarrow n+1 \in P$. Therefore $\forall P \in \mathcal{P}$ we have $n+1 \in P$. Hence $n+1 \in \mathbb{N}_0$.
- Let $A \subseteq \mathbb{N}_0$ such that $A \in \mathcal{P}$. First $A \subseteq \mathbb{N}_0$. Now if $n \in \mathbb{N}_0$ then $\forall P \in \mathcal{P}, n \in P$. Since $A \in \mathcal{P}$, we have $n \in A$. It follows $A = \mathbb{N}_0$.
- Now we prove that $\forall n \in \mathbb{N}_0 \setminus \{0\}$ there exists $p \in \mathbb{N}_0$ such that $n = p+1$. Let

  $$A = \{0\} \cup \{n \in \mathbb{N}_0, \exists p \in \mathbb{N}_0 \text{ such that } n = p+1\}.$$

  By definition of A, we have $0 \in A$. It is clear that $0 \in \mathbb{N}_0$ and $1 \in \mathbb{N}_0$. Since $1 = 0+1$, we see that $1 \in \{n \in \mathbb{N}_0, \exists p \in \mathbb{N}_0 \text{ such that } n = p+1\}$, which implies $A \setminus \{0\} \neq \emptyset$. Let $n \in A \setminus \{0\}$ then there exists $p \in \mathbb{N}_0$ such that $n = p+1$. Since $n, p \in \mathbb{N}_0$, we have $n+1 \in \mathbb{N}_0$ and $p+1 \in \mathbb{N}_0$. Hence $n+1 = (p+1)+1$ belongs to A. Hence $(0 \in A) \wedge (\forall x \in A, x+1 \in A)$. Therefore $A \in \mathcal{P}$ and frim the previous point, since $A \subseteq \mathbb{N}_0$ we obtain $A = \mathbb{N}_0$.
- We want to prove that there is no element of $\mathbb{N}_0$ between 0 and 1: Suppose there exists $m \in \mathbb{N}_0$ such that $0 < m < 1$. Since $m \neq 0$, $\exists p \in \mathbb{N}_0$ such that $m = p+1$. Hence $p \in \mathbb{N}_0 \subseteq \mathbb{N}$ and $p < 0$ which is not possible by definition of $\mathbb{N}$.
- Let $n \in \mathbb{N}_0$ and $A_n = \{p \in \mathbb{N}_0, (n-p) \in \mathbb{N}_0 \vee (n-p) \in \{-k, k \in \mathbb{N}_0\}\}$. It is clear that $0 \in A_n$ because $n \in \mathbb{N}_0$. Let $p \in A_n$.
  - If $(n-p) \in \mathbb{N}_0$ then
    - either $n - p = 0 \Rightarrow n - (p+1) = -1 \in \{-k, k \in \mathbb{N}_0\}$
    - or $n - p \neq 0$ and there exists $q \in \mathbb{N}_0$ such that $n - p = q + 1$ which implies $n - p - 1 = n - (p+1) = q \in \mathbb{N}_0$.
  - If $n - p \in \{-k, k \in \mathbb{N}_0\}$, let $r \in \mathbb{N}_0$ such that $-(n-p) = r$. $r \in \mathbb{N}_0$ implies $r+1 \in \mathbb{N}_0$. Hence $n - (p+1) = n - p - 1 = -r - 1 = -(r+1) \in \{-k, k \in \mathbb{N}_0\}$.

  Hence : $0 \in A_n$ and $\forall p \in A_n$, $p+1 \in A_n$. Hence $A_n = \mathbb{N}_0$.

- By the two previous points, if there exists $n, m \in \mathbb{N}_0$ such that $n < m < n+1$ then $0 < m - n < 1$ and since $m - n \in \mathbb{N}_0$ we found an element of $\mathbb{N}_0$ between 0 and 1. Absurd.
- Let $n \in \mathbb{N}_0$ and $B_n = \{m \in \mathbb{N}_0 \text{ such that } n + m \in \mathbb{N}_0\}$. First $0 \in B_n$ because $n = n+0 \in \mathbb{N}_0$. Suppose $m \in B_n$ then $(n+m \in \mathbb{N}_0)$ implies $n+(m+1) = (n+m)+1 \in \mathbb{N}_0$. And we conclude that $B_n = \mathbb{N}_0$.
- Let $n \in \mathbb{N}_0$ and $C_n = \{m \in \mathbb{N}_0 \text{ such that } n \times m \in \mathbb{N}_0\}$. First $0 \in C_n$ because $0 \times n = 0 \in \mathbb{N}_0$. Suppose $m \in C_n$ then $n \times (m+1) = n \times m + n \in \mathbb{N}_0$ because $m \in C_n \Rightarrow n \times m \in \mathbb{N}_0$ and the previous point implis that the sum of two elements of $\mathbb{N}_0$ belongs to $\mathbb{N}_0$.
- Let $\mathbb{Z}_0 = \mathbb{N}_0 \cup \{-n, n \in \mathbb{N}_0\}$. We want to prove that $\mathbb{Z}_0 = \mathbb{Z}$. Clearly $\mathbb{Z}_0 \subseteq \mathbb{Z}$. Let $p, q \in \mathbb{Z}_0$. we have $0 \in \mathbb{Z}_0$, $1 \in \mathbb{Z}_0$, $p - q \in \mathbb{Z}_0$, and $p \times q \in \mathbb{Z}_0$. It is sufficient to prove that $\mathbb{Z}_0$ is a subring of $(\mathbb{Q}, +, \times)$ which is contained in $\mathbb{Z}$ defined as the infimum of the set of subrings of $(\mathbb{Q}, +, \times)$. Hence $\mathbb{Z}_0 = \mathbb{Z}$. Therefore the positive part $\mathbb{N}_0$ of $\mathbb{Z}_0$ corresponds to $\mathbb{N}$. And we conclude that $\mathbb{N}_0 = \mathbb{N}$.

□

Theorem 20 (Weak principle of induction)**.** Let $p(n)$ be a predicate on $\mathbb{N}$. Suppose the two following propositions hold

(i) $p(0)$ is true

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

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

Proof. 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 by Theorem 19(i), $A = \mathbb{N}$. Which implies that $\forall n \in \mathbb{N}$, $p(n)$ is true. □

Corollary 1. Let $p(n)$ be a predicate on $\mathbb{N}$. Let $k \in \mathbb{N}$ Suppose the two following propositions hold

(i) $p(k)$ is true

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

Then $\forall n \in \mathbb{N}, such that \mathrm{n} \geq k$, we have $p(n)$ is true.

Example 19. Prove that $n^2 \geq 3n$ for $n \geq 3$.

Warning:

(i) Be careful not to overlook the basis! Example: $p(n)$: ”$n > n$”

(ii) If the basis is $P(n_0)$, then do not forget to check that $p(n) \Rightarrow p(n+1)$ for all $n \geq n_0$. Example : Find the mistake in the next proof: All humans have the same gender. So consider a room with n people. For n=1 the statement is obviously true. Now the inductive step: If there are n+1 people in the room we ask one arbitrary person to leave the room. So now only n people are left in the room. By the induction hypothesis all these people have the same gender. The person outside now comes back and another person has to leave the room. So again there are n people in the room and all having the same gender. Hence the n+1 people all have the same gender.

Theorem 21 (Strong principle of induction)**.** $\forall n[(\forall m < n, p(m)) \Rightarrow p(n)]$ then $\forall n, p(n)$.

Proof. The Strong principle of induction follows from the weak principle of induction. Assume that $\forall n[(\forall m < n, p(m)) \Rightarrow p(n)]$ holds. We show by weak induction that $\forall n, p(n)$. We define on $\mathbb{N}$ the predicate $Q(n)$:$'\ \forall m < n, p(m)'$. Our induction hypothesis becomes $\forall n[Q(n) \Rightarrow p(n)]$. We prove by weak induction that $\forall n, Q(n)$. The proposition $Q(0)$ is true because there does not exists natural integer m such that $m < 0$. Suppose $Q(n)$ is true, we shall show $Q(n+1)$. We assumed $\forall n[Q(n) \Rightarrow p(n)]$ therefore $Q(n)$ true implies $p(n)$ true. Hence we have proved $\forall m \leq n$, $p(m)$ holds. Or by Theorem 19(iii), $p(m)$ holds $\forall m < n+1$, ie, $Q(n+1)$ is true. This complete the proof that $\forall n, Q(n)$. □

Theorem 22 (The Least Number Principle, infinite descent of Fermat)**.** The LNP principle states: If $M \subseteq \mathbb{N}$ and $M \neq \emptyset$, then M has a minimum.

Proof. The Least Number Principle follows from the strong principle of induction. Let $p(n)$ be the predicate defined on $\mathbb{N}$ by $p(n)$:$'\ n \notin M'$. Suppose $\forall m < n, p(m)$ holds. This means $\forall m < n, m \notin M$. Hence $m < n \Rightarrow m \notin M$. The contrapositive gives $m \in M \Rightarrow \neg(m < n)$. But $\leq$ is complete, then $\forall x, y \in \mathbb{N}$, $(x < y \vee x = y \vee y < x)$ is true. Therefore, $m < n$ false implies $n \geq m$ true. It follows $\forall m \in M, n \geq m$. Therefore $n \notin M$ otherwise it would be the minimum of M, a contradiction. Hence $p(n)$ holds. □

Note that a nonempty subset of $\mathbb{N}$ does not have always a maximum. Think for example to the odd numbers. However...

Theorem 23. If A is a nonempty subset of $\mathbb{N}$ with an upper bound, then $\max(A)$ exists.

Proof. Since A is a nonempty subset of $\mathbb{N} \subseteq \mathbb{R}$ with an upper bound, we have with the definition of $\mathbb{R}$, $\sup(A) \in \mathbb{R}$. By definition of sup, there exists $a \in A$ such that $\sup(A) - 1 < a \leq \sup(A)$. Hence $\sup(A) < a + 1$. By Theorem 19(iii) there is no integer between a and $a + 1$ □

The following proposes a second proof of the Theorem 20 by using the Least Number Principle: Hence it is possible to prove the strong induction principle from the weak induction principle, the Least Number Principle from the strong induction principle and the weak induction principle from the Least Number Principle: all three principles are equivalent[9].

[9] Usefull when the weak induction principle is an axiom.

A second proof of Theorem 20. Let p be a property such that $p(0)$ holds and $\forall n[p(n) \Rightarrow p(n+1)]$. We must prove $\forall n, p(n)$. This amount to showing that the set $M := \{n \in \mathbb{N}, p(n) \text{ does not hold}\}$ is empty. By the LNP principle, it is enough to show that M has no minimum. Suppose M has a minimum, say m. Since $p(0)$ holds, $0 \notin M$, hence $m \neq 0$. Therefore by Theorem 19(ii), there exists $n \in \mathbb{N}$ such that $m = n + 1$, hence $n < m$. the element m is the minimum of M and $n < m$ means $n \notin M$, which means that $p(n)$ holds. From our assumption, we have then $p(n+1)$ holds, ie, $p(m)$ holds, which means $m \notin M$, a contradiction. □

Lesson 8: liminf and limsup.

Let A be a set and $\leqq$ an order relation on A. We suppose that A satisfies the following property:

$$\forall B \subseteq A, \inf(B) \in A \text{ and } \sup(B) \in A.^{10}$$

Example 20. In the following we consider the two following examples of set together with an order relation which satisfies the previous property:

- $[-\infty, +\infty]$ together with $\leq$.
- If X is a set, 2^X together with $\subseteq$.

Definition 49. A sequence of elements of A (or simply a sequence in A) is a mapping $a : \mathbb{N} \to A$ which associates to every integer $n \in \mathbb{N}$ an element $a_n \in A$ (the notation a_n instead of $a(n)$ is standard). The sequence is usually denoted by $(a_n)_{n\in\mathbb{N}}$, or simply by $(a_n)_n$ or (a_n). The set of sequences in A is denoted $A^{\mathbb{N}}$, that is, the set of mappings from $\mathbb{N}$ to A.

Example 21.

- $(a_n) \in [-\infty, +\infty]^{\mathbb{N}}$ defined by $a_0 = +\infty$ and $a_n = \frac{1}{n} \in \mathbb{R}$ for $n \geq 1$.
- A sequence of subsets of A is a mapping from $\mathbb{N}$ to 2^A which associates to every integer $n \in \mathbb{N}$ a set $A_n \subseteq A$. It is usually denoted by $(A_n)_{n\in\mathbb{N}}$, or simply by $(A_n)_n$ or (A_n).
  - $(A_n) \in (2^{\mathbb{R}})^{\mathbb{N}}$ defined by $A_n = \{[1-n, 1+n]\}$ for $n \in \mathbb{N}$.

Do not make the confusion between a sequence in A, which is a mapping from $\mathbb{N}$ to A and the set of values of the sequences, which is the image of $\mathbb{N}$ by this mapping, that is the set $\{a_n, n \in \mathbb{N}\} \subseteq A\}$. For example, consider the real-valued sequence $(a_n) \subseteq \mathbb{R}$ defined by $a_n = (-1)_n$. Then its set of values is $\{a_n | n \in \mathbb{N}\} = \{-1, +1\}$.

Definition 50. A sequence $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ is said to be:

- increasing if $a_n < a_{n+1}$ for every $n \in \mathbb{N}$,
- decreasing if $a_n > a_{n+1}$ for every $n \in \mathbb{N}$,
- nondecreasing if $a_n \leqq a_{n+1}$ for every $n \in \mathbb{N}$,
- nonincreasing if $a_n \geqq a_{n+1}$ for every $n \in \mathbb{N}$,
- monotonic or monotone if it is either nondecreasing or nonincreasing.

Definition 51. Let $a = (a_n)_{n\in\mathbb{N}}$ be a sequence in A, a subsequence of $(a_n)_{n\in\mathbb{N}}$ is a sequence $b = (a_{nk})_{k\in\mathbb{N}}$ where $\phi = (n_k)_{k\in\mathbb{N}}$ is an increasing sequence of integers. A subsequence of $a = (a_n)_{n\in\mathbb{N}}$ can be equivalently defined as the sequence $a \circ \phi$ for any increasing sequence ϕ of integers.

[10] A set which satisfies this property is called a complete lattice.

Let $a = (a_{nn\in\mathbb{N}}$ be a sequence in A, examples of subsequences of (a_n) are given by the subsequences of its even terms and odd terms, defined respectively by $(a_{2k})_{k\in\mathbb{N}}$ and $(a_{2k+1})_{k\in\mathbb{N}}$.

Definition 52. A family of elements of A indexed by a set I is a mapping from I to A. It associates to every element $i \in I$ an element $a_i \in A$ and is usually denoted by $(a_i)_{i\in I}$, or simply $(a_i)_i$ or (a_i). A family of subsets of A indexed by a set I associates to every element $i \in I$ a subset A_i of A. It is denoted by $(A_i)_{i\in I}$, or simply $(A_i)_i$ or (A_i). A finite family of elements (resp. subsets) of A is a family indexed by a finite set I.

Definition 53. Let us consider a family of sets $(A_i)_{i\in I}$ of A:

(i) The union of the A_i denoted by $\cup_{i\in I} A_i$ is the set defined by

$$\cup_{i\in I} A_i = \{x \in A, \exists i \in I, x \in A_i\}.$$

(ii) The intersection of the A_i denoted by $\cap_{i\in I} A_i$ is the set defined by

$$\cap_{i\in I} A_i = \{x \in A, \forall i \in I, x \in A_i\}.$$

Proposition 12. $\forall (a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}, \sup_{n\in\mathbb{N}} \inf_{k\geq n} a_k \in A$ and $\inf_{n\in\mathbb{N}} \sup_{k\geq n} a_k \in A$.

Proof. Let $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$. We prove $\sup_{n\in\mathbb{N}} \inf_{k\geq n} a_k \in A$ [11]. Let $n \in \mathbb{N}$. We put $A_n = \{a_k, k \geq n\}$. Forall $k \geq n$, $a_k \in A$ therefore $A_n \subseteq A$. By assumption on A,

$$\inf(A_n) = \inf_{k\geq n} a_k \in A.$$

For each $n \in \mathbb{N}$, we put $b_n = \inf(A_n)$. For any $n \in \mathbb{N}$, b_n is an element of A therefore the set

$$B = \{b_n, n \in \mathbb{N}\} \subseteq A.$$

Now by assumption on A, we obtain

$$\sup(B) = \sup_{n\in\mathbb{N}} b_n = \sup_{n\in\mathbb{N}} \inf_{k\geq n} a_n \in A.$$

□

Definition 54. The superior limit of a sequence $(a_n)_{n\in\mathbb{N}}$ is the element $\limsup_n a_n$ of A defined by

$$\limsup_n a_n = \inf_{n\in\mathbb{N}} \sup_{k\geq n} a_k.$$

The inferior limit of a sequence $(a_n)_{n\in\mathbb{N}}$ is the element $\liminf_n a_n$ of A defined by

$$\liminf_n a_n = \sup_{n\in\mathbb{N}} \inf_{k\geq n} a_k.$$

[11] It is similar to prove that $\inf_{n\in\mathbb{N}} \sup_{k\geq n} a_k \in A$

Example 22. • Let $(a_n) \in [-\infty, +\infty]^{\mathbb{N}}$ defined by $a_n = (-1)^n \ \forall n \in \mathbb{N}$. We have:

$$\limsup_n a_n = 1 \text{ and } \liminf_n a_n = -1.$$

Proposition 13. Let X be a set. We consider 2^X together with $\subseteq$. Let $(A_n)_{n\in\mathbb{N}} \in (2^X)^{\mathbb{N}}$:

$$\limsup_n A_n = \bigcap_{n\in\mathbb{N}} \bigcup_{k\geq n} A_k \text{ and } \liminf_n A_n = \bigcup_{n\in\mathbb{N}} \bigcap_{k\geq n} A_k.$$

Proof. Let $n \in \mathbb{N}$. We put $\mathcal{A}_n = \{A_k, k \geq n\}$. It is not difficult to prove that for the order relation $\subseteq$,

$$\inf(\mathcal{A}_n) = \bigcap_{A_k\in\mathcal{A}_n} A_k = \bigcap_{k\geq n} A_k.$$

For each $n \in \mathbb{N}$, we put

$$B_n = \bigcap_{k\geq n} A_k.$$

For any $n \in \mathbb{N}$, B_n is an element of 2^X therefore the set

$$\mathcal{B} = \{B_n, n \in \mathbb{N}\} \subseteq 2^X.$$

It is not difficult to prove that

$$\sup(\mathcal{B}) = \bigcup_{B_k\in\mathcal{B}} B_k = \bigcup_{n\in\mathbb{N}} \bigcap_{k\geq n} A_k.$$

Hence

$$\liminf_n A_n = \sup_{n\in\mathbb{N}} \inf_{k\geq n} A_k = \bigcup_{n\in\mathbb{N}} \bigcap_{k\geq n} A_k.$$

The proof is similar for lim sup... □

Example 23. Let $(A_n) \in (2^{\mathbb{R}})^{\mathbb{N}}$ defined by $A_n = \{(-1)^n\} \ \forall n \in \mathbb{N}$. We have:

$$\limsup_n a_n = \{-1, 1\} \text{ and } \liminf_n A_n = \emptyset.$$

The superior limit of a sequence $(A_n)_{n\in\mathbb{N}}$ of subsets of a set X can be seen as the set of elements in X that belong to infinitely many A_n.

$$x \in \limsup_n A_n \Leftrightarrow x \in \bigcap_{n\in\mathbb{N}} \bigcup_{k\geq n} A_k \Leftrightarrow \forall n \in \mathbb{N}, \exists k \geq n, x \in A_k.$$

The inferior limit of a sequence $(A_n)_{n\in\mathbb{N}}$ of subsets of a set X can be seen as the set of elements in X that belong all A_n from a certain n.

$$x \in \liminf_n A_n \Leftrightarrow x \in \bigcup_{n\in\mathbb{N}} \bigcap_{k\geq n} A_k \Leftrightarrow \exists n \in \mathbb{N}, \forall k \geq n, x \in A_k.$$

Definition 55. If $\limsup_n a_n = \liminf_n a_n$ we use the notation $\lim_n a_n$. This element is called the limit of $(a_n)_{n\in\mathbb{N}}$.

Lemma 5. Let $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$. The sequence $(b_n)_{n\in\mathbb{N}}$ defined by $b_n = \inf_{k\geq n} a_k$ is nondecreasing and the sequence $c_n = \sup_{k\geq n} a_k$ is nonincreasing.

Proof. Let n be an element of $\mathbb{N}$. For all $k \geq n+1$, we have $b_n \leqq a_k$ which implies that b_n is a lower bound of $\{a_k, k \geq n\}$. Since b_{n+1} is the greatest lower bound of $\{a_k, k \geq n\}$, we have immediatly $b_n \leqq b_{n+1}$. Hence b_n is nondecreasing. The proof is similar for $(c_n)_{n\in\mathbb{N}}$. □

Proposition 14. Let $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$.

$$\liminf_n a_n \leqq \limsup_n a_n.$$

Proof. $\forall n \in \mathbb{N}$, $\inf_{k\geq n} a_k \leqq a_n$ and $a_n \leqq \sup_{k\geq n} a_k$. By transitivity of we have

$$\forall n \in \mathbb{N}, \inf_{k\geq n} a_k \leqq \sup_{k\geq n} a_k.$$

We put $b_n = inf_{k\geq n} a_k$ and $c_n = \sup_{k\geq n} a_k$. Hence for any $n \in \mathbb{N}$, we have $b_n \leqq c_n$. By definition $\sup_n b_n \in A$ satisfies $b_n \leqq \sup_n b_n$ for all n and $\forall M \in A$ such that $b_n \leqq M$ for all n, we have $\sup_n b_n \leqq M$. Let $n \in \mathbb{N}$. We want to prove that $\forall r \in \mathbb{N}$, $b_n \leqq c_r$. If $n = r$ we have seen $b_n \leqq c_n$. Since (b_n) is nondecreasing and (c_n) nonincreasing,

- If $n < r$, we have
$$b_n \leqq b_r \leqq c_r \leqq c_n$$
- if $r < n$, we have
$$b_r \leqq b_n \leqq c_n \leqq c_r$$

In all cases, $b_n \leqq c_r$. Hence $\forall r \in \mathbb{N}$, $b_n \leqq c_r$. Therefore $b_n \leqq \inf_{r\in\mathbb{N}} c_r$. Since n is arbitrary, we have

$$\forall n \in \mathbb{N}, b_n \leqq \inf_{r\in\mathbb{N}} c_r.$$

Therefore $\inf_{r\in\mathbb{N}} c_r$ is an upper bound of $\{b_n, n \in \mathbb{N}\}$ which implies that

$$\sup(b_n) \leqq \inf_{r\in\mathbb{N}} c_r.$$

This last expression is equivalent to

$$\liminf_n a_n \leqq \limsup_n a_n.$$

□

Theorem 24. If $(a_n)_{n\in\mathbb{N}}$ is nondecreasing then $lim_n a_n$ exists and we have:

$$\lim_n a_n = \sup_{n\in\mathbb{N}} a_n.$$

If $(a_n)_{n\in\mathbb{N}}$ is nonincreasing then $lim_n a_n$ exists and we have:

$$\lim_n a_n = \inf_{n\in\mathbb{N}} a_n.$$

Proof. Let $(a_n)_{n\in\mathbb{N}}$ be a nondecreasing sequence in A. For all $n \in \mathbb{N}$,

$$\inf_{k\geq n} a_k = a_n$$

Hence

$$\liminf_n a_n = \sup_n \inf_{k\geq n} a_k = \sup_{n\in\mathbb{N}} a_n \geqq \inf_{n\in\mathbb{N}} \sup_{k\geq n} a_k = \limsup_n a_n.$$

Therefore $\limsup_n a_n \leqq \liminf_n a_n$. Since we always have $\liminf_n a_n \leqq \limsup_n a_n$, we deduce, by antisymmetry of $\leqq$ that:

$$\lim_n a_n = \limsup_n a_n = \liminf_n a_n = \sup_{n\in\mathbb{N}} a_n.$$

The proof is similar in the case where $(a_n)_{n\in\mathbb{N}}$ is nonincreasing. □

Lesson 9: Cardinality.

Let $p, n \in \mathbb{N}$, we denote by $\{p, \dots, n\}$ the set defined by

$$\{p, \dots, n\} := \{k \in \mathbb{N}, p \leq k \leq n\}.$$

Proposition 15. If $f : E \to \{1, \dots, n\}$ and $g : E \to \{1, \dots, p\}$ are two bijections, then $n = p$.

Proof.

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

(ii) suppose $n \geq p$. g is a bijection, then g^{-1} is a bijection, therefore $h_2 = g \circ f^{-1} : \{1, \dots, n\} \to \{1, \dots, p\}$ is a bijection. Hence h_2 is a surjection, therefore $\forall j \in \{1, \dots, p\}, \exists i \in \{1, \dots, n\}$ such that $h_2(i) = j$ which implies $p \geq n$. $\Rightarrow n = p$. □

Definition 56. A set E is finite if $E = \emptyset$ or if there exists $n \in \mathbb{N} \setminus \{0\}$ and a bijection $f : E \to \{1, \dots, n\}$. By previous Proposition, n is well defined, it is called the cardinality of E. Notation : $|E|$. We put $|\emptyset| = 0$.

Proposition 16. Let E and F be two finite sets.

$$|E| = |F| \iff \text{There exists } f : E \to F \text{ bijective.}$$

Proof.
- "$\Rightarrow$". Let $|E| = |F| = n$. $f_1 : E \to \{1, \dots, n\}$, $f_2 : F \to \{1, \dots, n\}$ bijective implies $f_2^{-1} \circ f_1 : E \to F$ bijective as composition of two bijections.
- "$\Leftarrow$". E and F finite implies the existence of two bijections $f_1 : E \to \{1, \dots, |E|\}$ and $f_2 : F \to \{1, \dots, |F|\}$. Let $f : E \to F$ bijective. We have $f_2 \circ f : E \to \{1, \dots, |F|\}$ et $f_1 : E \to \{1, \dots, |E|\}$ two bijective functions. By Proposition 15, we have $|E| = |F|$. □

Definition 57. A set which is not finite is said to be infinite.

Definition 58. We say that two sets A and B have the same cardinality (or same power) if there is a bijection between A and B.

Theorem 25 (Cantor-Schröder-Bernstein)**.** Let A and B be two sets. Exactly one of these cases holds:

(i) There exists an injection from A to B, but no injection from B to A. (In this case, there is a surjection from B to A but no surjection from A to B).

(ii) There exists an injection from B to A, but no injection from A to B. (In this case, there is a surjection from A to B but no surjection from B to A).

(iii) There is a bijection from A to B. This case is consequently the only case where we can find

  (a) an injection from A to B and an injection from B to A

  (b) a surjection from A to B and a surjection from B to A

In order to prove there exists a bijection from A to B, it suffices to find :

(i) either an injection from A to B and an injection from B to A

(ii) or a surjection from B to A and a surjection from A to B

Theorem 26 (Cantor)**.** Let E be a set, there is no injection from 2^E to E. (equivalently, there is neither surjection nor bijection from E to 2^E).

Proof. Suppose there exists a surjection $f : E \to 2^E$. We define a set $A := \{x \in E, x \notin f(x)\}$. Since f is surjective $\exists y \in E$ such that $f(y) = A = \{x \in E, x \notin f(x)\}$. Either $y \in A$ and we have $y \notin f(y) = A$ (absurd); or $y \in E \setminus A$ and we have $y \in f(y) = A$ (absurd). Hence there is no surjection from E to 2^E. □

A set with the same cardinality than $\mathbb{N}$ is said to be countably finite. Sets being finite or countably infinite are countable. Others are uncountable.

Proposition 17.(i) Subsets of countable sets are countable

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

(iii) A set E is countable if and only if there exists an injection from E to $\mathbb{N}$

Theorem 27. If E is infinite, then it countains at least a countable set.

Proof. Apply Cantor-Shröder-Bernstein Theorem and the last point of the previous Proposition. □

Theorem 28. A set E is finite if and only if $\forall A \subsetneq E$, there is no bijection between A and E.

Theorem 29. Let $n \in \mathbb{N}$, the union of a n countable sets is countable. Particularly, $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ is countable.

Theorem 30. Let $n \in \mathbb{N}$, the cartesian product of n countable sets is countable.

Theorem 31. $\mathbb{Q}$ is countable

Theorem 32. $\mathbb{N}^{\mathbb{N}}$, $[0, 1]$ and $\mathbb{R}$ are uncountable.