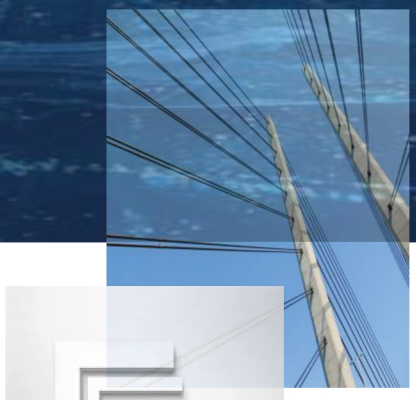
HDBOM

HANDBOOK OF MATHEMATICS



T. VIALAR

HANDBOOK OF MATHEMATICS

Thierry VIALAR

Edition : BoD - Books on Demand
12/14 rond-point des Champs Elysées, 75008 Paris
Imprimé par Books on Demand GmbH, Norderstedt, Allemagne

ISBN 978-2-32200-967-1 (Print)
ISBN 978-2-32200-082-1 (EPDF)

Dépôt légal : Juin 2015

Thierry Vialar. Doctor of:
University of Paris X Nanterre
200, avenue de la République
92001 Nanterre Cedex - France

Contents

Introduction

The book consists of XI Parts and **28** Chapters, introduced as follows:
PART I. FOUNDATIONS OF MATHEMATICS. **1. Mathematical Logic.** Mathematical logic (formerly known as *symbolic logic*, or sometimes *bivalent logic*) can be described as the formal mathematical study of the methods, structure, and validity of mathematical deduction and proof. This discipline defines the language used to express a mathematical proposition, and it establishes the rules used to deduce new statements from given statements; it studies the forms of assertion and the methods of demonstration. Mathematical logic is the study of mathematical theories from the viewpoint of model theory, recursive function theory, proof theory, and set theory. **2. Set Theory.** In set theory, the concept of set is the main tool for the construction of pure mathematics, especially by stating relationships between sets. The properties of the algebra of sets and its symbolism allow a unified description of the different disciplines of mathematics. **3. Relations and Structures.** *Relations* allow to establish relationships between the elements of the same set. e.g. classification by an equivalence relation) or of different sets. *Structures* on sets results from specific relationships. Examples of structures are the algebraic structure, topological structure, order structure. **4. Arithmetic.** Arithmetic is the science of numbers and more specifically that of *whole numbers*, whether *natural* (0,1,2,...) or *integer* (...,-2,-1,0,1,2,...). It studies thus the sets $\mathbb{N}$ and $\mathbb{Z}$. The main tools are the four operations, addition, multiplication, subtraction, division, to which we have to add the order relation $\leqslant$. In this chapter, the objective is not to study $\mathbb{N}$ and $\mathbb{Z}$ for themselves but in connection with many areas of mathematics (or applications) in which they operate. Of course, this chapter is closely related to the chapters "*Construction of Number System*" and "*Number Theory*"; but in this chapter the theorems are given with their proofs. **5. Construction of Number System.** All mathematical disciplines make use of appropriate numerical domains. The construction of number system requires the definition of natural numbers and their successive extensions; so we describe the problem of the completion of a space with respect to structural properties determined. The use of objects such as numbers, geometric objects, structures, leads to divide mathematics into several branches; such a partitioning also results from the history of mathematics and from the influences of many other sciences, such as engineering, materials science, physics, computer science,...
PART II. ALGEBRA. **6. Algebra.** In algebra, we study sets with algebraic structure (groups, rings, fields, vector spaces,..) and also methods for solving equations and systems of equations. Thus, we are led in the framework of linear algebra to the notions of matrix and determinant, and to their applications to systems of linear equation. We describe the Galois theory; and especially by algebraic equations in relation to geometric problems.
PART III. NUMBER THEORY. **7. Number Theory.** In number theory, we can deal with the divisibility and its applications in the ring of integers, we can also deal with the calculations in the field of reals. The tools of number theory belong to analysis as well as to algebra.
PART IV. GEOMETRY. **8. Geometry.** This discipline deals with the study of shapes and sizes of figures.Clearly, the visual space is the source of concepts of geometry. By extension, depending on the chosen axiomatic system, we are axiomatically led to abstract spaces which have significant differences.
PART V. ANALYTIC GEOMETRY. **9. Analytic Geometry.** Vector spaces and its ramifications, especially the use of coordinates, are the basic means of analytic geometry; i.e. the algebra serves the geometry.
PART VI. TOPOLOGY. **10. Topology.** This branch studies the topological structure that we can assign to sets. The fundamental concepts used (open parts, neighborhoods, etc) are part of the analysis. The axiomatic definition of a topology allows to assign a topology to any set. An essential issue is the choice of an "efficient" topology (metric topologies often have this ability). **11. Topology II.** This chapter is independent and an advanced presentation of the topology; theorems, propositions, lemmas, corollaries are mostly provided with their proofs.
PART VII. ALGEBRAIC TOPOLOGY. **12. Algebraic Topology** (formerly known as **analysis situs**, sometimes used to directly denote *Topology*). Algebraic topology involves algebraic means (groups, modules, etc) to solve topological problems. Homotopy and Homology theories have been developed to this end. Note that **graph theory** follows from the topology, and deals with the study of theoretical and practical problems that we can reduce to problems on a set of points of which some are connected by segments. **13. Algebraic Topology II**. Algebraic topology is a mixture of algebra and topology. The main purpose is to convert problems about topological spaces and continuous functions into problems about algebraic objects (e.g. groups, rings, vector spaces) and their homomorphisms. In this independent Chapter, we deepen algebraic topology and provide a more advanced treatment. Algebraic topology are introduced using standard material about the fundamental groups of spaces, and Brouwer fixed point theorem, and fundamental theorem of algebra.
PART VIII. ANALYSIS. **14. Real Analysis.** Real Analysis is the branch of mathematics dealing with functions of real variables. While this includes some parts of topology, it is most commonly used to distinguish that part of calculus dealing with real numbers as opposed to complex numbers. **15. Differential Calculus.** Together *differential calculus* with *integral calculus* (both together are also known as **infinitesimal calculus**) are based on the notion of limit; they allow to show special properties of certain real functions of the real variable, i.e. differentiability (in connection with to the notion of tangent to a curve) and integrability (in connection with the notion of area bounded by a curve). Differential calculus and integral calculus are also compatible with higher dimensions. **16. Integral Calculus.** The above comments about the differential calculus also hold for the integral calculus. Integral calculus may be defined as the study of integration and its applications to finding areas, volumes, or solutions of differential equations. The **measure theory** is a generalization of the integration theory; it studies the way to associate with a set of points a real number that gives the value of its content. In practice, we know that many problems lead to differential equations involving functions with one or several variables. The **theory of differential equations** provides methods that allow to study and solve such equations. **17. Functional Analysis.** Functional analysis is a branch of mathematics concerned with infinite dimensional vector spaces (mainly function spaces) and mappings between them. The spaces may be of different, and possibly infinite, dimensions. These mappings are called operators or, if the range is on the real line or in the complex plane, functionals. Certain handbooks define simply the functional analysis as the branch of analysis which studies the properties of mappings of classes of functions from one topological vector space to another. Indeed, if we apply topological methods to certain sets of maps or functions (function spaces), we are led to a generalization (whose scope is particularly important) of the differential calculus and integral calculus (*infinitesimal calculus*), it is the object of the *functional analysis*. Here the topologies involved are those of particular normed vector spaces. **18. Differential Equations.** A differential equation is an equation expressing a relationship between functions and their derivatives; so a differential equation involves the derivatives of a function as well as the function itself. If only ordinary derivatives are present, the equation is called an ordinary differential equation; if partial derivatives are involved, the equation is called a partial differential equation. Differential equations play an essential role in applied math., engineering, physics, and much mathematical and numerical machinery has been developed for the solution of differential equations. **19. Differential Geometry.** The differential geometry deals with geometric figures that can be approached by the *infinitesimal calculus*. Differential geometry includes the theories of curves and surfaces which are essential subdivisions; this is why many handbooks define this branch as the study of curves and surfaces using the methods of *differential calculus*. **20. Function Theory (Complex Analysis).** The methods of infinitesimal calculus can be applied and adapted to the complex function of the complex variable, this transposition leads to a particularly elegant theory, which is called *function theory*; the method of the analytic continuation leads to the fundamental concept of Riemann surface. **21. Complex Analysis II.**

This chapter is an independent and more advanced presentation of the complex analysis; Here, theorems, propositions, lemmas and corollaries are often provided with their proofs. Note that this chapter is more difficult and is preferably reserved for readers involved in the field.

PART IX. CATEGORY THEORY. **22. Areas involved in category theory.** Category theory is explicitly presented in chapter **23**. This recent theory, and its vast extent, implicitly involves other areas of mathematics, this leads us (as preconditions) to first group and define number of underlying notions from these areas. **23. Category theory.** This chapter provides concepts, statements and definitions that explicitly involve the notion of category.

PART X. PROBABILITY AND STATISTICS. **24. Probability.** Here, we mean *combinatorial analysis* or *combinatorics,* which is the branch of mathematics studying the enumeration (meaning counting in combinatorics), combination and permutation of sets of elements and the mathematical relations characterizing their properties; it also helps to solve certain enumeration problems of finite sets, whether in geometry, in number theory, in graph theory or in *calculation of probability.* **25. Probability Calculation, Statistics.** The **probability calculation** provides theorems concerning the occurrence of a random event and contributes to the foundation of the **statistics**. More recently, the **statistical models** have been developed; such models are formal presentations of phenomena in the form of equations whose variables are quantities belonging to a science. The statistician makes hypotheses and makes explicit relationships. The model specification generally refers to a theory (in physics, chemistry, economics, etc) and tries to explain the behaviors of variables. Statistical modelling is known as *econometrics*; It also deals with *time series analysis.*

PART XI. APPLIED MATHEMATICS. **26. Miscellaneous.** The present chapter describes fundamental areas and concepts having many applications in practice, i.e. the integral transformations, Fourier transformations and series and distribution theory. **27. Optimization.** Optimization is the maximizing or minimizing of a given function possibly subject to some type of constraints. Optimization theory consists of specific methods, techniques and procedures used to decide on the one specific solution in a defined set of possible alternatives that will best statisfy a selected criterion; includes *linear programming*, *nonlinear programming*, *stochastic programming*, *control theory.* It also includes convex optimization, queuing systems, decision theory, game theory, Markov chains, network analysis, and calculus of variations. **28. Dynamical systems.** A dynamical system describes a phenomenon depending on time. Dynamical systems theory is an area of applied mathematics used to describe the behavior of complex dynamical systems (often equated with chaos theory), usually by employing differential equations or difference equations. When differential equations are employed, the theory is called continuous dynamical systems. When difference equations are employed, the theory is called discrete dynamical systems. Fixed points, steady states, periodic points, attractive sets, attractors, strange attractors,... are objects studied by this theory and by chaos theory. Even simple nonlinear dynamical systems can exhibit very complex behaviors.

*

Scope and vocabulary of analysis: (1) Analysis. The **analysis** in the broad sense (not only reduced to the **real analysis**) can be regarded as the study of real-valued and complex-valued continuous functions. Important branches of analysis include **calculus**, **differential equations**, and **functional analysis**. The term is generally reserved for advanced topics which are not encountered in an introductory calculus sequence, although many ideas from those courses, such as derivatives, integrals, and series are studied in more detail. Real analysis and complex analysis are two broad subdivisions of analysis which deal with real-values and complex-valued functions, respectively. Analysis is generally described as "the study of limits". Indeed, **analysis** is the area of mathematics generally taken to include those topics that involve the use of limiting processes. Thus **differential calculus** and **integral calculus** certainly come under this heading. Besides these, there are other topics, such as the summation of infinite series, which involve "infinite" processes of this sort. "*Binomial theorem*", a theorem of algebra, leads on into analysis when the index is no longer a positive integer, and the study of sine and cosine, which begins as trigonometry, becomes analysis when the power series for the functions are derived. The term "analysis" has also come to be used to indicate a rather more rigourous approach to the topics of calculus, and to the foundations of the real number system. (2) Calculus. The **calculus**, which is more properly called **analysis** or **real analysis** or in older literature **infinitesimal analysis,** is the branch of mathematics studying the rate of change of quantities (which can be interpreted as slopes of curves) and the length, area, and volume of objects. As previously seen, the *calculus* is divided into **differential and integral calculus**. (3) Calculus and analysis. Given the proximity of the two branches and their subdivisions, many handbooks merge calculus and analysis in a single branch, namely, **calculus and analysis**.

*

The list of Parts and Chapters is as follows:

Parts

Chapters

*
* *
*

Part I

Foundations of Mathematics

Chapter 1

Mathematical Logic

1. Propositions, Connections

1.1. Logical propositions, truth value.
A statement that makes an assertion that is either false or true or has been designated as false or true. A *proposition* is a mathematical statement for which a proof is either required or provided. It belongs to the class of true propositions or false propositions. This is the two-valued principle (also called bivalence principle, two-value principle, or double value principle) of the two-valued logic. If a statement is true, its truth value is T (*True*). If a statement is false, its truth value is F (False). If p is a proposition, $v(p)$ is its truth value (using notation v). *Examples of proposition*: 1) p_1: 1 is an odd number. $v(p_1)=T$. 2) p_2: 5 is an even number. $v(p_2)=F$. 3) p_3: The non differentiable continuous functions exist. $v(p_3)=T$. 4) p_4: Any quadrilateral with two equal opposite sides and two equal opposite angles is a parallelogram. $v(p_4)=F$. 5) p_5: Any even number greater than 2 is a sum of two prime numbers. (Goldbach's conjecture). $v(p_5)=Unknown$.

1.2. Connection of propositions, logical connectives. Of course, every sequence of letters or numbers is not necessarily a proposition. For example, the two followings sequences are propositions: "7 is a prime", "11 is greater than 7". But the following sequences are not propositions: "7 is smaller", "$P(.)$", "$P(9)$", "$P(12,5,7)$", "x+7=11". Note that sequence x+7=11 contains what is called a *variable*. Indeed, x can be replaced by an integer number and immediately the sequence which is obtained becomes a *proposition*. The following sentences, which are *predicates*: " ... is a prime number" or " ... is an even number" can be assigned to $P(.)$, then introducing any number, we obtain the following sentences, for example: "2 is an even number" or "5 is a prime number". Such sentences are propositions. In the same way, we can assign the predicate " ... is the sum of ... and ... " to P in the sequence: $P(12,5,7)$. Thus the predicate becomes the following proposition: "12 is the sum of 5 and 7". All these kinds of proposition are called *propositional formulas*. The truth value of this last propositional formula is T.
Many propositions, or propositional formulas, consist of parts which are themselves propositions. Intermediate words are then introduced, such as : no, and, or, if ...then, if and only if. Usually, mathematics uses "symbols", which are "*logical connectives*". A function, or the symbol representing a function, which corresponds to English conjunctions such as "and," "or," "not,", "nor", etc. that takes one, or more, truth values as input and returns a unique truth value as output. The terms "logical connective" and "*propositional connective*" are also used. Unfortunately, each symbol is still not universal, but the following writings seem to be accepted : $\neg\ A$ for "non A", $A \wedge B$ for "A and B", $A \vee B$ for "A or B", $A \Rightarrow B$ for "A implies B", $A \Leftrightarrow B$ for "A equivalent B", $A \Leftrightarrow B$ for "A if only if B"). The table below summarizes some common connectives:

Connective	*Symbol*	*Less common symbol*
and	$A \wedge B$	$A \cdot B$,$A.B$,AB,$A\&B$.
or	$A \vee B$	$A+B$, $A\|B$, $A\|\|B$.
not	$\neg\ A$	$!A$, $\overline{A}$, $\sim A$.
implies	$A \Rightarrow B$	$A \supset B$, $A \rightarrow B$.
equivalent	$A \Leftrightarrow B$	$A \equiv B$, $A \rightleftharpoons B$.
nand	$A \barwedge B$	$A \mid B$, $\overline{A.B}$.
nor	$A \barvee B$	$A \downarrow B$, $\overline{A+B}$.
xor	$A \veebar B$	$A \oplus B$.
non-equivalent	$A \not\Leftrightarrow B$	
xnor	A *xnor* B	

These logical connectives are defined in such manner that the truth value of a proposition can be determined by the knowledge of truth values of its parts. By an *assignment* associating a truth value with each (part or) subproposition, we get the truth value of a combined statement via truth values of its components. Truth table is a table giving the result of truth values of the combined statement. Truth table for $\neg p$ is

$v(p)$	$v(\neg p)$
T	F
F	T

.
Combined truth tables for $v(p \wedge q)$,$v(p \vee q)$,$v(p \Rightarrow q)$ are

$v(p)$	$v(q)$	$v(p \wedge q)$	$v(p \vee q)$	$v(p \Rightarrow q)$
T	T	T	T	T
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

From this, any other truth table can be completed.

$v(p)$	$v(q)$	$v(k)$	$v(p \wedge q)$	$v((p \wedge q) \vee (\neg k))$
T	T	T	T	T
T	T	F	T	T
T	F	T	F	F
T	F	F	F	T
F	T	T	F	F
F	T	F	F	T
F	F	T	F	F
F	F	F	F	T

Last column above (giving the truth table for the compound statement $(p \wedge q) \vee (\neg k)$) is found by first completing columns for $p \wedge q$ and $\neg k$. From the following truth values for p and q propositions

$v(p)$	$v(q)$
T	T
T	F
F	T
F	F

for the main 5 logical connectives, the truth table is:

$v(\neg p)$	$v(p \wedge q)$	$v(p \vee q)$	$v(p \Rightarrow q)$	$v(p \Leftrightarrow q)$
T	T	T	T	T
	F	T	F	F
F	F	T	T	F
	F	F	T	T

We can design 16 common logical connectives (partially shown in the first table) with the 5 precedent logical connectives. In addition, these 5 main connectives can also be reduced. For example, using (Sheffer) the "*nand*" and "*nor*" logical connectives, a description of $\neg$, $\wedge$, $\vee$, $\Rightarrow$ connectives can be provided as follows:

	"*nor*"	"*nand*"
$\neg p$	$p \mid p$	$p \barvee p$
$p \wedge q$	$(p \mid q) \mid (p \mid q)$	$(p \barvee p) \barvee (q \barvee q)$
$p \vee q$	$(p \mid p) \mid (q \mid q)$	$(p \barvee q) \barvee (p \barvee q)$
$p \Rightarrow q$	$p \mid (p \mid q)$	$(q \barvee (p \barvee q)) \barvee (q \barvee (p \barvee q))$

If we give up the two-valued logic, more then 2 truth values become possible. This logic with more then 2 truth values was applied in mathematics or physic in different fields but never played a first role.
A *sentential variable*, also called a *propositional variable*, that can be substituted for in arbitrary sentential formulas. An expression which is a sentence or which contains variables and becomes a sentence upon appropriate substitutions for these variables (Carnap). *Sentential formulas* are also known as *propositional formulas* (or, for short, simply "formulas"). A "*tautology*" is a logical statement in which the conclusion is equivalent to the premise. If p is a tautology, it is written $\models p$. A sentence whose truth table contains only "T" is called a tautology. These sentences are examples of tautologies: $p \wedge q \equiv !(!p \vee !q)$, $p \vee q \equiv !p \Rightarrow q$, $p \wedge q \equiv !(p \Rightarrow !q)$, where $\wedge$ denotes "*and*", $\equiv$ denotes "is equivalent to ", ! denotes "*not*", $\vee$ denotes "*or*", and $\Rightarrow$ denotes "implies". The tautologies are particular propositional formulas because they are true for all substitutions. For example: $p \Rightarrow p$, or $((p \Rightarrow q) \wedge (q \Rightarrow p)) \Rightarrow (p \Leftrightarrow q)$. However, propositional formulas: $((p \Rightarrow q) \wedge p) \wedge \neg q$ or $\neg p \wedge p$ are false for all substitutions. These propositional formulas are said "contradictory".

1.3. Propositional calculus theorems.
The formal basis of logic dealing with the notion and usage of words such as "*not*", "*or*" "*and*", and "*implies*". (Many systems of propositional calculus were devised to try to achieve *consistency*, *completeness*, and *independence* of *axioms*.) The term "*sentential calculus*" is sometimes used as a synonym for "*propositional calculus*". *Axioms* (or their schemata) and *rules of inference* define a proof theory, and various equivalent proof theories of propositional calculus can be devised. Below, list (Kleene) of axiom schemata of propositional calculus.
(1) $a \Rightarrow (b \Rightarrow a)$
(2) $(a \Rightarrow b) \Rightarrow ((a \Rightarrow (b \Rightarrow c))(a \Rightarrow c))$
(3) $a \Rightarrow (b \Rightarrow a \wedge b)$
(4) $a \Rightarrow (a \vee b)$

(5) $a \Rightarrow (b \vee a)$
(6) $a \wedge b \Rightarrow a$
(7) $a \wedge b \Rightarrow b$
(8) $(a \Rightarrow b) \Rightarrow ((c \Rightarrow b) \Rightarrow (a \vee c \Rightarrow b))$
(9) $(a \Rightarrow b) \Rightarrow ((a \Rightarrow \neg b) \Rightarrow \neg a))$
(10) $\neg\neg a \Rightarrow a$.
In each schema a, b, c can be replaced by any sentential formula. Usually the simplest way to write the rule called "*Modus Ponens*" is: $(a \Rightarrow b) \wedge a \Rightarrow b$. Alternatively, the Modus Ponens rule, which is the sole rule of inference (deductive reasoning), can also be written as: (11) $\frac{a, a \Rightarrow b}{b}$. This rule states that if each of a and $a \Rightarrow b$ is either an axiom or a theorem formally deduced from axioms by application of inference rules, then b is also a formal theorem. Other rules are derived from Modus Ponens and then used in formal proofs to make proofs shorter and more understandable. (These rules serve to directly introduce or eliminate connectives. "*Modus Ponens*" is basically $\Rightarrow$-elimination, and the deduction theorem is $\Rightarrow$-introduction, that will be presented in the section relative to *demonstrations*).
Proof theories based on "*Modus Ponens*" are called Hilbert-type whereas those based on introduction and elimination rules as postulated rules are called Gentzen-type. All formal theorems in propositional calculus are tautologies and all tautologies are formally provable. Thus, proofs can be used to discover tautologies in propositional calculus, and truth tables can be used to discover theorems in propositional calculus. *Fundamental theorems in propositional calculus* are given by:

Th. 1. *(Propositional Calculus theorems):*
Excluded third principle: $a \vee \neg a$.
Law of non-contradiction: $\neg(a \vee \neg a)$.
Law of double negation: $\neg(\neg a) \Leftrightarrow b$.
Laws of Morgan: $\neg(a \wedge b) \Leftrightarrow \neg a \vee \neg b$, *and* $\neg(a \vee b) \Leftrightarrow \neg a \wedge \neg b$.
Rule of contraposition: $a \Rightarrow b \Leftrightarrow \neg b \Rightarrow \neg a$.
Rule of modus ponens: $(a \Rightarrow b) \wedge a \Rightarrow b$.
Rule of modus tollens: $(a \Rightarrow b) \wedge \neg b \Rightarrow \neg a$.
Rule of modus barbara: $(a \Rightarrow b) \wedge (b \Rightarrow c) \Rightarrow (a \Rightarrow c)$.
Rules of distributivity: $a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c)$, *and* $a \vee (b \vee c) \Leftrightarrow (a \vee b) \vee (a \wedge c)$.

The theorems in propositional calculus determine the argument rules with which it is possible to construct new propositions. The precedent table presents the few (not complete) theorems which are particularly important in propositional calculus. In this table, to simplify the writing, some brackets have been removed via the following conventions: the connectives $\wedge, \vee, \Rightarrow, \Leftrightarrow$ have, in this order, an increasing priority. From (7) and (9), we infer the following fundamental rules:
(1) *Syllogism* rule or *Modus ponens*: If $a \Rightarrow b$ and a are true, b is true.
(2) *Modus tollens*: If $a \Rightarrow b$ and $\neg b$ are true, $\neg a$ is true.
(3) *Transitivity* rule or *Modus barbara:* If $a \Rightarrow b$ and $b \Rightarrow c$ are true, $a \Rightarrow c$ is true.
Another formulation is: $\frac{a \Rightarrow b \quad a}{b}$ $\frac{a \Rightarrow b \quad \neg b}{\neg a}$ $\frac{a \Rightarrow b \quad b \Rightarrow c}{a \Rightarrow c}$
We can always determine the validity of a propositional formula in a finite number of steps, and so to know if it forms a propositional calculus theorem. Indeed, it suffices to assign to propositional variables all the authorized truth values. This comes down to consider the connectives as functions operating on the truth values; this method is said to be "semantic".
The other method, called "syntactic", aiming at constructing a complete system of theorems in propositional calculus. Then, we can construct a system of propositional formulas (axioms) and derived rules from which we can deduce the *theorems of propositional calculus*. The term "**axiom**" has been just introduced and a definition can be proposed: *an axiom is a proposition regarded as self-evidently true without proof.* An axiom can be seen as a synonym for *postulate*.

2. Propositional and Predicate Calculus

2.1. Predicates, quantifiers. As already mentioned, the propositional calculus is the mathematical study of logical connectives between propositions and deductive inference, and the term "sentential calculus" is sometimes used as a synonym for propositional calculus. However, the propositional calculus is not sufficient for elaborate the mathematics theories. It is necessary to introduce the notions of *individuals*, *predicates* and *terms of quantization* as "for all" which is written by the symbol "$\forall$" and "there exists" which is written by the symbol "$\exists$". *Individual* is one of the basic objects treated in a given formal language system. The term is sometimes also used as a synonym for *urelement*. An urelement contains no elements, belongs to some set, and is not identical with the empty set. "Ur" is a prefix which has a meaning close to "primeval." Urelement is also called "atoms" or "individual" (see Moore). However, *in the pure set theory, all elements are sets and there are no urelements.* So "individual" is one of the basic objects treated in a given formal language system and the term is sometimes also used as a synonym for "urelement" or "atom". A predicate could be defined as a relation on a set of individuals. *A predicate is that which is affirmed or denied concerning a subject.* For example, in the conclusion of the following syllogism: "Socrates is mortal", the issue is "Socrates" and the "attribute" is "mortal". "Socrates is mortal" is a *predicate* with a single subject. Such a predicate, with also a single argument, can be called a *property.* A predicate with more than one subject is a *relation.* Finally, the *terms of quantization* are introduced, which are also called "*Quantifiers*": one of the operations exists $\exists$, called the *existential quantifier*, or for all $\forall$, called the *universal quantifier*, or sometimes, the *general quantifier*. There also exist specific scientific logics which use quantifiers other than these.

2.2. First-order predicate calculus. As said before, a predicate is an expression which ascribes a property to one or more subjects. "Socrates is mortal" is a *predicate* with a single subject. Such a predicate with also a single argument can be called a *property.* A predicate with more than one subject is a *relation.* "Mary, Kathleen and Tracey are sisters" is a predicate with multiple binary relations between pairs of subjects. A variable can be associated with quantifiers as follows: $\forall x$ or $\exists x$. A predicate could be also defined as a relation on a set of individuals. x is a *variable* associates with an element of a set of individuals. For example: choosing a predicate with a single argument such as: "is prime number", then calling this predicate: P, and considering the proposition (which is not a propositional formula): "there exists a prime number between 20 and 28 ", this can be written: $\exists x, P(x) \wedge 20 < x < 28$, x belonging to natural numbers. Or, can also be written: $\exists x \in \mathbb{N}, P(x) \wedge 20 < x < 28$. It is generally said that x is *linked* to quantifier. A *predicate with 3 arguments* can be written for example as follows: $\forall x, \forall y, x \in \mathbb{R} \wedge y \in \mathbb{R} \Rightarrow \exists z, z \in \mathbb{R} \wedge P_3(x, y, z)$, where P_3 means: "z is the difference between x and y". P_3 is a predicate with 3 arguments. In this case, the *variable x is linked* to the quantifier. A *free variable* in logic is a variable that has an occurrence which is not within the scope of a quantifier and thus can be replaced by a constant. By contrast, a *linked variable* in logic is within the scope of a quantifier. Note that a *dummy variable* is a variable that has no true mathematical significance and is used only to facilitate notation (usually a variable which is integrated over). Dummy variables are also called *bound variables* or *dead variables.* Comtet adopts a notation in which dummy variable appearing as indices in sums are denoted by placing a dot underneath them, as follows $x_{\dot{}}$ (not common notation).

2.3. Semantic or syntactic methods: ω assignments, or set of axioms. The construction of the theorems of predicate calculus is reached with semantic or syntactic methods, in accordance with the construction of propositional calculus theorems. Remember that "*Individual"* is one of the basic objects treated in a given formal language system and the term is also used as a synonym for "urelement" or "atom".
Semantic method: This method is based on the use of truth tables and it applies the set of the expressions in the set of the truth values *{T,F}* using the concept of ω-assignment. *ω is a given "set of individuals".* A *ω-assignment* is a Φ map, which associates any variable of individual with one element of ω and which also associates any variable of n arguments predicate with an n arguments relation in ω. Then, Φ_ω induces a truth value Φ^*_ω with $P(x_1, x_2, ..., x_n)$.This is equal to "T" if only if $(\Phi_\omega(x_1), ..., \Phi_\omega(x_1)) \in \Phi_\omega(P)$. The linked variables are treated according to the meaning of quantifiers. An expression is called *satisfiable* if it takes at least one true value in some interpretation. (A formula whose truth table contains only false in any interpretation is called *unsatisfiable).* An expression E is called *ω-satisfiable* if there exists Φ_ω such that $\Phi^*_\omega(E) = T$. The expression E is called *ω-identical* if $\Phi^*_\omega(E) = T$ for all Φ_ω. E is a *tautological propositional formula* or *universally true* or a *theorem of predicate calculus,* if E is *ω-identical* for all the ω set. Löwenheim-Skolem theorem, which explaines that an expression is tautological if there exists ω countable[1] for which this expression is *ω-identical*, can be very useful. A *ω-assignment* for which

[1] *Countable*: A set X is *countable* if there is a *one-to-one correspondence* between X and a subset of the set of natural numbers. Thus, a countable set is either finite or *denumerable.* Some authors use "countable" to mean denumerable. (Also known as enumerable).
Denumerable: A set X is *denumerable* if there is a *one-to-one correspondence* between X and the set of natural numbers. It can be shown that the set of natural numbers is denumerable but that the set of real numbers is not. Some authors use "denumerable" to mean *countable.*

all an M set of expressions is *unsatisfiable* is called an M *model* according to ω.

Ex. 1. *Example of a ω-assignment: Let $\omega = \mathbb{N}$ be a set of individuals and the following expression:* $P_1(x_1, x_2) \wedge P_2(x_2, x_4) \Rightarrow P_3(x_5)$.

With x_1, x_2, x_3, x_4, x_5 the variables that are associated with the set of individuals. $\Phi_\omega(x_1) = 2$, $\Phi_\omega(x_2) = 7$, $\Phi_\omega(x_3) = 1$, $\Phi_\omega(x_4) = 3$, $\Phi_\omega(x_5)$=16.$\Phi_\omega(P_1)$={(1, 2), (2, 7), (7, 10)},$\Phi_\omega(P_2)$={(2, 3, 4), (3, 4, 5)}, $\Phi_\omega(P_3) = \{16, 32, 48, 64, 80\}$. $(\Phi_\omega(x_1), \Phi_\omega(x_2)) \in \Phi_\omega(P_1)$ then: $\Phi^*_\omega(P_1(x_1, x_2)) = V$. $(\Phi_\omega(x_1), \Phi_\omega(x_3), \Phi_\omega(x_4)) \notin \Phi_\omega(P_2)$ then: $\Phi^*_\omega(P_2(x_1, x_3, x_4)) = F$. $\Phi_\omega(x_5) \in \Phi_\omega(P_3)$ then: $\Phi^*_\omega(P_3(x_5)) = V$. Truth value induced by the Φ_ω assignement is: $\Phi^*_\omega(P_1(x_1, x_2) \wedge P_2(x_2, x_4) \Rightarrow P_3(x_5)) = V$.
Syntactic method: Instead of working with semantic method, we can choose a *set of axioms* and a set of *syntactical rules (reasoning, argument, logical thought,..)* to deduce new formulas from the axioms. A *deductive system* is a set of *axioms* and a set of *rules of inference*. A *proof* in a deductive system is a sequence of sets of formulas such that each element is etheir an axiom or it can be inferred from previous elements of sequence using a rule of inference. From a *system* we can derive all the theorems of predicate calculus (*Gödel's completeness theorem* - see infra). However, it is not possible for any expression to determine, in a finite number of steps, if it is or not a theorem of predicate calculus (*Undecidability theorem*: see Gödel, Church and also Turing, Chaitin and the Richardson's theorem).
Gödel's completeness theorem: If T is a set of axioms in a first-order language, and a statement p holds for any structure M satisfying T, then p can be formally deduced from T in some appropriately defined fashion.

2.4. Theorems of predicate calculus. Theorems of predicate calculus (obtained with semantic or syntactic methods in accordance with the construction of propositional calculus theorems) are given by:

Th. 2. *(Predicate Calculus theorems):*
(1) $\neg\forall x\ Q(x) \Leftrightarrow \exists x \neg Q(x)$
(2) $\neg\forall x\ \neg Q(x) \Leftrightarrow \exists x\ Q(x)$
(3) $\neg\exists x\ Q(x) \Leftrightarrow \forall x\ \neg Q(x)$
(4) $\neg\exists x\ \neg Q(x) \Leftrightarrow \forall x\ Q(x)$
(5) $\forall x \forall y\ Q(x, y) \Leftrightarrow \forall y \forall x\ Q(x, y)$
(6) $\exists x \exists y\ Q(x, y) \Leftrightarrow \exists y \exists x\ Q(x, y)$
(7) $\exists x \forall y\ Q(x, y) \Rightarrow \forall y \exists x\ Q(x, y)$
(8) $\forall x\ Q(x) \Rightarrow Q(x)$
(9) $Q(x) \Rightarrow \exists x\ Q(x)$
(1), (2), (3), (4) *are called the negation rules and* (5)(6)(7) *are called the exchange rules.*

3. Extension of First-order Predicate Calculus

3.1. First-order predicate calculus with identity. One of the extensions of the first-order predicate calculus is to introduce the mathematical symbol of the *equality* sign "=" in order to introduce the identity. Commonly, this sign formalizes the mathematical statement of the equivalence of two quantities. The equality "A is equal to B" is written A=B. The particularity of the identity is that each element is only in relation with itself and not with an other one. Thus define equality is not possible, so this sign is classified among the logical constants.
In the previous sections, the predicates have been defined as relations in a *set of individuals*: ω. Given a n variables function in ω. This defines a relation with $n + 1$ arguments; so the map which associates any ordered pair $(x, y) \in \mathbb{R}$ with the sum $x + y = z$ $(x, y, z \in \mathbb{R})$ is a 2 variables function and is also defined as a 3 arguments predicate (cf paragraph on *First-order predicate calculus*: $\forall x, \forall y, x \in \mathbb{R} \wedge y \in \mathbb{R} \Rightarrow \exists z, z \in \mathbb{R} \wedge P_3(x, y, z)$, with P_3 means: "z is the difference between x and y". P_3 is a predicate with 3 arguments. In this case the *variable x is linked* to the quantifier).
Thus, the functions simplify the writings of expressions. The variables associated with the functions are called "*functorial variables*" (but note that they have nothing to do with the concept of functor relating to algebraic topology and homology theory) or *operator variables*. These variables are used in the writing of the propositional formulas. About our example if numbers replace variables, the *sum* $x + y$ becomes a number by the use of the sum operator $+$ and has not the status of a proposition. This expression is interesting if the equality sign "=" is introduced. The introduction of the *identity* and *"functorial variables"* allows an additional step in the construction of the mathematical logic architecture.

3.2. Higher-order predicate calculus. Previously, quantization (or quantification) only concerned the variables of individuals. But in many cases, it becomes necessary to take into account the *predicate variables*. A predicate with n arguments relative to ω (a *set of individuals)* corresponds to a subset of cartesian products of ω calculated n times with itself. Then, the quantization use the set of all the subsets of this product, this a *second-order predicate calculus*. Introduce predicates of predicates, and so on, is the first step in the logic of predicates by level. Each level is defined from the knowledge of the lower levels. If there is predicates until n level, this calculus is called the *n-order predicate calculus*. Finally if there is absence of limit in the construction of levels, then the calculus is called the *logic of orders*. It is interesting to present the following second-order case: let be the identity $x = y \Leftrightarrow \forall P, P(x) \Leftrightarrow P(y)$, and we assume that the quantization is relative to all the 1 *argument* predicates. Then it is not necessary to have the "=" equality sign as a logical constant. At this point, it is important to say that we cannot have a correspondence between the semantic and syntactic methods or construction, thus we say that there is *incompleteness* (of the extended predicate calculus).

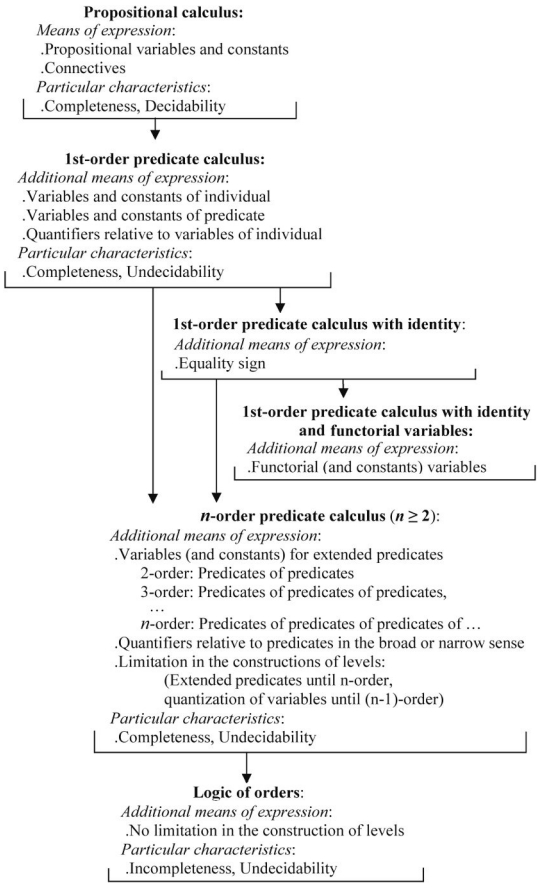


Fig. Structure of the classical logic.

The above leads to the consistency of a mathematical theory and to the linked notions of contradiction and incompleteness. The absence of contradiction (called *non-contradiction*) can be defined by the ability to prove that a statement and its negative such as for example $A \wedge \neg A$ are both true. The absence of contradiction (non-contradiction) in an axiomatic system is known as *consistency*. For example, a sentence is called a contradiction if its truth table contains only "F". And an *axiomatic system* is a *logical system* that has an explicitly stated set of axioms from which *theorems can be derived*. Consistency of many mathematics fields has not been demonstrated still.
Gödel's incompleteness theorem (1931): This states that all consistent axiomatic formulations of number theory include undecidable propositions. It's called Gödel's first incompleteness theorem and answers in the negative Hilbert's problem asking whether mathematics is "*complete*", in the sense that every statement in the language of number theory can be either proved or disproved. A statement known as Gödel's second incompleteness theorem states that if number theory is *consistent*, then a proof of this fact does not exist if the methods of first-order predicate calculus are used. Stated in a common way, any formal system that is interesting enough to formulate its own consistency can prove its own consistency iff it is inconsistent. It can be shown (cf. Gentzen) that the consistency and completeness of arithmetic can be proved if transfinite induction is used. It is well-known that this approach does not allow proof of the consistency of all mathematics.

3.3. Intuitionism. The study of the extended predicate calculus brings to light the concept of incompleteness, and the incompleteness leads to some critics about the foundations of what is called the "classical logic" which have been previously described. In this regard, the case of natural numbers and there properties is particularly interesting. Indeed, the study of natural numbers leads to reject the *law of excluded middle* and the *two-valued principle* when they are used with infinite sets. The *intuitionistic logic* develops a logic which excludes the utilization of the *non-constructive existence demonstrations*, as the indirect demonstrations. Furthermore, the intuitionistic logic and the "intuitionism" *reject the axiomatic method* (which searches to stick out the constructive approach). The purpose of intuitionistic logic is to propose a new logic frame, different from the cramped or confined classical logic. However, actually the intuitionistic logic is considered as a part of the classical logic, because all formulas provable in intuitionistic logic are also provable in classical logic. However, some basic theorems of classical logic do not hold in intuitionistic logic. An important point is that the *law of the excluded middle* $A \vee \neg A$ does not hold in intuitionistic propositional logic. The propositional formulas are not provable in intuitionistic propositional logic, as it is possible to observe with the following examples which are not provable:

$$\neg(A \wedge B) \equiv \neg A \vee \neg B, \quad A \wedge B \equiv \neg A \Rightarrow B.$$

The first-order formulas are not provable in intuitionistic predicate logic, as we can see with the following examples that are not provable:

$$A \vee \forall x B(x) \equiv \forall x(A \vee B(x)), \quad A \Rightarrow \exists x B(x) \equiv \exists x(A \Rightarrow B(x)).$$

The *proofs by contradiction* are not permissible in the intuitionistic logic. The intuitionistic proofs are *constructive* and justified by the following properties. Intuitionistic propositional logic has the *disjunction property*: If $A \vee B$ is provable in intuitionistic propositional calculus, then either A or B is provable in intuitionistic propositional calculus. Intuitionistic predicate logic has the *existence property*: If $\exists x A(x)$ is a formula without free variables, and it is provable in intuitionistic predicate logic, then there is term y without free variables such that $A(y)$ is provable in intuitionistic predicate logic. *The deduction theorem* holds in intuitionistic propositional and predicate logics. The following theorem shows the relation between intuitionistic and classical logics: If A is provable in classical propositional calculus, then $\neg\neg A$ is provable in intuitionistic propositional calculus. However there is no extension of this theorem in intuitionistic predicate logic.

In classical logic, a formula — say, A — asserts that A is true in an abstract sense. In intuitionistic logic, a formula is only considered to be true if it can be proved. An interesting example of this difference, as seen before, is relative to the *principle of excluded middle*. Indeed, while it is valid in the classical logic, it is not valid in the intuitionistic logic, because in a logical calculus it is possible to argue $A \vee \neg A$ even if we don't know which one is the case. In intuitionistic logic, it is not permitted to assert a disjunction such as $A \vee \neg A$ without also being able to say specifically which one is true. The formula $A \vee \neg A$ is not a theorem of intuitionistic logic. In classical logic, $A \vee \neg A$ means that one of A or $\neg A$ is true. In intuitionistic logic, $A \vee \neg A$ means that one of A or $\neg A$ can be proved. Intuitionistic logic replaces truth by *justification* in its logical calculus. Instead of a bivalent truth assignment scheme, intuitionistic logic allows for a third case, which is the indeterminate truth value. Indeed, a proposition may be justified or not justified or undetermined.

4. Formal System

4.1. Non contradiction problem, and Hilbert program. The non-contradiction problem can be seen in the following way: since Descartes, the Euclidean geometry and the geometries since Riemann and Poincaré were boiled down to the analysis, and this one, essentially since Dedekind, were boiled down to a structure on the infinite sets of rationals and therefore of (natural) integers; up to concepts of infinite sets of rationals, the non-contradiction in mathematics was fundamentally boiled down to the non-contradiction of the theory of (natural) integers, in other words, that of the arithmetic. And about the non-contradiction of this one "went without saying"; it suffices to remind the pretentions to the Absolute of various philosophical and scientific systems during the XVIIIth and XIXth centuries to understand that doubts on the system of number theory, "the science by excellence," were unthinkable at that time. However, the contradictions in set theory (the paradox of the set of all the sets, Russell's paradox) occur in a formulation apparently quite elementary of this theory and, in spite of the natural intuition that we can have (and which suffices for some) of the set of integers, the privileged position of the arithmetic appeared less obvious. After the work of Peano on the part strictly arithmetic and after that of Frege on the bases of the logic in which is articulated the discourse of the arithmetic, the axiomatic structure of this one was elucidated; in addition to the axioms and rules of logical deductions and of arithmetical axioms having an elementary combinatorial charactere, the arithmetic is based on this axiom:

Induction axiom: Let P *be a property relative to the integers, if* P *is true for* O *and if, in a general way, the fact that* P *is true for* n *implies that it is true for* $n+1$*, then* P *is true for all the integers.* By the notion of property, even accurate, this axiom introduces reasonings on infinite sets of integers which no longer have the immediate wished character.

It's Hilbert, partially influenced by the critics of Brouwer, who has expressed the idea that if certain statements and reasonings use the infinity, they must nevertheless be able to be *reduced* (without that theory loses its strength) to processes having the immediate characters, elementary combinatorial of reasonings and processes used for the *finite* sets; the objects of infinite character being introduced only for the completness of a theory based itself in a perfectly convincing manner on finite processes. In the same way as the "algebraics" or "imaginaries" are introduced for the theory of polynomials with integer coefficients as *ideal elements*, as were introduced the infinitely small and large quantities eliminated of the analysis during the XIXth century, in the same way the introduction of the *infinity* corresponds only to the introduction of propositions or *ideal objects* which can (and must for the foundations) be eliminated or at least reduced to real propositions concerning only the finite iterations of elementary calculations on the integers; this at least concerning the arithmetic, but also, in the project of Hilbert, for the theory of real numbers in general. *Hilbert was convinced that the analysis is fundamentally based on the same evidence that the one, immediate, which is the base of the study of finite sets.* This evidence that Hilbert called *finitist*, and which, being given its immediat and cpncrete character, did not need for Hilbert to be specified,corresponds today to *algorithmic* or *recursive* processes.(refer to decidability and recursive functions in Mathematical logic). To reveal this finite fundament, the idea of Hilbert is to formalize the theory to be studied, i.e. to reduce it to a system of symbols and rules of mechanical character relative to finite sequences of these symbols. To the intuitive and stated true proofs of the theory correspond, in the formalized system, to *formal proofs*, i.e. finite sequences of symbols constructed by elementary operations in accordance with the rules. In particular, to the notion of truth concerning propositions relative to the infinity corresponds the notion of formal proof which is of finite character. Therefore, the theory is represented and reduced to finitist processes in the formalized theory. But in the formal theory, or *formal system*, if some symbols represent mathematical being and some sequences of symbols of true or false propositions, it is important to see that, when we study the action of rules on sequences of symbols, the only important thing is the respect of these imposed rules in the system, out of any possible meaning of symbols. As in the chess game, what matters in how to play the knight for example are the rules specifying the possible moves and not that the knight is represented by a horse's head made of wood or ivory, thus the formal proofs are mathematical beings to be studied in themselves, as well as are studied numbers, equations or structures of groups; and, *via* the formalization, the reasonings themselves become the object of a precise theory, and in particular the problems of *non-contradiction* and of fundaments. Note nevertheless the importance of the proposed goal regardless of the specific problem of non-contradiction. This problems should be resolved if, inversely to any formal statements (finite series of symbols) for which there exists a formal proof and an intuitive interpretation in the initial theory, actually corresponded (in a finitist way) a statement of *true finite character* (verifiable by the elementary processes) in this theory; because a contradiction of the theory would come down to a contradiction $(0 = 1)$ in the elementary finitist part of the theory, which is not possible (and is easily proved). The study of formalized theories in accordance with a *finitist conception* is *Metamathematics,* and it's within Metamathematics that, according Hilbert, are located the obvious fundamental essence of the mathematics, upon which the mathematicians of constructive tendencies called (since Kronecker) to reconstruct these ones. Were it possible, the proposed finitist formalization would certainly have been admitted as a valid fundament or else definitive by Brouwer himself.

4.2. Formal system. In logic a formal system is a formal grammar used for modelling purposes. *Formalization* is the creation of a formal system, in order to try to capture the features of real phenomena or in order to write a conceptual system in formal language. *Formal proofs* are the product of formal systems, which are axioms and rules of deduction. *Theorems* could be defined as the possible last lines of

formal proofs. This general mathematics approach is called formalist.
A mathematical formal system is constituted by the following objects:
(1) *A finite set of symbols* which can be used for constructing formulas. A set of symbols is also called a *vocabulary*.
(2) A procedure for the construction of formulas. (The notion of formula is like a well-formed grammatical sentence. and consists of a finite sequence of the symbols of the vocabulary) It's a *grammar*, which means a way of constructing well-formed formulas out of the symbols, such that it is possible to find a decision procedure for deciding whether a formula is a well-formed formula or not.
(3) A *set of axioms* or *axiom schemata*: each axiom has to be a well-formed formula.
(4) A *set of inference rules* (deductive reasoning), which permits deducing formulas.
(5) A *set of theorems*. This set includes the axioms, with also all well-formed formulas which can be derived from previously-derived theorems by using rules of inference. Unlike the grammar for well-formed formulas, there is no guarantee that there will be a decision procedure for deciding whether a given well-formed formula is a theorem or not.

4.3. Axiomatic method. As seen before, the construction of axiomatic systems imposes the *consistency (called "absolute consistency"). Non-contradiction in an axiomatic system is known as consistency. Independence* is also imposed and none axiom can be derived from another axiom which precedes. Furthermore, an important issue is to know if all true propositions can be derived and deduced from axioms. The answer to this question is negative for many theories constructed with mathematical logic.

5. Demonstrations and Definitions

5.1. Demonstrations. Recall briefly that an *axiom* is a proposition regarded as self-evidently true without proof. Axiom is considered as a synonym for postulate. Compare conjecture or hypothesis, both of which connote apparently true but not self-evident statements. Mathematics base theories on propositions postulated as true, which are called *axioms* and use only demonstrations deriving from these axioms. A demonstration deduces a proposition from others propositions in compliance with logical rules of reasoning. But obviously all the mathematical propositions are not demonstrable. Thus there exists propositions which cannot be deduced from none other proposition. Thereby this is the reason why the *mathematics base theories on axioms, which are propositions postulated as true and use only demonstrations deriving from these axioms.* Then, this is the choice of the reasoning rules which are going to determine, from a system of axioms, the deduced results. The propositional calculus and the predicate calculus permit to construct systems of reasoning rules in order to formalize correctly the deduced results.
Direct demonstration is based on the rule of the *modus ponens* (see Propositional calculus theorems). The rules of the direct demonstration are the ones which concern the *introduction* and the *elimination* of *connectives* and *quantifiers,* and also the ones which concern the *substitution. Indirect demonstration,* also called the *demonstration by the absurd,* is based on the *modus tollens* rule. The use of the demonstration by the absurd can be explain basically with the following approach: when we want derived a P *proposition* from M a *set of axioms*, it is possible, and sometimes more interesting, to assume $\neg P$, and to deduce a Q proposition, whose $\neg Q$, can be deduced from M the set of axioms. From $\neg P \Rightarrow Q$ and $\neg Q$ we can deduce, by means of *modus tollens*, that $\neg\neg P$ and then P. An usual example of an indirect demonstration is to prove that $\sqrt{2}$ is irrational.
If the proposition P is of the type $a \Rightarrow b$, then $\neg P$ is equivalent to the expression $a \wedge \neg b$, which is useful to construct many indirect demonstrations. Moreover, when $a \Rightarrow b$ is true, we say that a is a *sufficient condition* for b. Then b is a *necessary condition.* It is important to associate the modus ponens and modus tollens rules with the *necessary and sufficient conditions.*
Thus, in a direct demonstration, in order to show that $P \Rightarrow Q$, we begin to assume that P is true, then we deduce that Q must be necessary true. This type of demonstration is the opposite of the contraposition reasoning, in which we start from the hypothesis that Q is false, and we attempt to demonstrate that in this case P must be false too.

Ex. 2. *(Direct demonstration): The purpose is to prove that if n is odd-numbered then n^2 is odd-numbered.*
(1) *Thus, we state P : "the integer n is odd-numbered" and Q : "the integer n^2 is odd-numbered".*
(2) *We choose the hypothesis P is true and we want to show that Q must be true.*
(3) *n is odd-numbered, therefore this implies (cf. odd-numbered definition) that $n = 2k + 1$, with $k \in \mathbb{Z}$.*
(4) *Then, $n^2 = (2k+1)(2k+1) = 4k^2+4k+1 = 2(2k^2+2k)+1 = 2t+1$ with $t = 2k2 + 2k$ is an integer.*
Then we conclude: $2t+1$ is odd-numbered therefore n^2 is odd-numbered.

Necessary condition (NC): A condition which must hold for a result to be true, but which does not guarantee it to be true. If a condition is both necessary and sufficient, then the result is said to be true if and only if the condition holds.
Sufficient condition (SC): A condition which, if true, guarantees that a result is also true. However, the result may also be true if the condition is not met. If a condition is both necessary and sufficient, then the result is said to be true if and only if ("iff") the condition holds.

5.2. Proof by mathematical induction (by recurrence). If the proposition, to be demonstrated, is of the following type: $\forall n$, $F(n)$, with $F(n)$ which is a function in the $\mathbb{N}$ natural number set, we can base the demonstration on a particular propertie of natural numbers which is described in the 5^{th} *Peano's axiom* (cf. heading "*Semi-group of natural numbers*"). The method proves first $F(0)$, then, proves $\forall n$, $F(n) \Rightarrow F(n+1)$ (which consists in deducing $n+1$ from n). By the repetitive use of the *modus ponen* rule, we can deduce $F(1)$,$F(2)$,$F(3)$, etc... and then $\forall n$, $F(n)$.The procedure can be extended via the *transfinite induction.* More precisely, the *principle of induction* (or *principle of recurrence)* can also be presented as follows:
Given $P(n)$ a proposition dependent of n an integer. If the purpose is to demonstrate that:
1. each time that $P(n)$ is true, $P(n+1)$ is true;
2. *there exists an integer $n = n_0$*;
then, it'll be demonstrated that for any integer $n \geq n_0, P(n)$ is true. Indeed, since $P(n_0)$ was true, either $n_1 = n_0 + 1$, (in line with *i)*), $P(n_1)$ is true; or either $n_2 = n_1 + 1$, then $P(n_2 + 1)$ is true, etc...

Proof by mathematical induction (i.e. by recurrence, also called *recursive, or recursion*) can be outlined by using three steps. In order to show by recurrence (by induction) that a proposition $P(n)$ is true for any integer $n \geq n_0$, it is necessary to proceed step by step:
i) Assume (i.e. "*hypothesis of recurrence*", mainly called "*induction hypothesis*", or "*inductive hypothesis*") that there exists an integer $n \geq n_0$ such that $P(n)$ is true;
ii) Prove that, under this hypothesis, $P(n+1)$ is true;
iii) Show that $P(n_0)$ is true.

The principle of induction (or principle of recurrence) allows to conclude. Indeed, we can replace *i)* by the induction hypothesis (hypothesis of recurrence), called *strong*, which is equivalent to it:
i)′ there exists an integer $n \geq n_0$ such that $P(n_0), ..., P(n)$ are true.

Ex. 3. *Given A_n the sum of the n first integers, i.e the sequence defined as: $A_{n+1} = \begin{cases} 1 & : \text{if } n=0 \\ A_n+(n+1) & : \text{otherwise} \end{cases}$. The exercise is to prove by induction that for any integer $n \geq n_0 = 1$, we have an $A_n = n(n+1)/2$. Let the proposition $P(n) =$"A_n is equal to $n(n+1)/2$".*
1. *Suppose there exists an integer $n \geq 1$ such that $P(n)$ is true (which is the induction hypothesis).*
2. *We have by definition $A_{n+1} = A_n + (n+1)$; by the induction hypothesis (hypothesis of recurrence), $A_n = n(n+1)/2$ then $A_n + (n+1) = n(n+1)/2 + (n+1) = (n+1)(n+2)/2$; that is, $P(n+1)$ is true.*
3. *Thus $A_1 = (1).(1+1)/2 = 1$, i.e. $P(1)$ is true.*
The mathematical induction (principle of recurrence) allows to conclude that $P(n)$ is true for any integer $n \geq 1$.

5.3. Definition. The *definition* is the demarcation, or precise delimitation, of a concept in a general frame using others concepts. The approach of the definition is similar to the approach of the demonstration. At this point, it is necessary to introduce both notions of *definiendum* and *definiens. Definiendum* is the concept (or more generally the thing) to be defined and *definiens is* (are) the concept(s) that allow(s) to explain it. The link between this two notions can be written as follows: **Definiendum** := **Definiens**, or **Definiendum** :⇔ **Definiens**, relative to the *definiens* is a word or a proposition. The use of the definiendum simplifies the writings and the definiens can be used in order to replace definiendum if necessary. *Beth's definability* theory explains that we can articulate or formulate in an *explicit* form any *implicit* definition of a relation or a function obtained with the help of the first-order predicate calculus tools. The *recursive definition*, also called *inductive definition* (sometimes *definition by recurrence*) is also defined, as the demonstration. $\forall n \in \mathbb{N}$, $n!$ is defined by: $0! = 1$ and $(n+1)! = n!(n+1)$.

5.4. Methods of proof. What demarcates mathematical activity, is not that it deals with mathematical objects (numbers, figures, ...), but the fact that it is based on theorem proofs. The mathematician starts from axioms and definitions, and has also at disposal theorems already demonstrated; then the mathematician obtains new theorems by means of demonstrations. These ones are chains of deduction that obey logical rules. This activity can be formalized in such a way to make possible the mechanical verification of demonstrations (but not their invention) - but it's very difficult beyond the most superficial theories. Specific case: the calculation, which is a form of proof, is more easily mechanizable. This is well known for the numerical calculation but is also true for the symbolic calculation. Actually, mistakes arise even for seasoned mathematicians. To avoid them as much as possible, this requires common sense, method, rigor, and trial of peers (i.e. proofreading). Here are examples of methods.

1. Direct proof. In direct proof, the conclusion is established by logically combining the axioms, definitions, and earlier theorems. For example, direct proof can be used to establish that the sum of two even integers is always even: "*Consider two even integers x and y. Since they are even, they can be written as x=2a and y=2b respectively for integers a and b. Then the sum $x+y$=2a+2b=2($a+b$). From this it is clear x+y has 2 as a factor and therefore is even, so the sum of any two even integers is even.*" This proof uses definition of even integers, as well as distribution law.

2. Proof by mathematical induction (Proof by descent). It is a method typically used to establish that a given statement is true of all natural numbers (positive integers). It is done by proving that the first statement in the infinite sequence of statements is true, and then proving that if any one statement in the infinite sequence of statements is true, then so is the next one. Indeed, it is a general method of proving statements concerning a positive integral variable: if a statement is proven true for $x = 1$, and if it is proven that, if the statement is true for $x = 1, ..., n$, then it is true for $x = n + 1$, it follows that the statement is true for any integer. Also known as *complete induction*; *method of infinite descent*; *proof by descent*.

The method can be extended to prove statements about more general well-founded structures, such as trees; this generalization, known as structural induction, is used in mathematical logic and computer science. Mathematical induction in this extended sense is closely related to recursion. Mathematical induction should not be misconstrued as a form of inductive reasoning, which is considered non-rigorous in mathematics. Mathematical induction is a form of rigorous deductive reasoning.

. Proof by mathematical induction (by recurrence).

a) Simple induction (simple recurrence). To prove $\forall n \in \mathbb{N}$, $P(n)$, we prove $P(0)$ and, $\forall n$, $P(n) \Rightarrow P(n+1)$.

Ex. 4. *Prove by induction (by recurrence): $\forall n \in \mathbb{N}$, $n < 2^n$. Solution: This is true for $n = 0$ since $0 < 1$. To prove $P(n) \Rightarrow P(n+1)$, we assume the induction hypothesis $P(n) : n < 2^n$, "for certain n": this is a case of subsidiary (or auxiliary) hypothesis. Suppose $n < 2^n$, we have $n+1 < 2^n+1$, and, since $1 \leqslant 2^n$, $n+1 < 2^n+2^n = 2^{n+1}$, that is, $P(n+1)$. Thus we have demonstrated the implication $P(n) \Rightarrow P(n+1)$ (it is sometimes said "heredity"). The principle of induction allows to conclude.*

b) Two-step induction (two-step recurrence). To prove $\forall n \in \mathbb{N}$, $P(n)$, we prove $P(0)$ and $P(1)$, and, for any n, $(P(n) \wedge P(n+1)) \Rightarrow P(n+2)$. Of course, there exists a version with k steps. Let us prove thus that, for any $n \in \mathbb{N}$, $2^n - (-1)^n$ is multiple of 3. This is true for $n := 0$ and 1 (immediate verification). Suppose $a := 2^n - (-1)^n$ and $b := 2^{n+1} - (-1)^{n+1}$ are multiple of 3. Then we observe that (little calculation) that $2^{n+2} - (-1)^{n+2} = 2a + b$, which is multiple of 3. Actually, this method of demonstration often applies to sequences defined by a two-step inductions (recurrences): $u_{n+2} = u_{n+1} + 2u_n$. Precaution to keep in mind is that the *initialization of the induction (recurrence)* should be in $n := 0$ and $n := 1$, or $n := 1$ and $n := 2$. For example, the property "$2^n + (-1)^n$ is multiple of 3" verifies the same relation of " heredity", and it is true for $n := 0$ but false for $n := 1$.

c) Strong induction (strong recurrence). We want also to prove $\forall n \in \mathbb{N}$, $P(n)$. Here, the heredity takes the form: $(\forall m < n, P(m)) \Rightarrow P(n)$. In principle, initialization is even not required.

3. Reductio ad absurdum (Proof by contradiction). A method of demonstration in which it is first supposed that the fact to be proved is false, and then it is shown that this supposition leads to the contradiction of accepted fact. Also known as *indirect*; *proof by contradiction*. The supposition that P is false followed necessarily by the conclusion Q from not-P, where Q is false, which implies that P is true, (e.g. the second of Euclid's theorems starts with the assumption that there is a finite number of primes).

Ex. 5. *Prove by contradiction $\sqrt{2}$ is rational. Solution: If $\sqrt{2}$ were irrational, we could write $\frac{p}{q}$ with $p, q \in \mathbb{Z}$ relatively prime (coprime). Thus we would have p^2=2q^2, so p even: p=2n, so q^2=2n^2, so q even: q=2m, but then p and q would not be relatively prime, contradicting the assumption. Thus, we can write n=$\frac{p}{q}$ and $\sqrt{2}$ is indeed irrational.*

4. Proof by construction (constructive proof). A proof that directly provides a specific example, or which gives an algorithm for producing an example. Constructive proofs are also called *demonstrative proofs*. That is, proof by construction, or proof by example, is the construction of a concrete example with a property to show that something having that property exists (e.g. Liouville proved the existence of transcendental numbers by constructing an explicit example).

5. Noncontructive proof. A proof which indirectly shows a mathematical object exists without providing a specific example or algorithm for producing an example. Nonconstructive proofs are also called existence proofs. Indeed, a nonconstructive proof establishes that a certain mathematical object must exist (e.g. "Some X satisfies $f(X)$"), without explaining how such an object can be found. Often, this takes the form of a proof by contradiction in which the nonexistence of the object is proved to be impossible. In contrast, a constructive proof establishes that a particular object exists by providing a method of finding it. A well known example of a nonconstructive proof shows that there exist two irrational numbers a and b such that a^b is a rational number: "Either $\sqrt{2}^{\sqrt{2}}$ is a rational number and we are done (with a=b=$\sqrt{2}$), or $\sqrt{2}^{\sqrt{2}}$ is irrational so we can write a=$\sqrt{2}^{\sqrt{2}}$ and b=$\sqrt{2}$. This gives $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$=$\sqrt{2}^{\sqrt{2}}$=2, which is thus a rational of the form a^b."

6. Elementary proof. A proof which can be accomplished using only real numbers (i.e. real analysis instead of complex analysis). More specifically, the term is used in number theory to refer to proofs that make no use of complex analysis.

7. Method of the auxiliary hypothesis (Bourbaki, 1970. Theory of Sets). This method applies when we want to prove an implication $P \Rightarrow Q$. We temporarily assume P true (it's the "auxiliary hypothesis"), and we proceed with deductions until proving that Q is true. To illustrate it, we combine it with the two next methods.

8. Method by disjunction of cases. If we are sure that $P \vee Q$ is true, to prove R, it suffices to prove $P \Rightarrow R$, then, to prove $Q \Rightarrow R$. Let us prove thus that the square of any real is positive or zero. Given $x \in \mathbb{R}$. It is itself positive or zero, or negative or zero. In the first case, $x^2 = xx$ is the product of two positive or zero reals, therefore it is positive or zero. In the second case, $x^2 = (-x)(-x)$ is still the product of two positive or zero reals, therefore positive or zero.

9. Proof by transposition (proof by contrapositive). Proof by transposition or proof by contrapositive establishes the conclusion "if P then Q" by proving the equivalent contrapositive statement "if not Q then not P". In other words, this method applies when we want to demonstrate $P \Rightarrow Q$. Instead, we prove the contrapositive implication $(\neg Q) \Rightarrow (\neg P)$, which is equivalent to it. Let us prove thus the implication: $f \in \mathcal{C}(\mathbb{R}, \mathbb{R})$ is invertible $\Rightarrow$ f has a constant sign; here, $\mathcal{C}(\mathbb{R}, \mathbb{R})$ denotes the set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. The assumption P means: $\exists g \in \mathcal{C}(\mathbb{R}, \mathbb{R}) : fg = 1$. The conclusion Q means: $(\forall x \in \mathbb{R}, f(x) > 0) \vee (\forall x \in \mathbb{R}, f(x) < 0)$. We are going to prove that $(\neg Q) \Rightarrow (\neg P)$. To this end, let us introduce the subsidiary (or auxiliary) hypothesis $\neg Q$, in other words, during the demonstration we assume $\neg Q$ true. Explain the negation of Q is a little exercise on Morgan laws and quantifiers. We find $(\exists x \in \mathbb{R} : f(x) \leqslant 0) \wedge (\exists x \in \mathbb{R} : f(x) \geqslant 0)$. Say that "$A$ and B" is true means that A is true and that B is true. Since $\exists x \in \mathbb{R} : f(x) \leqslant 0$ is true, we can choose $a \in \mathbb{R}$ such that $f(a) \leqslant 0$. Since $\exists x \in \mathbb{R} : f(x) \geqslant 0$ is true, we can choose $b \in \mathbb{R}$ such that $f(b) \geqslant 0$. Note that by the relationship between $\exists$ and $\wedge$, we cannot require that a and b are the same; $a \leqslant b$ or $b \leqslant a$ (disjunction of cases). In the first case, f vanishes at a point of $[a; b]$; in the second case, at a point $[b; a]$ (intermediate value theorem). In all the cases, there exists c such that $f(c) = 0$. Let us show then (by contradiction) that g is not invertible. If it had an inverse, we would have $fg = 1$, so $0 = 0g(c) = f(c)g(c) = 1$, which is impossible. We have therefore shown $\neg P$, by supposing $\neg Q$. We have therefore shown $\neg Q \Rightarrow \neg P$. Therefore we have demonstrated $P \Rightarrow Q$.

10. Two-column proof. A formal type of proof most frequently encountered in elementary geometry courses in which known or derived statements are written in the left column, and the reason that each statement is known or valid is written next to it in the right column.

The proof then proceeds from the known facts to the theorem to be demonstrated. This form of proof can therefore be pedagogically useful by teaching logical thinking, since steps incrementally build of previous results and each step can be made only if it can be explicitly justified. However, this form of proof is not used by practicing mathematicians because its confining and verbose format render it of very limited utility to any but the most simple of theorems.

11. Visual proof (proof without words). A proof that is only based on visual elements, without any comments. An arithmetic identity can be demonstrated by a picture showing a self-evident equality between numerical quantities. Another form of proof without words frequently used in elementary geometry is the *dissection proof.* Although not a formal proof, a visual demonstration of a mathematical theorem is indeed sometimes called a "proof without words".

12. Proof by exhaustion. In proof by exhaustion, the conclusion is established by dividing it into a finite number of cases and proving each one separately. The number of cases sometimes can become very large; e.g. the first proof of the four color theorem was a proof by exhaustion (with 1,936 cases). This proof was controversial because the majority of the cases were checked by a computer program, not by hand.

13. Dissection proof. A proof based on a dissection which shows the formula for the area of a plane figure or of the volume of a solid. (Many different dissection proofs are known for the Pythagorean theorem.)

14. Combinatorial proof. Combinatorial proof establishes the equivalence of different expressions by showing that they count the same object in different ways. A bijection between two sets is often used to show that the expressions for their two sizes are equal. Alternatively, a double counting argument provides two different expressions for the size of a single set, again showing that both expressions are equal.

Chapter 2

Set Theory

1. Basic Concepts

In the most recent way, a set can be defined as a finite or infinite collection of objects in which order has no significance, and multiplicity is generally also ignored. These objects are like elements of a set and the notation $a \in A$ is used to denote that a is an element of a set A. The study of sets and their properties is the subject of set theory. The mathematical theory of sets is closely associated with the branch of mathematics known as logic. There are a lot of versions of the set theory, each version with its own rules and axioms. Each version of the set theory with its own rules and axioms, having a more or less large capability to provide a consistency strength, several versions of set theory include Peano arithmetic (ordinary algebra), second-order arithmetic (analysis), Zermelo-Fraenkel set theory, Mahlo, weakly compact, hyper-Mahlo, ineffable, measurable, Ramsey, supercompact, huge, and n-huge set theory. The original definition of a set have been provide by Cantor. This definition is actually considered as naive because of its deficiencies but was fundamental for a long time.

Set: A set is a collection of objects which come originally from our perceptions or our thoughts, all determinate and distinct. This objects are called elements of the set.

Generally, the $a, b, c, ...$ lowercase alphabetic letters are used in order to name the elements of a set, and $A, B, C, ..$ uppercase letters are used in order to name the sets. The notation $a \in A$ is used to denote that a is an element of a set A. The notation $a \notin A$ is used to denote that a is not an element of a set A. The main objects included in a set are the numbers, the geometrical figures, the maps, etc..However it's also possible to create a set with any object, concept or event. The sets can be finite or infinite. The finite sets can be described by the complete list of its elements, represented between braces (e.g. a set of vowels $\{a, e, i, o, u, y\}$, a set of numbers $\{2, 4, 6, 8, 10\}$). Arbitrary sets can be described by characteristic properties; we write then $\{x|F(x)\}$ for the set of elements x verifying $F(x)$; meaning that $y \in \{x|F(x)\}$ if and only if $F(y)$ is true. Another example can be given by: if $P(x)$ means "x is a prime number", $\{x|P(x) \wedge x < 8\}$ is the set of prime numbers less than 8, such a set can be represented by: $\{3, 5, 7\}$. In the opposite, it is not possible to describe the set of all prime numbers by a list, because this list is infinite.

Ex. 6. *Examples of Set, elements, representation of sets:* $A = \{2, 3, 4, 7\}$, $B = \{6, 7, 9, 10\}$ $7 \in A, 7 \in B, 3 \in A, 6 \in B, 3 \notin B, 6 \notin A, 8 \notin A, 8 \notin B$.

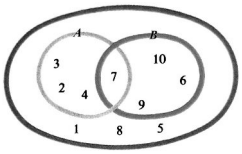


Fig. Euler or Venn representation (Venn diagram).

The symbols $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, describe the following well-known sets: $\mathbb{N}$ denotes the set of natural numbers, $\mathbb{Z}$ denotes the set of integer numbers, $\mathbb{Q}$ denotes the set of rational numbers, $\mathbb{R}$ denotes the set of reals, and $\mathbb{C}$ denotes the set of complex numbers.

Def. 1. *(Equal sets). Two sets are equal if they contain exactly the same elements,* $A = B :\Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B)$.

Thus, the order of the elements is not important. The *equality relation* between the sets is an *equivalence relation.* An impossible condition of the type $\{x|P(x) \wedge (53 < x < 59)\}$, with $P(x)$= "x is a prime number", allows to introduce the notion of empty set. "$\varnothing$" is the symbol of the empty set that is defined as follows:

Def. 2. *(Empty set).* $\varnothing := \{x|x \neq x\}$.

The Euler or Venn representation is used to provide the picture of a collection of objects included in sets. The elements are represented with points in a plane surrounded by a circle or by a closed curve.

1.1. Subset, set of the parts of a set.

Ex. 7. *(Examples of subset):* (1) $A \subseteq B$, $A \subset B$. (2) $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$; $A \subset B \wedge B \subset C \Rightarrow A \subset C$ *(Fig.).*

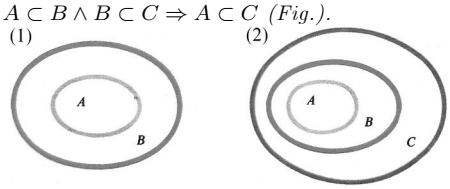


Fig. Subsets.

A is a *subset* of B, if all elements of A are elements of B, which is written $A \subseteq B$. There exists also a stronger definition of a subset.

Def. 3. *(Subset).* $A \subseteq B :\Leftrightarrow \forall x(x \in A \Rightarrow x \in B)$.

Def. 4. *(Strict subset).* $A \subset B :\Leftrightarrow A \subseteq B \wedge A \neq B$.

The last definition means that there exists elements of B which are not elements of A. *Proper subset:* A proper subset A' of a set A is a *subset* which is strictly contained in A and so necessarily excludes at least one member of A. The *empty set* is therefore a proper subset of any nonempty set. Thus, if A is a proper subset of B (i.e, a subset other than the set itself), this is written $A \subset B$. If A is not a subset of B, this is written $A \subsetneq B$. The *binary relation* $\subseteq$ verifies the following properties:
Reflexivity: $A \subseteq B$
Antisymmetry: $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$
Transitivity: $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
This is what we call an *order relation* (or ordering relation, or also *partial order*). The sets can be also elements of a set. The *set of the parts of a set* A (meaning "*set of all parts of*") is defined as follows:

Def. 5. *(Set of the parts of a set A).* $\mathfrak{P}(A) := \{x|x \subseteq A\}$.

Consider the followings sets $A_0, A_1, A_2, .., A_n$:
$A_0 = \varnothing$
$A_1 = \{a_1\}$
$A_2 = \{a_1, a_2\}$
$\vdots$
$A_n = \{a_1, a_2, .., a_n\}$
The set of the parts of each set is respectively named: $\mathfrak{P}(A_0)$, $\mathfrak{P}(A_1)$, $\mathfrak{P}(A_2), .., \mathfrak{P}(A_n)$ and written:
$\mathfrak{P}(A_0) = \{\varnothing\}$
$\mathfrak{P}(A_1) = \{\varnothing, \{a_1\}\}$
$\mathfrak{P}(A_2) = \{\varnothing, \{a_1\}, \{a_2\}, \{a_1, a_2\}\}$
$\vdots \qquad \vdots$

$$\mathfrak{P}(A_n) = \mathfrak{P}(A_{n-1}) \cup \{\{a_n\}\} \cup \{\{a_1, a_n\}, \{a_2, a_n\}, .., \{a_{n-1}, a_n\}\} \cup \{\{a_1, a_2, a_n\}, \{a_1, a_3, a_n\}, .., \{a_{n-2}, a_{n-1}, a_n\}\} \cup ... \cup \{\{a_1, a_2, .., a_n\}\}$$

Th. 3. *(Number of elements of a set). The set of parts of a set of* n*-elements contains* 2^n *elements* ($n \in \mathbb{N}$).

Def. 6. *We say that the set* F *is included in the set* A*, denoted by* $F \subset A$*, if all the elements of* F *are elements of* $A : F \subset A \Leftrightarrow (\forall x, x \in F \Rightarrow x \in A)$. *We say also that* F *is a part or a subset of* A.

We also say that A contains F (but it is ambiguous). Empty set is a subset of any set. Any set is subset of itself. The set $\{x \subset A | P(x)\}$ (i.e. the set of elements of A which have the property P) is a subset of A.

Def. 7. *(Collectivizing relation). Let A be a set. The relation $x \subset A$ is collectivizing and defines the* ***set of the parts of*** *A, denoted $\mathfrak{P}(A)$. We have therefore $\mathfrak{P}(A) := \{x | x \subset A\}$.*

Power set: Given a set A, the power set of A is the set of all subsets of A . The order of a power set of a set of order n is 2^n . Power sets are larger than the sets associated with them. The power set of A is variously denoted 2^A.

1.2. Paradoxical set construction. Construction of a set of sets requires particular precautions. Indeed, can we conceive that a set contains itself or does not contain itself as element? If yes, Russel has suggested the study of the set R of the sets do not containing themselves as element, that is, $R := \{x | x \notin x\}$. We have thus $x \in R \Leftrightarrow x \notin x$. This definition-property should be especially verified for R; but if $R \in R$, then $R \notin R$, and if $R \notin R$, then $R \in R$. This is *Russell's paradox..R* is the Russel paradoxical set.
The *set of all the sets*, called *universal set*, is also a paradoxical notion. By avoiding such constructions we attempt thus in naive set theory to escape from these paradoxes.

Universal set: A set fixed within the framework of a theory and consisting of all objects considered in this theory. (Its complement is the empty set.)

A *paradoxical set* in set theory can be described as a set that has a paradoxical decomposition. A *paradoxical decomposition* of a set is a partitioning of the set into two subsets, along with an appropriate *group* of functions that operate on some universe (whose set in question is a subset), such that each *partition* can be mapped back onto the entire set using only finitely many distinct functions (or compositions of them) to do the mapping. Since a paradoxical set as defined requires a suitable group (here denoted G), it is then called "*paradoxical with respect to G*" or "*G-paradoxical*". Paradoxical sets exist as a consequence of the Axiom of Infinity. Admitting infinite classes as sets is sufficient to allow paradoxical sets. A well-known case of paradoxical set is the Banach-Tarski paradox (cf. heading "*Banach-Tarski paradox*"), which splits the sphere into paradoxical sets for the special orthogonal group.

1.3. Russell paradoxical set. Bertrand Russell has highlighted a paradox that may be encountered during the construction of a set of sets. This paradox concerns the concept of all sets which are not members of themselves which forces distinctions in set theory between sets and classes. This important topic is carefully avoided in the general framework of *naive set theory* (the paradox shows that naive set theory is inconsistent). This paradox can be formulated as follows:

Russell's paradox: Using notation of set theory, a set can be defined as the set of all x that satisfy some properties. Now it is clearly possible for a set not to belong to itself: any set of numbers, say, does not belong to itself because to belong to itself it would have to be a number. But it is also possible to have that does belong to itself: for example, the set of all sets belongs to itself. In 1901, Bertrand Russel drew attention to what has become known as *Russell's paradox* (also called *Russell's antinomy*), by considering the set R defined by $R := \{x | x \notin x\}$. If $R \in R$ then $R \notin R$; and if $R \notin R$ then $R \in R$. The paradox points out the danger of the unrestricted use of abstraction, and various solutions have been proposed to avoid the paradox. Moreover, we can say that it concerns the concept of all sets which are not members of themselves which forces distinctions in set theory between *sets* and *classes*.

2. Set Algebra

2.1. Algebraic operations in sets. Algebraic operations have properties similar to those of the arithmetic or propositional calculus. Likewise they also have an great interest for maps. The algebraic operation denoted by $A \backslash B$" (read "A minus B") is defined by (Fig.):

Def. 8. *(Set difference).* $A \backslash B := \{x | x \in A \wedge x \notin B\}$.

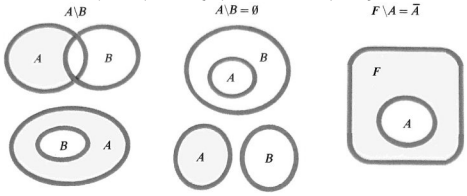


Fig. Remaining part, complement.

$A \backslash B$ exactly contains the elements of A which are not elements of B. When $A \subset F$, $F \backslash A$ is also called the *complement* of A *in* F (Fig. supra), denoted by $\complement_F A$, or $\complement A$ if there is no ambiguity about the set F. Indeed, we can write $\complement A$ when in a given theory, F represents the set elements upon which the theory is based, i.e the "*universal set*" (sometimes called "*fundamental set*"). In other words, in a particular piece of work, it may be convenient to fix the universal set F, a set to which all the objects to be discussed belong. Then all the sets considered are subsets of F.
A *complement* of a set A refers to things not in (i.e. things outside of) A. *Relative complement* of A with respect to a set B, is the set of elements in B but not in A; (also called "*set-theoretic difference*"). If all sets under consideration are taken to be subsets of a given set U, the *absolute complement* of A is the set of all elements in U but not in A. Notions of complement, absolute and relative complements are specified in the heading "*Constructors*" (in "*Foundations of Sets*").
If we combine the concepts of complement and negation, we can write the following expression: $x \in F \Rightarrow (x \in F \backslash A \Leftrightarrow \neg x \in A)$. Main algebraic operations between sets are intersection and union:

Def. 9. *(Intersection).* $A \cap B := \{x | x \in A \wedge x \in B\}$.

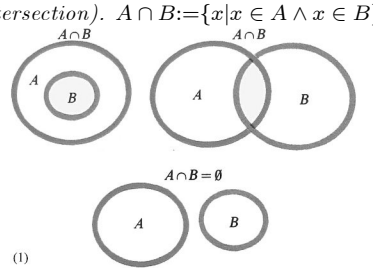


Fig. Intersection.

Def. 10. *(Union).* $A \cup B := \{x | x \in A \vee x \in B\}$.

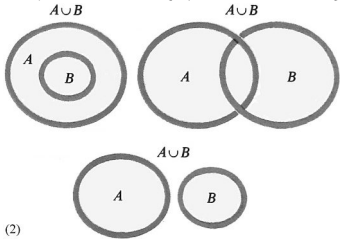


Fig. Union.

The intersection $A \cap B$ is the set of all the elements which belong at the same time to A and B. The symbol $\cap$ conjures up the symbol $\wedge$. The union $A \cup B$ is the set of all the elements which belong to A or to B. It's easy to note that the symbol $\cup$ conjures up the symbol $\vee$. The properties of $\cap$ and $\cup$ are deduced from the properties of $\wedge$ and $\vee$:

$$\text{Commutativity}\begin{cases} A \cap B = B \cap A \\ A \cup B = B \cup A \end{cases}$$

$$\text{Associativity:}\begin{cases} (A \cap B) \cap C = A \cap (B \cap C) \\ (A \cup B) \cup C = A \cup (B \cup C) \end{cases}$$

$$\text{Distributivity}\begin{cases} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{cases}$$

$$\text{Absorption}\begin{cases} A \cap (A \cup B) = A \\ A \cup (A \cap B) = A \end{cases}$$

$$\text{Idempotence}\begin{cases} A \cap A = A \\ A \cup A = A \end{cases}$$

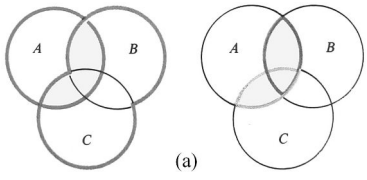


Fig.(a) Distributivity. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

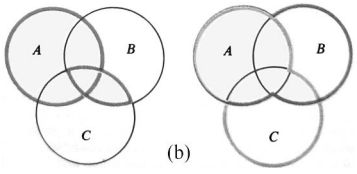


Fig.(b) Distributivity. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Due to the similitude between these operations and the rules of addition and multiplication in the sets of numbers (see algebraic structures), the mathematical field that studies the operations on the sets is called the "*algebra of sets*".

It is also possible to define the intersection and union for more than two sets. Let I be a finite or infinite set of indexes, then each index $i \in I$ is associated with a set A_i. By definition we write:

Def. 11. *(Inters.).* $\bigcap_{i\in I} A_i = \{x | \forall i, i \in I \Rightarrow x \in A_i\}$

Def. 12. *(Union).* $\bigcup_{i\in I} A_i = \{x | \exists i, i \in I \wedge x \in A_i\}$

Empty set $\varnothing$ and the *universal set (sometimes called fundamental set)* F have also the properties:
$A\cap\varnothing=\varnothing$, $A\cap F=A$, $A\cap(F\backslash A)=\varnothing$, $A\cup\varnothing=A$, $A\cup F=F$, $A\cup(F\backslash A)=F$.
Morgan's laws are also verified:

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

2.2. Maps. Algebraic operations on sets are present in all the mathematical domains. In algebra the solutions set of a equations system is the intersection of solutions sets of each equation. There is a graphical method allowing to visualize this principle. Indeed, *the graphical method visualizes the intersection of solutions sets of each equation as a common section of graphs of functions associated with each equation.* A simple way to define a map can be given by the following definition:

Map: A way of associating unique objects to any point in a given set. Thus a map $f : A \to B$ from A to B is a function f such that for every $a \in A$, there is a unique object $f(a) \in B$. The terms function and mapping are taken as synonyme for map (sometimes improperly).

2.3. Partition.

Def. 13. *(Partition). If* $\bigcup_{i\in I} A_i = F$ *and if all the* A_i *are assumed* $\neq \varnothing$ *and pairwise disjoint (i.e. mutually disjoint), the set* $\{A_i\}$ *is called a partition of* F.

Main partitions in mathematics come from *equivalence classes* according to an *equivalence relation.* Thus, the vectors or the rational numbers and many others mathematical objects are defined in the form of equivalence classes that we'll see in a next section. Thus in geometrical constructions, it is simply essential to put in place a representative of a class of given congruent figures.

3. Lattice Theory

As seen in propositional calculus, some results of propositions connections and connectives $(\wedge, \vee, ..)$ are very close to the results of the minus $-$, intersection $\cap$ and union $\cup$ algebraic operations in the theory of sets. These operations are also present in others domains of mathematics. These transversal and common notions lead up to a *generalization,* i.e a theory called theory of lattices.
The theory of lattices is the study of sets of objects known as lattices. This theory is the consequence of *Boolean algebras*, and provides a framework for unifying the study of classes or ordered sets in mathematics (see especially Birkhoff). *A lattice* can be defined as a *partially ordered set ("poset")* in which each pair of elements has both a greatest lower bound and least upper bound. A similar short presentation of a lattice is to write that a lattice is a poset (partially ordered set) with least upper bounds and greatest lower bounds for every nonempty finite subset. Before giving a definition of a lattice, it is necessary to present the axioms which constitute the lattices, these axioms constitute an axiomatic system. To present these axioms we introduce $\overline{\cap}, \underline{\cup}$ the *internal (composition) laws* of a lattice. The axioms are:

- Axiom (1)
  . *Commutativity:*
  $\forall x\ \forall y\ (x\overline{\cap}y = y\overline{\cap}x)$
  $\forall x\ \forall y\ (x\underline{\cup}y = y\underline{\cup}x)$
  . *Associativity:*
  $\forall x\ \forall y\ \forall z\ ((x\overline{\cap}y)\overline{\cap}z = x\overline{\cap}(y\overline{\cap}z))$
  $\forall x\ \forall y\ \forall z\ ((x\underline{\cup}y)\underline{\cup}z = x\underline{\cup}(y\underline{\cup}z))$
  . *Absorption:*
  $\forall x\ \forall y\ (x\overline{\cap}(x\underline{\cup}y) = x)$
  $\forall x\ \forall y\ (x\underline{\cup}(x\overline{\cap}y) = x)$
- Axiom (2)
  . *Existence of a null element and an universal element:*
  $\exists n\ \forall x\ (x\overline{\cap}n = n \wedge x\underline{\cup}n = x)$
  $\exists e\ \forall x\ (x\overline{\cap}e = x \wedge x\underline{\cup}e = e)$
- Axiom (3)
  . *Complementation:*
  $\forall a\ \exists a'\ (a\overline{\cap}a' = n \wedge a\underline{\cup}a' = e)$
- Axiom (4)
  . *Distributivity:*
  $\forall x\ \forall y\ \forall z\ (x\overline{\cap}(y\underline{\cup}z) = (x\overline{\cap}y)\underline{\cup}(x\overline{\cap}z))$
  $\forall x\ \forall y\ \forall z\ (x\underline{\cup}(y\overline{\cap}z) = (x\underline{\cup}y)\overline{\cap}(x\underline{\cup}z))$

3.1. Lattices, lattices of sets.

Def. 14. *(Lattice). A lattice is a set* L *in which two internal laws* $\overline{\cap}$ *and* $\underline{\cup}$ *are defined, which verify the axiom* (1). *If* (1) *and* (2) *are verified, then it is said that* L *contains a null element and an universal element. If* (1),(2) *and* (3) *are verified, then* L *is said "complemented". If* (1) *and* (4) *are verified, then* L *is said "distributive". If* (1),(2),(3) *and* (4) *are verified, then* L *is said "Boolean".*

Def. 15. *(Lattice of sets). A set* S' *of subsets of a set* S*, containing* S *and* $\varnothing$*, and such that* S' *contains also the intersection and the union of all pairs of elements of* S' *is called a lattice of sets.*

The distributive lattices have the following propriety (which furthermore implies the uniqueness of a *complement* in a Boolean lattice):

Th. 4. *(Uniqueness of a distributive lattice).* $x\overline{\cap}z = y\overline{\cap}z \wedge x\underline{\cup}z = y\underline{\cup}z \Rightarrow x = y$.

Proof. From the following expression $x\overline{\cap}z = y\overline{\cap}z$, it is deduced that: $x\underline{\cup}(x\overline{\cap}z) = x\underline{\cup}(y\overline{\cap}z)$, then by the distributivity and the absorption, this expression becomes: $x = (x\underline{\cup}y)\overline{\cap}(x\underline{\cup}z)$. Due to the commutativity and by the exchange of x and y, it is deduced that: $y = (x\underline{\cup}y)\overline{\cap}(y\underline{\cup}z)$. Futhermore from the following expression: $x\underline{\cup}z = y\underline{\cup}z$, the second part of the two previous equalities: $x = (x\underline{\cup}y)\overline{\cap}(x\underline{\cup}z)$ and $y = (x\underline{\cup}y)\overline{\cap}(y\underline{\cup}z)$ are equal, therefore $x = y$ □

A simple case of a lattice can be given by: The set $\mathfrak{P}(S)$ of the parts of a set S is a Boolean lattice for the laws $-, \cap$ and $\cup$ with $\varnothing$ as null element and S as universal element.
Another case of lattice is the set $\mathbb{N}$ of the natural numbers, which is a not complemented distributive lattice, where $x\overline{\cap}y$ is the lower bound and $x\underline{\cup}y$ is the upper bound of x, y for the relation $\leqslant$.
A lattice in $\mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$ which spans the real vector space $\mathbb{R}^n$. Every lattice in $\mathbb{R}^n$ can be generated from a basis for the vector space by considering all linear combinations with integral coefficients. A simple example of a lattice in $\mathbb{R}^n$ is the subgroup $\mathbb{Z}^n$. A more complicated example is the *Leech lattice*, which is a lattice in $\mathbb{R}^{24}$. Thereby a typical lattice L in $\mathbb{R}^n$ can be written: $L = \left\{\sum_{i=1}^{n} \alpha_i\phi_i | \alpha_i \in \mathbb{Z}\right\}$, where $\{\phi_1, ..., \phi_n\}$ is a basis for $\mathbb{R}^n$. Different bases can generate the same lattice.

3.2. Lattices and order relations. Here, we have first to define (at least briefly) an *order relation* (also called *ordering, partial ordering, partial order,* or sometime *order).*

Def. 16. *(Order relation). Let* S *be a set. An order relation is a relation* $\leqslant$ *on* S *such that, for every* $x,y,z \in S$ *: Either* $x \leqslant y$*, or* $y \leqslant x$*, If* $x \leqslant y$ *and* $y \leqslant z$*, then* $x \leqslant y$*, If* $x \leqslant y$ *and* $y \leqslant x$*, then* $x = y$.

Similarly, an order relation is a relation $\leqslant$ on which makes the pair $(S, \leqslant)$ into a totally ordered set. (Sometimes, the term *ordering relation* is used to mean a *partial order* instead of a *total order).*
Let L be a lattice, the binary relation in L defined by $x \leqslant y :\Leftrightarrow x = x\overline{\cap}y$ satisfies all the properties of an order relation. In accordance with this order relation, $x\overline{\cap}y$ is the lower bound of x and y, $x\underline{\cup}y$ is the upper bound of x and y. Likewise, if we consider an ordered set S_o wherein every pair of elements has a lower bound $x\overline{\cap}y$ and an upper bound $x\underline{\cup}y$, it is easy to check that this set satisfies the axioms of the theory of lattices. When S_o contains a smallest element and a greatest element, these elements can be taken as the null element and the universal element, respectively.

Hasse diagram: If $(S, \leqslant)$ is a finite partially ordered set, then it can be represented by a graph which is called the *Hasse diagram,* whose vertices are elements of S and the *edges* correspond to the cover relation. An edge from $x \in S$ to $y \in S$ is present if $x < y$.There is no $z \in S$ such that $x < z$ and $z < y$. This means there is no in-between element. If $x < y$, then in the diagram y is drawn higher than x, due to this, the direction of the edges is not indicated in the Hasse diagrams.

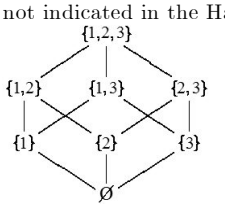


Fig: *Hasse diagram.* This diagram results from the following statements: if $S = P(\{1, 2, 3\})$, the *power set* of $\{1, 2, 3\}$, and $\leqslant$ is the *subset relation* $\subseteq$. Note that even if $\{3\} < \{1, 2, 3\}$ knowing that $\{3\} \subset \{1, 2, 3\}$, there is no direct edge between them because there in-between elements $\{2, 3\}$ and $\{1, 3\}$.

Such a link with the *order relations* allows to draw the *finite lattices* using *Hasse diagram*; see examples below (Fig.(a),(b))

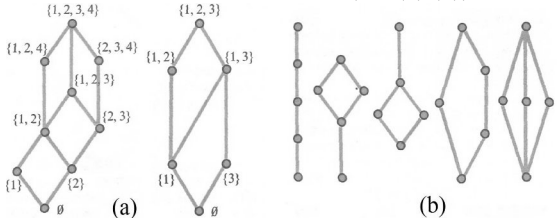


Fig. Hasse diagrams for: (a) 2 lattices of sets; (b) All lattices with 5 elements.

The set of parts of a k-elements set forms a 2^k Boolean lattice (i.e. a Boolean lattice with 2^k elements). The picture below is constructed with all possible subsets which is the *power set* (see "*subset, set of the parts of a set*") of the three elements a, b, c belonging to the set.

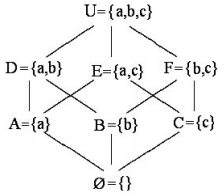


Fig: Lattice of the power set {a,b,c}.

These subsets constitute a partial order that is referred to as a lattice. The set U (top of the diagram) consists of all of the elements of the set. The sets D,E, and F are each in the subset relation to U, this means for example that every element of D is an element of U. This subset relation is a basis for partially ordering the sets. Note that the set A is a subset of D and of E. B is a subset of D and F, etc. The position in diagram indicates the ordering relations that hold under the subset relation. *Empty set* is represented at the bottom and is ordered in the diagram with respect to sets A,B and C.

Atom of a lattice: An *atom* of a finite Boolean lattice L is any minimal element of $L\backslash\{n\}$ for the order relation $\preccurlyeq$. Then any element a of $L\backslash\{n\}$ is formulated by the following expression: $\underline{\cup}\alpha_i$, and the terms α_i are the atoms. This means that any *finite Boolean lattice* is *isomorphic* to the set of the parts of a finite set. Any distributive lattice is isomorphic to a lattice of sets. The *cardinal* of this set is always a power of 2.

Isomorphic: This term means "having the same form", and is used to identify mathematical objects which have the same structural properties. Such objects can be represented, or *embedded*, differently but have the same essential structure, and are said to be similar to an isomorphism. The statement *"A is isomorphic to A'"* is denoted $A \cong A'$. (Unfortunately, the symbol $\cong$ is also used to denote geometric congruence).

Cardinal number: The number of members of a set. It is usually taken as a particular well-ordered set representative of the class of all sets which are in one to one correspondence with one another.

3.3. Lattices and Boolean rings. *Boolean lattices* have important properties that are introduced by the following operations:

$$x \cdot y := x\overline{\cap}y$$
$$x + y := (x\overline{\cap}y')\underline{\cup}(x'\overline{\cap}y).$$

Thus, a lattice is structured as a *commutative unit ring* (see ring). Furthermore, $\forall x(x \cdot x = x)$: *idempotent ring* and $\forall x(x + x = n)$. In the opposite, from a *commutative unit and idempotent ring*, a *Boolean lattice* can be constructed, with the following conditions:

$$x\overline{\cap}y := x \cdot y$$
$$x\underline{\cup}y := x + y + x \cdot y$$
$$x' := e + x$$

Boolean ring: A ring with a unit element in which every element is idempotent.
Unit element: An element in a ring which acts as a multiplicative identity.

4. Foundations of Sets

Set theory has been created by Cantor in the late nineteenth-century to solve problems of real analysis. It has given rise to psychological resistance (some mathematicians saw it as being metaphysics) and posed important logical problems (the "crisis of foundations", in the early nineteenth-century). However, it has quickly invested other parts of mathematics, in particular, modern algebra, founded in Germany between the two world wars, is fully formulated in the language of sets.

In its modern version, all the mathematics are based on set theory and *any mathematical object is a set.* Thus, in the theory of von Neumann, the natural number n is defined as a particular set of n elements, for example, $0 := \varnothing$. Here we adopt a *naive* point of view. Our sets and maps contain (or involve) elements, which are more or less elementary mathematical object, and their nature is not necessarily specified. All of these "entities" are however subject to the axioms that we will explicit.

4.1. Set membership, elements. The sets consist of elements; what are these elements is not specified. Thus, we introduce a particular relation between an element x and a set E, the *set membership.* This relation is written $x \in E$, which is read "x belongs to E", "x is an element of E", "x is a member of E", "x lies in E", or also "x is in E". The relation "is an element of" is called *set membership* (sometimes also called *mathematical relation of belonging*). The expressions "E includes x" or "E contains x" are also used to mean set membership, however some authors use them to mean instead "x is a subset of E". Note also that the formulation "E contains x" is ambiguous due to the inclusion (def.). The negation of set membership is written $x \notin E$, meaning $x \in E$ is false, or $\neg(x \in E)$ is true. It is read "x does not belong to E", or "x is not an element of E", etc.

(A) **Axiom** *of Extensionality: The fundamental axiom is the axiom of extensionality for the sets, which asserts that a set is totally characterized by its elements:*

(†) $$(\forall x, x \in E \Leftrightarrow x \in F) \Rightarrow E = F;$$

read "two sets having the same elements are equal".

In the sentence between quotation marks, the use of the indefinite article "the" (same elements) says that it is *all* the elements: this why the above formula (†) contains the quantifier $\forall x$, which must be read "whatever x", or "far all x". Note that $\forall$ is called the "*universal quantifier*", or sometimes, the "*general quantifier*".
Note that the converse implication is self-evident for pure logic reasons. Mathematical usage wants that if we have an equality E=F, then any property verified by E is verified by F ("substitutivity of the equality"); besides, this is the way in which Leibniz defined the equality. Anyway, if we have E=F and $x \in E$, it follows that $x \in F$. In practice we can prove *by equivalence* the equality of two sets.

Ex. 8. *Determine the intersection of lines $L : y = 2x + 1$ and $L' : y = 3x - 2$. Solution: It is the set of points (x, y) that belong to L and L', i.e. satisfying the system of equations $(y = 2x + 1, y = 3x-2)$. Elementary methods of solving (fittingly, by equivalence) allow to deduce that (x, y) is solution of this system if and only if $x = 3$, $y = 7$. As we'll see, there is a set of which the only one element is the point $p = (3, 7)$. This is the singleton $\{p\}$. Thus we have $m \in L \cap L' \Leftrightarrow m \in \{p\}$, hence $L \cap L' = \{p\}$.*

Most axioms appearing in this heading involve some property $P(x)$ of an indeterminate element x (P is called a *predicate*); an axiom then will say that the elements x such that $P(x)$ is true form a set, in other words, there is a set E such that $\forall x, x \in E \Leftrightarrow P(x)$. This is read "whatever x, x belongs to E if and only if $P(x)$". The axiom of extensionality will allow to deduce that E is *unique*.Indeed, if F is a (other) set such that $\forall x, x \in F \Leftrightarrow P(x)$, the usual rules about the logical equivalence imply $\forall x, x \in E \Leftrightarrow x \in F$, so $E = F$.

Construction of finite sets. We consider here the "finite" sets in an intuitive sense.

(B) **Axiom** *of the Empty set: There exists a set that has no element.*

(‡) $$\exists E : \forall x, x \notin E;$$

it is denoted by "$\varnothing$" and called "empty set".

The existence of a (underlying: "at least") set that has no element ("a", indefinite article, expresses the existence, quantifier "$\exists$") is the content of this axiom. But according to the axiom of extensionality, the set that has no element is unique. This is why, in the second portion of the sentence, we say *the*, which underlies the uniqueness. Note that $\exists$ denotes the "*existential quantifier*". The formula (‡) can thus be reinforced as follows:

$$\exists! E : \forall x, x \notin E,$$

where the symbol $\exists!$ means "*there exists a unique*".

(C) **Axiom** *of Singletons: Given a a mathematical object. The axiom of singletons asserts that there exists a set of which the only element is a. It is denoted by $\{a\}$, read "singleton a."*

Setting $E = \{a\}$, we have thus: $\forall x, x \in E \Leftrightarrow x = a$. According to the axiom of extensionality, such a set is unique. Any mathematical object is therefore element of a set, and we call *element* this object. Naturally, $\{a\}$=$\{b\}$ is logically equivalent to a=b.

(D) **Axiom** *of the Pair: Let* a, b be *two (not necessarily distinct) elements. The axiom of the pair asserts that there exists a set of which the only elements are* a *and* b*. It is denoted* "$\{a, b\}$"*. If* $a \neq b$*, it is called* "*pair consisting of* a *and* b*.*"

According to the axiom of extensionality, the set $\{a, b\}$ is unique. The axiom of the pair implies, besides, the axiom of singletons: when $a = b$, we find $\{a, a\} = \{a\}$. Similarly, we show that $\{a, b\} = \{b, a\}$ by the pure logic! For any x: $x \in \{a, b\} \Leftrightarrow (x = a$ or $x = b) \Leftrightarrow (x = b$ or $x = a) \Leftrightarrow x \in \{b, a\}$ and we apply the axiom of extensionality. Beware not to confuse the pair $\{a, b\}$ and the pair (a, b), indeed, we have $(a, b) = (b, a)$ only if $a = b$.

Ex. 9. *Show that the sets* $\varnothing, \{\varnothing\}, \{\{\varnothing\}\}$ *and* $\{\varnothing, \{\varnothing\}\}$ *are pairwise distinct. Solution: Only the first has no element, it is therefore different from each of other three; besides, since* $\varnothing \neq \{\varnothing\}$ *(we have just seen it), the corresponding singletons are different. The last set is a pair because* $\varnothing \neq \{\varnothing\}$*, it is thus equal to none of other three.*

The previous axiom of the pair (D) (also called *axiom of pairing*) can be formulated as follows:

(D)′ **Axiom** *of the Pair (Axiom of Pairing):* $\forall a$,$\forall b$ *there exists a set* $\{a, b\}$ *that contains exactly* a and b.

$$\forall a \forall b \exists c \forall x (x \in c \longleftrightarrow x = a \vee x = b),$$

where $\longleftrightarrow$ (or $\Leftrightarrow$) is the *material equivalence.*

Using the Axiom of Extensionality, we see that the set c is unique, so it makes sense to define the pair: "$\{a, b\}$ =the unique c such that $\forall x (x \in c \longleftrightarrow x = a \vee x = b)$."

Using the Axiom of Pairing, we may define, for any set a, the singleton: $\{a\} = \{a, a\}$.

We can also define for any a and b, the ordered pair:

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

Note that this definition satisfies the condition: $(a, b) = (c, d)$ iff $a = c$ and $b = d$.

We may define the ordered n-tuple recursively:

$$(a_1, ..., a_n) = ((a_1, ..., a_{n-1}), a_n).$$

Extensional definition (i.e. "**by extension**", specifying its extension). Whenever we give ourselves objects $a_1, ..., a_n$, we get a more general version of axioms.

(E) *Extensional* ***definition*** *(and* **axiom**): *There exists a set of which the only elements are* $a_1, .., a_n$ *(according to Axiom of Extensionality, it is unique). This set is denoted* $\{a_1, .., a_n\}$*. We say that we have defined this set "by extension", i.e. by enumerating its elements.*

Ex. 10. *Find a necessary and suffisant condition so that we have* $\{a_1, ..., a_n\} = \{a\}$ *or* $\{a_1, ..., a_n\} = \varnothing$*. Solution: The first equality arises if and only if the objects* $a_1, ..., a_n$ *are all equals to* a*. In principle, the second is impossible. However, there exists a convention (actually, an abuse of language) in which when* $n = 0$ *(no object!), the notation* $\{a_1, ..., a_n\}$ *denotes the empty set.*

For $n = 1, 2$, we find again the previous axioms. Beyond we the set $\{a, b, c\}$, $\{a, b, c, d\}$, etc. The general notation $a_1, .., a_n$ is slightly abusive because it underlies that we know how to interpret the... intermediates. In practice, one permits oneself "incomplete extensional definitions" such as {0,1,2,...} we easily discern the "law of formation" of enumerated elements: here, the integers of the form $2k$, where the integer k varies between 0 and n. By current abuse, the same notation is used to enumerate infinite sets, as $\mathbb{N}$={0, 1, 2, ...} or the set $2\mathbb{N}$={0,2,4,...} of the even integers. This can be dangerous (ambiguity of the law of formation) and this hides, actually, more powerful axioms. Actually, to anticipate, we have a sequence $(u_n)_{n\in\mathbb{N}}$ and the set $\{u_0, u_1, ...\}$ is the image set of this sequence, i.e. the set $\{u_n | n \in \mathbb{N}\}$.

Ex. 11. *Recognize the set* $\{0, 1, -1, 2, -2...\}$*. Solution: It is, of course, the set* $\mathbb{Z}$*. We can describe it by using the sequence* $(u_n)_{n\in\mathbb{N}}$ *defined by the formulas* $u_{2p} = -p$ *and* $u_{2p+1} = p + 1$*.*

4.2. Definition by comprehension. In many situations, we have a predicate $P(x)$ (i.e. a property dependent on the indeterminate element x) and we wonder if there exists a set E such that $\forall x, x \in E \Leftrightarrow P(x)$. If it is the case, E is unique (axiom of extensionality).

Def. 17. *(Collectivizing property). If such a set exists, we denote it by* $\{x | P(x)\}$*, which is read "the set of the* x *such that* $P(x)$*". We say then that the property* P *is "collectivizing".*

Ex. 12. *As we have seen it, the property* $x \neq x$*,* $x = a$*,* $(x = a$ *or* $x = b)$ *(with* a *and* b *fixed) are collectivizing. For a given set* E*, the property* $x \in E$ *is obviously collectivizing, and we have equality* $E = \{x | x \in E\}$*.*

All these precautions are necessary because we cannot declare all the collectivizing predicates:

Ex. 13. *One of the oldest paradoxes of set theory concerns "the set of elements that are not elements of themselves", i.e. the set* $E := \{x | x \notin x\}$*. Thus,* $\forall x, x \in E \Leftrightarrow x \notin x$*. Apply this assertion to* $x := E$*. Solution: We find the famous contradiction* $E \in E \Leftrightarrow E \notin E$*. The existence of such a set* E *leads to a contradiction. Given the principles of the mathematical logic, this existence is therefore false, the set* E *does not exist and the property* $\{x | x \notin x\}$ *is not therefore collectivizing.*

Thus, we'll have to expressly declare by axioms that certain predicates are collectivizing and that certain sets indeed exist, as we have shown for extensional definition. However, in most of cases, this will be facilitated by the following axioms, called *axiom of separation.*

(F) **Axiom** *of Separation: Given* E *a set and* $P(x)$ *a property of elements of* E*, then the property* "$P(x)$ *and* $x \in E$" *is collectivizing and we denote the associated set* $\{x \in E | P(x)\}$*, which is read "the set of the* x *elements of* E *such that* $P(x)$*".*

Thus there does not exist set of all the sets: indeed, if such a set existed (according to the axiom of separation), any property would be collectivizing.

Ex. 14. *Do the sets* $\{x \in \mathbb{R} | x^2+1=0\}$ *and* $\{x \in \mathbb{N} | x+1=0\}$ *exist? Solution: Yes, according to axiom of separation! But they are empty (thus equal); actually it's their elements that do not exist..*

Inclusion, parts.

Def. 18. *(Inclusion, part, subset). We say that the set* F *is included in* E*, denoted by* $F \subset E$*, if all the elements of* F *are elements of* E*:*

$$F \subset E \Leftrightarrow (\forall x, x \in F \Rightarrow x \in E).$$

We say also that F *is a part or a subset of* E*.*

We also say that E contains F (but it is ambiguous). Empty set is a subset of any set. Any set is subset of itself. The set $\{x \in E | P(x)\}$ (i.e. the set of elements of E which have the property P) is a subset of E.

Ex. 15. *Find the condition such that:* $\{a\} \subset E$*;* $\{a, b\} \subset E$*;* $\{a\} \subset \{b\}$*. Solution: The inclusion* $\{a\} \subset E$ *(resp.* $\{a, b\} \subset E$*) is equivalent to the belonging* $a \in E$ *(resp. to the belongings* $a \in E$ *and* $b \in E$*). The inclusion* $\{a\} \subset \{b\}$ *is equivalent to the equality* $a = b$*.*

Anticipating ulterior definitions we see that the relation of inclusion is reflexive: $E \subset E$, transitive: $(E \subset F$ and $F \subset G) \Rightarrow E \subset G$ and antisymmetric: $(E \subset F$ and $F \subset E) \Rightarrow E \subset F$; the two first properties are immediate, the third is a simple transcription of the axiom of extensionality. The inclusion is thus an *order relation* (def. in heading "*Lattices and order relations*").

(G) **Axiom** *of the set of the parts of a set: Let* E *be a set. The relation* $x \subset E$ *is collectivizing and defines the set of the parts of* E*. We have:* $\mathfrak{P}(E) := \{x | x \subset E\}$*.*

Ex. 16. *The only subset of* $\varnothing$ *is* $\varnothing$*, hence* $\mathfrak{P}(\varnothing) = \{\varnothing\}$*. We have also* $\mathfrak{P}(\{a\}) := \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$*. Moreover,* $\mathfrak{P}(\mathfrak{P}(\varnothing)) = \{\varnothing, \{\varnothing\}\}$*.*

4.3. Constructors.

Elementary constructors. Another axiom is needed to construct the union of two arbitrary sets.

(H) **Axiom** *of Union: Let* E *and* F *be two sets. There exists then a set* G *such that:*

$$\forall x, x \in G \Leftrightarrow x \in (E \text{ or } x \in F).$$

This set (unique according to the axiom of extensionality) is called union of E *and* F *and is denoted* $E \cup F$*. Thus,* $E \cup F := \{x | x \in E$ *or* $x \in F\}$*.*

Recall that the "or" of the mathematicians is not exclusive: the affirmation $x \in E$ *or* $x \in F$, does not exclude that we have $x \in E$ *et* $x \in F$. Thus, $E \cup F$ contains in particular the elements common to E *and* to F.

Def. 19. *(Intersection). Let* E *and* F *be two sets. The set of elements of* E *that are in* F *exists (axiom of separation) and is unique (axiom of extensionality). We call it "intersection" of* E *and* F*, denoted by* $E \cap F$*:*

$$\forall x, x \in E \cap F \Leftrightarrow (x \in E \text{ and } x \in F).$$

Thus, $E \cap F := \{x | x \in E$ *and* $x \in F)$*. We say that* E *and* F *are disjoint if their intersection is empty.*

We have of course $E \cap F = F \cap E$.

Def. 20. *(Set difference). Let* E *and* F *be two sets. The set of elements of* E *that are not in* F *exists (axiom of separation) and is unique (axiom of extensionality). It is called "difference" of* E *and* F *and is denoted* $E \backslash F$*:*

$$\forall x, x \in E \backslash F \Leftrightarrow (x \in E \text{ and } x \notin F).$$

Thus, $E \backslash F := \{x | x \in E \text{ and } x \notin F)$.

If $F \subset E$, the set $E \backslash F$ is called "*complement*" of F *in* E and is denoted by $\complement_E F$. We cannot say that it is a *complement* "*in the absolute*" of the set F, but only relatively to a set embedding E.

Complement: In set theory, a complement of a set A refers to things not in (i.e. things outside of) A. The relative complement of A with respect to a set B, is the set of elements in B but not in A. If all sets under consideration are considered to be subsets of a given set U, the absolute complement of A is the set of all elements in U but not in A.

Relative complement: If A and B are sets, then the *relative complement* of A in B, also termed the "*set-theoretic difference*" of B and A, is the set of elements in B, but not in A. The relative complement of A in B is denoted $B \backslash A$ (sometimes written $B - A$, but this notation is ambiguous, because it can be interpreted in some contexts as the set of all $b - a$, where b is taken from B and a from A).

Absolute complement: If a universe U is defined, then the relative complement of A in U is called the *absolute complement* (or simply *complement*) of A, and is denoted by A^c (or sometimes A'), also the same set often is denoted by $\complement_U A$ or $\complement A$ if U is fixed, that is: $A^c = U \backslash A$.

The union and intersection operations satisfy many rules of algebraic nature, which are all very easy to check once written. In the equalities below, A, B and C denote three arbitrary sets:

Associativity of the union:
$A \cup (B \cup C) = (A \cup B) \cup C$.
Commutativity of the union:
$A \cup B = B \cup A$.
Empty set is absorbing[1] for the intersection:
$\varnothing \cap A = A \cap \varnothing = \varnothing$.
Empty set is neutral for the union:
$\varnothing \cup A = A \cup \varnothing = A$.
Every set is idempotent for the union:
$A \cup A = A$.
Associativity of the intersection:
$A \cap (B \cap C) = (A \cap B) \cap C$.
Commutativity of the intersection:
$A \cap B = B \cap A$.
Every set is idempotent for the intersection:
$A \cap A = A$.
Distributivity of intersection with respect to union:
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
Distributivity of union with respect to intersection:
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
$A \subset B \Leftrightarrow A \cap B = A$,
$A \subset B \Leftrightarrow A \cup B = B$.

Proof. By way of example, the last two rules can be proved. Start with the direct implications (meaning, from left to right). Assume thus the inclusion $A \subset B$. Concerning the first equality to be demonstrated, we have a priori the inclusion $(A \cap B) \subset A$. Moreover, we have at the same time $A \subset A$ (always true) and $A \subset B$ (this is the assumption), therefore $A \subset (A \cap B)$ (by definition of the intersection). From the double inclusion $(A \cap B) \subset A$ and $A \subset (A \cap B)$, we finally deduce the first equality sought: $(A \cap B) = A$. The other equality can be similarly proved using a double inclusion: the inclusion $B \subset (A \cup B)$ is always true. The reverse inclusion $(A \cup B) \subset B$ results (by definition of the union) from the fact that $A \subset B$ (this is the assumption) and $B \subset B$ (always true). Consider now the reverse implication (meaning, from right to left). Assume first $(A \cap B) = A$. Then every element of A is element of $A \cap B$ (these sets have same elements since they are equal) therefore of B: that is, $A \subset B$, as sought. Assume now that $(A \cup B) = B$. Then every element of A is element of $A \cup B$ (of course) so of B (which is equal to the previous), and we have also $A \subset B$. □

Ex. 17. *What is the condition for* $A \cup B = A \cap B$*?*
Solution: Since $(A \cap B) \subset A \subset (A \cup B)$ *and* $(A \cap B) \subset B \subset (A \cup B)$*, the above equality leads to* $A = B$*; the reverse is immediate.*

Union, intersection and difference of two parts of a set A are also parts of A. Slightly anticipating some concepts (internal composition laws, morphisms,..), we can then consider them as internal composition laws on $\mathfrak{P}(A)$. Beyond the above algebraic rules stated, the set $\mathfrak{P}(A)$ endowed with the laws $\cup$ and $\cap$ verify the following properties (where F and G denote **parts of** A):

The set A is neutral for the intersection:
$A \cap F = F \cap A = F$.
The set A is absorbing for the union:
$A \cup F = F \cup A = F$.
Involutivity of the passage to complement:
$\complement_A(\complement_A F) = F$.
The passage to complement is a morphism $\cup \to \cap$:
$\complement_A(F \cup G) = (\complement_A F) \cap (\complement_A G)$.
Passing to complement is a morphism $\cap \to \cup$:
$\complement_A(F \cap G) = (\complement_A F) \cup (\complement_A G)$.

Last two formulas are known as *Morgan's laws*. The first two laws are immediate according to the previous rules. The third law results from the equivalence: $\forall x \in A,\ x \notin F \Leftrightarrow x \in \complement_A F$. The proof of Morgan's laws lies on rules of logic: Let P and Q be two statements; then the negation of "P and Q" is "non P or non Q", and the negation of "P or Q" is "non P and non Q". We apply here these rules to the statement $P := (x \in F)$ and to the statement $Q := (x \in G)$.

Cartesian product. Suppose that we know how to form, starting from two objects a and b, a *pair* (a, b) to satisfy the following rule:
$\forall a, \forall b, \forall c, \forall d,\ (a, b) = (c, d) \Leftrightarrow a = c$ and $b = d$.
(For such a construction see Kuratowski). The elements a and b are respectively called first and second *components* (or *coordinates*) of the pair (a, b). If $x = (a, b)$, we write $a = p_1(x)$ and $b = p_2(x)$.

(I) **Axiom** *of Cartesian product: Given* E,F *two sets. There exists a set* G *whose elements are the pairs* (a, b) *consisting of an element* $a \in E$ *and of an element* $b \in F$:

$$G := \{x | \exists a \in E \text{ and } \exists b \in F : x = (a, b)\}.$$

According to the axiom of extensionality, such a set is unique. It is denoted "$E \times F$*" and called "Cartesian product" of the sets* E *and* F*. Equivalently,*

$$E \times F := \{(a, b) | a \in E \text{ and } b \in F\}.$$

More generally, from the n elements $a_1, .., a_n$, we can form the *n-tuple* $x = (a_1, .., a_n)$, of which the n components (or coordinates) are $a_1 = p_1(x), .., a_n = p_n(x)$. For n=3,4,5,.., we say *triplet*, *quadruplet*, *quintuplet*, etc. We have then the rule: $\forall a_1, .., \forall a_n, \forall b_1, .., \forall b_n$, $(a_1, .., a_n) = (b_1, .., b_n) \Leftrightarrow a_1 = b_1$ and $\cdots$ and $a_n = b_n$.
Above axiom can be generalized as follows: the n-tuples $(a_1, ..., a_n)$ consisting of the elements $a_1 \in E_1, ..., a_n \in E_n$ form a set, the *Cartesian product* $E_1 \times \cdots \times E_n$. If one of the E_i is empty, we can form no n-tuple since there is no possibility for its i^{th} component. If all the E_i are non empty, by selecting an element a_i in each E_i, we form an n-tuple $(a_1, ..., a_n)$ which is element of $E_1 \times ... \times E_n$. We conclude that the Cartesian product $E_1 \times \cdots \times E_n$ is empty if and only if one of the sets E_i is empty.
The strict application of rules leads to $(x, (y, z)) \neq ((x, y), z)$ (these two pairs do not have the same first projection). But we often identify them with (x, y, z). Likewise, we will identfy the product sets $E \times (F \times G)$ and $(E \times F) \times G$ with $E \times F \times G$. This convention can be naturally generalized to more complicated products. We often set: $E^n = E \times \cdots \times E$ (n factors). With the previous identifications, this comes down to set: $E^1 = E$, then, by induction (by recurrence), $E^{n+1} = E \times E^n$ (or optionally $E^n \times E$). The *diagonal* of E^n is the set $\{x \in E^n | p_1(x) = \cdots = p_n(x)\}$. We can also describe it as $\{(x, ..., x) | x \in E\}$, where the tuple $(x, ..., x)$ has n components.

5. Problems of Set Theory

5.1. Basic definitions and context.

Set theory: Mathematical theory of sets is associated with the branch of mathematics known as logic. Set theory is the branch of mathematical logic that studies sets, which are collections of objects. There are different versions of set theory. Each version with its own rules and axioms, having a more or less large capability to provide a consistency strength. The modern study of set theory was initiated by Georg Cantor and Richard Dedekind in the 1870s. After the discovery of paradoxes in naive set theory, numerous axiom systems were proposed in the early twentieth century, of which the Zermelo-Fraenkel axioms, with the axiom of choice, are the best-known. There are several versions of set theory, each with its own rules and axioms. In order of increasing consistency strength, some of these versions of set theory include Peano arithmetic (ordinary algebra), second-order arithmetic (analysis), Zermelo-Fraenkel set theory, Mahlo, weakly compact, hyper-Mahlo, ineffable, measurable, Ramsey, supercompact, huge, and n-huge set theory, etc.

[1] *Absorbing element (annihilating element)*: An absorbing element is a special type of element of a set with respect to a (binary) operation on that set. The result of combining an absorbing element with any element of the set is the absorbing element itself. In semigroup theory, the absorbing element is called a zero element, because there is no risk of confusion with other notions of zero. An absorbing element may also be called an *annihilating element*.
Absorption laws: For all sets A and B (subsets of some *universal set*), $A \cap (A \cup B) = A$ and $A \cup (A \cap B) = A$.

Naive set theory: Naive set theory is that branch of mathematics which tries to formalize the nature of the set using a minimal collection of independent axioms. However, naive set theory runs into a number of paradoxes, such as Russell's paradox, so a less large and more formal theory must be used, this leads up to the *axiomatic set theory.*

Axiomatic set theory: Axiomatic set theory is the presentation of a set theory as comprising axioms together with rules of inference. In other words, axiomatic set theory is a system of set theory which differs from so-called naive set theory in that the sets which are allowed to be generated are strictly constrained by the axioms. An axiomatic theory (e.g. geometry) is said to be a *complete axiomatic theory* if each valid statement in the theory is capable of being proven true or false.

Context. In the 1870s, Cantor, with Dedekind and Peano and others, created the set theory. It was initially unpopular and later led to a violent crisis but fruitful. Today this theory (at least at its elementary level), with its language and its main notations, is the basic tool of the mathematician.
After Cantor, a number of problems appeared: discussions between Lebesgue, Baire and Borel on the axiom of choice, serious paradoxes of set theory discovered by Russel (**the set of all sets**). In the early XX^{th} century, Hilbert undertook to give a solid foundation, totally compelling (in the historical line of Aristotle, Leibniz, Boole, Frege, Peano..). He aspired to completely formalize *all* the mathematical reasoning. But despite the genius of Hilbert, the program ended with a resounding failure in 1931, an astounding discovery of Gödel (incompleteness theorem, connected to classical paradoxes: *a Cretan said that all Cretans are liars*).
However, if the Hilbert's answer was wrong, his *question* was good! Indeed, it led, among other things, to the invention of computers and to an extraordinary development of programming and calculation... initiated by the work of von Neumann and Turing (themselves greatly influenced by the Gödel's results). The story is not over and continues in important recent research in theoretical computer science (e.g. G.J. Chaïtain's work in connection with the physical concept of entropy).

5.2. Basic concepts of set theory. Set theory starts with a fundamental binary relation between an object m and a set A. If m is a *member* (or *element*) of A, we write $m \in A$. Since sets are objects, the membership relation can relate sets also. A derived binary relation between two sets is the subset relation, also called *set inclusion.* If all the members of the set A are also members of the set B, then A is a subset of B, denoted $A \subseteq B$; (e.g. $\{0,1\}$ is a subset of $\{0,1,2\}$, but $\{1,3\}$ is not.) From this definition, a *set is a subset of itself*; when we want to exclude this feature, we get then the term *proper subset*; A is called a *proper subset* of B if and only if A is a subset of B, but B is not a subset of A. As arithmetic with binary operations on numbers, set theory has binary operations on sets, namely:
▪ **Union** of the sets A and B (denoted "$A \cup B$") is the set of all objects that are a member of A, or B, or both; (e.g. the union of {1,2,3} and {2,3,4} is the set {1,2,3,4}).
▪ **Intersection** of the sets A and B (denoted "$A \cap B$") is the set of all objects that are members of both A and B; (e.g. the intersection of $\{1,2,3\}$ and $\{2,3,4\}$ is the set $\{2,3\}$).
▪ **Set difference** of U and A (denoted "$U \setminus A$") is the set of all members of U that are not members of A; (the set difference $\{1,2,3\} \setminus \{2,3,4\}$ is $\{1\}$, while, conversely, the set difference $\{2,3,4\} \setminus \{1,2,3\}$ is $\{4\}$). When A is a subset of U, the set difference $U \setminus A$ is also called the *complement* of A in U. In this case, if the choice of U is clear from the context, the notation A^c is sometimes used instead of $U \setminus A$, particularly if U is a *universal set* as in the study of Venn diagrams.
▪ **Symmetric difference** of sets A and B (denoted "$A \Delta B$", or sometimes "$A \ominus B$") is the set of all objects that are a member of exactly one of A and B (elements which are in one of the sets, but not in both); (e.g. for the sets $\{1,2,3\}$ and $\{2,3,4\}$, the symmetric difference set is $\{1,4\}$. It is the set difference of the union and the intersection, $(A \cup B) \setminus (A \cap B)$ or $(A \setminus B) \cup (B \setminus A)$).
▪ **Cartesian product** of A and B (denoted "$A \times B$") is the set whose members are any ordered pairs (a,b) where a is a member of A and b is a member of B; (the cartesian product of $\{0,1\}$ and $\{E,F\}$ is $\{(0,E), (0,F), (1,E), (1,F)\}$). The Cartesian product is also called product set, set direct product or cross product.
▪ **Power set** of a set A (denoted "$\mathcal{P}(A)$", "$P(A)$", "$\mathbb{P}(A)$", "$\wp(A)$" or "2^A") is the set whose members are all subsets of A, i.e. the set of all subsets of A including the empty set and A itself; (e.g. the power set of $\{1,2\}$ is $\{\{\}, \{1\}, \{2\}, \{1,2\}\}$.) In axiomatic set theory (as developed for instance in the ZFC axioms), the existence of the power set of any set is postulated by the axiom of power set. Any subset of $\mathcal{P}(A)$ is called a *family of sets* over A.

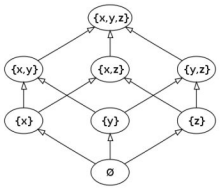


Fig. Hasse diagram of the power set {x,y,z}; that is, the elements of the power set of the set {x,y,z} ordered according the inclusion.

5.3. Antinomies, theory of types. As seen before, especially about Russell's paradox, we know that the *naive set theory* can give rise to contradictions. The paths leading to contradictions are called *antinomies,* and have been used in order to reanalyze set theory. There are two types of *antinomy: semantic* and *syntactic* antinomies. A *syntactic antinomy* leads to a contradiction by purely formal deduction (Ex.[II]). By contrast, a *semantic antinomy* has a contradictory content (Ex.[I]). If we examine a semantic antinomy we see an abuse of language, since there is no distinction between common meanings and more elaborate meanings [I]-1), between trivial properties and refined properties [I]-3). An *antinomy* is a term used in logic and epistemology, which, loosely, means a paradox or unresolvable contradiction.

Ex. 18. [I] (*Examples of semantic antinomies*):
1) [*Epimenides of Knossos in Crete (Greece), about 600 BC*]. *"What I say is a lie". If Epimenides lies, his statement is false and so he did not lie. If he tells the truth, then his statement is true and so he lied. There is a contradiction.*
2) [*Proklos (Proclus), Greece, about 450 BC*]. *Protagoras teaches Law to a disciple, and has agreed with him that he will have to pay tuition fees only after winning his first trial. After his studies, as the disciple takes responsibility of no trial, Protagoras decides to file a claim to compel him to pay the tuition. His argument is as follows: If I win the trial, I get my money back because of original agreement. The disciple argues the opposite way: in any case he has nothing to pay either because of the original agreement or because of the trial.*
3) [*Grelling*]. *The set of english adjectives (word characterizing a property) discerns two classes:*
a) Heterological adjectives: They are not what they mean; e.g. the adjective "long" that is short, the adjective "french" that is english, the adjective "monosyllabic" that is multisyllabic."
b) Autological adjectives: They are what they mean; e.g. adjectives: "short", "english", "multisyllabic".
The class of the adjective "heterological" is paradoxical. If we suppose that it belongs to a), we deduce that it belongs to b) and vice-versa.

Ex. 19. [II] (*Examples of syntactic antinomies*):
1) [*Burali-Forti, 1897*]. *"Consider the set B, if it exists, of all ordinals. As every set of ordinals is well ordered, B has an ordinal B′ obviously higher than all the elements of B. According to the definition of B, B′∈B. However, B′ ∪ {B′} is an ordinal strictly higher than B′, whereas it belongs itself also to B. There is a contradiction. (cf. heading "Burali-Forti paradox" in "Ordinals").*
2) [*Cantor, 1899*]. *"Consider the set C, if it exists, of all the sets (universal set). In particular every part of C is an element of C, and thus $\mathfrak{P}(C) \subset C$ (with $\mathfrak{P}(C)$=set of the parts of C). It follows $\text{card}(\mathfrak{P}(C)) < \text{card}(C)$. But $\text{card}(\mathfrak{P}(C)) > \text{card}(C)$ (cf. heading "Power, Cardinal, Denumerability" in "Relations and Structures). There is a contradiction.*
3) [*Russel, 1903*]. *"Consider the set R, if it exists, of all the sets E such that $E \notin E$. If $R \notin R$, then $R \in R$, and if $R \in R$, then $R \notin R$. There is a contradiction (see Russell's paradox in heading "Russell paradoxical set" in "Basic Concepts").*

A semantic antinomy leads to the contradiction through a formal deduction.
The syntactic antinomies belong to the mathematical theory of sets. In order to transpose the sentences and possible antinomies into set theory, it is necessary to structure the elements, the objects and the relations between them. Thus, a *fundamental set* F is defined, then the elements of this fundamental set F, and the sets of the elements of the fundamental set F, and so on.. In addition, it is also necessary to call differently the variables at each level. The notions of level and belonging are crucial in this set theory. The *theory of types* (Russell) is also based on these concerns. The *theory of types* (or *type theory*) forbids expressions of the kind: $x \in x$ or $\neg x \in x$ *b*; The *theory* of *types* stops the occurrence of antinomies mentioned above.
The concept of *type* has been defined by Whitehead and Russell. They organize the *types* in a hierarchy in order to eliminate self-referential statements from *Principia Mathematica (see infra)*, which want to

derive all the mathematics from the logic. A set of the lowest type contained only objects, but not sets, and a set of the higher type could contain objects or sets of the lower type, etc... (However, Gödel incompleteness theorem (1931) proved that Principia Mathematica and all consistent formal systems must be incomplete).

Principia Mathematica (1910-1913): Taking back the previous work of Isaac Newton (1687), this publication "Principia mathematica" corresponds to the foundations of mathematics written by A.N.Whitehead and B.Russell. *The goal was to try to derive all mathematical truths from a well-defined set of axioms and inference rules in symbolic logic*, and have been inspired from the work of Frege about logic. The Russell's contradictions and paradoxes have been derived from the work of Frege, and were avoided in the Principia Mathematica by a *system of types.* A set has a higher type than its elements and it is not possible to use the notions as the "**set of all sets**" which generates paradoxes (see Russell's paradox). In the Principia Mathematica, the statement "there are no contradictions in the Principia system" cannot be proven true or false in the Principia system unless there are contradictions in the system, so in which case it can be proven both true and false

Later on, *axiomatic set theory* has been developed. This theory is derived from the same principle of the *theory of types* (cf. supra), calling *"sets" only some classes of objects having characteristic properties defined by an axiomatic way. In order to construct an axiomatic system, it is however always necessary to consider objects, denoted by the variables x,y,z,.. and called classes.* Then, we can *define between them the* **binary relation** $x \in y$. *The classes that are elements of at least a class will be called then called "**sets**".* (In order to simplify the notations, in the following section, we will write "*Set* x" that means "x is a set")

Def. 21. *(Set x). Set* $x :\Leftrightarrow \exists y, x \in y$.

If two sets are elements of the same class and have the same elements, these two sets are said *equal.*

Def. 22. *(Equal sets).* $x = y \Leftrightarrow \forall z(x \in z \Leftrightarrow y \in z) \wedge \forall z(z \in x \Leftrightarrow z \in y)$.

5.4. Axioms of set theory. Here is an introduction to set theory axioms; (these will be discussed and detailed in the heading "*Zermelo-Fraenkel Set Theory (ZFC)*"). The axioms below (with f *a function* and $\mathfrak{P}(x)$ the *set of the parts of a set* x) are imposed to the sets previously defined (above heading) in the frame of axiomatic set theory:

(1).**Axiom of Existence**:
$\exists x, Set\ x$

(2).**Axiom of Extensionality**:
$\forall z(z \in x \Leftrightarrow z \in y) \Rightarrow x = y$

(3).**Axiom of Comprehension**:
$\forall x(A(x) \Rightarrow Set\ x) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow A(x))$

(4) **Axiom of the Empty set**:
$Set\ \varnothing$

(5) **Axiom of Singletons**:
$Set\ x \Rightarrow Set\ \{x\}$

(6) **Axiom of Union** n° 1:
$Set\ x \wedge Set\ y \Rightarrow Set\ (x \cup y)$

(7) **Axiom of Union** n° 2:
$Set\ x \Rightarrow Set \bigcup_{y \in x} y$

(8) **Axiom of Infinity**:
$\exists x(Set\ x \wedge \varnothing \in x \wedge (y \in x \Rightarrow y \cup \{y\} \in x))$

(9) **Functional Axiom**:
$Set\ x \wedge f : x \to y \Rightarrow Set\ y$

(10) **Axiom of the set of the parts of a set** (that is, we can associate with any set x the set $\mathfrak{P}(x)$ of its parts): $Set\ x \Rightarrow Set\ \mathfrak{P}(x)$

(11) **Axiom of Choice***:* "Whatever the class y of the empty sets x, there exists a function f such that $f(x) \in x$ for all $x \in y$." The function f chooses in each set an element of this set (Fig.).

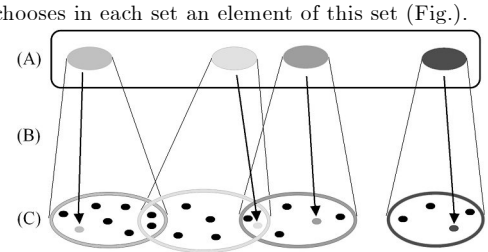


Fig. *Axiom of Choice.* (A): Class y of nonempty sets. (B): The map f associates with any set of class y one of its own elements $f(x) \in x$. (C): Diagram for the sets of y and their images (grayscale).

Comments on axioms: If we go back to the first four axioms, we can see that with this partial system consisting of the axioms (1) to (4), the Russell syntactic antinomy can be slightly modified. Indeed, after the transformation, the initial "*contradiction*" becomes the following statement: "*it exists a class which is not a set*". The steps of this transformation can be written:
In the axiom (3), that is $\forall x(A(x) \Rightarrow Set\ x) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow A(x))$, if $A(x)$ is replaced by $\neg x \in x$, we get first $\forall x(\neg x \in x \Rightarrow Set\ x) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow \neg x \in x)$, then if we select $x = y$ in the second member to study y, it follows: $\forall x(\neg x \in x \Rightarrow Set\ x) \Rightarrow (y \in y \Leftrightarrow \neg y \in y)$. Since the second member is not valid, we can deduce that the first is not valid either. Hence $\neg \forall x(\neg x \in x \Rightarrow Set\ x)$, that is, $\exists x(\neg x \in x \wedge \neg Set\ x)$.
The axiom (8) justifies the existence of infinite sets, especially the set of natural numbers $\mathbb{N}$. In the construction of this axiom, the set x contains $\varnothing$ and the elements $\{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, ...$ The *set is infinite.* Note that this axiom (8) (Axiom of Infinity) can also be reformulated as follows: "$\exists x(\varnothing \in x \wedge \forall y \in x(y' \in x))$, *where* $\exists$ *denotes exists,* $\varnothing$ *is the empty set,* $\wedge$ *is logical AND,* $\forall$ *means for all, and* $\in$ *denotes "is an element of".*" (Following von Neumann, $0=\varnothing$, $1=0'=\{0\}$, $2=1'=\{0,1\}$, $3=2'=\{0,1,2\}$,...).
We can now define *pairs of classes*, then, construct *relations* and *functions* (def. infra) between classes. If the domain (of definition) of such a function is a *set*, we need that the "*image*" is also a *set* (the "*image*" can be assimilated to the "*range*") .
After the axiom (9) ($Set\ x \wedge f : x \to y \Rightarrow Set\ y$), finally we can associate with any set x, the set $\mathfrak{P}(x)$ of its parts: Axiom (10), $Set\ x \Rightarrow Set\ \mathfrak{P}(x)$ (Axiom of the set of the parts of a set).
The axiom (11) *certifies only the existence of the function* f, and doesn't provide information on the way to construct this function. If we assume *consistency* about the axiomatic theory of sets, it is possible to *proof that the axiom of choice* (11) *is independent of the others axioms.* It means that we can find cases where the axioms (1) to (10) are verified and the axiom (11) is not verified. Thus, this observation leads to think that we can develop two type of axiomatic set theories, the first one is an *axiomatic set theory without the axiom of choice*, and the *second one theory includes this axiom of choice* (11). Both are possible even if usually the theories include this axiom of choice. The intuitionism doesn't accept this axiom of choice (11) (see Zorn's lemma) due to the fact that this axiom certifies only the existence of the function f and doesn't give informations about how to construct it. This fundamental axiom in set theory is sometimes called Zermelo's axiom of choice, because it was formulated by Zermelo in 1904. This axiom of choice is related to the first of Hilbert's problems.

Function: A function is a relation that uniquely associates members of one set with members of another set. This means that a function from E to F is an object f such that every $\alpha \in E$ is uniquely associated with an object $f(\alpha)$. Thus, a function is a *many-to-one*, or sometimes *one-to-one*[2], *relation.* The set E of values at which a function is defined is called its "*domain*", while the set of values that the function can produce is called its "*range*". The set F within which the values of a function lie is called *"codomain*", as opposed to the range, which is the set of values that the function actually takes. The term "*map*" is synonymous of *function (*but the term "function" tends to be used when the domain E is the set $\mathbb{R}$ of reals, or some subsets of $\mathbb{R}$, and the codomain F is $\mathbb{R}$, see real functions). The notation $f : E \to F$, read as "f from E to F" is used. If $\alpha \in E$, then $f(\alpha)$ is the "*image*" of α under f. The subset of F consisting of those elements that are images of elements of E under f, that is, the set $\{\beta | \beta = f(\alpha)$, for some α in $E\}$ is the range of f. If $f(\alpha)=\beta$,.*we say that* f *maps* α *to* β, written $f : \alpha \mapsto \beta$. If the graph of f is then taken to be $\beta = f(\alpha)$, it may be said that β is a function of α.

5.5. Von Neumann universe.
The context is to restrict the notion of set to that of *pure set.* A set is pure if all of its members are sets, all members of its members are sets, etc (e.g. the set $\{\{\}\}$ (equivalently $\{\varnothing\}$) containing only the empty set $\varnothing$ is a nonempty pure set).

Def. 23. *(Pure set). A set is a* ***pure set*** *(or* ***hereditary set****) if all elements of the set are temselves sets, as are all elements of the elements, and so on. In other words, a hereditary set (or pure set) is a set all of whose elements are hereditary sets.*

Today, it is usual to focus on von Neumann universe of pure sets, and a lot of systems of axiomatic set theory are designed to only axiomatize the pure sets. In the von Neumann universe, sets have a cumulative hierarchy, depending on the nesting depth level of members (i.e. members, members of members, etc.). In this hierarchy, an ordinal number

[2] *One-to-one correspondence*: A pairing between two classes of elements whereby each element of either class is made to correspond to one and only one element of the other class.

α (called its **rank**) is assigned (by transfinite recursion) to each set. The rank of a pure set S is defined to be the least upper bound of all successors of ranks of members of S (e.g. the rank of the empty set is 0; the rank of the set $\{\{\}\}$ containing only the empty set is 1; and every ordinal has a rank equal to itself). For each ordinal α, the set V_α is defined to consist of all pure sets with rank less than α. The rank of a well-founded set is defined inductively as the smallest ordinal number greater than the ranks of all members of the set.
Von Neumann universe in its entirety is denoted "V", also called **von Neumann hierarchy of sets**, and is the class of hereditary well-founded sets. This collection, formalized by Zermelo-Fraenkel set theory (cf. heading "*Zermelo-Fraenkel Set Theory (ZFC)*"), is often used to interpret or discuss the axioms of Zermelo-Fraenkel set theory (abbreviated "ZFC").The sets in V are divided into a transfinite hierarchy, called the cumulative hierarchy, based on their rank.

Def. 24. *(Cumulative hierarchy of sets). The cumulative hierarchy is a collection of sets V_α indexed by the class of ordinal numbers, specifically, V_α is the set of all sets having ranks less than α. There is thus one set V_α for each ordinal number α. V_α can be defined by transfinite recursion as follows:*
▪ *Let V_0 be the empty set $\varnothing$ or $\{\}$: $V_0 := \{\}$.*
▪ *For any ordinal number β, let $V_{\beta+1}$ be the power set $\mathcal{P}(V_\beta)$ of V_β: $V_{\beta+1} := \mathcal{P}(V_\beta)$.*
▪ *For any limit ordinal λ, V_λ is the union of all the V-stages such that $V_\lambda := \bigcup_{\beta<\lambda} V_\beta$.*

We have so a single formula $\varphi(\alpha, x)$ in the language of ZFC defining "*the* set x is in V_α". Class V is def. to be the union of all the V-stages: $V := \bigcup_\alpha V_\alpha$.
If we consider an arbitrary set E, the rank of E is the smallest α such that $E \subseteq V_\alpha$.
An equivalent definition is: $V_\alpha := \bigcup_{\beta<\alpha} \mathcal{P}(V_\beta)$ for each ordinal α, where $\mathcal{P}(A)$ is the powerset of A.

▪ **Set theory and von Neumann universe.** Suppose that ω denotes the set of natural numbers, V_ω is then the set of hereditarily finite sets (which is a model of set theory without the axiom of infinity). $V_{\omega+\omega}$ is the universe of *ordinary mathematics* and is a model of Zermelo set theory. If κ is an *inaccessible cardinal* (def. below), V_κ is then a model of Zermelo-Fraenkel set theory (ZFC), and $V_{\kappa+1}$ is a model of Morse-Kelley set theory (MK) (cf. heading "*Axiomatic set theory*"). *V is not "the set of all sets"* since: (1) It is not a set; although each individual stage V_α is a set, their union V is a proper class; (2) the sets in V are only the well-founded sets. The axiom of foundation (or regularity) requires that any set is well-founded and thus in V, and so in ZFC any set is in V. However other axiom systems can omit the axiom of foundation or replace it by a strong negation. These non-well-founded set theories are not frequently examined but may be still considered.

Def. 25. *(Inaccessible cardinal). First recall that a cardinal is said to be **limit** if it is of the form $\aleph_\alpha$, where α is a **limit ordinal** (otherwise, we say that $\aleph_{\alpha+1}$ is the **successor** of $\aleph_\alpha$); on the other hand, we say that ordinal α is **cofinal** with a lower ordinal β if there exists a strictly increasing map f from β to α such that α is the limit of f in the following sense: $\forall\gamma \in \alpha, \exists\delta \in \beta, \gamma \leq f(\delta)$; we'll say then that a cardinal is **regular** if it is cofinal with no strictly smaller cardinal, and that it is **singular** otherwise. All the successor cardinals are regular; $\aleph_0$ is also regular (but for instance $\aleph_\omega$ is singular, since it is the limit of the denumerable sequence of the $\aleph_n$). We say then finally that a non-denumerable cardinal $\aleph_\alpha$ is **weakly inaccessible** if it is limit and regular; and that it is **strongly inaccessible** (or simply **inaccessible**) if moreover it verifies the condition $\mathrm{card}(x) < \aleph_\alpha \Rightarrow 2^{\mathrm{card}(x)} < \aleph_\alpha$. If we admit the Generalized Continuum Hypothesis (cf. heading "Continuum hypothesis and set theory"), the two concepts coincide. A characteristic condition to be a weakly inaccessible ordinal is to be regular and limit of regular ordinals.*

5.6. Continuum hypothesis and set theory. Cantor stated that there is no infinite set with a cardinal number between that of the "small" infinite set of integers $\aleph_0$ and the "large" infinite set of real numbers $\mathfrak{c}$ (the "continuum"). The continuum hypothesis can be written $\aleph_1 = \mathfrak{c}$. Hilbert's problem 1a asks if the continuum hypothesis is true.
Gödel stated that no contradiction would appear if the continuum hypothesis were added to conventional *Zermelo-Fraenkel set theory.* But using a method called forcing, Cohen stated that no contradiction would appear if the *negation* of the continuum hypothesis were added to set theory. Gödel's and Cohen's assertions together stated that the validity of the continuum hypothesis depends on the version of set theory used, and is thus undecidable, assuming *Zermelo-Fraenkel axioms* together with the *axiom of choice.*
Conway-Guy proposed a generalized version of the continuum hypothesis (dating back to Hausdorff) that is also undecidable: we have to know if $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ for every α. Continuum Hypothesis (CH) results from Generalized Continuum Hypothesis (GCH), thus: $\mathrm{ZF} + \mathrm{GCH} \vdash \mathrm{CH}$; ($\vdash$: inference).
Woodin (2001) stated another axiom (in addition to Zermelo-Fraenkel axioms and axiom of choice) whose introduction would imply that Continuum Hypothesis is false. Prospects of this "axiom" are important for theoreticians concerning the conjecture that this Continuum Hypothesis could be false.

5.7. Axiomatic set theory. Axiomatic set theory is a system of set theory which differs from so-called naive set theory in that the sets which are allowed to be generated are strictly constrained by the axioms. The best known systems of axiomatic set theory are ZF (Zermelo-Fraenkel) and ZFC (Zermelo-Fraenkel with the Axiom of Choice). Axiomatic set theory was initially designed to rule out the paradoxes of set theory. Zermelo-Fraenkel set theory (ZFC) is described in the heading "*Zermelo-Fraenkel Set Theory (ZFC)*".

(I) In axiomatic set theory, most systems assume that all sets form a **cumulative hierarchy**. Such systems are of two types, those consisting of:
- *The sets alone:* Including the most usual Zermelo-Fraenkel set theory (ZFC) with the axiom of choice (AC). There are other constructions derived from ZFC but with (more or less substantial) changes: *a) Zermelo set theory* (replacing the axiom schema of replacement by that of separation); *b) General set theory* (small piece of Zermelo set theory sufficient for Peano axioms and finite sets); *c) Kripke-Platek set theory* (KP) (ruling out the axioms of infinity, powerset, and choice, and weakens the axiom schema of separation and that of replacement).
- *The sets and proper classes:* Including von Neumann-Bernays-Gödel set theory (NBG), whose strength is the same as ZFC (for sets alone); Morse-Kelley set theory (MK) ; Tarski-Grothendieck set theory (TG); last two are stronger than ZFC.

Von Neumann-Bernays-Gödel set theory (NBG) is a conservative extension of the canonical axiomatic set theory ZFC. A statement in the language of ZFC is provable in NBG if and only if it is provable in ZFC. The structure of NBG includes proper classes, objects having members but that cannot be members of other entities. NBG's principle of class comprehension is predicative; quantified variables in the defining formula can range only over sets. Allowing impredicative comprehension turns NBG into Morse-Kelley set theory (MK). NBG, unlike ZFC and MK, can be finitely axiomatized. Indeed, Zermelo-Fraenkel set theory is not finitely axiomatized (e.g. the axiom of replacement is not truly a single axiom, but an infinite family of axioms, since it is associated with a stipulation that it is true for every set-theoretic formula $A(u, v)$). In fact, Montague stated that Zermelo-Fraenkel set theory is not finitely axiomatizable, namely, *there is no finite set of axioms which is logically equivalent to the infinite set of Zermelo-Fraenkel axioms.* By contrast, von Neumann-Bernays-Gödel set theory has only finitely many axioms, which was the main reason of its construction. This was performed by extending the language of Zermelo-Fraenkel set theory to be able to talk about *set classes.*

Morse-Kelley set theory (KM) or (MK) is a first order axiomatic set theory that is closely related to von Neumann-Bernays-Gödel set theory (NBG). Whereas von Neumann-Bernays-Gödel set theory restricts the bound variables in the schematic formula appearing in the axiom schema of Class Comprehension to range over *sets alone*, Morse-Kelley set theory allows these bound variables to range over *proper classes* as well as *sets.* Whereas von Neumann-Bernays-Gödel set theory is a *conservative extension* of Zermelo-Fraenkel set theory (ZFC, the canonical set theory) in the sense that a statement in the language of ZFC is provable in NBG if and only if it is provable in ZFC, Morse-Kelley set theory is a *proper extension* of ZFC. Unlike NBG, where the axiom schema of Class Comprehension can be replaced by finitely many of its instances, MK cannot be finitely axiomatized.

Tarski-Grothendieck set theory (TG) is an axiomatic set theory designed as part of Mizar system for formal verification of proofs; note that Mizar system consists of a formal language for writing mathematical definitions, a proof assistant capable to automatically check proofs written in this language, and a library of formalized mathematics that can be used in the proof of new theorems. Tarski-Grothendieck set theory (TG) is a *non-conservative extension* of Zermelo-Fraenkel set theory (ZFC) and differs from other axiomatic set theories by the

adjunction of Tarski's axiom which says that for each set there is a *Grothendieck universe* (infra). TG consists of the following axioms (conventional since also part of ZFC):
-*Set axiom*: Quantified variables range over sets alone; everything is a set (as ZFC);
-*Axiom of extensionality*: Two sets are identical if they have the same members;
-*Axiom of regularity*: No set is a member of itself, and circular chains of membership are impossible;
-*Axiom schema of replacement*: Given a set A, the domain of the function F, then the range of F (values of $F(x)$ for all members x of A) is also a set.
-*Tarski's axiom: For every set x, there exists a set y* whose members include:
1. x itself,
2. *every subset of every member of y*,
3. *the power set of every member of y*,
4. *every subset of y whose cardinality is less than the cardinality of y*
Tarski's axiom also implies the *axioms of infinity*, the *axioms of choice*, and the *axiom of the power set*. It also implies the *existence of inaccessible cardinals* (which makes the structure of TG richer than that of conventional set theories such as ZFC).

Def. 26. *(Grothendieck universe). A Grothendieck universe is a set (not a proper class) having the properties of the universe $\mathbb{U}$ of sets in the sense of the Zermelo-Fraenkel axioms with the properties:*
(1) If $u \in \mathbb{U}$ and $t \in u$ then $t \in \mathbb{U}$ ($\mathbb{U}$ is a transitive set).
(2) If $u, v \in \mathbb{U}$ then $\{u, v\} \in \mathbb{U}$.
(3) If $u \in \mathbb{U}$ then the power set $\mathcal{P}(u) \in \mathbb{U}$.
(4) If $I \in \mathbb{U}$, and $\{u_\alpha : \alpha \in I\}$ is a family of elements of $\mathbb{U}$, then $\bigcup_{\alpha \in I} u_\alpha \in \mathbb{U}$.
*The elements of a Grothendieck universe are sometimes called **small sets**.*

Here are notions related to the above definition:

Def. 27. *(Proper class). A proper class is a class which is not a set.*

Def. 28. *(Small class). A class which is not a proper class is a small class. A **set** is **small class**.*

Def. 29. *(Pure set). A set is a **pure set** (or **hereditary set**) if all elements of the set are temselves sets, as are all elements of the elements, and so on. In other words, a hereditary set (or pure set) is a set all of whose elements are hereditary sets.*

Def. 30. *(Urelements). Objects that can be members of sets but that are not themselves sets and do not have any members.*

(See also the related notions of "inaccessible cardinal", and "Hereditarily finite set").
All the above systems can be modified to admit *urelements.*

(II) Systems of **New Foundations** NFU (admitting urelements) and NF (not admitting urelements) *are **not** based on a* **cumulative hierarchy**. NF and NFU include a "set of everything," relative to which any set has a complement. Here, urelements are important since NF (but not NFU) provides sets where the axiom of choice does not hold. NF is is an axiomatic set theory was developed as a simplification of the *theory of types* of *Principia Mathematica* (for theory of types see heading "*Antinomies, theory of types*").

(III) Systems of the **Constructive Set Theory** (e.g. Aczel's constructive Zermelo-Fraenkel (CZF), Intuitionistic Zermelo-Fraenkel (IZF)) formulate their set axioms in intuitionistic logic instead of first-order logic; nevertheless other systems admit standard first-order logic but include a nonstandard membership relation. They include *fuzzy set theory* (infra) and *rough set theory* (infra), in which the value of an *atomic formula* (infra) stating the membership relation is not simply true or false.
Fuzzy set: Extension of the concept of a set, in which the characteristic function which determines membership of an object in the set is *not limited to* be the two values 1 (for membership in the set) and 0 (for nonmembership), but can take on any value between 0 and 1 as well; considering thus there are *degrees of membership* for elements. In fuzzy set theory, classical bivalent sets are usually called *crisp sets.*
Crisp set: A conventional set, wherein the degree of membership of any object in the set is 0 or 1.
Rough set: Formal approximation of a conventional set in terms of a pair of sets which give the lower and the upper approximation of the original set.
Atomic formula: A formula with no deeper propositional structure, i.e. a formula containing no logical connectives or equivalently a formula having no strict subformulas.

(IV) Internal Set Theory (IST) was introduced (Nelson, 1977) as a unified axiomatic foundation of "non-standard" mathematics. IST theory describes the universe of all sets in such a way that, in addition to "standard" sets (which identify with regular objects of "standard" mathematics and obey the axioms of Zermelo-Fraenkel theory ZFC), there are objects such as infinitely large and infinitely small numbers, etc. incompatible with the present-day "standard" system of foundations of mathematics. In fact, IST is an enrichment of ZFC where all axioms of ZFC are satisfied for all classical predicates, while the new unary[3] predicate "standard" satisfies three additional axioms I,S,T (Idealization, Standardization, Transfer). IST approach modifies the axiomatic foundations through syntactic enrichment. The axioms introduce a new term, "standard", which can be used to make discriminations not possible under the conventional axioms for sets.

6. Zermelo-Fraenkel Set Theory (ZFC)

Zermelo-Fraenkel set theory with the axiom of choice (abbreviated "ZFC") is emblematic of set theory and is regarded as the standard form of axiomatic set theory and as such is the most common foundation of mathematics. It is one of several axiomatic systems that were introduced in the early twentieth century to elaborate a theory of sets without the paradoxes of naive set theory such as Russell's paradox. Note that ZFC does not allow unrestricted comprehension (see axiom schema of comprehension (unrestricted)).

6.1. Zermelo-Fraenkel axioms. The Zermelo-Fraenkel axioms are the basis for Zermelo-Fraenkel set theory. Zermelo-Fraenkel set theory is a formal system expressed in first-order predicate logic. Given the symbols, $\exists$ for "there exists", $\forall$ for "for all", $\in$ for "is an element of," $\varnothing$ for "the empty set", $\Rightarrow$ for "implies", $\wedge$ for "AND", $\vee$ for "OR", $\equiv$ for "is equivalent to".

1.Axiom of Extensionality: If X and Y have the same elements, then $X = Y$.
$$\forall u(u \in X \equiv u \in Y) \Rightarrow X = Y.$$
2.Axiom of the Unordered Pair: For any a and b there exists a set $\{a, b\}$ that contains exactly a and b. (also called **Axiom of Pairing**)
$$\forall a \forall b \exists c \forall x(x \in c \equiv (x = a \vee x = b)).$$
3.Axiom of Subsets (also called **Axiom of Separation** or **Axiom of Comprehension**)**:** If φ is a property (with parameter p), then for any X and p there exists a set $Y = \{u \in X : \varphi(u, p)\}$ that contains all those $u \in X$ that have the property φ.
$$\forall X \forall p \exists Y \forall u(u \in Y \equiv (u \in X \wedge \varphi(u, p))).$$
4.Axiom of Union (Also called **Axiom of the Sum Set**)**:** For any X there exists a set $Y = \bigcup X$, the union of all elements of X.
$$\forall X \exists Y \forall u(u \in Y \equiv \exists z(z \in X \wedge u \in z)).$$
5.Axiom of the Power Set: For any X there exists a set $Y = P(X)$, the set of all subsets of X.
$$\forall X \exists Y \forall u(u \in Y \equiv u \subseteq X).$$
6.Axiom of Infinity: There exists an infinite set.
$$\exists S[\varnothing \in S \wedge (\forall x \in S)[x \bigcup \{x\} \in S]].$$
7.Axiom of Replacement: If F is a function, then for any X there exists a set $Y = F[X] = \{F(x) : x \in X\}$.
$$\forall x \forall y \forall z[\varphi(x, y, p) \wedge \varphi(x, z, p) \Rightarrow y = z]$$
$$\Rightarrow \forall X \exists Y \forall y[y \in Y \equiv (\exists x \in X)\varphi(x, y, p)].$$
8.Axiom of Foundation (also called **Axiom of Regularity**)**:** Every nonempty set has an in ϵ-minimal element. $\exists S[S \neq \varnothing \Rightarrow (\exists x \in S)S \bigcap x = \varnothing]$.
9.Axiom of Choice (AC): Every family of nonempty sets has a choice function[4].
$$\forall x \in a \; \exists A(x, y) \Rightarrow \exists y \forall x \in a \; A(x, y(x)).$$
The set of axioms 1 to 9 *with the axiom of choice* (AC) is usually denoted "ZFC."
The system of axioms 1 to 8 is called *Zermelo-Fraenkel set theory*, denoted "ZF".
The system of axioms 1 to 8 minus the axiom of replacement (i.e. axioms 1 to 6 plus 8) is called *Zermelo set theory*, denoted "Z".
But it seems there are ambiguities about axioms forming "*Zermelo set theory*". Indeed, Mendelson does not include the axioms of choice or

[3] *Unary operation*: An operation in which only a single operand is required to produce a unique result. Examples are negation, complementation, square root, transpose, factorial, inverse, conjugate, etc.

[4] *Choice function* (*selector*): A function f that is defined on some collection $\mathcal{C}$ of nonempty sets and assigns to each set E in that collection some element $f(E)$ of E. Thus, f is a choice function for $\mathcal{C}$ iff it belongs to the direct product (or cartesian product) of $\mathcal{C}$.

foundation in Zermelo set theory, but include the axiom of replacement. Enderton includes the axioms of choice and foundation, but does not include the axiom of replacement. Itô introduces an Axiom of the empty set, which can be obtained from 6 and 3 by setting $\exists X(X{=}X)$ and $\varnothing{=}\{u : u \neq u\}$.

6.2. Comments on ZFC axioms.

There are many equivalent formulations of the ZFC axioms. Here is another equivalent way to formulate them, then, to comment them.

1.Axiom of Extensionality. Two sets are equal (are the same set) if they have the same elements. This axiom can also be written:

$$\forall x \forall y[\forall z(z \in x \Leftrightarrow z \in y) \Rightarrow x = y].$$

The inverse of this axiom results from the substitution property of equality. If the underlying logic does not include equality "=", $x = y$ can be defined as an abbreviation for the expression $\forall z[z \in x \Leftrightarrow z \in y] \wedge \forall w[x \in w \Leftrightarrow y \in w]$. It follows that the axiom of extensionality can be rewritten:

$$\forall x \forall y[\forall z(z \in x \Leftrightarrow z \in y) \Rightarrow \forall w(x \in w \Leftrightarrow y \in w],$$

meaning that if x and y have the same elements, then they belong to the same sets.

2.Axiom of Pairing (also called **Axiom of the Unordered Pair**). If x and y are sets, then there exists a set which contains x and y as elements.

$$\forall x \forall y \exists z(x \in z \wedge y \in z).$$

The axiom schema of specification must be used to reduce this to a set with exactly these two elements. This axiom is part of Z, but is redundant in ZF since it results from the axiom schema of replacement, if we are given a set with at least two elements. The existence of a set with at least two elements is assured by either the axiom of infinity, or by the axiom schema of specification and the axiom of the power set applied twice to any set.

3.Axiom Schema of Specification (also called **Axiom Schema of Separation** or **of Restricted Comprehension**). If z is a set, and ϕ is any property which may characterize the elements x of z, then there is a subset y of z containing those x in z which satisfy the property. The restriction to z is needed to avoid Russell's paradox and its variants. Formally, given ϕ any formula in the language of ZFC with free variables among $x, z, w_1,...,w_n$. Thus y is not free in ϕ. Then:

$$\forall z \forall w_1 \forall w_2 ... \forall w_n \exists y \forall x[x \in y \Leftrightarrow (x \in z \wedge \phi)].$$

In certain other axiomatizations of ZF, this axiom is redundant in that it follows from the axiom schema of replacement.

The set constructed by the axiom of specification is often denoted using *set builder notation*. Given a set z and a formula $\phi(x)$ with one free variable x, the set of all x in z that satisfy ϕ is denoted

$$\{x \in z : \phi(x)\}.$$

The axiom of specification can be used to prove the existence of the empty set, denoted $\varnothing$, once the existence of at least one set is established (see above). A common way to do this is to use an instance of specification for a property which all sets do not have. For example, if w is a set which already exists, the empty set can be constructed as $\varnothing = \{u \in w | (u \in u) \wedge \neg(u \in u)\}$.

If the background logic includes equality, it is also possible to define the empty set as $\varnothing = \{u \in w | \neg(u = u)\}$. Thus the axiom of the empty set is implied by the nine axioms presented here. The axiom of extensionality implies the empty set is unique (does not depend on w). It is common to make a definitional extension that adds the symbol $\varnothing$ to the language of ZFC.

4.Axiom of Union (also called **Axiom of the Sum of Set**). For any set $\mathcal{F}$ there exists a set A containing every set that is a member of some member of $\mathcal{F}$.

$$\forall \mathcal{F} \exists A \forall Y \forall x[(x \in Y \wedge Y \in \mathcal{F}) \Rightarrow X \in A].$$

5.Axiom of the Power Set. By definition a set z is a subset of a set x if and only if every element of z is also an element of x:

$$(z \subseteq x) \Leftrightarrow (\forall q(q \in z \Rightarrow q \in x)).$$

This asserts that for any set x, there is a set $Q(x)$ that contains every subset of x: $\forall x \exists Q(x) \forall z[z \subseteq x \Rightarrow z \in Q(x)]$. The axiom schema of specification is then used to define the power set $P(x)$ as the subset of $Q(x)$ containing the subsets of x exactly: $P(x) = \{z \in Q(x) : z \subseteq x\}$.

6.Axiom of Infinity. Let $S(w)$ abbreviate $w \bigcup \{w\}$, where w is some set (We can see that $\{w\}$ is a valid set by applying the axiom of pairing with $x = y = w$ so that the set z is $\{w\}$. Then there is a set X such that the empty set $\varnothing$ is a member of X and, whenever a set y is a member of X, then $S(y)$ is also a member of X.

$$\exists X[\varnothing \in X \wedge \forall y(y \in X \Rightarrow S(y) \in X)].$$

Meaning that there is a set X with infinitely many members. The minimal set X satisfying the axiom of infinity is the von Neumann ordinal ω, which can also be seen as the set of natural numbers $\mathbb{N}$.

7.Axiom Schema of Replacement. Let ϕ be any formula in the language of ZFC whose free variables are among $x, y, A, w_1,...,w_n$, so that in particular B is not free in ϕ. Then: $\forall A \forall w_1 \forall w_2 ... \forall w_n[\forall x(x \in A \Rightarrow \exists! y\, \phi) \Rightarrow \exists B \forall x(x \in A \Rightarrow \exists y(y \in B \wedge \phi))]$. This axiom states that if the domain of a definable function f (represented here by the relation ϕ) is a set (denoted here by A), and $f(x)$ is a set for every x in that domain, then the range of f is a subclass of a set (where the set is denoted here by B). The form stated here, in which B may be larger than strictly necessary, is sometimes called the axiom schema of collection.

8.Axiom of Foundation (also called **Axiom of Regularity**). If we rewrite this axioms as follows: Every nonempty set x contains a member y such that x and y are disjoint sets

$$\forall x[\exists a(a \in x) \Rightarrow \exists y(y \in x \wedge \neg \exists z(z \in y \wedge z \in x))].$$

Axioms 1 to 8 define ZF. Some ZF axiomatizations include an axiom stating that the empty set exists. Axioms of pairing, union, replacement, and power set are often stated so that the members of the set x whose existence is being asserted are just those sets which the axiom asserts x must contain. The axiom below is added to turn ZF into ZFC:

9.Well-ordering theorem (also known as **Zermelo's theorem** and is equivalent to the **Axiom of Choice (AC)**). For any set X, there is a binary relation R which well-orders X. This means R is a linear order on X such that any nonempty subset of X has a member which is minimal under R.

$$\forall X \exists R(R \text{ well-orders } X).$$

From axioms 1 to 8, there are several equivalent formulations of axiom 9, the best known is obviously the axiom of choice, written as follows. Let X be a set whose members are all non-empty. Then there exists a function f from X to the union of the members of X, called a "*choice function*", such that for all $Y \in X$ one has $f(Y) \in Y$. Since the existence of a choice function when X is a finite set is easily proved from axioms 1 to 8, the *axiom of choice* only matters for certain infinite sets. Axiom of choice is characterized as nonconstructive since it asserts the existence of a choice set but says nothing about how the choice set is to be constructed.

Well-ordering theorem states that any set can be well-ordered. A set X is well-ordered by a strict total order if every non-empty subset of X has a least element under the ordering. This is also known as Zermelo's theorem and is equivalent to the Axiom of Choice. Zermelo introduced the Axiom of Choice as an "unobjectionable logical principle" to prove the well-ordering theorem. This is important because it makes any set susceptible to the powerful technique of transfinite induction. The well-ordering theorem has consequences that may seem paradoxical, such as the Banach-Tarski paradox.

7. Banach-Tarski paradox and ZF

This section offers the opportunity to anticipate some notions addressed later in the book, the reader may ignore them and come back later.

7.1. Banach-Tarski paradox.

Banach-Tarski paradox is a theorem stating that, for any two bounded sets, with interior points in a Euclidean space of dimension at least three one of the sets can be disassembled into a finite number of pieces and reassembled to form the other set by moving the pieces with rigid motions (translations and rotations). The reassembly process involves only moving the pieces around and rotating them, without changing their shape. But the pieces themselves are not *solids* in the usual sense, but infinite scatterings of points. Here is the theorem of Banach-Tarski paradox (proof can be ignored since using notions addressed later):

Th. 5. *(Banach-Tarski paradox). The unit ball $\mathbb{D}^3 \subset \mathbb{R}^3$ is equidecomposable to the union of two disjoint unit balls.*

Proof. Consider $\mathbb{D}^3$ is centered at the origin, and D^3 is some other unit ball in $\mathbb{R}^3$ such that $\mathbb{D}^3 \cap D^3 = \varnothing$. (1) Let $\mathbb{S}^2 = \partial\mathbb{D}^3$ (with $\mathbb{S}^2$: sphere; $\partial\mathbb{D}^3$: boundary of $\mathbb{D}^3$). By the *Hausdorff paradox*[5] (see infra), there exists a decomposition of $\mathbb{S}^2$ into four sets A, B, C, D such that A, B, C, and $B \cup C$ are congruent, and D is countable. For $r \in \mathbb{R}^*_+$, consider a function $r^* : \mathbb{R}^3 \to \mathbb{R}^3$ as $r^*(\mathbf{x}) = r\mathbf{x}$ and the sets: $W = \bigcup_{0<r\leq 1} r^*(A)$, $X = \bigcup_{0<r\leq 1} r^*(B)$, $Y = \bigcup_{0<r\leq 1} r^*(C)$, $Z = \bigcup_{0<r\leq 1} r^*(D)$. (2) Let $T = W \cup Z \cup \{\mathbf{0}\}$. W and $X \cup Y$ are congruent by the congruency of A with $B \cup C$, so W and $X \cap Y$ are

[5] **Th.**(*Hausdorff paradox*). *There is a disjoint decomposition of the sphere $\mathbb{S}^2$ into four sets A, B, C, D such that $A, B, C, B \cup C$ are all congruent and D is countable.*

equidecomposable[6]. Since X and Y are congruent, and W and X are congruent, $X \cup Y$ and $W \cup X$ are equidecomposable. W and $X \cup Y$ are congruent, and X and W are congruent too, so $W \cup X$ and $W \cup X \cup Y$ are equidecomposable. It follows: W and $W \cup X \cup Y$ are equidecomposable since the *equidecomposability is an equivalence relation*[7]. T and $\mathbb{D}^3$ are equidecomposable, since unions of equidecomposable sets are equidecomposable. Analogously, X, Y, and $W \cup X \cup Y$ are equidecomposable. Since D is only countable, but $\mathbb{SO}(3)$ (i.e. rotation group in 3-dimensional space) is not, we have: $\exists \varphi \in \mathbb{SO}(3) : \varphi(D) \subset A \cup B \cup C$ so that $I = \varphi(D) \subset W \cup X \cup Y$. Since X and $W \cup X \cup Y$ are equidecomposable, using a theorem on equidecomposability and subsets, $\exists H \subseteq X$ such that H and I are equidecomposable. Finally, consider a point $p \in X - H$ and define $S = Y \cup H \cup \{p\}$. Since: Y and $W \cup X \cup Y$, H and Z, $\{0\}$ and $\{p\}$ are all equidecomposable in pairs, S and $\mathbb{D}^3$ are equidecomposable by the *equidecomposability of unions*[8]. Since $\mathbb{D}^3$ and D^3 are congruent, D^3 and S are equidecomposable, since equidecomposability is an equivalence relation. By the *equidecomposability of unions*, $T \cup S$ and $\mathbb{D}^3 \cup D^3$ are equidecomposable. Thus $T \cup S \subseteq \mathbb{D}^3 \subset \mathbb{D}^3 \cup D^3$ are equidecomposable and so, by the chain property of equidecomposability, $\mathbb{D}^3$ and $\mathbb{D}^3 \cup D^3$ are equidecomposable. □

This theorem depends on the axiom of choice (by way of Hausdorff Paradox). A proof can be provided by using the axiom of choice, which allows the *construction of nonmeasurable sets* (i.e. *collections of points that do not have a volume* in the ordinary sense and that for their construction would require performing an uncountably infinite number of choices).
The set under consideration is not necessarily a ball. Every two set with non empty interior are equidecomposable in $\mathbb{R}^3$. The ambient space can also be chosen larger. The theorem is true in all $\mathbb{R}^n$ with $n \geqslant 3$ but it is not true in $\mathbb{R}^2$ nor in $\mathbb{R}$.
The theorem harbors a *paradox* and contradicts basic geometric intuition. Indeed, doubling the ball by splitting it into parts and moving them around by translations and rotations, without any bending, stretching, or adding new points, seems impossible since all these operations preserve the volume, whereas the volume is ultimately doubled. This theorem can be generalized: Any two bodies in $\mathbb{R}^3$ that do not extend to infinity and each containing a ball of arbitrary size can be dissected into each other, i.e. they are *equidecomposable*. More formally, we say that for a set $A \subset \mathbb{R}^n$ is *decomposable* into N pieces $A_1, \ldots, A_N$ if there exist some isometries[9] $\sigma_1, \ldots, \sigma_N$ of $\mathbb{R}^n$ such that $A = \sigma_1(A_1) \cup \ldots \cup \sigma_N(A_N)$ while $\sigma_1(A_1), \ldots, \sigma_N(A_N)$ are all disjoint. We then say that two sets $A, B \subset \mathbb{R}^n$ are *equidecomposable* if both A and B can be decomposed in the same pieces $A_1, \ldots, A_N$.
Here is a *strong form of Banach-Tarski paradox*:

Th. 6. *(Banach-Tarski paradox - Strong form). Given any two bounded subsets A and B of a Euclidean space in at least three dimensions, both of which have a nonempty interior, there are partitions of A and B into a finite number of disjoint subsets, $A = A_1 \cup ... \cup A_k$, $B = B_1 \cup ... \cup B_k$, such that for each i between 1 and k, the sets A_i and B_i are congruent.*

This version of the paradox is false in dimensions 1 and 2, but it has been shown that an analogous statement remains true if countably many subsets are allowed. The difference between the dimensions 1 and 2 on the one hand, and three and higher, on the other hand, is due to the richer structure of the group G_n of the Euclidean motions in the higher dimensions, which is solvable for $n = 1, 2$ and contains a free group with two generators for $n \geqslant 3$. John von Neumann studied the properties of the group of equivalences that make a paradoxical decomposition possible and introduced the notion of *amenable groups* (amenable group is a locally compact topological group carrying a kind of averaging operation on bounded functions that is invariant under translation by group elements.). He also found a form of the paradox in the plane which uses area-preserving affine transformations in place of the usual congruences.

7.2. Countable, measure. Here, we need to outline "countable" and "measure" notions (treated elsewhere throughout parts).
1) Countable, denumerable, countable set, countably or uncountable infinite set.
Countable: Either finite or *denumerable*. Also known as enumerable.
Countable: A set X is *countable* if there is a *one-to-one correspondence* between X and a subset of the set of natural numbers. X is countable iff it is finite or countably infinite. Thus, a countable set is either finite or *denumerable* (see below). Some authors use "countable" to mean denumerable.
Countably infinite = Denumerable.
Denumerable: A set X is *denumerable* if there is a *one-to-one correspondence* between X and the set of natural numbers. It can be shown that the set of rational numbers is denumerable but that the set of real numbers is not. Some authors use "denumerable" to mean *countable.*
Enumerable: ref. to countable.
Countably infinite set: ref. to *denumerable set.*
Denumerable set: A set which may be put in one-to-one correspondence with the positive integers. Also known as *countably infinite set.*
Countable set: A set which is either finite or denumerable. But some authors use the def. "equipollent to the finite ordinals," commonly used to define a denumerable set, to define a countable set.
Denumerable set: A set is denumerable iff it is equipollent to the finite ordinal numbers. But authors call "countable" this property. Aleph-0 is most commonly called "denumerable" to "countably infinite".
Countably infinite set: Any set which can be put in a one-to-one correspondence with the natural numbers (or integers) so that a prescription can be given for identifying its members one at a time is called a countably infinite (or denumerably infinite) set. Once one countable set S is given, any other set which can be put into a one-to-one correspondence with S is also countable. Countably infinite sets have cardinal number aleph-0. Examples of countable sets include the integers, algebraic numbers, and rational numbers. Cantor showed that the number of real numbers is rigorously larger than a countably infinite set, and the postulate that this number, the so-called "continuum," is equal to aleph-1 is called the continuum hypothesis. Examples of nondenumerable sets include the real, complex, irrational, and transcendental numbers.
Uncountably infinite set: An infinite set, such as the real numbers, which is not countably infinite.

The terms *denumerable* and *enumerable* are encountered usually meaning countably infinite. Some authors use countable to mean countably infinite, but this usage seems inappropriate, as the very concept of the term countable implies that a set can be counted, which a finite set can be.

Def. 31. *(Countable set). A set X is said to be countable if there exists an injection $f : X \to \mathbb{N}$.*

Def. 32. *(Countable set)'. Let S be a set. Then S is countable iff it is finite or countably infinite.*

Def. 33. *(Countably infinite set). Let S be a set. Then S is countably infinite if and only if there is a bijection $f : S \to \mathbb{N}$, where $\mathbb{N}$ is the set of natural numbers. That is, it is an infinite set of the form: $\{s_0, s_1, \ldots, s_n, \ldots\}$, where n runs over all the natural numbers.*

2) Measure, measure set, measure space, σ algebra, pushforward measure, measurable function, invariant measure.
Measure: A nonnegative real-valued function defined on a sigma-algebra of subsets of a set S whose value is zero on the empty set, and whose value on a countable union of disjoint sets is the sum of its values on each set.
Measurable set: A member of the sigma-algebra of subsets of a measurable space.
Measurable space: A set X together with a sigma-algebra of subsets of this set. If M denotes this sigma-algebra of subsets of this set X, i.e. the nonempty collection of subsets of X, then (X, M) denotes the measurable space.
Sigma-algebra (σ-*algebra*): A σ-algebra over a set X is a nonempty collection M of subsets of X that is closed under the complement and countable unions of its members and contains X itself. It is an algebra of sets, completed to include countably infinite operations. The pair (X, M) is also a field of sets, called a *measurable space.*

[6] *Equidecomposable:* The property of two planes or two space regions, either of which can be disassembled into finite number of pieces and reassembled to form the other one.

[7] **Th.**(*Equidecomposability is an equivalence relation*). *The property of being equidecomposable is an equivalence relation on the power set $\mathcal{P}(\mathbb{R}^n)$.*

[8] **Th.**(*Equidecomposability unaffected by union*). *Assume $\{S_1, \ldots, S_m\}, \{T_1, \ldots, T_m\}$ are collections of point sets in $\mathbb{R}^n$ such that for each $k \in \{1, \ldots, m\}$, S_k and T_k are equidecomposable. Then the set $S = \bigcup_{i=1}^m S_i$ is equidecomposable with $T = \bigcup_{i=1}^m T_i$.*

[9] *Isometry.* A bijective map between two metric spaces that preserves distances $d(f(x), f(y)) = d(x, y)$, where f is the map and $d(a, b)$ is the distance function. Isometries are sometimes also called *congruence transformations.* **1.** A map f from a metric space X to a metric space Y where the distance between any two points of X equals the distance between their images under f in Y. **2.** A linear *isomorphism* θ of a vector space E onto itself such that, for a given bilinear form g, $g(\theta x, \theta y) = g(x, y)$ for all x and y in E.
Isomorphism: A one to one function of an algebraic structure (for example, group, ring, module, vector space) onto another of the same type, preserving all algebraic relations; its inverse function behaves likewise.

Sigma-algebra (*σ-algebra*)': A collection of subsets of a given set which contains the empty set and is closed under countable union and complementation of sets. Also known as *sigma field* or *σ-field*. The σ-algebras allow to rigorously define the notion of measurable set.

Def. 34. *(σ-algebra). Let X be a set. Then a σ-algebra F is a nonempty collection of subsets of X such that the following hold:*
1. *X is in F.*
2. *If A is in F, then so is the complement of A.*
3. *If A_n is a sequence of elements of F, then the union of the A_n is in F.*
If Q is any collection of subsets of X, then we can always find a σ-algebra containing Q, namely the power set of X. By taking the intersection of all σ-algebras containing Q, we obtain the smallest such σ-algebra. The smallest σ-algebra containing Q is called the σ-algebra generated by Q.

Def. 35. *(Invariant measure). Let (X, M) be a measurable space and let f be a measurable function from X to itself. A measure μ on (X, M) is said to be invariant under f if, for every measurable set A in M,*

$$\mu(f^{-1}(A)) = \mu(A).$$

($f_*(\mu)$=μ via "pushforward measure" notation)

Measurable function: **1.** A function on a measurable space to a measurable space such that the inverse image od a measurable set is a measurable set. **2.** A real-valued function f defined on a measurable space X where for every real number a all those points x in X for which $f(x) \geq a$ form a *measurable set.*

Def. 36. *(Measurable function). Let (X, M) and (Y, T) be measurable spaces, meaning that X and Y are sets equipped with sigma algebras M and T respectively. A function $f : X \to Y$ is said to be measurable if for every $E \in T$ the preimage of E under f is in M, i.e. $f^{-1}(E) := \{x \in X | f(x) \in E\} \in M$, $\forall E \in T$. The notion of measurability depends on the sigma algebras M and T.*

Pushforward measure: A *pushforward measure* (or *push forward*, *pushforward* or *image measure*) is obtained by transferring (i.e. "*pushing forward*") a measure from one measurable space to another using a measurable function.

Def. 37. *(Pushforward). Let (X_1, M_1),(X_2, M_2) be measurable spaces. A measurable map $f : X_1 \to X_2$ and a measure $\mu : M_1 \to [0, +\infty]$, the pushforward of μ is defined to be the measure $f_*(\mu) : M_2 \to [0, +\infty]$ given by $(f_*(\mu))(S) = \mu(f^{-1}(S))$ for $S \in M_2$.*

7.3. Hausdorff paradox. It is a key of the proof of Banach-Tarski paradox.

Th. 7. *(Hausdorff paradox). There exists a disjoint decomposition of the unit sphere $\mathbb{S}^2$ in the Euclidean space $\mathbb{R}^3$ into four subsets A, B, C, D, such that the following conditions are satisfied:*
Any two of the sets A,B,C and $B \cup C$ are congruent,
D is countable.

A key of its proof is the axiom of choice.
Hausdorff paradox can be written: "*For $n \geq 3$, there exist no additive finite and invariant measures for the group of displacements in $\mathbb{R}^n$.*"
This involves notions of *group of displacement* (geometry) and.*invariant measure* (analysis)

7.4. Axioms ADC and ACC. 1) **Axiom of dependent choice** (**ADC**) or (**DC**), also called principle of dependent choices: "*Let E be a set and a binary relation $R \neq \emptyset$ on E such that* $\mathrm{ran}(R) \subseteq \mathrm{dom}(R)$, *then there is a sequence $(a_n)_{n\in\mathbb{N}}$ in E such that $a_n R a_{n+1}$.*"
Here is another formulation of ADC: "*For any nonempty set E and any entire binary relation R on E, there is a sequence $(x_n)_{n\in\mathbb{N}}$ in E such that $x_n R x_{n+1}$ for each n in $\mathbb{N}$.*" (Where an *entire* binary relation on S is one such that for each a in E there is a b in E such that aRb.)
If the set E above is restricted to be the set $\mathbb{R}$ of all real numbers, the resulting axiom is called $\mathrm{DC}_{\mathbb{R}}$.
ADC is the part of AC required to show the existence of a sequence constructed by transfinite recursion of countable length, if we have to make a choice at each step.
ADC, is a weak form of the axiom of choice (AC) which is sufficient to develop most of real analysis. ADC implies the axiom of countable choice (ACC), and is strictly stronger.
2) **Axiom of countable choice** (**ACC**): "*Any countable collection of nonempty sets must have a choice function* (infra)." (or "*Any countable set of nonempty sets has a choice function.*")
ACC (sometimes called *axiom of denumerable choice*) is also abbreviated CC, $\mathrm{AC}_{\mathbb{N}}$, AC_{ω}. ACC is a special case of the axiom of choice (AC). ACC can also formulate as follows: "*Let A be a function with domain $\mathbb{N}$ (set of natural numbers) and $A(n)$ is a nonempty set for every $n \in \mathbb{N}$, then there exists a function f with domain $\mathbb{N}$ such that $f(n) \in A(n)$*, for every $n \in \mathbb{N}$."
ACC is a weaker form of the axiom of dependent choice (ADC). ACC is not provable in Zermelo-Fraenkel set theory (ZF) without the axiom of choice (AC). ACC has two forms:
. **Axiom of countable choice** (**ACC** - form 1): *Let $(S_n)_{n\in\mathbb{N}}$ be a sequence of nonempty sets. The axiom of countable choice states that there exists a sequence: $(x_n)_{n\in\mathbb{N}}$ such that $x_n \in S_n$ for all $n \in \mathbb{N}$.*
. **Axiom of countable choice** (**ACC** - form 2): *Let S be a countable set of nonempty sets. Then S has a choice function* (infra).

Choice function (*selector*): A function f that is defined on some family or collection $\mathcal{C}$ of nonempty sets and assigns to each set E in that collection some element $f(E)$ of E. Thus, f is a choice function for $\mathcal{C}$ iff it belongs to the direct product (or cartesian product) of $\mathcal{C}$. For instance, if C={{0,2,3,9},{6},{1,9}}, then the function that assigns 9 to the set {0,2,3,9}, 6 to {6}, and 1 to {1,9} is a choice function on the collection $\mathcal{C}$.

7.5. Banach-Tarski paradox and AC, ADC, ZF, ZFC.
Banach-Tarski paradox involve Vitali's (set) and Hausdorff's constructions (Hausdorff paradox) themselves related to axiom of choice (AC). The statement "*Two Euclidean polygons, one of which strictly contains the other, are not equidecomposable*" has also played a part in the construction of the paradox. This last statement can be proved in ZF set theory (see Morse) and *therefore does not require the axiom of choice.* The axiom of choice cannot be proved from ZF (see Cohen). A weaker version of the axiom of choice (AC) is the *axiom of dependent choice* (ADC).
▪Banach-Tarski paradox is not a theorem of ZF, nor of ZF+ADC.
▪Banach-Tarski paradox follows from ZF plus the *Hahn-Banach theorem* (see heading *"Hahn-Banach Theorems"*). Hahn-Banach theorem doesn't rely on the full axiom of choice but can be proved using a weaker version of AC called **ultrafilter lemma** (infra). Then it was shown that set theory needed to prove Banach-Tarski paradox is weaker than full ZFC while being stronger than ZF.

*

Ultrafilter lemma: A **filter** on a set S is a family of nonempty subsets of S that is closed under finite intersection and under superset. An **ultrafilter** is a *maximal filter.* The *ultrafilter lemma* states that "*every filter on a set S is a subset of some ultrafilter on S (a maximal filter of nonempty subsets of S).*" This lemma is most often used in topology. An ultrafilter that does not contain finite sets is called *non-principal filter* (Tarski).
Ultrafilter lemma is equivalent to **Boolean prime ideal theorem** (**BPI**) with the equivalence provable in ZF set theory without axiom of choice (AC). Underlying idea of its proof is that the subsets of any set form a Boolean algebra partially ordered by inclusion, and any Boolean algebra is representable as an algebra of sets.

8. Hahn-Banach Theorems

This theorem belongs, stricto sensu, to functional analysis, but having deep sources in set theory and involving many transversal notions to mathematics, we introduce it in this chapter for didactic purposes. It will also be met in other chapters.
The Hahn-Banach theorem is a fundamental result in mathematics, especially in analysis, complex analysis, functional analysis, geometry and topology. It allows to prove the existence of many continuous functions; it also allows the **extension** of **bounded linear functionals** (see "*Prerequisites*") defined on a subspace of some vector space **to the whole space**, and it also shows that there are enough continuous linear functionals defined on any normed vector space to make interesting the study of the **dual space** (see "*Prerequisites*"). The Hahn-Banach theorem asserts the existence of a great variety of bounded (and thus continuous) linear *functionals* on an normed vector space, even if that space happens to be infinite-dimensional.
Hahn and Banach have established the theorem independently in the late 1920s (while a specific version was established earlier by Helly), and a general extension theorem from which the Hahn-Banach theorem can be derived was shown by Riesz.
Another version of the Hahn-Banach theorem is known as *Hahn-Banach separation theorem* (or *Separating hyperplane theorem)* and is especially used in convex geometry. By its geometric interpretation in terms of hyperplanes, avoiding a convex set, the Hahn-Banach theorem also plays a essential role in the study of the geometry of convex sets, and beyond, in convex analysis.

In the scientific literature, the statements known as "Hahn-Banach theorem" are numerous, sometimes differing by simple details, sometimes having significant differences. Nevertheless, two distinct classes clearly appear: some of them guarantee that we can extend a linear form under certain conditions on upper bound ("analytical" forms of theorem) and others guarantee that we can separate two convex sets by an affine hyperplane ("geometric" forms).

8.1. Prerequisites. The formulation of Hahn Banach theorem needs some prerequisites, so we have to regroup, and in most cases, to introduce by anticipation some notions:
- *operator, linear operator, bounded linear operator,*
- *functional, linear functional, sublinear functional,*
- *norm, semi-norm, bounded function,*
- *bounded linear functional,*
- *scalar product, inner product,*
- *inner-product space, pre-Hilbert space,*
- *Banach space, Hilbert space,*
- *Riesz representation th., projection th.,*
- *dual space,*
- *totally and partially ordered sets, well-ordered set,*
- *maximal element, greatest element,*
- *well-ordering principle,*
- *Zorn lemma,*
- *ideal, proper, maximal, principal and prime ideals,*
- *filter, filter base, ultrafilter,*
- *Boolean algebra,*
- *lattice, distributive lattice, bounded lattice,*
- *lattice ideal, lattice proper ideal,*
- *lattice prime ideal, lattice maximal ideal,*
- *directed set, upper set, lower set, preorder,*
- *order ideal, order filter,*
- *order principal ideal, order principal filter*
- *residual, cofinal, confinality,*
- *Birkhoff prime ideal th., Boolean prime ideal th.,*
- *ultrafilter lemma,*
- *Banach algebra,*
- *spectrum (of operator),*
- *spectral radius,*
- *spectral theorems,*
- *separable space.*

Below, for simplificity, vectors are not boldfaced (e.g. x instead of $\mathbf{x}$):

*

Operator: It is a function between vector spaces (or space of functions). Synonym of map and function. Often used to refer to maps where the domain and codomain are, in some sense a space of functions.

Def. 38. *(Linear operator). A function A defined in a vector space E and having its values in another vector space over the same field, such that if u and v are vectors in E, and λ is a scalar, then:*
(1) $A(\lambda u) = \lambda Au$,
(2) $A(u + v) = Au + Av$.
*Also known as **linear transformation**, homogeneous transformation, linear function.*

Def. 39. *(Bounded linear operator). Let X, Y be normed vector spaces. A map A which assigns to each element x of a set $D(A) \subset X$ a unique element $y \in Y$ is called an **operator** (or transformation). The set $D(A)$ on which A acts is called the domain of A. The operator A is called **linear** if*
(1) *$D(A)$ is a subspace of X, and*
(2) *$A(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 Ax_1 + \alpha_2 Ax_2$ for all scalars α_1, α_2 and all elements $x_1, x_2 \in D(A)$. Here for simplicity we only consider operators A with $D(A) = X$. An operator A is called **bounded** if there is a constant M such that*
$$(a) \qquad \|Ax\| \leq M \|x\|, \; x \in X.$$
The norm of such an operator is defined by
$$(b) \qquad \|A\| = \sup_{x \neq 0} \frac{\|Ax\|}{\|x\|}.$$
*Again, it is the smallest M which works in (a). An operator A is said to be **continuous** at a point $x_0 \in X$ if $x_n \to x$ in X implies $Ax_n \to Ax$ in Y. A **bounded linear operator** is **continuous** at each point. For if $x_n \to x$ in X, then*
$$\|Ax_n - Ax\| \leq \|A\| \cdot \|x_n - x\| \to 0.$$

Th. 8. *If a linear operator A is continuous at one point $x_0 \in X$, then it is bounded, and hence continuous at every point.*

(Denote $B(X,Y)$ the *set of bounded linear operators* from X to Y (where X and Y are vector spaces). Under the above norm (b), we easily check that $B(X,Y)$ is a normed vector space. In addition, if Y is a Banach space, so is $B(X,Y)$.)

*

Functional: In short, a*ny function from a vector space into its scalar field.* (*Scalar product* and *norm* are examples of functional.)

Def. 40. *(Linear functional). A linear functional (or linear form) is a map $f : V \to K$ such that for all $x, y \in V$, $\lambda \in K$:*
(1) $f(\lambda x) = \lambda f(x)$,
(2) $f(x + y) = f(x) + f(y)$.
V can be a real or complex vector space.
(Equivalently, a linear functional on a vector space V is a linear map $f{:}V \to K : f(\alpha x + \beta y){=}\alpha f(x) + \beta f(y)$ for all $x, y \in V$ and $\alpha, \beta \in K$.)

Linear functional (as an important special case of the notion of *linear operator*) is a central concept in linear algebra and in analysis. The *generalized functions* are a special case of *linear functionals*.

Def. 41. *(Sublinear function). A sublinear function (in linear algebra and related domains) is a function $f : V \to \mathbb{F}$ on a vector space V over $\mathbb{F}$, an ordered field (e.g. $\mathbb{R}$), which satisfies $\forall x, y \in V$:*
1) *$f(\lambda x){=}\lambda f(x)$, $\forall \lambda{>}0 \in \mathbb{F}$ (positive homogeneity),*
2) *$f(x + y) \leq f(x) + f(y)$ (subadditivity).*

In functional analysis, the name "*Banach functional*" is used for "*sublinear function*", especially when formulating Hahn-Banach theorem.
. Every sublinear *function* is a convex functional.
. A norm is a convex functional.
. Every (semi-)norm is a sublinear function. Opposite is not true, since (semi-)norms can have their domain vector space over any field (not necessarily ordered) and must have $\mathbb{R}$ as their codomain.

Def. 42. *(Sublinear functional). Let V be a vector space. A functional $p(x)$ on V is called sublinear if the following conditions hold:*
1) *$p(\lambda x){=}\lambda p(x)$, $x \in V$, $\lambda > 0$,*
2) *$p(x + y) \leq p(x) + p(y)$, $x, y \in V$.*

Note that the *norm* in a *normed vector space* is a *sublinear functional*.

*

Norm: A norm of a mathematical object is a measure which describes some sense of the lenght or size of the object. So the *absolute value of real numbers*, *modulus of a complex number*, *matrix norms* and *vector norms* are all examples of norms. It is a scalar-valued function on a vector space.

Def. 43. *(Norm). Given a vector space V over a subfield $\mathbb{F}$ of the complex numbers, a norm on V is a function $p : V \to \mathbb{R}$ with the following properties, for all $\lambda \in \mathbb{F}$ and all $x, y \in V$:*
1) *If $p(x){=}0$, x is the zero vector (separates points)*
2) *$p(\lambda x) = |\lambda| \, p(x)$ (positive homogeneity)*
3) *$p(x{+}y) \leq p(x) + p(y)$ (subadditivity).*
*By the axiom (2) (positive homogeneity, also called positive scalability), we have $p(0){=}0$ and $p(-x){=}p(x)$, so that by the "subadditivity" also called "triangle inequality" we have $p(x){\geq}0$ (positivity). A **seminorm** is a norm with the axiom (1) (separating points) removed.*

Def. 44. *(Norm -version 2). A map $x \to \|x\|$ from a vector space V over the field of real or complex numbers into the real numbers, satisfying the conditions for all $x, y \in V$ and for every scalar λ:*
1) *$\|x\| \geq 0$, and $\|x\|{=}0$ iff $x{=}0$*
2) *$\|\lambda x\| = |\lambda| \, \|x\|$*
3) *$\|x + y\| \leq \|x\| + \|y\|$ (triangle axiom).*
The number $\|x\|$ is called norm of the element x.

A vector space V endowed with a norm is called *normed space*. A norm induces on V a *metric* by the formula $\mathrm{dist}(x,y){=}\|x{-}y\|$, and so a *topology* compatible with this metric. And so a *normed space* is provided with the *natural structure* of a *topological vector space*. A *normed space* that is *complete* in this metric is called "*Banach space*". Any *normed space* has a *Banach completion*.
Topological vector space: A vector space which has a topology with the property that vector addition and scalar multiplication are continuous functions. Also called linear topological space; topological linear space.
Topology: In short, a topology can be seen as a geometry of transformations in which the only invariant is continuity.
. A *topological vector space* is said to be *normable* if its *topology* is compatible with some norm.
. *Normability* is equivalent to the *existence of a **convex** bounded neighbourhood of zero.*

Semi-norm: A scalar-valued function on a real or complex vector space satisfying the axioms of a norm, except that the semi-norm of a nonzero vector may equal zero.

Def. 45. *(Semi-norm). A finite non-negative function p on a vector space V (over the field of real or complex numbers) such that $\forall x, y \in V$ and any scalars λ the following conditions hold:*
1) $p(\lambda x) = |\lambda|\, p(x)$,
2) $p(x+y) \leq p(x) + p(y)$.

An example of a semi-norm is a norm; the difference is that a semi-norm may have $p(x)$ with $x \neq 0$. If a semi-norm p is defined on a vector space and if f is a *linear functional* on a subspace obeying the condition $|f(x)| \leqslant p(x)$, then *this functional can be extended to the entire space so that the extension satisfies the same condition* (Hahn-Banach th.).

Def. 46. *(Semi-norm -version 2). A semi-norm is a function on a vector space V, denoted $\|x\|$, such that the following conditions hold for all $x, y \in V$ and any scalar λ:*
1) $\|x\| \geq 0$,
2) $\|\lambda x\| = |\lambda|\, \|x\|$ *and*
3) $\|x+y\| \leq \|x\| + \|y\|$.
Note that for nonzero x we can have $\|x\| = 0$; e.g. the functional $\|f\| = |f(0)|$ for continuous functions is a semi-norm which is not a norm. A seminorm is a norm if $\|x\| = 0$ is equivalent to $x = 0$.

Normed vector space: Vector space which has a norm. Also known as *normed linear space*, or *normed space*.

*

Bounded: A mathematical object (such as a set or function) is said to *bounded* if it possesses a bound, i.e. a value which all members of the set, functions, etc., are less than.

Def. 47. *(Bounded function). A **real** function f, defined on a domain S, is bounded (on S) if there is a number M such that, for all x in S, $|f(x)| < M$ (i.e. if the absolute value of the function is bounded from above.) The fact that, if f is continuous on a closed interval $[a, b]$ then it is bounded on $[a, b]$, is a property for which a rigourous proof is not elementary (refer to continuous functions).*

Def. 48. *(Bounded function)'. Let X be a nonempty set. Then a **complex** function $f : X \to \mathbb{C}$ is a bounded function if there exist a $\omega < \infty$ such that $|f(x)| < \omega$ for all $x \in X$. The set of all bounded functions on E is usually denoted by $B(X)$. (Under standard point-wise addition and point-wise multiplication by a scalar, $B(X)$ is a complex vector space. If $f \in B(X)$, then the sup-norm or uniform norm of f is defined as $\|f\|_\infty = \sup_{x \in X} |f(x)|$. It is easy to check that $\|\cdot\|_\infty$ makes $B(X)$ into a normed vector space, i.e. to check that $\|\cdot\|_\infty$ satisfies the assumptions for a norm.)*

Def. 49. *(Bounded linear functional). Let $(X, \|\cdot\|)$ be a normed vector space over the field $\mathbb{K}$. A linear functional $f : X \to \mathbb{K}$ is said to be bounded if there exists a real number $c \geq 0$ such that*
$$|f(x)| \leq c\, \|x\|,\ \forall x \in X.$$

. A **linear functional** on a **normed space** is **bounded** if and only if it is **continuous**.
. A **linear functional** on a **Hilbert space** is **bounded** if and only if it is **continuous**.
. All of the **bounded linear functionals** on a **Hilbert space** are just the **scalar product**.

*

Scalar product: **1.** A symmetric, alternating, or Hermitian form. **2.** See **inner product** (which is a generalization of the scalar product).

Inner product: **1.** A scalar-valued function of pairs of vectors from a vector space, denoted by "(x, y)" (or also $(x|y)$,$\langle x, y\rangle$,$\langle x|y\rangle$) where x and y are vectors, and with the properties that (x, x) is always positive and is zero only if $x = 0$, that $(ax + by, z) = a(x, z) + b(y, z)$ for any scalars a and b, and that $(x, y) = (y, x)$ if the scalars are *real numbers*, $(x, y) = \overline{(y, x)}$ if the scalars are *complex numbers*. Also known as *Hermitian inner product*; *Hermitian scalar product*. **2.** The inner product of vectors $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ from n-dimensional Euclidean space is the sum of $x_i y_i$ as i ranges from 1 to n. Also known as *dot product*; **scalar product**. **3.** The inner product of two functions f and g of a real or complex variable is the integral of $f(x)\overline{g(x)}\mathrm{d}x$, where $\overline{g(x)}$ denotes the conjugate of $g(x)$.

Inner-product space: A vector space that has an **inner product** defined on it. Also known as generalized Euclidean space; Hermitian space; **pre-Hilbert space**. They also provide the means of defining **orthogonality** between vectors (*zero inner product*).

Pre-Hilbert space: see inner-product space.

Banach space: A real or complex vector space in which each vector has a non-negative **length**, or **norm** and in which **every Cauchy sequence converges** to a point of the space. That is, a normed vector space in which every Cauchy sequence converges. A *complete normed vector space* on the real or complex numbers. Also called complete normed linear space.

Hilbert space: A **Banach space** which also is an **inner-product space** with the inner product of a vector with itself being the same as the square of the norm of the vector. A Hilbert space is always a Banach space, but the converse need not hold. A Hilbert space is a *complete pre-Hilbert space* (for the norm associated with the inner product).

. An inner product naturally induces an associated norm, so an inner product space is also a normed vector space. *A complete space with an inner product is called Hilbert space.* An incomplete space with an inner product is called pre-Hilbert space, since its completion with respect to the norm, induced by the inner product, becomes a Hilbert space.
. Let us consider a Hilbert space H, and its **scalar product** denoted here by (x, y). If we fix y, then the expression (x, y) assigns to each $x \in H$ a number. An assignment F of a number to each element x of a vector space is called a **functional** and is denoted here by $F(x)$. The **scalar product** is not the only **functional** we can encounter. In any normed vector space, the **norm** is also a **functional**.

*

Th. 9. *(Riesz representation th.). For every **bounded linear functional** F on a Hilbert space H there is a unique element $y \in H$ such that $F(x) = (x, y)$ for all $x \in H$. Moreover,*
$$\|y\| = \sup_{x \in H, x \neq 0} \frac{|F(x)|}{\|x\|}.$$

Th. 10. *(Projection th.). For every point x in a Hilbert space H and every closed convex $C \subset H$, there exists a unique point $y \in C$ for which $\|x - y\|$ is minimized over C. This is in particular true for any closed subspace N of H. In that case, a necessary and sufficient condition for y is that the vector $x - y$ be orthogonal to N.*

This Hilbert projection theorem is a famous result of convex analysis. Another version can be written:

Th. 11. *(Projection th.)'. Let N be a closed subspace of a Hilbert space H. Then for each $x \in H$, there are a $v \in N$ and a w **orthogonal** to N such that $x = v + w$. This decomposition is unique.*

This theorem is called the projection theorem because of its obvious geometrical interpretation. It can be viewed as a formalization of the result that the closest point on a plane to a point not on the plane can be found by dropping a *perpendicular*.

Cor. 1. *($\Diamond$). If N is a closed subspace of a Hilbert space H but is not the whole of H, then there is an element $y \neq 0$ in H which is **orthogonal** to N.*

*

Def. 50. *(Dual space). The dual space of a (topological) vector space V is the vector space V^* whose elements are the **continuous linear functionals** on V.*

Note that addition and scalar multiplication are defined in V^* by $(\Lambda_1 + \Lambda_2)x = \Lambda_1 x + \Lambda_2 x$, $(\alpha\Lambda)x = \alpha \cdot \Lambda x$ (where Λ_1, Λ_2, Λ are operators). These operations do indeed make X^* into a vector space.

*

Def. 51. *(Totally ordered set). A totally ordered set (also called linearly ordered set, simply ordered set, chain) is a set plus a relation "$\preccurlyeq$" on the set (called total order) that satisfies the conditions for a partial order plus an additional condition known as the totality condition. A relation "$\preccurlyeq$" is a total order on a set S ("$\preccurlyeq$ totally orders S") if the following conditions hold:*
1) $a \preccurlyeq a$ *for all* $a \in S$ *(reflexivity)*
2) $a \preccurlyeq b$ *and* $b \preccurlyeq a$ *implies* $a = b$ *(antisymmetry)*
3) $a \preccurlyeq b$ *and* $b \preccurlyeq c$ *implies* $a \preccurlyeq c$ *(transitivity)*
4) $\forall a, b \in S$, *either* $a \preccurlyeq b$ *or* $b \preccurlyeq a$ *(totality).*
*The first three are the axioms of a partial order, while addition of the totality (also called **comparability**) defines a total order.*

Def. 52. *(Partially ordered set). A partially ordered set (poset) is a set plus a relation "$\preccurlyeq$" on the set, which satisfies the conditions for a partial order. The relation $\preccurlyeq$ is a partial order on a set S if the following conditions hold:*
1) $a \preccurlyeq a$ *for all* $a \in S$ *(reflexivity)*
2) $a \preccurlyeq b$ *and* $b \preccurlyeq a$ *implies* $a = b$ *(antisymmetry)*
3) $a \preccurlyeq b$ *and* $b \preccurlyeq c$ *implies* $a \preccurlyeq c$ *(transitivity).*
A partially ordered set is also called a poset.

Maximal element: In a partially ordered set a maximal element is one for which no other element follows it in the ordering. A *maximal element* of a subset U of some partially ordered set is an element of U that is not smaller than any other element in U. The notions of maximal and minimal elements are weaker than those of *greatest element* and least element which are also known, respectively, as maximum and minimum.

Def. 53. *(Maximal element). Let $(P, \preccurlyeq)$ be a partially ordered set and $S \subset P$. Then $m \in S$ is a maximal element of S if for all $s \in S$, $m \preccurlyeq s$ implies $m = s$.*

Def. 54. *(Greatest element). Let $(P, \preccurlyeq)$ be a partially ordered set, then an element g of a subset S of P is the greatest element of S if $s \preccurlyeq g$, for all elements s of S.*

Def. 55. *(Well-ordered set). A linearly ordered set (also called totally ordered set) where every subset has a least element. Such a set is then said to be well-ordered or have a well-founded order.*

Well-ordering principle: The proposition that every set can be endowed with an order so that it becomes a well-ordered set; *this is* **equivalent to the axiom of choice (AC)**.

*

Lem. 1. *(Zorn lemma). If P is a partially ordered set such that each totally ordered subset has an upper bound in P, then P has a maximal element.*

Or, equivalently: "*If every linearly ordered subset of a partially ordered set has a maximum element in the set, then the set has a maximal element.*" This statement is equivalent to **axiom of choice (AC)**. Zorn lemma is also equivalently written: "*Suppose a partially ordered set P has the property that every chain (i.e. totally ordered subset) has an upper bound in P. Then the set P contains at least one maximal element.*" The terms can be defined by: Assume $(P; \preccurlyeq)$ is a *partially ordered set* (i.e. the set P endowed with the relation $\preccurlyeq$ satisfying the conditions of a partial order). A subset T is *totally ordered* if for any s, t in T we have $s \preccurlyeq t$ or $t \preccurlyeq s$. Such a set T has an upper bound u in P if $t \preccurlyeq u$ for all t in T. Note that u is an element of P but need not be an element of T. An element m of P is called a **maximal element** (or *non-dominated*) if there is no element x in P for which $m \prec x$.
Zorn lemma is equivalent to the **well-ordering theorem** (i.e. "*every set can be well-ordered*") and the **axiom of choice (AC)**, in the sense that any one of them, together with the **Zermelo-Fraenkel axioms** of *set theory*, is sufficient to prove the others. (It appears in the proofs of several important theorems, for instance the Hahn-Banach theorem in functional analysis, the theorem that every vector space has a basis, Tychonoff's theorem in topology stating that every product of compact spaces is compact, and the theorems in abstract algebra that every nonzero ring has a *maximal ideal* and that every field has an algebraic closure.)

*

. Although the term **ideal** historically was derived from the notion of *ring ideal* of abstract algebra, it has subsequently been generalized to a different notion. Ideals are of great importance for many constructions in order and lattice theory. The construction of *ideals* and *filters* is an important tool in many applications of order theory. In order theory, an ideal is a special subset of a poset.
. In *ring theory* (in algebra), an ideal is defined by:

Def. 56. *(Ideal). A subset I of a ring R where $x - y$ is in I for every x, y in I and either rx is in I for every r in R and x in I or xr is in I for every r in R and x in I; in the first case I is called a left ideal, and in the second a right ideal; an ideal is two-sided if it is both a left and a right ideal. Indeed, in the noncommutative rings, there are left ideals, right ideals and two-sided ideals. An ideal is a particular subring. The only ideals of $\mathbb{Z}$ are the subrings $n\mathbb{Z}$ with $n \in \mathbb{N}$. Furthermore, in any ring, the null ideal $\{0\}$ and the ring itself are ideals.*

Def. 57. *(Proper ideal). Any ideal of a ring which is strictly smaller than the whole ring. Suppose R is a ring and I is an ideal of R. We say that I is a proper ideal if I is not equal to R.*

(In a commutative ring, every proper ideal can be extended to a maximal ideal.)

Def. 58. *(Maximal ideal). An ideal I in a ring R which is not equal to R, and such that there is no ideal containing I and not equal to I or R.*

Def. 59. *(Maximal ideal)'. A maximal ideal of a ring R is an ideal I, not equal to R, such that there are no ideals "in between" I and R. In other words, if J is an ideal which contains I as a subset, then either $J = I$ or $J = R$.*

Def. 60. *(Principal ideal). The smallest ideal of a ring which contains a given element of the ring.*

Def. 61. *(Prime ideal). A prime ideal is an ideal I such that if $ab \in I$, then either $a \in I$ or $b \in I$. For example, in the integers, the ideal $\mathfrak{a} = \langle p \rangle$ (multiples of p) is prime whenever p is a prime number. (Note the use for "$\mathfrak{a}$" of a Gothic typeface).*

Def. 62. *(Prime ideal)'. A principal ideal of a ring given by a single element that has properties analogous to those of the prime numbers.*

. A **maximal ideal** is always a **prime ideal**, but some prime ideals are not maximal.
. In algebra, a *prime ideal* is a subset of a ring which shares many important properties of a *prime number* in the ring of integers. Prime ideals for Integers are the sets that contain all the multiples of a given prime number, together with the zero ideal.
. The dual notion of an ideal is a filter.

*

Filter: A filter is a nonempty subset F of a partially ordered set P satisfying the conditions: (1) if $a, b \in F$ and if the infimum $\inf\{a, b\}$ exists, then $\inf\{a, b\} \in F$; and (2) if $a \in F$ and $a \leq b$, then $b \in F$. (The concept of a **filter** is **dual** to that of an **ideal** of a *partially ordered set*). A filter over a nonempty set E (or in a set E) is a *proper filter* of the set of subsets of E, ordered by inclusion i.e. any nonempty collection F of subsets of E satisfying the conditions: If $A, B \in F$, then $A \cap B \in F$; if $A \in F$ and $A \subseteq B$, then $B \in F$; the empty set does not belong to F. Note that the set of all filters over a given set is *partially ordered by inclusion*. A **maximal element** of it is called an **ultrafilter** (a **maximal proper filter** in any **Boolean algebra** is also called an **ultrafilter**).

Filter base: A filter base is a system of subsets of E satisfying the two conditions: (1) the empty set does not belong to it; and (2) the intersection of two subsets belonging to it contains some third subset belonging to it. Every filter is completely determined by any of its filter bases. The system of all subsets of E that contain some element of a given filter base is a filter. It is said to be spanned by this base.

Ultrafilter: A filter which is maximal, in the sense that every filter containing it coincides with it. An ultrafilter may be defined as a system of subsets satisfying three conditions: (1) the empty set is not included; (2) the intersection of two subsets in the system again belongs to it; and (3) for any subset, either it or its complement belongs to the system. For every filter there is an ultrafilter containing it; moreover, every filter is precisely the intersection of all the ultrafilters containing it. Note that all *ultrafilters* are divided into two classes: *trivial* (or *fixed* or *principal*) and *free ultrafilters*. An ultrafilter is called *trivial* or *principal* if it is the system of all subsets containing a given point; such an ultrafilter is also called *fixed* in that point. An ultrafilter is called *free* if the intersection of all its elements is the empty set, in other words, if it is not fixed in any point. The existence of *free ultrafilters* is unprovable without the **axiom of choice**.

*

Boolean algebra: Boolean algebra is the area of algebra in which the values of the variables are the truth values true and false (usually denoted 1 and 0 respectively). Boolean algebra is a structure similar to a *Boolean ring* but that is defined using the operators of conjunction AND (denoted $\wedge$, also called *meet*) and of disjunction OR (denoted $\vee$, also called *join*) instead of the usual addition and multiplication operators. A *Boolean algebra* is the **partial order** on subsets defined by inclusion, i.e. the Boolean algebra $B(A)$ of a set A is the set of subsets of A that can be obtained using a finite number of the set operations union (OR), intersection (AND), and complementation (NOT). A Boolean algebra also forms a **lattice**, and each of the elements of $B(A)$ is called a *Boolean function*. A Boolean algebra is a **complemented distributive lattice** (see below). Boolean algebras have a recursive structure visible in Hasse diagrams.

*

Def. 63. *(Lattice). A lattice is any partially ordered set (poset) L in which any two elements x and y have a least upper bound, $x \vee y$, and a greatest lower bound, $x \wedge y$. The operation $\wedge$ is called meet, and the operation $\vee$ is called join. Some authors require that L is nonempty. Lattices, like posets, can be visualized by Hasse diagrams.*

Def. 64. *(Sublattice). A sublattice of L is a subposet of L which is a lattice, that is, which is closed under the operations $\wedge$ and $\vee$ as defined in L.*

Def. 65. *(Distributive lattice). A lattice is said to be distributive if it satisifes either (and therefore both) of the distributive laws:* (1)

$x\wedge(y\vee z)=(x\wedge y)\vee(x\wedge z)$; (2) $x\vee(y\wedge z)=(x\vee y)\wedge(x\vee z)$; e.g. Boolean lattices, totally ordered sets, subgroup lattices of locally cyclic groups.

Def. 66. *(Bounded lattice). A lattice L is said to be bounded from below if there is an element $0 \in L$ such that $0 \leq x$ for all $x \in L$. Dually, L is bounded from above if there exists an element $1 \in L$ such that $x \leq 1$ for all $x \in L$. A bounded lattice is one that is bounded both from above and below.*

Def. 67. *(Complemented lattice). Let L be a bounded lattice (with 0 and 1), and $a \in L$. A complement of a is an element $b \in L$ such that $a \wedge b = 0$ and $a \vee b = 1$.*

Def. 68. *(Complemented distributive lattice).*

Def. 69. *(Lattice ideal). Let L be a lattice. A ideal I of L is a nonempty subset of L such that:*
(1) I is a sublattice of L, and
(2) for any $a \in I$ and $b \in L$, $a \wedge b \in I$.

Note the analogy with the definition of an ideal in a ring (except in a ring with 1, an ideal is almost never a subring).
Due to redundancy in this definition, we can replace the first condition by a weaker; thus we get an equivalent def.:

Def. 70. *(Lattice ideal). An ideal I in a lattice L is*
(1) for any $a, b \in I$, $a \vee b \in I$, and
(2) for any $a \in I$, if $b \leq a$, then $b \in I$.

Def. 71. *(Lattice proper ideal). Let I be an ideal of a lattice L. I is proper if $I \neq L$.*

Def. 72. *(Lattice non-trivial ideal). Let I be an ideal of a lattice L. If L contains 0, I is said to be non-trivial if $I \neq 0$.*

Def. 73. *(Lattice prime ideal). Let I be an ideal of a lattice L. I is a prime ideal if it is proper, and for any $a \wedge b \in I$, either $a \in I$ or $b \in I$.*

Def. 74. *(Lattice maximal ideal). Let I be an ideal of a lattice L. I is a maximal ideal of L if I is proper and the only ideal having I as a proper subset is L.*

*

In *order theory*, order ideals, order filters and related notions can be defined as follows:

Def. 75. *(Upper set). Let P be a poset and A a subset of P. The upper set of A is defined to be the set $\{b \in P | a \leq b$ for some $a \in A\}$, and is denoted by $\uparrow A$. In other words, $\uparrow A$ is the set of all upper bounds of elements of A.*

Def. 76. *(Lower set). Dually, the lower set (or lower closure) of A is the set of all lower bounds of elements of A. The lower set of A is denoted by $\downarrow A$. If the lower set of A is A itself, then A is a called a lower set, or a lower closed set.*

Def. 77. *(Directed set). A directed set (or upward-directed set) is a partially ordered set (A) such that whenever $a, b \in A$ there is an $x \in A$ such that $a \leq x$ and $b \leq x$.*

Def. 78. *(Filtered set). Dually, a filtered set (or downward-directed set) is a partially ordered set (A) such that whenever $a, b \in A$ there is an $x \in A$ such that $x \leq a$ and $x \leq b$.*

Def. 79. *(Order ideal). Let P be a poset. A subset I of P is said to be an order ideal (or simply a ideal) if:*
(1) I is a lower set: $\downarrow I = I$, and
(2) I is a directed set: I is non-empty, and every pair of elements in I has an upper bound in I.
In other words, an order ideal is a (non-empty) directed lower set.

Def. 80. *(Order filter). Dually, an order filter (or simply a filter) in P is a non-empty subset F which is both an upper set and a filtered set (every pair of elements in F has a lower bound in F). A principal filter is a filter of the form $\uparrow x$ for some $x \in P$.*

Def. 81. *(Principal order ideal). An order ideal is said to be principal if it has the form $\downarrow x$ for some $x \in P$.*

Def. 82. *(Principal order filter). A principal filter is a filter of the form $\uparrow x$ for some $x \in P$.*

Def. 83. *(Residual; Cofinal). A subset $B \subseteq A$ is said to be residual if there is $a \in A$ such that $b \in B$ whenever $a \leq b$, and cofinal if for each $a \in A$ there is $b \in B$ such that $a \leq b$.*

Def. 84. *(Cofinality). Let (P) be a poset. A subset $A \subseteq P$ is said to be cofinal in P if for every $x \in P$ there is a $y \in A$ such that $x \leq y$. A function $f : X \to P$ is said to be cofinal if $f(X)$ is cofinal in P. The least cardinality of a cofinal set of P is called the cofinality of P. Equivalently, the cofinality of P is the least ordinal α such that there is a cofinal function $f : \alpha \to P$. The cofinality of P is written $\mathrm{cf}(P)$ or $\mathrm{cof}(P)$.*

Properties of the operator $\uparrow$: $\uparrow$ can be viewed as a (unary) operator on the power set 2^P sending $A \in 2^P$ to $\uparrow A \in 2^P$. $\uparrow$ has the following properties: (1) $\uparrow \emptyset = \emptyset$, (2) $A \subseteq \uparrow A$, (3) $\uparrow \uparrow A = \uparrow A$, (4) if $A \subseteq B$, $\uparrow A \subseteq \uparrow B$. Thus, $\uparrow$ is a closure operator.
Several of above notions are equivalently defined by

Def. 85. *(Order ideal). A non-empty subset I of a partially ordered set $(P, \leq)$ is an ideal, if the following conditions hold:*
(1) For every x in I, $y \leq x$ implies that y is in I. (I is a lower set)
(2) For every x, y in I, there is some element z in I, such that $x \leq z$ and $y \leq z$. (I is a directed set)

While this is the most general way to define an ideal for arbitrary partially ordered sets (posets), it was originally defined for lattices only.

Def. 86. *(Upper set). An upper set (also called an upward closed set) of a partially ordered set $(X, \leq)$ is a subset U with the property that, if x is in U and $x \leq y$, then y is in U.*

Def. 87. *(Lower set). The dual notion of an upper set is a lower set (or down set, decreasing set, initial segment; the set is downward closed), which is a subset L with the property that, if x is in L and $y \leq x$, then y is in L.*

Def. 88. *(Directed set). A directed set (or a filtered set or a directed preorder) is a nonempty set A together with a reflexive and transitive binary relation $\leq$ (i.e. a preorder), with the additional property that every pair of elements has an upper bound: In other words, for any a and b in A there must exist a c in A with $a \leq c$ and $b \leq c$.*

Def. 89. *(Directed set)'. A directed set is a set A with a preorder such that every finite subset of A has an upper bound. In this definition, we take the upper bound of the empty subset to be any existing element of A and require that A be nonempty.*

Directed sets are a generalization of nonempty totally ordered sets, i.e. all totally ordered sets are directed sets (in contrast partially ordered sets which need not be directed).

Def. 90. *(Preorder). A preorder (or quasiorder) is a binary relation that is reflexive and transitive. All partial orders and equivalence relations are preorders, but preorders are more general.*

*

Th. 12. *(Birkhoff - Prime ideal th.). Let L be a distributive lattice and I a proper lattice ideal of L. Pick any element $a \notin I$. Then there is a prime ideal P in L such that $I \subseteq P$ and $a \notin P$.*

Before stating Boolean prime ideal th., consider again some notions: Let B be a Boolean algebra. Recall that an *ideal* I of B if it is closed under $\vee$, and $\forall a \in I$, $\forall b \in B$, $a \wedge b \in I$. I is *proper* if $I \neq B$ and non-trivial if $I \neq (0)$, and I is *prime* if it is *proper*, and, given $a \wedge b \in I$, either $a \in I$ or $b \in I$.

Th. 13. *(Boolean prime ideal th.). Every Boolean algebra contains a prime ideal.*

Proof. Let B be a Boolean algebra. If B is trivial (the two-element algebra), then (0) is the prime ideal we want. Otherwise, take $a \in B$, where $0 \neq a \neq 1$, and let be the trivial ideal. Given Birkhoff's prime ideal theorem (see above) for distributive lattices, B, considered as a *distributive lattice*, has a prime ideal P (containing (0) of course) such that $a \notin P$. Then P is also a prime ideal of B considered as a Boolean algebra. □

▪ There exist several equivalent versions of the Boolean prime ideal theorem, some are listed here: (1) Every Boolean algebra has a prime ideal. (2) Every ideal in a Boolean algebra can be enlarged to a prime ideal. (3) Given a set S in a Boolean algebra A, and an ideal I disjoint from S, then there is a prime ideal P containing I and disjoint from S. (4) An ideal and a filter in a Boolean algebra, disjoint from one another, can be enlarged to an ideal and a filter that are complement (as sets) of one another.
▪ *Boolean prime ideal theorem* is abbreviated as **BPI**. Since the **prime ideal theorem** *for distributive lattices* uses the **axiom of choice**,

ZF+AC implies **BPI**. But there are models of **ZF+BPI** where **AC** fails.
A prime ideal theorem ensures the existence of some types of subsets in a given algebra. An usual example is the Boolean prime ideal theorem (which states that ideals in a Boolean algebra can be extended to prime ideals). A variant of this statement for filters on sets is known as *ultrafilter lemma*. Other theorems result from the use of different mathematical structures with appropriate notions of ideals, for example, rings and prime ideals (of ring theory), or distributive lattices and maximal ideals (of order theory). While the various prime ideal theorems may appear intuitive, they cannot be derived in general from the axioms of Zermelo-Fraenkel set theory without the axiom of choice (abbreviated ZF). Instead, some of the statements are equivalent to the axiom of choice (AC), while others (e.g. Boolean prime ideal theorem) express a property that is strictly weaker than AC. It is due to this intermediate status between ZF and ZF+AC (ZFC) that the Boolean prime ideal theorem is frequently taken as an axiom of set theory.
▪ **Ultrafilter lemma** *is equivalent to* **Boolean prime ideal theorem (BPI**) with the equivalence provable in ZF set theory without the **axiom of choice (AC)**. The underlying idea of its proof is that the subsets of any set form a *Boolean algebra partially ordered by inclusion*, and a*ny Boolean algebra is representable as an algebra of sets.*

Lem. 2. *(Ultrafilter lemma). Every filter on a set S is contained in an ultrafilter on S.*

Or, equivalently: "*Every filter on a set S is a subset of some ultrafilter on S (a maximal filter of nonempty subsets of S).*"

*

Def. 91. *(Banach algebra). A Banach algebra $\mathcal{B}$ is a Banach space, over the field $\mathbb{C}$, with a multiplication law compatible with the norm which turns $\mathcal{B}$ into an algebra. The compatibility with the norm means that it is the case $\forall a, b \in \mathcal{B}$ that the following product inequality holds $\|ab\| \leq \|a\| \, \|b\|$.*

. When we relax Banach space to normed space the analogous structure is called a *normed algebra.*
. A Banach algebra is called "commutative" if its multiplication is commutative", and unital" if it has an identity element for the multiplication whose norm is 1.
. Banach algebra $\mathcal{B}$ (whether it has an identity element or not) can be embedded isometrically into a unital Banach algebra $\mathcal{B}_e$ so as to form a closed ideal of $\mathcal{B}_e$.
The *algebra of* **bounded operators** on a Banach space is a **Banach algebra** for the operator norm.

*

In functional analysis, the concept of the *spectrum* of a (bounded) operator is a generalisation of the concept of eigenvalues for matrices.

Def. 92. *(Spectrum). If T is a linear operator of a normed space X to itself and I is the identity transformation $(I(x) \equiv x)$, the spectrum of T consists of all scalars λ for which either $T - \lambda I$ has no inverse or the range of $T - \lambda I$ is not dense in X.*

Def. 93. *(Spectral radius) For the spectrum of an operator, this is the least upper bound of the set of all $|\lambda|$, where λ is in the spectrum.*

Def. 94. *(Spectral radius)'. If V is a vector space (over $\mathbb{C}$), the spectrum of a linear map $T : V \to V$ is the set*

$$\sigma(T) = \{\lambda \in \mathbb{C} : T - \lambda I \text{ is not invertible}\},$$

where I denotes the identity map. If V is finite dimensional, the ***spectrum*** *of T is precisely the* ***set of its eigenvalues****. For infinite dimensional spaces this is not generally true, although it is true that each eigenvalue of T belongs to $\sigma(T)$.* ***Spectral radius*** *of T is*

$$\rho(T) = \sup\{|\lambda| : \lambda \in \sigma(T)\}.$$

More generally, the ***spectrum*** *and* ***spectral radius*** *can be defined for* ***Banach algebras with identity element****: If $\mathcal{B}$ is a Banach algebra over $\mathbb{C}$ with identity element e, the spectrum of an element $a \in \mathcal{B}$ is the set*

$$\sigma(a) = \{\lambda \in \mathbb{C} : a - \lambda e \text{ is not invertible in } \mathcal{B}\}.$$

Spectral radius of a is $\rho(a) = \sup\{|\lambda| : \lambda \in \sigma(a)\}$.

Spectral theorems: Spectral theorems enable detailed study of various types of operators on Banach spaces by giving an integral or series representation of the operator in terms of its spectrum, eigenspaces, and simple projectionlike operators.

Def. 95. *(Operator spectrum - in separable Hilbert space). Let T be a linear operator on a separable Hilbert space. The spectrum $\sigma(T)$ of T is the set of λ such that $(T - \lambda I)$ is not invertible on all of the Hilbert space, where the λ are complex numbers and I is the identity operator. The definition can also be expressed in terms of the resolvent of an operator $\rho(T) = (\lambda : (T - \lambda I)$ is invertible), and thus the spectrum is defined to be the complement of $\rho(T)$ in the complex plane. ($\rho(T)$ is an open set, and thus the spectrum $\sigma(T)$ is closed.)*

Def. 96. *(Separable space). A separable space is a topological space which has a countable subset that is* ***dense****.*

An example is the Euclidean space $\mathbb{R}^n$ with the Euclidean topology, since it has the rational lattice $\mathbb{Q}^n$ as a countable dense subset and it is easy to show that every open n-ball contains a point whose coordinates are all rational.

Separable: adj. (of a topological space) containing a countable dense subset. Every compact metric space or space is separable, as is Euclidean space since it contains the rational n-tuples, which are countable and dense.

Dense: adj. (of a set in a topology) having a closure that contains a given set. More simply, one set is dense in another if the second is contained in the closure of the first; e.g. the rationals $\mathbb{Q}$ are dense in the reals $\mathbb{R}$, since the latter are contained in the closure of the former.

Closure: The topological closure of a subset A of a topological space X is the smallest closed subset of X containing A.

8.2. Hahn-Banach theorem. The first general formulation, emphasized here, is particularly interesting since not involving any particular formalism and allowing immediate understanding; The second formulation uses a classic formalism for "real" and "complex" cases.

▪ **A 1st general formulation of the theorem.**

Th. 14. (**Hahn-Banach th.**). *A linear functional defined on a subspace of a vector space V and which is dominated by a sublinear function defined on V has a linear extension which is also dominated by the sublinear function.*

▪ **A 2nd general formulation of the theorem.**
We have previously mentioned that *all of the bounded linear functionals on a Hilbert space are just the scalar products*, but we may wonder whether Banach spaces which are not Hilbert spaces have any non-zero bounded linear functionals at all. To this end, take for example the simplest case possible; given X a Banach space, and $x_0 \neq 0$ a fixed element of X. The set of all elements of the form αx_0 forms a subspace X_0 of X. Do there exist bounded linear functionals on X_0. One candidate is

$$F(\alpha x_0) = \alpha,$$

clearly, this is a linear functional and is also bounded since

$$|F(\alpha x_0)| = |\alpha| = \tfrac{\|\alpha x_0\|}{\|x_0\|}.$$

Thus there are bounded linear functionals on such subspaces. If we could only extend them to the whole of X we would have what we want; but difficulties appear. Besides the difficulty of how extend a bounded linear functional to larger subspaces, we have to know if the norm of the functional is increased in doing so, and what happens if we need an infinite number of steps to complete the procedure. The answers to these questions are given by the Hahn-Banach theorem (Theorem [**I**] below).

Before stating the theorem, let us introduce a sublinear functional: Let V be vector space. A functional $p(x)$ on V is called *sublinear* if

(1) $\quad p(x + y) \leq p(x) + p(y),\ x, y \in V,$
(2) $\quad p(\alpha x) = \alpha p(x),\ x \in V, \alpha > 0.$

Note that the norm in a norm vector space is a sublinear functional.

Th. 15. [**I**] (**Hahn-Banach th.**). *Let V be a vector space, and let $p(x)$ be a sublinear functional on V. Let M be a subspace of V, and let $f(x)$ be a linear functional on M satisfying:*

(3) $\quad f(x) \leq p(x),\ x \in M,$

Then there is a linear functional $F(x)$ on the whole of V such that

(4) $\quad F(x) = f(x),\ x \in M,$
(5) $\quad F(x) \leq p(x),\ x \in V.$

Before giving a proof of Hahn-Banach th., let us show how it applies to the case initially set.

Th. 16. (✠). *Let M be a subspace of a normed vector space X, and suppose that $f(x)$ is a bounded linear functional on M. Set*

(6) $\quad \|f\| = \sup_{x \in M, x \neq 0} \frac{|f(x)|}{\|x\|}.$

Then there is a bounded linear functional $F(x)$ on the whole of X such that vector space, and let $p(x)$ be a sublinear functional on V. Let M be a subspace of V, and let $f(x)$ be a linear functional on M satisfying:

(7) $\quad F(x) = f(x),\ x \in M,$
(8) $\quad \|F\| = \|f\|.$

PROOF. Set $p(x)$ is a sublinear functional and $f(x) \le p(x)$, $x \in M$. Then by the Hahn-Banach theorem there is a functional $F(x)$ defined on the whole of X such that (7) holds and $F(x) \le p(x) = \|F\| \cdot \|f\|$, $x \in X$. Since $-F(x) = F(-x) \le \|f\| \cdot \|-x\|$, $x \in X$, we have $|F(x)| \le \|f\| \cdot \|x\|$, $x \in X$. Thus $\|F\| \le \|f\|$. Since F is an extension of f, we must have $\|f\| \le \|F\|$. Hence, (8) holds. □

Since it is now shown that every normed vector space having nonzero elements has a subspace having a nonzero bounded linear functional, it follows that every normed vector space having nonzero elements has nonzero bounded linear functionals. Here is a proof of theorem [I]:

PROOF. It consists of two parts (A) and (B):
(A) First note that the theorem says nothing if $M = V$. Thus we suppose that there is an element x_1 of V which is not in M. Let M_1 be the set of elements of V of the form

(9) $$\alpha x_1 + x,\ \alpha \in \mathbb{R},\ x \in M.$$

Then we check easily that M_1 is a subspace of V and that the representation (9) is unique. Now let us consider the less ambitious task of extending f to M_1 so as to preserve (3). If such an extension F exists on M_1, it must satisfy $F(\alpha x_1 + x) = \alpha F(x_1) + F(x) = \alpha F(x_1) + f(x)$. Thus, F is completely determined by the choice of $F(x_1)$. Moreover, we must have:for all scalars α and $x \in M$:

(10) $$\alpha F(x_1) + f(x) \le p(\alpha x_1 + x).$$

If $\alpha > 0$, this means $F(x_1) \le \frac{1}{\alpha}(p(\alpha x_1 + x) - f(x)) = p(x_1 + \frac{x}{\alpha}) - f(\frac{x}{\alpha}) = p(x_1 + z) - f(z)$, where $z = \frac{x}{\alpha}$. If $\alpha < 0$, we have $F(x_1) \ge \frac{1}{\alpha}(p(\alpha x_1 + x) - f(x)) = f(y) - p(-x_1 + y)$, where $y = -\frac{x}{\alpha}$. Thus, we need for all $y, z \in M$:

(11) $$f(y) - p(y - x_1) \le F(x_1) \le p(x_1 + z) - f(z).$$

Conversely, if we can select $F(x_1)$ to satisfy (11), then for $\alpha > 0$, we have $\alpha F(x_1) + f(x) = \alpha(F(x_1) + f(\frac{x}{\alpha})) \le \alpha p(x_1 + \frac{x}{\alpha}) = p(\alpha x_1 + x)$, and for $\alpha < 0$ we have $\alpha F(x_1) + f(x) = -\alpha(-F(x_1) + f(-\frac{x}{\alpha})) \le -\alpha p(-x_1 - \frac{x}{\alpha}) = p(\alpha x_1 + x)$. Thus, we have now reduced the problem to finding a value of $F(x_1)$ to satisfy (11). In order for such a value to exist, we must have for all $y, z \in M$:

(12) $$f(y) - p(y - x_1) \le p(x_1 + z) - f(z).$$

In other words we need: $f(y + z) \le p(x_1 + z) + p(y - x_1)$. This is true by (3) and property (1) of a sublinear functional. Hence, (12) holds. If we fix y and let z run through all elements of M, we get $f(y) - p(y - x_1) \le \inf_{z \in M}(p(x_1 + z) - f(z)) \equiv C$. Since this is true for any $y \in M$, we have

$$c \equiv \sup_{y \in M}(f(y) - p(y - x_1)) \le C.$$

We now select $F(x_1)$ to satisfy

$$c \le F(x_1) \le C.$$

Note that the extension F is unique only when $c = C$. Thus, we have been able to extend f from M to M_1 in the desired way. If $M_1 = V$, we are finished. Otherwise there is an element x_2 of V not in M. Let M_2 be the space "spanned" by x_2 in M_1. By repeating the process we can extend f to M_2 in the sought way. If $M_2 \ne V$. We get a sequence M_k of subspaces each containing the preceding and such that f can be extended from one to the next. If, finally, we reach a k such that $M_k = V$, we are finished. Even if,

(13) $$V = \bigcup_{k=1}^{\infty} M_k,$$

then we are through since each $x \in V$ is in some M_k, and we can define F by induction. But what if (13) does not hold? We can complete the proof easily when V is a Hilbert space and $p(x) = \gamma \|x\|$ for some positive constant γ. For then we can extend f to the closure $\overline{M}$ of M by continuity. By this we mean that if $\{x_n\}$ is a sequence of elements in M which converges to $x \in V$, then $\{f(x_n)\}$ is a Cauchy sequence of real numbers and hence has a limit. We then define $F(x) = \lim f(x_n)$. The limit is independent of the sequence chosen. We chek easily that $F(x)$ is a bounded linear functional on the set $\overline{M}$ and coincides with $f(x)$ on M. Since $\overline{M}$ is a Hilbert space, there is an element $y \in \overline{M}$ such that $F(x) = (x, y)$ (scalar product) for all $x \in \overline{M}$ (Hahn-Banach theorem [I]). Moreover, $\|y\| = \|f\| \le \gamma$. But $F(x)$ can be defined as (x, y) on the whole of V, and its norm will not be increased.
What do we do when the space V is *not a Hibert space* and (13) does not hold? This is not a trivial situation. In this case we need a statement known as Zorn's lemma concerning **maximal elements** (see def.) of chains in partially ordered sets. **Zorn's lemma** is *equivalent* to the **axiom of choice (AC)**. The proof of the Hahn-Banach theorem for those spaces that requires Zorn's lemma in the second part below:
(B) Remember the definitions of a *partially ordered set* and a *maximal element* (see "*Prerequisites*"). Now consider the collection S of all *linear functionals* g defined on subspaces $D(g)$ of V such that
.$D(g) \supset M$,
.$g(x) = f(x)$, $x \in M$,
.$g(x) \le p(x)$, $x \in D(g)$.
Introduce a *partial order* in S by: If $D(g_1) \subset D(g_2)$ and $g_1(x) = g_2(x)$ for $x \in D(g_1)$, then write $g_1 \preccurlyeq g_2$. Now consider the following **Zorn's lemma** which is equivalent to the axiom of choice (AC):
Zorn's lemma: "*If S is a partially ordered set such that each totally ordered subset has an upper bound in S, then S has a maximal element.*"
If we can show that every totally ordered subset of S has an upper bound, it will follow from the above *Zorn's lemma* that S has a maximal element F. We claim that F is the sought functional. In fact, we must have $D(F) = V$. Otherwise, we have shown in the proof of theorem [I] that there would be an $h \in S$ such that $F \preccurlyeq h$ and $F \ne h$ (for we can take a vector $x \notin D(F)$ and extend F to $D(F) \oplus \{x\}$). This would violate the maximality of F. Hence, $D(F) = V$, and F satisfies the stipulations of the theorem. Thus, it remains to show that every totally ordered subset of S has an upper bound. Let W be a totally ordered subset of S. Define the functional h by

$$D(h) = \bigcup_{g \in W} D(g)$$
$$h(x) = g(x),\ g \in W,\ x \in D(g).$$

This definition is not ambigious, for if g_1 and g_2 are any elements of W, then either $g_1 \preccurlyeq g_2$ or $g_2 \preccurlyeq g_1$. At any rate, if $x \in D(g_1) \cap D(g_2)$, then $g_1(x) = g_2(x)$. Clearly, $h \in S$. Hence, it is an upper bound for W, and the proof is complete. □

Th. 17. [**II**] (**Complex Hahn-Banach th.**). *Let V be a complex vector space, and let p be a real-valued functional on V such that*
(*i*) $$p(u + v) \le p(u) + p(v),\ u, v \in V,$$
(*ii*) $$p(\alpha u) = |\alpha|\, p(u),\ \alpha \text{ complex},\ u \in V.$$
Assume that there exists a linear subspace M of V and a linear (complex-valued) functional f on M such that
(1) $$\operatorname{Re} f(u) \le p(u),\ u \in M.$$
Then there is a linear functional F on the whole of V such that
(2) $$F(u) = f(u),\ u \in M,$$
(3) $$|F(u)| \le P(u),\ u \in V.$$

PROOF. Let us try to reduce the complex case to the real case. To be sure, we can consider V as a real vector space by allowing multiplication by real scalars only. If we do this, M becomes a subspace of a real vector space V. Next, we can define the real-valued functional $f_1(u) = \operatorname{Re} f(u)$, $u \in M$. Then, by (1), we have

$$f_1(u) \le p(u),\ u \in M.$$

We can now apply the "real" Hahn-Banach theorem [I] to conclude that there is a real functional $F_1(u)$ on V such that

$$F_1(u) = f_1(u),\ u \in M,$$
$$F_1(u) \le p(u),\ u \in V.$$

But we wanted to extend the whole of f, *not just its real part.* The *key* is that there is a connection between the real and imaginary part of a linear functional on a complex vector space. In fact,

$$f_1(iu) = \operatorname{Re} f(iu) = \operatorname{Re} if(u) = -\operatorname{Im} f(u).$$

Hence, $f(u) = f_1(u) - if_1(iu)$. This suggests a candidate for $F(u)$. Set

$$F(u) = F_1(u) - iF_1(iu),\ u \in V.$$

$F(u)$ is clearly linear if real scalars are used. To see that it is linear in the complex sense, note that
$F(iu) = F_1(iu) - i\,F_1(-u) = i[F_1(u) - iF_1(iu)] = iF(u)$.
Note also that $F(u) = f(u)$ for $u \in M$. To complete the proof we must show that (3) holds. Note that

$$p(u) \ge 0,\ u \in V.$$

In fact, by (*ii*) we see that $p(0) = 0$, while by (*i*) we see that $p(0) \le p(u) + p(-u) = 2p(u)$. Hence, (3) holds whenever $F(u) = 0$. If $F(u) \ne 0$, we write it in polar form $F(u) = |F(u)|\, e^{i\theta}$. Then $|F(u)| = e^{-i\theta} F(u) = F(e^{-i\theta} u) = F_1(e^{-i\theta} u) \le p(e^{-i\theta} u) = p(u)$. This completes the proof. □

A corollary of theorem [II] is:

Cor. 2. *Let M be a subspace of a complex normed vector space X. If f is a bounded linear functional on M, then there is a bounded linear functional F on X such that*

$$F(x) = f(x),\ x \in M,$$
$$\|F\| = \|f\|.$$

(This follows from th.[II] as in the real case.)

▪ **Consequences of Hahn-Banach theorem.** Hahn-Banach theorem is one of the most important theorems in functional analysis and has many far-reaching consequences. Here is one of them:

Th. 18. [A]. *Let X be a normed vector space and let $x_0 \ne 0$ be an element of X. Then there is a bounded linear functional $F(x)$ on X such that $\|F\| = 1$, $F(x_0) = \|x_0\|$.*

PROOF. Let M be the set of all vectors of the form αx_0. Then M is a subspace of X. Define f on M by $f(\alpha x_0) = \alpha \|x_0\|$. Then f is linear, and $|f(\alpha x_0)| = |\alpha| \cdot \|x_0\| = \|\alpha x_0\|$. Thus, f is bounded on M, and $\|f\| = 1$. By the Hahn-Banach theorem, there is a bounded linear functional F on X such that $\|F\|=1$, and $F(\alpha x_0) = \alpha \|x_0\|$. □

Cor. 3. *If x_1 is an element of X such that $f(x_1)=0$ for every bounded linear functional f on X, then $x_1=0$.*

PROOF. This corollary is an immediate consequence of the previous theorem. If $x_1 \neq 0$, there would be a bounded linear functional F on X such that $F(x_1) = \|x_1\|$. Thus, $x_1 = 0$. □

Another consequence of theorem (✠) is:

Th. 19. [B]. *Let M be a subspace of a normed vector space X, and x_0 an element of X satisfying*

(∗) $$d = d(x_0, M) = \inf_{x\in M} \|x_0 - x\| > 0.$$

Then there is a bounded linear functional F on X such that $\|F\| =1$, $F(x_0)=d$, and $F(x)=0$ for $x\in M$.

PROOF. If M_1 is the set of all elements $z\in X$ written

(∗∗) $$z = \alpha x_0 + x,\ \alpha \in \mathbb{R},\ x \in M.$$

Define the functional f on M_1 by $f(z) = \alpha d$. Now the representation (∗∗) is unique, for if $z = \alpha_1 x_0 + x_1$, we have $(\alpha - \alpha_1)x_0 = x_1 - x \in M$, which contradicts (∗) unless $\alpha_1 = \alpha$ and $x_1 = x$. Thus, f is well defined and linear on M_1. It also vanishes on M. And it is bounded on M_1, since $|f(\alpha x_0 + x)| = |\alpha| d \leq |\alpha| \cdot \left\|x_0 + \frac{x}{\alpha}\right\| = \|\alpha x_0 + x\|$. Hence, f is a bounded linear functional on M_1 with $\|f\| \leq 1$. However, $\forall \varepsilon > 0$ we can find an $x_1 \in M$ such that $\|x_0 - x_1\| < d+\varepsilon$. Then $f(x_0 - x_1) = d$, and hence,

$$\frac{|f(x_0-x_1)|}{\|x_0-x_1\|} > \frac{d}{d+\varepsilon} = 1 - \frac{\varepsilon}{d+\varepsilon},$$

which is as close to one as we like. Hence, $\|f\|=1$. We now apply theorem (✠) to conclude that there is a bounded linear functional F on X such that $\|F\|=1$ and $F=f$ on M_1. This completes the proof. □

Th.[B] is a weak substitute in general Banach spaces for *Projection th.* (cf. corollary (◊) of projection th. in "*Prerequisites*") in Hilbert space.

For any normed vector space X, let X^* denote the set of bounded linear functionals on X. If $f, g \in X^*$ we say that $f = g$ if $f(x) = g(x)$ for all $x \in X$. The "zero" functional is the one assigning zero to all $x \in X$. We define $h = f + g$ by $h(x) = f(x) + g(x)$, $x \in X$, and $g = \alpha f$ by $g(x) = \alpha f(x)$, $x \in X$, Under these definitions, X^* becomes a vector space. We have been employing the expression

(¥) $$\|f\| = \sup_{x\neq 0} \frac{|f(x)|}{\|x\|},\ f \in X^*.$$

This is easily seen to be a norm. In fact

$$\sup \frac{|f(x)+g(x)|}{\|x\|} \leq \sup \frac{|f(x)|}{\|x\|} + \frac{|g(x)|}{\|x\|}.$$

Thus X^* is a normed vector space. It is thus natural to ask when X^* is complete; an answer is:

Th. 20. [C]. *X^* is a Banach space whether or not X is.*

PROOF. Let $\{f_n\}$ be a Cauchy sequence in X^*. Thus $\forall \varepsilon > 0$ there is an N such that $\|f_n - f_m\| < \varepsilon$ for $m, n > N$, or, equivalently:

(†) $$\|f_n(x) - f_m(x)\| < \varepsilon \|x\|,\ m,n>N,\ x\in X,\ x\neq 0.$$

Thus for each $x \neq 0$, $\{f_n(x)\}$ is a Cauchy sequence of real numbers, and hence has a limit c_x depending on x. Define $f(x) = c_x$. Clearly f is a functional on X. It is linear, since $f(\alpha_1 x_1 + \alpha_2 x_2) = \lim f_n(\alpha_1 x_1 + \alpha_2 x_2) = \lim\{\alpha_1 f_n(x_1) + \alpha_2 f_n(x_2)\} = \alpha_1 f(x_1) + \alpha_2 f(x_2)$. It is also bounded. For let n be fixed in (†), and let $m \to \infty$ Then have

(‡) $$\|f_n(x) - f(x)\| \leq \varepsilon \|x\| \text{ for } n>N,\ x\in X.$$

Hence $|f(x)| \leq \varepsilon \|x\| + |f_n(x)| \leq (\varepsilon + \|f_n\|) \|x\|$ for $n > N$, $x \in X$. Hence, $f \in X^*$. But we are not finished. We must show that f_n approaches f in X^*. For this we use (‡). It gives $\|f_n - f\| \leq \varepsilon$ for $n > N$. Since ε was arbitrary, the result follows. □

Now, here is an interesting counterpart of the expression (¥). From it we see that $|f(x)| \leq \|f\| \cdot \|x\|$, and hence

$$\|x\| \geq \sup_{f\in X^*, f\neq 0} \frac{|f(x)|}{\|f\|}.$$

But by theorem [A], for each $x \in X$ there is an $f \in X^*$ such that $\|f\| = 1$ and $f(x) = \|x\|$. Hence,

$$\|x\| = \max_{f\in X^*, f\neq 0} \frac{|f(x)|}{\|f\|}.$$

▪**Hahn-Banach theorem and axiom of choice (AC)** The axiom of choice implies the Hahn-Banach theorem. The converse is not true. This can be seen by noting that the ultrafilter lemma (or equivalently, Boolean prime ideal theorem), which is strictly weaker than the axiom of choice, can be used to show the Hahn-Banach theorem, although the converse is not the case. Boolean prime ideal theorem is easily seen to be equivalent to the statement that there are always *probability charges* that take only the values 0 and 1.

In ZF, we can show that the Hahn-Banach theorem is sufficient to derive the existence of a non-Lebesgue measurable set. Moreover, the Hahn-Banach theorem implies the *Banach-Tarski paradox* (see heading "*Banach-Tarski paradox and ZF*").

▪**Bounded variation and dual space $C[a,b]^*$.** Another consequence of the theorem is the following proposition: "*Let $-\infty<A<B<\infty$. Then $F \in C[a,b]^*$ iff there is a function $\rho : [a,b] \to \mathbb{R}$ of* ***bounded variation*** *such that $\forall u \in C[a,b]$, $F(u)=\int_a^b u(x)\mathrm{d}\rho(x)$. Moreover, $|F|=\mathcal{V}(\rho)$, where $\mathcal{V}(\rho)$ is the* ***total variation*** *of ρ.*"

8.3. Hahn-Banach separation theorem.

Another version of Hahn-Banach theorem is known as the Hahn-Banach separation theorem or separating hyperplane theorem. It has many uses in convex geometry, optimization theory, and economics. It is derived from the original form of the theorem.

Th. 21. (**Hahn-Banach separation th.**). *Set $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$ and let V be a topological vector space over $\mathbb{K}$. Suppose A and B are convex, non-empty disjoint subsets of V.*

1) *If A is open there exists a* ***continuous linear map*** *$\Lambda : V \to \mathbb{K}$ and $\gamma \in \mathbb{R}$ such that $\forall a \in A, \forall b \in B$*

$$\mathrm{Re}(\Lambda(a)) < \gamma \leq \mathrm{Re}(\Lambda(b)).$$

2) *If V is locally convex, A is compact, and B closed, then there exists a* ***continuous linear map*** *$\Lambda : V \to \mathbb{K}$ and $\gamma_1, \gamma_2 \in \mathbb{R}$ such that $\forall a \in A, \forall b \in B$*

$$\mathrm{Re}(\Lambda(a)) < \gamma_1 < \gamma_2 < \mathrm{Re}(\Lambda(b)).$$

Knowing that "*the* **dual space** *of a topological vector space V is the vector space V^* whose elements are the* **continuous linear functionals** *on V*," we can reformulate the Hahn-Banach separation theorem according to Rudin (1991) as follows:

Th. 22. *(Hahn-Banach separation th.)'. Suppose A and B are disjoint, nonempty, convex sets in the topological vector space V.*

1) *If A is open there exists $\Lambda \in V^*$ and $\gamma \in \mathbb{R}$ such that $\forall x \in A, \forall y \in B$, $\mathrm{Re}(\Lambda(x)) < \gamma \leq \mathrm{Re}(\Lambda(y))$.*

2) *If A is compact, B is closed, V is locally convex, then there exist $\Lambda \in V^*$ and $\gamma_1, \gamma_2 \in \mathbb{R}$ such that $\forall x \in A, \forall y \in B$, $\mathrm{Re}(\Lambda(x)) < \gamma_1 < \gamma_2 < \mathrm{Re}(\Lambda(y))$.*

Note, here, that this is stated without specifying the scalar field; if it is $\mathbb{R}$, then $\mathrm{Re}\,\Lambda = \Lambda$ of course.

Cor. 4. *If V is a locally convex space then V^* separates points on V.*

Th. 23. *Suppose M is a subspace of a locally convex space V, and $x_0 \in V$. If x_0 is not the closure (cf. below) of M, then there exists $\Lambda \in V^*$ such that $\Lambda x_0 = 1$ but $\Lambda x = 0$, $\forall x \in M$.*

Th. 24. *If f is a continuous linear functional on a subspace M of a locally convex space V, then there exists $\Lambda \in V^*$ such that $\Lambda = f$ on M.*

Here is the geometric form of Hahn-Banach th.:

Th. 25. (**Hahn-Banach th. - Geometric form**). *Let E be a locally convex space, $A, B \subset E$ two convex, nonempty and disjoint sets. Suppose that A is closed and B is compact. Then there is a hyperplane which strictly separates A and B.*

∗

Compact space: A topological space which is a compact set.

Compact set: A set in a topological space with the property that every open cover has a finite subset which is also a cover. Also known as bicompact set.

Cover: **1.** An element x of a partially ordered set covers another element y if x is greater than y, and the only elements that are both greater than or equal to y and less than or equal to x are x and y themselves. **2.** See covering (cover).

Covering (cover): For a set E, a cover is a collection of sets whose union contains E. Also known as cover.

Disjoint sets: Sets with no elements in common.

Convex set: A set which contains the entire line segment joining any pair of its points.

Closed set: A set of points which contains all its *cluster points* (also called *limit points, accumulation points*). A closed set is the complement of an *open set* in a metric space.

Cluster point: A cluster point of a set in a topological space is a point p whose neighborhoods all contain at least one point of the set other than p. Also known as *accumulation point*; *limit point*.

Closure: **1.** The union of a set and its cluster points; the smallest closed set containing the set. **2.** Property of a mathematical set such

that a specified mathematical operation that is applied to elements of the set produces only elements of the same set.
The closure of an open set A is obtained by including in it all limit points (cluster points) of the set A. If A is the set $\{x : 1 < x < 2, x \in \mathbb{R}\}$ then the closure of A would include 1 and 2 as the limit point, giving $\{x : 1 \leqslant x \leqslant 2, x \in \mathbb{R}\}$.
Topological space: A set endowed with a topology.

Topology: A topology is a geometry of transformations in which the only invariant is continuity.

Open set: A set included in a *topology*; equivalently, a set which is a neighborhood of each of its points; a *topology* on a space is determined by a collection of subsets which are said open. The complement of an open set is a closed set.

Chapter 3

Relations and Structures

1. Relations

The notion of relation can be broached via the notions of property of object, predicate, binary relation, correspondence between sets, graph of a correspondence, and cartesian product.
. We already had the opportunity (for example in the sections *"Mathematical Logic"* and "*Set Theory*") to manipulate properties $P(x)$ involving only one unknown object x on which is based the analysis of "predicates"; for example $x \in E$, ($x = a$ or $x = b$), etc. We can also considered properties $R(x, y)$ involving *two* unknown objects x and y, for example $x < y$, $x \in y$, $x \subset y$, $x \equiv y \,(\mathrm{mod}\, 9)$, etc; or also properties $R(x_1, .., x_n)$ involving *several* unknown objects $(x_1, .., x_n)$, for example "the integers $x_1, .., x_n$ are relatively primes in their set". We are interested in properties of the form $R(x, y)$ that we call *binary relations*. Examples of such relations are $x = y$, $x \in y$ and $x \subset y$. However, just as the axiom of separation concerns a predicate $P(x)$ defined (as a relation) on a set, we distinguish the relations $R(x, y)$ which make sense only when x is element of a certain set E and y is element of a certain set F. A relation between elements of E and elements of F is called *correspondence* between E and F; (e.g. the relation $y{=}f(x)$ when f is a map from E to F, but also the relation $x{=}g(y)$ when g is a map from F to E and even the relation $\phi(x, y){=}0$ when ϕ is a map from $E \times F$ to $\mathbb{R}$ for example.)

Def. 97. *(Graph of a correspondence). The graph of the correspondence $R(x, y)$ between E and F is the set: $\Gamma_R := \{(x, y)|R(x, y)\}$.*

For example, the graph of the correspondence $y = f(x)$ is the graph Γ_f of the map f. Conversely, for every part $G \subset E \times F$, we can define a correspondence between E and F whose graph is G: it suffices to take for $R(x, y)$ the relation $(x, y) \in G$.
. The more useful binary relations concern the elements x and y of a same set E; they are called *binary relation on E*. If F is a part of E, the *relation induced* by R on E is simply the relation $R(x, y)$ between elements of F. Moreover, we can start from an arbitrary binary relation between objects of same nature (for example $x \subset y$) and consider the relation induced on a set (for example $\mathfrak{P}(E)$).
Generally, for a binary relation $R(x, y)$ on a set E, the "infix notation" xRy is often used, instead of $R(x, y)$; as examples, we know the relations $x \leqslant y$ and $x < y$ on $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$, the relation $x|y$ ("x divides y") on $\mathbb{N},\mathbb{Z}$, or even the ring $K[X]$ of polynomials over the field K, the relation $x \subset y$ on $\mathfrak{P}(E)$, etc.

Def. 98. *Let R be a binary relation on a set E.*
(1) *The relation R is reflexive if $\forall x \in E$, xRx.*
(2) *The relation R is transitive if $\forall x, y, z \in E$, (xRy and yRz) $\Rightarrow xRz$.*
(3) *The relation R is symmetric if $\forall x, y \in E$, $xRy \Rightarrow yRx$.*
(4) *The relation R is antisymmetric if $\forall x, y{\in}E$, (xRy and yRx)$\Rightarrow x{=}y$.*
An equivalence relation is a reflexive, transitive and symmetric relation.
An order relation is a reflexive, transitive and antisymmetric relation.

Above, these notions were defined for binary relations on a set, but they easily extend to arbitrary relations $R(x, y)$; e.g. we can state that the relation $x = y$ is an equivalence relation and that the relation $x \subset y$ is an order relation, without the need to specify a set of reference.

Ex. 20. (1) *The relations of equality (on any arbitrary set) and of congruence modulo a (on $\mathbb{Z}$) are equivalence relations.* (2) *The relation $\leqslant$ on $\mathbb{R}$, $\subset$ on $\mathfrak{P}(E)$, and $|$ (divisibility) on $\mathbb{N}$ are order relations.* (3) *The only relation that are, at the same time, of order and of equivalence is the equality.*

We immediately check that the relation induced on (a set) E by a reflexive (resp. transitive, symmetric, antisymmetric, equivalence, order) relation is itself a relation (resp. transitive, symmetric, antisymmetric, equivalence, order). Equivalence relations, and order relations will be study in specific headings.
. The notion of *relations* is based on the *Cartesian product of sets*. Relations establish links between elements belonging to a same set or between elements belonging to different sets. From these relations we can construct *maps* and *structures* for sets. Let's give a first definition of a Cartesian product:

Def. 99. *(Cartesian product). In reference to the product of X and Y, the set $X \times Y$ of all pairs (x, y), where x belongs to X and y belongs to Y.*

1.1. Cartesian product, relations. When the order of two elements x_1, x_2 is involved, the notion of pair is used (x_1, x_2), where x_1 is the first component of the pair and x_2 is the second. The *equality of two pairs* is defined by:

Def. 100. $(x_1, x_2) = (y_1, y_2) :\Leftrightarrow x_1 = y_1 \wedge x_2 = y_2$.

In set theory, a *pair* is defined by $(x_1, x_2) \neq \{x_1, x_2\}$ but $(x_1, x_2) := \{\{x_1\}, \{x_1, x_2\}\}$ verifies the definition of the equality of two pairs.
Before giving a definition of the Cartesian product of sets, we need to consider the object $(x_1, .., x_n)$, which is an extension to n of the pair (i.e. n-tuple), it can be seen as the generalization of a pair, and can be written by induction (i.e.by recurrence) $(x_1, .., x_n) := ((x_1, .., x_{n-1}), x_n)$. Then the equality of two pairs mentioned above, can be extended, for $(x_1, .., x_n)$ and $(y_1, .., y_n)$, to an equality of their components having same index.

Def. 101. *(Cartesian product). $S_1 \times \cdots \times S_n := \{(x_1, .., x_n)|x_i \in S_i\}$ is called Cartesian product of sets $S_1, ..., S_n$. Specifically, if $S_1 = S_2 \cdots = S_n = S$, we can write S^n. (Fig.).*

The *Cartesian product is used to define* new mathematical objects and the *notion of relation* (Fig.).

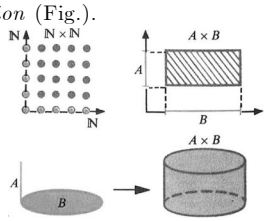


Fig. Cartesian product.

Def. 102. *(Binary relation)′. A binary relation on a set S is as a subset R of the Cartesian product $S \times S$. Thus, we can say that, for a given ordered pair (a, b) either $(a, b) \in R$ or $(a, b) \notin R$.*

But it is more natural to denote a relation by a symbol such as $\sim$ placed between a and b, where $\sim$ stands for the words "is related to". The letter R taken as a subset in the above def. of a binary relation can be considered as "$a\ R\ b$", meaning that "a is related to b". If this notation is used, the set $\{(a, b)|(a, b) \in S \times S$ and $a\ R\ b\}$ may be called the *graph* of R (the graph represents the relation).
The above def. of a binary relation implicitly was a particular case concerning a single set $S : R \subseteq S \times S$. We can extend the case considering a binary relation on the sets S_1 and S_2, with the elements x_1, x_2, then $R \subseteq S_1 \times S_2$ where R means, as before: "..is related to..", in this case it means that "x_1 is related to x_2", i.e. "$x_1\ R\ x_2$" which replaces $(x_1, x_2){\in}R$. The binary relations $R \subseteq S_1 \times S_2$ are fundamental and can be taken as a *correspondence*, where - according to a determined criterion - elements of S_2 correspond to elements of S_1.

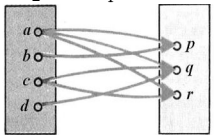


Fig. Graph of binary relation. $S_1{=}\{a, b, c, d\}$; $S_1{=}\{p, q, r\}$, ". is related to .".

A binary relation on the sets S_1, S_2, is defined by:

Def. 103. *(Binary relation)″. A binary relation on the sets S_1, S_2, is as a subset R of the Cartesian product $S_1 \times S_2$. Thus, we can say that, for a given ordered pair (x_1, x_2) either $(x_1, x_2){\in}R$ or $(x_1, x_2) \notin R$.*

Ex. 21. *(Binary relation). Familiar examples can be written: "$<$" can be a binary relation on the set of integers; "$\subseteq$" a relation of inclusion between the parts of a set and can also be a binary relation on*

the set of straight lines in the plane; "$\perp$" can be the orthogonality in the set of straight lines of an Euclidian space; "=" is the relation of equality; "$\leqslant$" is an ordering relation in $\mathbb{N}$ (Fig.).

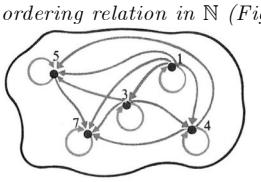


Fig. S=$\{1,3,4,5,7\}$; Equality relations (small loops); ordering relations (other loops).

The above definitions of a binary relation are similar to the following:

Def. 104. *(Binary relation)'''. All subsets $R \subseteq S_1 \times S_2$ is called a binary relation.*

Def. 105. *(Ternary relation). All subsets $R \subseteq S_1 \times S_2 \times S_3$ is called a ternary relation.*

Def. 106. *(n-ary relation). All subsets $R \subseteq S_1 \times \cdots \times S_n$ is called a "n-ary" relation.*

1.2. Properties of binary relations. ▪ Properties of $R \subseteq S_1 \times S_2$:
(1): R left surjective :$\Leftrightarrow \forall x_1 \exists x_2 (x_1 R x_2)$
(2): R right surjective :$\Leftrightarrow \forall x_2 \exists x_1 (x_1 R x_2)$
(3): R doubly surjective :$\Leftrightarrow$ (1) $\wedge$ (2)
(4): R injective :$\Leftrightarrow \forall x \forall y \forall z (xRy \wedge zRy \Rightarrow x{=}z)$
(5): R univocal :$\Leftrightarrow \forall x \forall y \forall z (xRy \wedge xRz \Rightarrow y{=}z)$
(6): R bijective (or biunivocal) :$\Leftrightarrow$ (3) $\wedge$ (4) $\wedge$ (5)
▪ Properties of $R \subseteq S \times S$:
(7): R reflexive :$\Leftrightarrow \forall x (xRx)$
(8): R symmetric :$\Leftrightarrow \forall x \forall y (xRy \Rightarrow yRx)$
(9): R asymmetric :$\Leftrightarrow \forall x \forall y (xRy \Rightarrow \neg(yRx))$
(10): R antisymmetric :$\Leftrightarrow \forall x \forall y (xRy \wedge yRx \Rightarrow x{=}y)$
(11): R total :$\Leftrightarrow \forall x \forall y (xRy \vee yRx)$
(12): R transitive :$\Leftrightarrow \forall x \forall y \forall z (xRy \wedge yRx \Rightarrow xRz)$

1.3. Equivalence relation, quotient set. 1) Equivalence relation.

Def. 107. *(Equivalence relation). A relation $\mathfrak{R} \subseteq S \times S$ is called an equivalence relation, if and only if, this relation is reflexive, symmetric and transitive.*

An equivalence relation on a set induces a *partition* on it, and any partition induces an equivalence relation. Equivalence relations are essential, because in many cases the *set* can be "transformed" into another set, which is called "*quotient space*", considering each *equivalence class* as a *single unit*. Any equivalence relations splits up S into nonempty *pairwise disjoint subsets*, i.e, *a partition of S into equivalence classes.*

Ex. 22. *The relation of logical equivalence on statements in first-order logic. The relation "is isomorphic to" on models of a set of sentences. The relation "has the same image under a function" on the elements of the domain of the function. Parallelism of two straight lines in an affine space. Equipotence of two parts of a set. Green's relations are five equivalence relations on elements of a semigroup.*

Ex. 23. *Other examples:* (1) *On any set S, the equality is an equivalence relation, and this is the strongest (it is contained in all the others). The weakest equivalence relation is the one whose graph is $S \times S$, i.e. the one that is satisfied by all the pairs $(x, y) \in S \times S$.* (2) *The relation $x \equiv y \,(\mathrm{mod}\ a)$ is an equivalence relation in $\mathbb{Z}$. The relation $x \equiv y \,(\mathrm{mod}\ 2\pi)$ is an equivalence relation in $\mathbb{R}$.* (3) *More generally, let G be a commutative group (cf. heading "Group" in "Algebraic Structures"), and let A be a subgroup of G. The relation of congruence modulo A is an equivalence relation. This applies especially to the case where G is a ring and A is an ideal (cf. def. in heading "Ring" in "Algebraic Structures") and to the case where G is a vector space and A a vector subspace.* (4) *In the set $\mathcal{F}(I, \mathbb{R})$ of numerical functions over the open interval I of $\mathbb{R}$, such that $0 \in I$, we define the relation $f\mathcal{R}g$ (for $n \in \mathbb{N}^*$ fixed) by the formula $f = g + o(x^n)$ (cf. Landau notations; and equivalence $\sim$), this is an equivalence relation. Likewise, if we set $f \sim g$ for $f = g + o(g)$, we get another equivalence relation.* (5) *In the set $\mathbb{N} \times \mathbb{N}$, we set $(a, b) \sim (c, d)$ if and only if $a+d{=}b+c$. This an equivalence relation, which can be used to construct the set $\mathbb{Z}$. Likewise, the equivalence relation $(a, b) \sim (c, d)$ if and only if $ad{=}bc$ in the set $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$, which can be used to construct the set $\mathbb{Q}$.* (6) *In planar euclidean geometry, it is improperly said that two triangles ABC and $A'B'C'$ are "equal" if we can move one to make it coincide with the other. We get thus an equivalence relation on all triangles.*

2) Equivalence class.

Def. 108. *(Equivalence class). The set of all the elements of S related to $x \in S$ under a given relation is called the equivalence class $[[x]]$ (or $\mathrm{Cl}(x)$) of x such that $[[x]] = \{z | x \in S \wedge z \in S \wedge xRz\}$.*

Variants of this definition can be given by:

Def. 109. *(Equivalence class)'. Let $\mathfrak{R}$ be an equivalence relation on a set S. We call equivalence class of $x \in S$, denoted $[[x]]$ (or $\mathrm{Cl}(x)$), the set of elements of S equivalent to x: $[[x]] := \{y \in S \,|\, x\mathfrak{R}y\}$. (The relation $\mathfrak{R}$ being reflexive, $x \in [[x]]$.)*

Def. 110. *(Equivalence class)". The equivalence classes are the collection of pairwise disjoint subsets determined by an equivalence relation on a set. Thus, two elements are in the same equivalence class if and only if they are equivalent under the given relation.*

An equivalence class constructs a new set, which is the set of the equivalence classes of S.
The reflexivity of $\mathfrak{R}$ induces that $[[x]] \neq \varnothing$. The symmetry and transitivity guarantee ($[[x]] = [[y]] \Leftrightarrow xRy$) and ($z \in [[x]] \wedge z \in [[y]] \Rightarrow [[x]] = [[y]]$), i.e. each element of S belongs to only one equivalence class. Thus these equivalence classes are pairwise disjoint. More formally, we can write the following proposition (and its proof):

Proposition *(i) Two elements of a set S are equivalent if and only if they have the same class: $\forall x, y \in S,\ x\mathfrak{R}y \Leftrightarrow [[x]] = [[y]]$. (ii) The equivalence classes form a partition of S. In other words, their union is S and they are pairwise disjoint.*

Proof. Suppose $x\mathfrak{R}y$. Given $z \in [[x]]$. Then $x\mathfrak{R}z$ (by definition of $[[x]]$), so $y\mathfrak{R}z$ (by symmetry and transitivity of $\mathfrak{R}$). We have thus proved that $[[x]] \subset [[y]]$. The reverse inclusion is similarly proved, and so we have indeed $[[x]] = [[y]]$. Now, suppose conversely that $[[x]] = [[y]]$. As we have noticed $y \in [[y]]$, so $y \in [[x]]$ (by assumption), so $x\mathfrak{R}y$ by definition of $[[x]]$. which completes the proof of (i). For every x of S, we have $x \in [[x]]$ (which is thus nonempty). The union of equivalence classes contains thus all the elements of S, this is indeed S. Let $[[x]]$ and $[[y]]$ be two equivalence classes. If they are not disjoint, there is $z \in [[x]] \cap [[y]]$, therefore such that $x\mathfrak{R}z$ and $y\mathfrak{R}z$ (by definition of $[[x]]$ and $[[y]]$). By symmetry and transitivity of $\mathfrak{R}$, we have $x\mathfrak{R}y$, so $[[x]]{=}[[y]]$, which completes the proof of (ii). □

Conversely, let $(S_i)_{I \in i}$ be a partition of S. By setting $x\mathfrak{R}y$ when x and y belong to the same subset S_i, we define an equivalence relation for which the equivalence classes are the S_i.

Ex. 24. *If $f : S \to T$ is a map, the relation defined by $x\mathfrak{R}y$ if and only if $f(x) = f(y)$ is an equivalence relation. The class of $x \in S$ is $[[x]] = f^{-1}(f(x))$. Conversely, every equivalence relation $\mathfrak{R}$ can be obtained as follows: we define $f : S \to \mathfrak{P}(S)$ by setting $f(x) = [[x]]$, and we have indeed $x\mathfrak{R}y$ if and only if $f(x) = f(y)$.*

3) Quotient set.

Def. 111. *(Quotient set). $S/\mathfrak{R} = \{[[x]] \,|\, x \in S\}$ is called quotient set of S by $\mathfrak{R}$. An element $y \in [[x]]$ is called a representative of the class $[[x]]$. T is called system of class representatives of $S/\mathfrak{R}$ if T contains exactly an element of each class of $S/\mathfrak{R}$.*

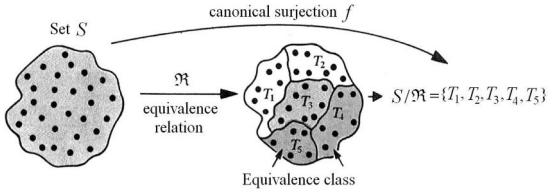


Fig. Quotient set and equivalence relation.

Def. 112. *(System of class representatives). T is called a system of class representatives of $S/\mathfrak{R}$ if T contains exactly one element of each equivalence class of $S/\mathfrak{R}$.*

Quotient set: The quotient set is the set of all the equivalence classes relative to a given equivalence relation on a given set.

Ex. 25. *The common property concerning two parallel straight lines is their direction. The common property relatives to congruent segments (cf. infra) of an Euclidian space is the length.*

Congruence: **1.** The property of geometric figures that can be made to coincide by a rigid transformation (also called *superposability*). **2.** The property of two integers having the same remainder on division by another integer.

$S/\mathfrak{R}$ results from an abstract process: the property allowing to form an equivalence class can identify with this class; the elements of this class losing their proper originality. We can associate with each partition of S a *surjective map* $f : S \to S/\mathfrak{R}$ (*canonical surjection)* (cf. surjective map in heading "*Definition of a map*").

1.4. Composition of relations. Consider the sets X, Y, Z and the relations R_1, R_2, such that: $R_1 \subseteq X \times Y$ and $R_2 \subseteq Y \times Z$, then it is possible to define a relation, which is the composition of R_1 and R_2, written as follows $R_1 \circ R_2 \subseteq X \times Z$, such that:

$$a(R_1 \circ R_2)c :\Leftrightarrow \exists b(aR_1b \wedge bR_2c),$$

where " $\circ$ " is called a "*law of composition*".

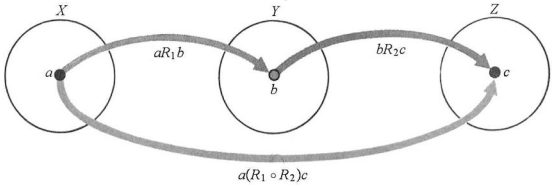


Fig. Composition of relations. $a(R_1 \circ R_2)c$ is subject to the existence of an intermediate y in Y (i.e. $R_1 \circ R_2$ can be nonempty).

1.5. Inverse relation. An inverse relation of the relation $R \subseteq S_1 \times S_2$ such that $R^{-1} \subseteq S_2 \times S_1$ can be defined as follows: $R^{-1} := \{(a_2, a_1)|(a_1, a_2) \in R\}$, i.e. $a_2R^{-1}a_1 \Leftrightarrow a_1Ra_2$.

2. Maps, Functions

2.1. Relations, functions and maps.

Function: A function is a relation that uniquely associates members of one set with members of another set. This means that a function from A to B is an object f such that every $x \in A$ is uniquely associated with an object $f(x) \in B$. Thus, a function is a many-to-one or sometimes one-to-one relation. The set A of values at which a function is defined is called its domain, while the set of values that the function can produce is called its "*range*". The set B within which the values of a function lie is called "*codomain*", as opposed to the range, which is the set of values that the function actually takes.

We consider hereafter the univocal relations $f \subseteq A \times B$, which are called functions from A to B.

2.2. Definition of a map.

Def. 113. *(Map). A map is a relation $f \subseteq A \times B$ which is "left surjective" and "univocal".*

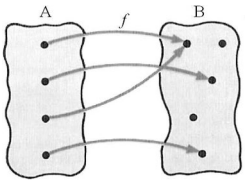


Fig. Map. (From each $x \in A$ starts one and only one arrow).

Therefore, a map $f : A \to B$ from A to B is a function f such that for every $x \in A$, there is a unique object $f(x) \in B$. The terms function and mapping are synonymous for map.

(1) Due to the fact that each $x \in A$ corresponds exactly to one $b \in B$, the expression $(x, y) \in f$ usually is replaced by $f : x \mapsto y$, or, $x \mapsto f(x)$ with $y = f(x)$.Likewise, the expression $f \subseteq A \times B$ is replaced by $f : A \to B$.

(2) A is called the "*domain*" (or *domain of definition*). Thus it is said that f is a map over a domain A. B is called the "*codomain*" of f. Then the phrase "f from A to B" is written "$f : A \to B$". The subset of B consisting of those elements that are images of elements of A under f, is the "*image*" or "*range*" of f. The word "image" is just as prevalent as "range". $f[U] = \{f(x)|x \in U \subseteq A\}$ is the *image of* U under f. Even if f^{-1} is not purely a map, using f^{-1} as a symbol, we can write, $f^{-1}[E] = \{f(x)|x \in E \subseteq B\}$ is the *inverse image of* E under f^{-1}; it is also called *pre-image* (or *preimage*).

(3) $\{(x, f(x))|x \in A\} \subseteq A \times B$ is called the *graph* of the map.

Def. 114. *(Surjective map). $f : A \to B$ is a surjective map if $f[A] = B$. (f is called a surjection).*

Def. 115. *(Injective map). $f : A \to B$ is an injective map if for all $y \in B$, $f^{-1}[\{y\}] = \{x\}$, i.e. a singleton, or $f^{-1}[\{y\}] = \varnothing$. ($f$ is called an injection).*

Def. 116. *(Bijective map). $f : A \to B$ is a bijective map if f is a surjective and injective map. (f is called a bijection).*

Ex. 26. *The isomorphisms are bijective maps.*

Bijective sets: Two sets A and B are called bijective if there is a bijective map from A to B. The term "**bijective**" is a synonym for **equipollent** or **equipotent**. And "bijectivity" is an equivalence relation on the class of sets.

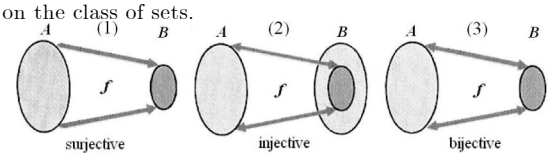


Fig. *Types of map*: (1) *Surjective:* $f[A]=B$. (2) *Injective:* $f^{-1}[\{y\}]=\emptyset$ or $=\{x\}$. (3) *Bijective*: f injective and surjective.

Equipollent: Two sets A and B are equipollent iff there is a one-to-one function, which means a bijection from A onto B. The term equipotent is used as a synonym for equipollent. In mathematical logic, two statements are equipollent if they are deducible from each other.

Ex. 27. *Given $Q \subseteq A$, the map $\psi : Q \to A$ defined by $a \mapsto \psi(a) = a$ is injective. ψ is the canonical injection of Q in A.*

Canonical surjection: Remember what was explained about *quotient sets,* in fact, we can *associate with each partition of a set S* a *surjective map $f : S \to S/\mathfrak{R}$* which is a *canonical surjection.* More formally, let be a map $\sigma_i : S_1 \times S_2 \times \cdots \times S_n \to S_i$ defined by $(\alpha_1, \alpha_2, ..., \alpha_n) \mapsto \alpha_i$ is *surjective.* Such a map corresponds to the ith transformation. Besides, a map $\sigma : S \to S/\mathfrak{R}$ defined by $\alpha \mapsto [[\alpha]]$ is surjective, and σ is a *canonical surjection,* as previously seen.

Illustration of these maps: (1) surjection, (2) injection, (3) bijection. If f is a function defined on a set A and takes values in a set B.

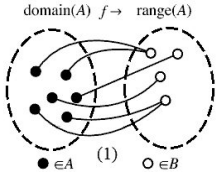


Fig. Surjection
(onto and not one-to-one)

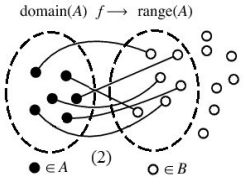


Fig. Injection, but not surjection
(one-to-one and not onto)

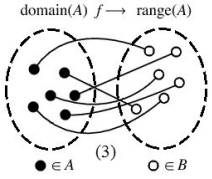


Fig. Bijection
(one-to-one and onto)

Rem. 1. *An injection is also called **embedding**.*

2.3. Particular maps.

Def. 117. *(Constant map). $f : A \to B$ is a constant map if $f(x) = f(y)$ for all $(x, y) \in A \times A$.*

Def. 118. *(Identity map). The map which assigns every member of a set A to the same element Id_A (which is written also id_A, or $\mathbf{1}_A$, or $\mathbb{I}_A$, or $\mathbf{I}_A$). Identity map is identical to the identity function.*

Identity function: Function $f(x)=x$ which assigns every real number x to the same real number x.

Def. 119. *(Restriction of a map). $g : R \to B$ is called restriction of $f : A \to B$ if $R \subseteq A$ and $f(x) = g(x)$ for all $x \in R$. Then instead of g we write $f|_R$ (meaning f restricted to R), also denoted f/R or $f \restriction R$).*

Def. 120. *(Extension of a map). $g : C \to B$ is called extension of $f : A \to B$ if $A \subseteq C$ and $g|_A = f$ (also written $g/A = f$).*

Any map, whose *domain of definition* is the set of naturals $\mathbb{N}$, is called a *sequence*. A sequence is denoted by $(x_0, x_1, x_2, ..)$.

Def. 121. *(Sequence). Let S be any set, a sequence in S is a map $f : \mathbb{N} \to S$ from the set of natural numbers to S. Sequences are usually written with subscript notation: $(x_0, x_1, x_2, ..)$ instead of $f(0), f(1), f(2), ...$*

2.4. Composition of maps. The composition of two maps (or mappings) f and g, denoted $g \circ f$, where the domain of g includes the range of f, is the map (or mapping) which assigns to each element x in the domain of f the element $g(y)$, where $y = f(x)$.
More formally, given the maps f and g such that $f : A \to B$ and $g : B \to C$, then we can create a *composed* map (coumpound) such that $g \circ f : A \to C$ defined by $(g \circ f)(x) = g(f(x))$. Obviously there is a clear analogy between the composition of maps and the composition of relations (see previously). The composition of maps $g \circ f$ is a map, where the symbol "$\circ$" is called a "*law of composition*".
The law of composition is *associative:* A property of the composition law is the *associativity;* given 3 maps $f : A \to B$, $g : B \to C$, $h : C \to D$, it is then possible to write $h \circ (g \circ f) = (h \circ g) \circ f$ (Fig.)

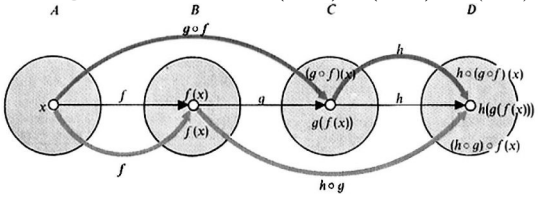


Fig. Associativity of the composition of maps.

In addition, the composition with an identity map (written Id_A or id_A, $\mathbf{1}_A$, $\mathbf{I}_A$, $\mathbb{I}_A$) gives the result: $Id_B \circ f = f$ and $f \circ Id_A = f$.
The composition of 2 surjective maps is surjective. The composition of 2 injective maps is injective. The composition of 2 bijective maps is bijective.

Bijective map defined by using compositions. A bijection can be defined by using compositions as follows: Let be a bijective map $f : A \to B \Leftrightarrow \exists g(g : B \to A \wedge g \circ f = Id_A \wedge f \circ g = Id_B)$. Besides, $g \circ f = Id_A$ confirms the injection, and $f \circ g = Id_B$ confirms the surjection.

2.5. Inverse map. The inverse relation f^{-1} of a map $f : A \to B$ is generally not a map (cf. Fig. in heading "*Definition of a map*"). The inverse symbol f^{-1} of a map $f : A \to B$, is a map $f^{-1} : B \to A$ if and only if f is bijective. In fact, usually f^{-1} is not a map, because f must be a bijection. Therefore, if f^{-1} is a map, it means that f is a bijection: $f^{-1} \circ f = Id_A$, $f \circ f^{-1} = Id_B$

2.6. Maps and operations on sets. The followings properties are verified for all maps $f : A \to B$ and $g : B \to C$:
. For all $X, Y \subseteq A$, $f[X \cap Y] \subseteq f[X] \cap f[Y]$
. $f[\bigcap_{i \in I} X_i] \subseteq \bigcap_{i \in I} f[X_i]$ where $X_i \subseteq A$
. For all $X, Y \subseteq A$, $f[X \cup Y] = f[X] \cup f[Y]$
. $f[\bigcup_{i \in I} X_i] = \bigcup_{i \in I} f[X_i]$ where $X_i \subseteq A$
. For all $X, Y \subseteq B$, $f^{-1}[X \cap Y] = f^{-1}[X] \cap f^{-1}[Y]$
. $f^{-1}[\bigcap_{i \in I} X_i] = \bigcap_{i \in I} f^{-1}[X_i]$ where $X_i \subseteq A$
. For all $X, Y \subseteq B$, $f^{-1}[X \cup Y] = f^{-1}[X] \cup f^{-1}[Y]$
. $f^{-1}[\bigcup_{i \in I} X_i] = \bigcup_{i \in I} f^{-1}[X_i]$ where $X_i \subseteq A$
. For all $X \subseteq B, Y \subseteq A$, $f\left[f^{-1}[X]\right] \subseteq X$, $f^{-1}\left[f[Y]\right] \supseteq Y$
. For all $X, Y \subseteq B$, $f^{-1}[X \backslash Y] = f^{-1}[X] \backslash f^{-1}[Y]$
. For all $X \subseteq C$, $(g \circ f)^{-1}[X] = f^{-1}\left[g^{-1}[X]\right]$
Note that $f^{-1}[E]$ is not the image of E under f^{-1} but denotes the *inverse image* of E under f. It does not necessarily exist.

2.7. Commutative diagram. Given the sets X, Y, Z and the maps $f : X \to Y$ and $g : Y \to Z$, a diagram is commutative if there exists a map $c : Z \to Y$ verifying the composition $c \circ g = f$. Then, the diagram is called a *commutative diagram.* Thereby, the diagram is said commutative if there exists a map $c : Z \to Y$ verifying $c \circ g = f$.

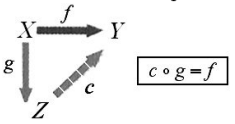


Fig. Commutative diagram.

2.8. n-variables functions. If the *domain* of a function $f : A \to B$ is a *subset of Cartesian product* $A_1 \times A_2 \times \cdots \times A_n$, then f is a *n-variables functions,* which should be written $f\left((x_1, x_2, ..., x_n)\right)$, but usually to simplify the writings such a function is written $f(x_1, x_2, ..., x_n)$.

2.9. Maps and graphs. We know that a map from a set A to a set B is (naively) a "process" (not specified) which associates with each element $x \in A$ an element $f(x) \in B$. Such a map is denoted $f : A \to B$, $x \mapsto f(x)$. The element $f(x) \in B$ is called image of the element $x \in A$ by the map f. The set A is called domain (i.e. the source) of the map f; the set B is called codomain (i.e. the goal) of f.
There exists an axiom of extensionality for the maps:

Axiom of extensionality (for maps): "*Two maps f and g from A to B are equal if and only if they assign the same image to every element of A : $f = g \Leftrightarrow \forall x \in A, f(x) = g(x)$.*"

In principle, when we know the map f, its source and its goal are then determined. In practice, we tend to identify two maps f, g of same source A as soon as they verify the relation $\forall x \in A : f(x)$=$g(x)$.

Ex. 28. (1) *For any set A, the map $x \mapsto x$ from A to itself is called **identity map** of A, denoted Id_A.* (2) *The sets A,B being arbitrary (the latter nonempty), we can define for any $a \in B$ the map $x \mapsto a$ from A to B: this is a **constant map**.* (3) *If $A \subset B$, the map $x \mapsto x$ from A to B is called **canonical map** or **canonical injection** from A to B.* (4) *If f is a map from A to B and if $A' \subset A$, we can define the map $x \mapsto f(x)$ from A' to B. It is called **restriction** of f to A' and is denoted by $f_{|A'}$.* (5) *If $B' \subset B$ is such that $\forall x \in A : f(x) \in B'$, the map $x \mapsto f(x)$ from A to B' is called **corestriction** of f to B'.* (6) *If $A = \varnothing$, we agree that there is one and only one map from A to B, called **empty map**.*

Def. 122. *(Graph of a map). A graph of a map $f : A \to B$ is the set $\Gamma_f := \{(x, y) \in A \times B | y = f(x)\}$.*

We can also describe it as $\{(x, f(x)) | x \in A\}$. According to the (previous) **axiom of extensionality**, two maps of same source (domain) and of same goal (codomain) are equal if and only if they have the same graph. Besides, certain hanbooks define a map as a triplet (A, Γ, B), where $\Gamma \subset (A \times B)$ verifies the property: $\forall x \in A, \exists! y \in B : (x, y) \in \Gamma$, i.e. any $x \in A$ has a unique image $y \in B$.

Ex. 29. (1) *The graph of Id_A is the diagonal of A^2.* (2) *The graph of the constant map $x \mapsto a$ is $A \times \{a\}$.* (3) *The graph of the restriction $f' = f_{|A'}$ is $\Gamma_{f'} = \Gamma_f \cap (A' \times B)$.* (4) *The graph of the empty map is the empty map.*

2.10. Images and antecedents.

Def. 123. *(Antecedent; Image). Let $f : A \to B$ be a map. We call **antecedent** of an element $y \in B$ by the map f any element $x \in A$ such that $f(x) = y$. The set of elements of B that has an antecedent by f is a part of B called **image** set or image of f and denoted:* $\operatorname{Im} f := \{y \in B | \exists x \in A : y = f(x)\}$.

We also write $\operatorname{Im} f := \{f(x) | x \in A\}$. Do not confuse *codomain* and *range*, especially when we deal with the surjectivity. For any subset E of A, the image $\operatorname{Im} f_{|E}$ of the restriction of f to E is the set of elements of B which have an antecedent in E. This subset of B is called image of E by f and denoted:

$$f(E) := \{y \in B | \exists x \in E : y = f(x)\}.$$

We write also $f(E) = \{f(x) | x \in E\}$. These two definitions are related: we check easily that $\operatorname{Im} f = f(A)$ and $f(E) = \operatorname{Im} f_{|E}$.

Ex. 30. *The image set of the map Id_A is A. The image set of a constant map $x \mapsto a$ is $\{a\}$. The image of the empty map is empty. The image of the map $x \mapsto x^2$ from $\mathbb{R}$ to $\mathbb{R}$ is $\mathbb{R}_+$.*

A case particularly interesting is the case where $A = B$; if $f : A \to B$, we say that $E \subset A$ is **stable** by f if $f(E) \subset E$. In this case, by restriction and corestriction we obtain an induced map on E. For example, $\{x\}$ is stable if and only if $f(x) = x$: then we say that x is a **fixed point** of f.
Here are some examples of calculation concerning the image of a part of A by a map $f : A \to B$. Here, E and F denote parts of A:
$f(\varnothing) = \varnothing$,
$f(E \cup F) = f(E) \cup f(F)$
$f(E \cap F) \subset f(E) \cap f(F)$
$f(F) \backslash f(E) \subset f(F \backslash E)$
$E \subset F \Rightarrow f(E) \subset f(F)$.
As an example, discuss the third rule. If $x \in E \cap F$, then $x \in E$ and $x \in F$, so $f(x) \in f(E)$ and $f(x) \in f(F)$, so $f(x) \in f(E) \cap f(F)$. Try the reverse reasoning. Given $y \in f(E) \cap f(F)$. Then $y = f(a)$ for a $a \in E$ and $y = f(b)$ for a $b \in F$. If f is injective (the definition of the injectivity is given again in the next heading), we have necessarily $a = b \in E \cap F$ and $y \in f(E \cap F)$, which gives an additional rule:

$$f \text{ injective} \Rightarrow f(E \cap F) = f(E) \cap f(F).$$

If we do not assume f injective, this equality can be false: take $A = B = \mathbb{R}$, $f : x \mapsto x^2$, $E = \mathbb{R}_-^*$ and $F = \mathbb{R}_+^*$. Then $E \cap F = \varnothing$, so $f(E \cap F) = \varnothing$, but $f(E) = f(F) = \mathbb{R}_+^*$, so $f(E) \cap f(F) = \mathbb{R}_+^*$.
Let us reintroduce some definitions of map:

Def. 124. *(Surjective map). The map $f : A \to B$ is said to be surjective if any element of B admits **at least** an antecedent, i.e. if $\operatorname{Im} f = B$:*

$$f \text{ surjective} \Leftrightarrow (\forall y \in B, \exists x \in A : y = f(x)).$$

Then we speak of map from A to B, or surjection.

Ex. 31. *The map Id_A is surjective. A constant map is surjective only if its codomain is a singleton. Given $f : A \to B$ an arbitrary map and $B' := \operatorname{Im} f$. Then the corestriction $f : A \to B'$ is surjective; e.g. the map $x \mapsto x^2$ from $\mathbb{R}$ to $\mathbb{R}$ is not surjective, whereas its corestriction to $\mathbb{R}^+$ is surjective.*

Def. 125. *(Injective map). We say that the map $f : A \to B$ is injective (or that is an injection) if any element of B admits **at most** an antecedent:*

$$f \text{ injective} \Leftrightarrow (\forall x, x' \in A, f(x) = f(x') \Rightarrow x = x').$$

Def. 126. *(Bijective map). We say that the map $f : A \to B$ is bijective (or that it is a bijection) if it is both surjective and injective, i.e. if any element of B admits **exactly** an antecedent:*

$$f \text{ bijective} \Leftrightarrow (\forall y \in B, \exists! x \in A : y = f(x)).$$

Ex. 32. (1) *The map Id_A is always bijective.* (2) *Given $f : A \to B$ an injective map and $B' = \operatorname{Im} f$. Then the corestriction $f : A \to B'$ is bijective.* (3) *Given I a part of $\mathbb{R}$. If $f : I \to \mathbb{R}$ is strictly increasing (or strictly decreasing), it is injective.*

Th. 26. *(Cantor th.). There exists no surjective map from a set A to $\mathfrak{P}(A)$ (set of the parts of A).*

Proof. Let $f : A \to \mathfrak{P}(A)$ be an arbitrary map. Consider the set $F := \{x \in A | x \notin f(x)\}$. Since, for $x \in A$, $f(x) \subset A$, the condition $x \notin f(x)$ has a meaning. The axiom of separation garantees the existence of $F \subset A$. We are going to show that the element F of $\mathfrak{P}(A)$ is the image by f of no element a of A, which will imply that f is not surjective. If we had $f(a) = F$ for a certain $a \in A$, of the equivalence $\forall x \in A$, $x \in f \Leftrightarrow x \notin f(x)$ (which is the definition of F) we would deduce, by replacing x by a, the equivalence: $a \in F \Leftrightarrow a \notin f(a)$, i.e., $a \in F \Leftrightarrow a \notin F$, which is absurd. Thus we cannot have $f(a) = F$. □

2.11. Set $\mathcal{F}(E, F)$ of maps from E to F. Axiom: *The maps from the set E to the set F forms a set denoted by $\mathcal{F}(E, F)$*

Ex. 33. (1) *The set $\mathcal{F}(\varnothing, F)$ is the singleton of which the unique element is the empty map.* (2) *The set $\mathcal{F}(\{a\}, F)$ is in natural bijection with F by the map $f \mapsto f(a)$ from $\mathcal{F}(\{a\}, F)$ to F. Indeed, know a map f from $\{a\}$ to F comes down to knowing the image $f(a) \in F$.* (3) *The $\mathcal{F}(\{a, b\}, F)$ is in natural bijection with F^2 by the map $f \mapsto (f(a), f(b))$ from $\mathcal{F}(\{a, b\}, F)$ to F^2 (know a map f from $\{a, b\}$ to F comes down to knowing the $f(a), f(b) \in F$).* (4) *The set $\mathcal{F}(E, \varnothing)$ is empty if $E \neq \varnothing$ (and is a singleton if $E = \varnothing$).* (5) *The set $\mathcal{F}(E, \{a\})$ is the singleton of which the unique element is the constant map with value a.* (6) *The set $\mathcal{F}(E, \{0, 1\})$ is in natural bijection with $\mathfrak{P}(E)$ (set of the parts of E); indeed, know a map f from E to $\{0, 1\}$ comes down to knowing the subset $A \subset E$ of antecedents of 1, since then $B = \complement_E A$ is the subset of antecedents of 0.* (7) *The composition of maps induces a map $(f, g) \mapsto g \circ f$ from $\mathcal{F}(E, F) \times \mathcal{F}(F, G)$ to $\mathcal{F}(E, G)$.* (8) *The map $(f, g) \mapsto \langle f, g \rangle$ from $\mathcal{F}(E, F) \times \mathcal{F}(F, G)$ to $\mathcal{F}(E, F \times G)$ is a bijection. Let $A \subset E$. The map $f \mapsto f|_A$ is from $\mathcal{F}(E, F)$ to $\mathcal{F}(A, F)$. If, moreover, $B \subset E$, we get thus a map $f \mapsto (f|_A, f|_B)$ from $\mathcal{F}(E, F)$ to $\mathcal{F}(A, F) \times \mathcal{F}(B, F)$. If $A \cup B = E$, this map is injective; if $A \cap B = \varnothing$, this map is surjective.*

3. Families

3.1. Family of elements of a set. To describe a map f from $\{1, 2, .., n\}$ to E, it suffices to specify the images $x_1 = f(1)$, $x_2 = f(2)$, ..., $x_n = f(n)$, of $\{1, 2, .., n\}$ by f. Thus we get a bijection $f \mapsto (x_1, x_2, ..., x_n) := (f(1), f(2), .., f(n))$ from $\mathcal{F}(\{1, 2, .., n\}, E)$ to E^n (where $\mathcal{F}(\{1, 2, .., n\}, E)$ denotes the set of maps from $\{1, 2, .., n\}$ to E; see heading "*Set $\mathcal{F}(E, F)$ of maps from E to F*"), which provides a notation of f in the form of a n-tuple $(x_1, x_2, ..., x_n)$. This leads to the following definition:

Def. 127. *(Family of elements). A family of elements of the set A indexed by the set I is the map from I to E. We denote by $\underline{x} := (x_i)_{i \in I}$ such a family, the image of the index $i \in I$ being the element $x_i \in E$. The set $\mathcal{F}(I, E)$ of these families is then denoted by E^I.*

This change of notation is an operation that highlights the values $x_i \in E$, and the role of indexes $i \in I$ is to spot them.

Ex. 34. (1) *An family indexed by $\{0, 1, 2, .., n\}$, or $\{1, 2, .., n\}$, is a finite sequence $(x_0, x_1, x_2, ..., x_n)$ or $(x_1, x_2, ..., x_n)$. A family indexed by $I = \mathbb{N}$ or $\mathbb{N}^*$ is a sequence $(x_n)_{n \geq 0} := (x_0, x_1, x_2, ...)$, or $(x_n)_{n \geq 1} := (x_1, x_2, ...)$.* (2) *Let $J \subset I$ be a subset of indexes. By restriction to J of the map $i \mapsto x_i$, we obtain a family $(x_n)_{i \in J}$: we say that this a extracted family. If $I = \mathbb{N}$ and $J \subset \mathbb{N}$, we recognize the notion of "extracted sequence" (also called "subsequence").* (3) *Let $\phi : K \to I$ be a map between the sets of indexes $(x_{\phi(k)})_{k \in K} \in E^K$. In the case where ϕ is injective, this is a bijection of K on a subset J of I, and this construction is equivalent to the previous one. For example, if $(u_n)_{n \in \mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ is a sequence of reals, by restricting to the set of even indexes $2\mathbb{N} \subset \mathbb{N}$, we get an extracted sequence $(u_{2n})_{n \in \mathbb{N}}$.* (4) *In practice, to define a subsequence (i.e. extracted sequence) of the sequence $(u_n)_{n \in \mathbb{N}}$, we define a strictly increasing sequence of indexes: $n_0 < n_1 < \cdots$, and we consider the sequence $(u_{n_k})_{k \in \mathbb{N}}$.* (5) *If the set I of indexes is a cartesian product: $I := J \times K$, usually we use two indexations $(x_{j,k})_{j \in J, k \in K} \in E^{J \times K}$. This the case of the family of coefficients of a matrix.* (6) *If I is the empty set, we say that this an "empty family".*

The notion of family of elements indexed by a set of indices is particularly useful. Thus, when one wants to process all the elements of an arbitrary set E, it is often preferred to consider them as the terms x_i of a family; to this end, it suffices to take $I = E$ and set $x_i = i$, in other words, take a family corresponding to the map Id_E. We say that this is the *family canonically associated with the set E*. Usually, it is denoted by $(x_i)_{i \in I}$, just like any family, but keeping in mind that each element of E appears only one time in it; e.g. in linear algebra, the bases are sometimes considered as sets of vectors, sometimes as families of vectors: in the last case the notation used is $\sum_{i \in I} \lambda_i x_i$, etc.

3.2. Family of sets. We call *family of sets indexed by the set I* the datum, for each index $i \in I$, of a set E_i. This is not really a definition since we do not attribute a precise meaning to the way the sets E_i are given. Such a family is denoted by $(E_i)_{i \in I}$. An *axiom* and *definition* are given by:

Def. 128. *Let $(E_i)_{i \in I}$ be a family of sets. There exists a set G such that $\forall x$, $x \in G \Leftrightarrow (\exists i \in I : x \in E_i)$. This set is unique (axiom of extensionality). We call it the union of the family $(E_i)_{i \in I}$, and it is denoted by $\bigcup_{i \in I} E_i$.*

Thus, we have $\bigcup_{i \in I} E_i := \{x | \exists i \in I : x \in E_i\}$. For example, the union of an empty family of sets is empty (as well as the union of a family of empty sets).
Above, we assume that the elements x_i belong all to a same initially given set E. But in fact, it is possible to define families $(x_i)_{i \in I}$, each x_i being taken in a set E_i that *depends on i*. Under the axiom above, this definition is not really more general: indded we can consider $(x_i)_{i \in I}$ as a family of elements of the set $E : \bigcup_{i \in I} E_i$. For the same reason every family of sets can be considered as a family of parts of a certain set E, i.e. as a family of elements of $\mathfrak{P}(E)$ (set of the parts of E).
Let $(E_i)_{i \in I}$ be a family of sets and I be nonempty, we deduce from the *separation axiom* (applied inside any of the E_i) that there exists a set such that: $\forall x$, $x \in G \Leftrightarrow (\forall i \in I : x \in E_i)$. This set is unique (axiom of extensionality), it is called *intersection* of the family $(E_i)_{i \in I}$, and it is denoted by $\bigcap_{i \in I} E_i$: $\bigcap_{i \in I} E_i := \{x | \forall i \in I : x \in E_i\}$.
In contrast, we do not know how to define the intersection of an empty family of sets; in this case, the above formula would determine a set containing all the x, unconditionally.
Let $(E_i)_{i \in I}$ be a family of sets whose union is $E = \bigcup_{i \in I} E_i$. The subset of E^I formed by the families $(x_i)_{i \in I}$ such that each x_i belongs to the set E_i is called *cartesian product*, or just *product* of the family $(E_i)_{i \in I}$, and denoted by $\prod_{i \in I} E_i$.

$$\prod_{i \in I} E_i := \{(x_i)_{i \in I} | \forall i \in I : x_i \in E_i\}.$$

For each index $j \in I$, we have then a map: j^{th} *projection* of $\prod_{i \in I} E_i$ on E_j, which associates its j^{th} *component*, or j^{th} *coordinate* x_j with the element $(x_i)_{i \in I}$. We easily check that when I is finite, we find again the previous notions. For example, if $I = \{1, .., n\}$: $\bigcup_{i \in I} E_i = E_1 \cup \cdots \cup E_n$, $\bigcap_{i \in I} E_i = E_1 \cap \cdots \cap E_n$, $\prod_{i \in I} E_i = E_1 \times \cdots \times E_n$
Of course, if one of the E_i is empty, then the product $\prod_{i \in I} E_i$ is also empty. To prove the converse, in the case of a finite product, we supposed the E_i nonempty and "chose" an element in each of them to form a particular family $(x_i)_{i \in I}$ which is an element of the product. In the early twentieth century, the possibility to simultaneously and arbitrarily "choose" an infinity of such elements has been questioned by many mathematicians. Modern resolution of this conflict was to

introduce an *ad hoc* axiom. Despite its appearence, this axiom has many interesting consequences.

Axiom of choice: I*f the E_i are nonempty, then $\prod_{i\in I} E_i$ is also empty.*

3.3. Family of parts of a set. Many calculation rules stated in the case of two sets (or in the case of a finite number of sets) extend here. We'll not state all these generalizations, but only some examples. To formulate the associativity of the union generalized and intersection generalized, we consider a family $(E_i)_{i\in I}$ of sets and we suppose that the set I of its indexes is itself an union of sets: $I=\bigcup_{j\in J} I_j$. We have then:
$\bigcup_{i\in I} E_i = \bigcup_{j\in J}(\bigcup_{i\in I_j} E_i)$,
$\bigcap_{i\in I} E_i = \bigcap_{j\in J}(\bigcap_{i\in I_j} E_i)$.
Now, suppose that the E_i are parts of a set E:
$\complement_E(\bigcup_{i\in I} E_i) = \bigcap_{i\in I} \complement_E E_i$,
$\complement_E(\bigcap_{i\in I} E_i) = \bigcup_{i\in I} \complement_E E_i$.
Suppose moreover that the F_j $(j\in J)$ are subsets of a set F and that f is a map from E to F:
$f(\bigcup_{i\in I} E_i) = \bigcup_{i\in I} f(E_i)$,
$f(\bigcap_{i\in I} E_i) \subset \bigcap_{i\in I} f(E_i)$,
$f^{-1}(\bigcup_{j\in J} F_j) = \bigcup_{j\in J} f^{-1}(F_j)$,
$f^{-1}(\bigcap_{j\in J} F_j) = \bigcap_{j\in J} f^{-1}(F_j)$.
Note that the second rule has an inclusion and not an equality. Note also that the bijection $(f,g)\to\langle f,g\rangle$ from $\mathcal{F}(E,F)\times\mathcal{F}(E,G)$ to $\mathcal{F}(E,F\times G)$ (see Ex.(8) in heading "*Set $\mathcal{F}(E,F)$ of maps from E to F*") generalizes in a bijection from $\prod_{j\in J}\mathcal{F}(E,F_j)$ to $\mathcal{F}(E,\prod_{j\in J}F_j)$. The reader can (easily) show all these rules and discover many more.

Partitions and covers. A *cover* of a set E is defined as a family $(E_i)_{i\in I}$ of parts of E such that $\bigcup_{i\in I} E_i = E$. This notion is used especially in topology. We define a *partition* of a set E as a cover of E by nonempty sets of pairwise disjoint. We have then:
$\bigcup_{i\in I} E_i = E$,
$\forall i\in I,\ E_i\neq\varnothing$,
$\forall i\neq j\in I,\ E_i\cap E_j=\varnothing$.

Parts and characteristic maps. Fix a set E. Suppose that we "code" the parts of E by using maps. With any part $A\subset E$, we associate its *characteristic function* $\chi_A : E\to\{0,1\}$ defined by the relations $\forall x\in E$, $\chi_A(x) := \begin{cases}1 \text{ if } x\in A\\ 2 \text{ if } x\notin A.\end{cases}$

Th. 27. (†). *The map $A\mapsto\chi_A(x)$ from $\mathfrak{P}(E)$ to $\mathcal{F}(E,\{0,1\})$ is bijective.*

Proof. Consider $f: E\to\{0,1\}$ an element of $\mathcal{F}(E,\{0,1\})$. Let $A{:=}f^{-1}(1)\subset E$. Clearly, we have then $\chi_A{=}f$, and, more precisely, A is the unique antecedent of f by the map under consideration; so this last is bijective. □

Thus, if $E=\{1,..,n\}$, fix a part of E comes down to fix n integers $x_1,..,x_n\in\{0,1\}$, that is, in computer language, a "vector of bits", or "bite vector". (This is base of the representation of sets in the Pascal programing language) This theorem allows to give an interesting interpretation of the Cantor theorem (in the heading "*Images and antecedents*" in "*Maps, Functions*"); since we have a bijection from $\mathcal{F}(E,\{0,1\})$ to $\mathfrak{P}(E)$, the Cantor theorem is equivalent to the non-existence of a surjection from E to $\mathcal{F}(E,\{0,1\})$. We can show that this non-existence by the *Cantor diagonal method.* Let ϕ be an arbitrary map from E to $\mathcal{F}(E,\{0,1\})$. Thus, for any $a\in E$, $\phi(a)$ is a map from E to $\{0,1\}$. We can also define a map f from E to $\{0,1\}$ as follows: $\forall a\in E$, $f(a) := \begin{cases}1 \text{ if } \phi(a)(a)=0\\ 0 \text{ if } \phi(a)(a)=1\end{cases}$. By construction, $f(a)\neq\phi(a)(a)$. And so $f\neq\phi(a)$. This is true $\forall a\in E$, f is not in the image of ϕ that is thus not surjective. The reader is exhorted to study this proof, in order to recognize a simple translation of the proof of Cantor theorem (in "*Images and antecedents*" in "*Maps, Functions*") in terms of characteristic functions. We will see in the heading "*Laws of composition*" that the use of characteristic functions allows to reduce the set-calculation to the calculation in $\{0,1\}$.

4. Laws of Composition

4.1. General vocabulary, notation.

We call **internal composition law** on a set E a map from $E\times E$ to E. The usage is to denote it in "*infix form*"; this means that we introduce a symbol distinct from those that serve to denote the elements of E, for example $+,\times,\cdot,*,\star$, or $\top$, and that we write the image of $(a,b)\in E\times E$ in E in the form $a+b$, $a\times b$, $a\cdot b$, $a*b$, $a\star b$, or $a\top b$ depending on the case. In some cases, which are similar to the multiplication of numbers, we can even omit any operation symbol and write $a.b$, or even ab instead of $a\times b$. When the law is denoted $+$, we speak of "*additive notation*", and the result of composition of elements is called sum. In the other cases, we speak of "*multiplicative notation*", and the result of composition of elements is called "product". The most famous examples of internal composition laws are the addition and the multiplication over the set of numbers: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$; but we can also mention the union and the intersection on $\mathfrak{P}(E)$ (where $\mathfrak{P}(E)$ is the set of the parts of E).
Given E endowed with an internal composition law denoted by $\star$. We say that a *part* A of E is "**stable**" for the law $\star$ if the image of $A\times A$ is icluded in A:

$$\forall(a,b)\in E\times E,\ a\star b\in A.$$

In this case, the induced map from $A\times A$ to A is a an "internal composition law on A", called "*induced law on A*"; in general, it is denoted in the same way as the law on E, therefore here $\star$. For example, each of the inclusions $\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$ define a stable part for the addition and for the multiplication. Likewise, if $E'\subset E$, the set $\mathfrak{P}(E')$ is a part of $\mathfrak{P}(E)$ that is stable for the union and the intersection.
With the same notations, let A and B be two parts of E. We then define the set $A\star B\subset E$ as the image of $A\times B\subset E\times E$ for the law $\star$:

$$A\star B := \{a\star b | a\in A, b\in B\}.$$

This allows to *extend* the law $\star$ to $\mathfrak{P}(E)$.
Let E and F be two sets respectively endowed with composition laws $*$ and $\star$. We can endowed the product $E\times F$ with a composition law $\top$ by setting: $(a_1,b_1)\top(a_2,b_2)=(a_1*a_2,b_1*b_2)$. The law $\top$ is then called the product of the laws $*$ and $\star$. This construction generalizes to the cartesian product of a family $(E_i)_{i\in I}$ of sets. Suppose that each of E_i endowed with a composition law and suppose that all these laws are denoted by $\star$ (this often occurs and in general does not cause confusions). The product of two elements $(x_i)_{i\in I}$, $(y_i)_{i\in I}\in\prod_{\in I}E_i$ is then the element $(x_i\star y_i)_{i\in I}\in\prod_{\in I}E_i$, in which each component $x_i\star y_i$ was obviously calculated with the law $\star$ of E_i.
For example, if E is endowed with the law $\star$ (now unique!), the product E^I is endowed with the product law that we will still denote by $\star$ and which is defined by the formula: $(x_i)_{i\in I}\star(y_i)_{i\in I}=(x_i\star y_i)_{i\in I}$. Recall that we have (see def. in heading "*Family of elements of a set*" in "*Families*") identified the sets E^I with $\mathcal{F}(I,E)$. Thus, from the law $\star$ on E we also have defined a law on $\mathcal{F}(I,E)$. This one is thus defined: Given f and g two maps from I to E; then $f\star g$ is the map $i\mapsto f(i)\star g(i)$ from I to E.

Special properties of composition laws. We say that the law $\star$ on the set E is associative if we have $\forall a,b,c\in E$, $a\star(b\star c)=(a\star b)\star c$. Then we can write in a simpler way: $a\star b\star c$. This convention generalizes to the product of n arbitrary elements. For example, the product of n arbitrary elements all equal to a is often denoted by a^n (read "a power n", and we say that n is the exponent). All law that we have mentioned (addition and multiplication of numbers, union and intersection of parts) are *associative.* Powers of an element and, more generally, the products of families of elements obey to many algebraic laws that will be studied in the heading "*Algebraic Structures*".

Ex. 35. *Suppose the law is not associative, denote c_n the number of (a priori) distinct products that we can form using $n+1$ times the only element a. For $n=0$, there is only a, so $c_0=1$. For $n=1$, there is only $a\star a$, so $c_1=1$. For $n=2$, there is $a\star(a\star a)$ and $(a\star a)\star a$ so $c_2=2$. The c_n are the Catalan numbers.*

We say that the law $\star$ is commutative if we have $\forall a,b\in E$, $a\star b=b\star a$. All the laws that we have mentioned (addition and multiplication of numbers, union and intersection of parts) are commutative.
We say that $e\in E$ is *left-neutral* or a *left-neutral element* for the law $\star$ if we have $e\star a=a$, $\forall a\in E$. Similarly we define *right-neutral element* by $a\star e=a$. We call *neutral* or *neutral element* any element that is right-neutral and left-neutral. All the laws that we have mentioned (addition and multiplication of numbers, union and intersection of parts) admit a neutral element.

Ex. 36. *If there is a left-neutral element e and a right-neutral element e', they are equal: we have $e\star e'=e'$ and $e\star e'=e$, so $e=e'$. In particular, if there is a neutral element, it is unique.*

Assume that the law $\star$ on E admits a neutral element; then we say that $a\in E$ is *invertible on the left* (left-invertible) if it admits an *inverse on the left* (a left-inverse). We say that $a\in E$ is *invertible on the right* (right-invertible) if it admits a *inverse on the right* (a right-inverse), i.e. an element a'' such that $a\star a''=e$. We say that a is *invertible* if it has an *inverse*, i.e. an element that is its inverse on the left and on the right.

Ex. 37. *Suppose the law is associative. If a admits an inverse a' on the left and an inverse a'' on the right, they are equal: the two ways*

to calculating $a' \star a \star a''$ give $a' = a''$. It follows that if the law is associative, the inverse of an element is unique (if it exists).

A less fundamental notion is that of *left cancellable element* (or *left regular element*): this is an element a such that $a \star x = a \star y \Rightarrow x = y$. Likewise, a is a *right cancellable element* if $x \star a = y \star a \Rightarrow x = y$. We say that a is *cancellable* (or *regular*) if it is left-cancellable and right-cancellable (or left-regular and right-regular).

Ex. 38. *If the law is associative and endowed with a neutral element, every left-invertible (resp. right-invertible) element is left-cancellable (resp. right cancellable). Indeed, with the previous notations, if $a \star x = a \star y$, by composing on the left by a', we find (via the associativity) $(a' \star a) \star x = (a' \star a) \star y$, i.e. $x = y$ (since $a' \star a = e$). Calculation on the right is similar.*

Note however that all the elements of $\mathbb{N}$ (resp. the nonzero elements of $\mathbb{Z}$) are cancellable for the addition (resp. for the multiplication), but that none is invertible, except 0 (resp. ± 1). For the addition in $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ (resp. for the multiplication in $\mathbb{Q},\mathbb{R},\mathbb{C}$), all the elements are invertible (resp. all the nonzero elements).
Here are two notions of less frequent use. We say that a is *idempotent* if $a \star a = a$. For example, any neutral is *idempotent* (and, in $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ endowed with the addition, they are the only ones, while for themultiplication there is in addition 0). We say that a is *absorbing on the left* (resp. *absorbing on the right*) if we have $a \star b = a$ whatever b (resp. $b \star a = a$). For example, 0 is absorbing for the multiplication in $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$.

Morphisms. Consider simultaneously two sets endowed with internal composition laws in order to express possible links between "structures" thus defined. Denote these structures by $(E, \star)$ and $(F, \top)$.

Def. 129. *A morphism from $(E, \star)$ to $(F, \top)$ is a map f from E to F such that:*

$$\forall a, b \in E : f(a \star b) = f(a) \top f(b).$$

A *bijective morphism* is called *isomorphism*. If there exists an isomorphism from $(E, \star)$ to itself (with the same law) it is called *endomorphism*. An isomorphism from $(E, \star)$ to itself (with the same law) is called *automorphism*.
The result of composition of two morphisms is a morphism. Identity, composition of two isomorphisms, inverse map of an isomorphism, are isomorphisms. The relation "being isomorphic" is therefore an equivalence relation.

Ex. 39. *The map $A \mapsto \complement_E A$ from $\mathfrak{P}(E)$ to itself is an isomorphism from $(\mathfrak{P}(E), \cap)$ to $(\mathfrak{P}(E), \cup)$, and also an isomorphism from $(\mathfrak{P}(E), \cup)$ to $(\mathfrak{P}(E), \cap)$ (Morgan's law). But this is not an automorphism (since the law is not the same at the start and at the end).*

If $(E, \star)$ and $(F, \top)$ are isomorphic, then one of these two laws is associative (resp. commutative) if and only if the other is also associative (resp. commutative). Similarly, isomorphisms turn (left, or right) neutral elements into (left, or right) neutral elements, (left, or right) inverse elements into (left, or right) inverse elements, (left, or right) cancellable elements into (left, or right) cancellable elements, and absorbing elements (on the left, or on the right) into absorbing elements (on the left, or on the right).

4.2. Application to set-calculation.

We already have introduced the bijection $A \mapsto \chi_A$ from $\mathfrak{P}(E)$ to $\mathcal{F}(E, \{0,1\})$ (in the heading "*Family of parts of a set*"). We will see that this bijection is (in many senses) an isomorphism (even if we may need to endow $\mathcal{F}(E, \{0,1\})$ with some natural composition laws). First, endow $\{0,1\}$ with various operations $\cup$, $\cap$, $\oplus$. By previous general constructions, these operations automatically extent to $\mathcal{F}(E, \{0,1\})$. The following tables define the laws on $\{0,1\}$:

$\cup$	0	1
0	0	1
1	1	1

$\cap$	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

We check then that the above bijection is an isomorphism from $(\mathfrak{P}(E),\cup)$ to $(\mathcal{F}(E, \{0,1\}), \cup)$, from $(\mathfrak{P}(E), \cap)$ to $(\mathcal{F}(E, \{0,1\}), \cap)$, $(\mathfrak{P}(E), \oplus)$ to $(\mathcal{F}(E, \{0,1\}), \oplus)$. The law $\oplus$ on $\mathfrak{P}(E)$ is the "*symmetric difference*" defined by: $A \oplus B := (A \backslash B) \cup (B \backslash A)$. Note that $(\mathfrak{P}(E), \oplus)$ is a group (and even a ring, with the law $\cap$), and that this is a vector space over the field with two elements.

5. Power, Cardinal, Denumerability

Working on sets, the number of elements in a set is particularly important; so we need to define the concept of *number* (leading us to that of *power*).

5.1. Number, equipotence and cardinality.

This definition can be given without using the set of natural numbers (integers).

Equipollent: Remember that two sets A and B are equipollent if and only if there is a one-to-one function, which means a bijection from A onto B. The term *equipotent* is used as a synonym for *equipollent*. In mathematical logic, two statements are equipollent if they are deducible from each other.

Def. 130. *(Equipotence). Let A and B be two sets. If there exists a bijection $A \to B$, then A and B are equipotent, usually denoted by $A \sim B$.*

Ex. 40. *The following sets are equipotent* $\{1, 2, 3, 4, 5, 6, 7, 8\}$ *and* $\{a, b, c, d, e, f, g, h\}$.

Ex. 41. *Similarly, the next sets are also equipotent* $\mathbb{N}=\{0, 1, 2, 3, 4, 5, ...\}$ *and* $B=\{0, 5, 10, 15, 20, ...\}$ *if we define $f : \mathbb{N} \to B$ such that $n \mapsto f(x) = 5n$ is a bijection (Fig.)*

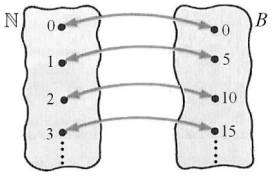


Fig. Equipotence.

Cardinality is a notion of the size of a set which does not rely on numbers. It is a relative notion. Indeed, two sets may each have an infinite number of elements, but one may have a greater cardinality (i.e, one may have a "more infinite" number of elements. See *Cantor diagonalization* for an example of *how the reals have a greater cardinality than the natural numbers*).

Cardinality: For a finite set A, the cardinality of A, denoted usually by $n(A)$, is the number of elements in A. The notation $|A|$, or $\#(A)$, is also used, also similar to $\mathrm{card}(A)$. For the subsets A, B, C, of some universal set S, we write the properties:
(1) $n(A \cup B) = n(A) + n(B) - n(A \cap B)$,
(2) $n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - (A \cap C) - n(B \cap C) + n(A \cap B \cap C)$.

Cardinal number: A number that gives the number of elements in a set. If two sets can be put in one-to-one correspondence with one another they have the same *cardinal number* or *cardinality*. For *finite sets the cardinal* numbers are $0, 1, 2, 3, ...$, *but infinite sets require new symbols* to describe their cardinality, see *aleph* (written $\aleph$), *aleph-0* (written $\aleph_0$) and *aleph-1* (written $\aleph_1$). Cardinal number is the number of member of set. Usually taken as a particular well-ordered set representative of the class of all sets which are in one-to-one correspondence with one another. For $|A| = |B|$, we would say, respectively, that "A is equipotent to B", "A is equipollent to B", or "A is equinumerous to B". In common usage, a cardinal number is a number used in counting (a *counting number or Natural number*), such as $1, 2, 3, ...$

Counting number (or Natural number): A positive integer 1,2,3,4,... also called a *natural number*. Zero (0) is sometimes included in the list of counting numbers. In practice, counting number, natural number, whole number are used interchangeably.

Whole number: The term **whole number** has a very general sense, it may refer to **natural numbers** in the sense (1,2,...) or **natural numbers** in the sense (0,1,2,...) or all **integers** (..,-2,-1,0,1,2,..).

Ex. 42. *(Same cardinality). The set of even integers $\mathbb{E}$ has the same cardinality as the set of integers $\mathbb{Z}$, when we define $f : \mathbb{E} \to \mathbb{Z}$ such that $f(x) = x/2$. Then f is a bijection, therefore $|\mathbb{E}| = |\mathbb{Z}|$.*

Cardinality 1: Set A has greater cardinality than set B if there is a one-to-one function f from B to A (an injection). It is written $|A| > |B|$.

Cardinality 2: Sets A and B have the same cardinality if there is a one-to-one and onto function f from A to B (a bijection). It is written $|A| = |B|$.

In set theory, the cardinality or the cardinal number is a type of number defined in such a way that any method of counting sets using it gives the same result. This is not true for *ordinal numbers* (infra). The cardinal numbers are obtained by collecting all ordinal numbers which are obtainable by counting a given set. A set has $\aleph_0$ (aleph-0) members if it can be put into a one-to-one correspondence with the finite ordinal numbers. The cardinality of a set is also frequently referred to as the *power* of a set.

Ordinal number: In common usage, an ordinal number is an adjective which describes the *numerical position* of an object, for example, first,

second, third,... An ordinal number is sometimes called an "ordinal" for short.

The *equipotence* of sets *has been defined without reference to the power of sets.* The power is a property which must be common (shared) in a class of equipotent sets. Then, the power is a theoritical notion based on a equivalence relation. Then the equipotence "$\sim$" is an equivalence relation in a given system of sets $\mathfrak{E}$, which can be proved by using the *bijectives maps.* Therefore, *a quotient set* $\mathfrak{E}/\sim$ *consists of classes of equipotent sets.*

5.2. Power, or cardinal.

Def. 131. *(Cardinal or Power). An element of a quotient set* $\mathfrak{E}/\sim$ *is called cardinal or power.*

It is possible to associate a cardinal with any set S of the system of sets (see canonical surjection). A cardinal map (written "card"): $\mathfrak{E} \to \mathfrak{E}/\sim$, is defined by $A \mapsto \text{card}(A) = [[A]]$.

5.3. Finite and infinite sets.

Concepts of equipotence and cardinality (as seen before) allow to give a definition of finite and infinite sets without using the set of natural numbers.

Def. 132. *(Infinite set). A set S is said infinite if there exists a strict subset $A \subset S$ verifying $S \sim A$. In the opposite case, the set is said finite.*

Def. 133. *(Infinite and finite Cardinal of set). The cardinal of a finite set is said a finite cardinal, and the cardinal of an infinite set is said an infinite cardinal or a transfinite cardinal.*

5.4. Operations on cardinals.

Addition, multiplication and exponentiation in the set of cardinals (of a system of sets) can be defined. Addition is associated with the union of sets, the multiplication is associated with the Cartesian product of sets, and the exponentiation of $\text{card}(E)$ by $\text{card}(F)$ (or $|E|$ by $|F|$)is associated with the maps from F into E.

Def. 134. *(Cardinal addition). Let E and F be any sets, with "empty" intersection and let be $|A|$ the cardinal number of a set A. Then cardinal addition is defined by* $|E| + |F| = |E \cup F|$.

Def. 135. *(Cardinal multiplication). Let E and F be any sets. Then the product of $|E|$ with $|F|$ is defined as the Cartesian product* $|E| * |F| = |E \times F|$.

Def. 136. ***(Cardinal exponentiation)****. Let E and F be any sets, and let be $|A|$ the cardinal number of a set A. Then cardinal exponentiation is defined by:* $|E|^{|F|} = |\text{set of all functions from } F \text{ into } E|$.

The cardinal of the *power set* of E is $2^{|E|}$, since $|\{0,1\}| = 2$ and there is a natural bijection between the subsets of E into $\{0,1\}$.

Def. 137. ***(Cardinal arithmetic)****. Let α and β be cardinal numbers, and let E and F be "disjoint" sets such that $|E| = \alpha$ and $|F| = \beta$, Where $|E|$ (respectively $|F|$) is the cardinality of the set E (respectively F), that is, the unique cardinal number equinumerous with E (respectively F.). We then define cardinal addition, cardinal multiplication and cardinal exponentiation by:*
(1) $\alpha + \beta = |E \cup F|$
(2) $\alpha\beta = |E \times F|$
(3) $\alpha^\beta = \left|E^F\right|$
E^F is the set of all functions from F to E. These operations are well-defined, i.e. they do not depend on the choice of E and F. For the multiplication and exponentiation E and F do not actually need to be disjoint.

Rem. 2. *(Operations on cardinals): Operations on cardinals can also mainly be written:*
(1) $\text{card}(E)+\text{card}(F)=\text{card}(E \cup F)$ *if* $E \cap F=0$
(2) $\text{card}(E) \cdot \text{card}(F)=\text{card}(E \times F)$
(3) $\text{card}(E)^{\text{card}(F)}=\text{card}(E^F)$ *if* $E^F:=\{f|f:F \to E\}$
(4) $\text{card}(G) \geq \aleph_0 \wedge \text{card}(E) \leq \aleph_0 \Rightarrow \text{card}(G \cup E)=\text{card}(G)$, *i.e.* $\text{card}(G) + n = \text{card}(G) + \aleph_0 = \text{card}(G)$.

5.5. Cardinal comparison. A total order relation can be defined in the set of cardinals of a sets system as follows:

$$|E| \leqslant |F| :\Leftrightarrow \exists G(G \subseteq F \wedge E \sim G);$$

which can also be written: $\text{card}(E) \leqslant \text{card}(F) :\Leftrightarrow \exists G(G \subseteq F \wedge E \sim G)$. By using the theorem of Zermelo and the ordinals, it is possible to prove that "$\leqslant$" is a well ordering.

Cardinal comparison: For any sets E and F, their cardinal numbers satisfy $|E| \leqslant |F|$ if and only if there is a one-to-one function f from E into F. About the properties, it is difficult to show the antisymmetry property, whose proof is known as Schröder-Bernstein theorem.

5.6. Denumerability, non denumerability.

Denumerability is closely related to infinite sets; note that the cardinals of infinite sets are not all identical.

Def. 138. *(Denumerable set). A set is denumerable if and only if it is equipollent to finite ordinal numbers. This property is also called "countable". (We'll see later the aleph-0 set, it is most commonly called "denumerable", "countably infinite").*

Ex. 43. *Cardinal of any set A is smaller than the cardinal of $\mathfrak{P}(A)$ which is the set of all the subsets of A ($|A| < |\mathfrak{P}(A)|$ or $\text{card}(A) < \text{card}(\mathfrak{P}(A))$). Cardinality is a relative notion, indeed, two sets may each have an infinite number of elements, but one may have a greater cardinality. Example of this case can be seen by Cantor diagonal method which shows how the reals $\mathbb{R}$ have a cardinality greater than natural numbers, then $|\mathbb{R}|>|\mathbb{N}|$.*

Ex. 44. *On the contrary, the set of the rational numbers $\mathbb{Q}$ has the same power or cardinality than the set $\mathbb{N}$, which is written $|\mathbb{Q}| = |\mathbb{N}|$. This can be proved by using Cantor diagonal method.*

Cantor diagonal method: The Cantor diagonal method, also called the Cantor diagonal argument, is a technique used by Cantor to show that the *integers* and *reals cannot be put into a one-to-one correspondence,* meaning that *the uncountably infinite set of real numbers is larger than the countably infinite set of integers.* In the set theory, Cantor considers that "*there are different degrees of infinity*". Indeed, *the rational numbers are countably infinite* (meaning that it is possible to enumerate all the rational numbers by means of an infinite list). On the contrary, *the real numbers are uncountable* (meaning that it is impossible to enumerate them by means of an infinite list). The notion of cardinality is of course underlying, and can be expressed by: "*two sets have the same cardinality if there exists a bijective correspondence between them*". Connected with these previous developments, there are two important Cantor theorems. One of both theorems shows that *the set of real numbers has the same cardinality as the power set of the naturals.* The other Cantor theorem shows that *a set and its power set have a different cardinality.* The proof of this theorem is based on the diagonalization argument. Cantor proves that for every given infinite sequence of reals r_1, r_2, r_3,... we can construct a real r which is not on the list of this sequence. Then it is impossible to enumerate the real numbers, thus they are uncountable. Cantor's original proof shows that the interval [0,1] is not countably infinite. Indeed, without loss of generality it is possible to suppose that all the numbers on the list are between 0 and 1. If this subset of the real numbers is uncountable, then the full set is uncountable also. Consider the sequence mentioned previously as a table of "*decimal expansions*":

$$\begin{array}{lllllll} r_0 = 0. & d_{11} & d_{12} & d_{13} & d_{14} & \cdots \\ r_1 = 0. & d_{21} & d_{22} & d_{23} & d_{24} & \cdots \\ r_2 = 0. & d_{31} & d_{32} & d_{33} & d_{34} & \cdots \\ r_3 = 0. & d_{41} & d_{42} & d_{43} & d_{44} & \cdots \\ \vdots \quad \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

where $r_n = 0.d_{n1}d_{n2}d_{n3}d_{n4}...$, and the expansion avoids an infinite trailing string of the digit 9. Then, a digit k_n is chosen for each $n = 1, 2, ...$, which is different from d_{nn} and which is not equal to 9, and we consider the real number r with decimal expansion:

$$0.k_1k_2k_3....$$

this "new" number r is different from every member of the initial given sequence. Process fully realized, for every n, the number r is different from the number r_n in the n^{th} decimal digit; "case made".

Ex. 45. *(Denumerability of the set $\mathbb{Q}$). A rational number is a number determined by the ratio of some integer p to some nonzero natural number q. The set of rational numbers is denoted $\mathbb{Q}$, and represents the set of all possible integer to natural number ratios $\frac{p}{q}$. If a and b are rational numbers such that $a < b$, then there exists a rational number x such that $a < x < b$. Whatsoever the difference between a and b, even very small, this reasoning is true, as long as a and b are not equal. It is also a way to explain that the set $\mathbb{Q}$ is "dense". In spite of this, $\mathbb{Q}$ is a denumerable set. Denumerability refers to the fact that, even though a set might contain an infinite number of elements, and even though those elements might be densely full, the elements can be defined by a list that assigns them for each one a unique number in a sequence corresponding to the set of natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$. Regarding the set of natural numbers $\mathbb{N}$ and the set of integers $\mathbb{Z}$, neither of which are dense, the lists are more directly reached. But in the case of the set $\mathbb{Q}$, the construction of such a list is less simple.*

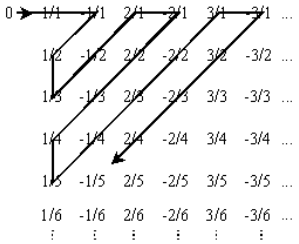


Fig: Cantor diagonal method for the set $\mathbb{Q}$.

We can illustrate this construction by a picture (Fig.) and the following example. The picture representes a matrix which contains all possible numbers $\frac{p}{q}$ *(where* p *is an integer and* q *is a nonzero natural number), then every possible rational number is represented in the array. In the figure, if one follows the "grey line",* 0 *is the first stop,* $\frac{1}{1}$ *is the second stop,* $-\frac{1}{1}$ *is the third stop,* $\frac{1}{2}$ *is the fourth stop, etc... This progression describes a sequential list, although redundant, of the rational numbers. There is a correspondence between the elements of the array and the set of natural numbers* $\mathbb{N}$. *In order to demonstrate a "one-to-one correspondence" between* $\mathbb{Q}$ *and* $\mathbb{N}$, *a modification must be introduced in the process. Indeed, some of the elements in the matrix are repetitions of previous numerical values. For example,* $\frac{2}{4} = \frac{3}{6} = \frac{4}{8} = \frac{5}{10} = \frac{6}{12} = \frac{7}{14} = \cdots$. *These repetitions and redundancies can be eliminated by introducting the following rule: "If a number represents a value previously encountered, skip over it". Thus, by this method, it can be proved that the set* $\mathbb{Q}$ *has exactly the same number of elements as the set* $\mathbb{N}$, *and consequently the same cardinality as seen before* $|\mathbb{Q}| = |\mathbb{N}|$.

The above picture depicts a process constructing a surjective map $d : \mathbb{N} \to \boxed{\mathbb{Q}}$. *If during the process we skip the values already encountered (e.g.* $\frac{6}{2} = \frac{3}{1} = ...$*), then the map becomes a* ***bijective map***.

Since "two sets have the same cardinality if there is a bijective correspondence between them", the one-to-one correspondence between the sets $\mathbb{N}$ *and* $\mathbb{Q}$ *leads to the identity between their respective cardinality:* $|\mathbb{N}| = |\mathbb{Q}|$.

Ex. 46. *(Numerable and non numerable sets). As opposed to the natural numbers, integers, and rational numbers, sets of irrational numbers, real numbers, imaginary numbers, and complex numbers are non denumerable. They have cardinality greater than that of the set* $\mathbb{N}$. *Then, we can write that some "infinities" are larger than others.*

Def. 139. *(Denumerability, non denumerability). A set* S *is said to be* ***at most denumerable*** *if* $\text{card}(S) \leqslant \aleph_0$, *where* $\aleph_0 = \text{card}(\mathbb{N})$. *A set* S *is said to be* ***denumerable*** *if* $\text{card}(S) = \aleph_0$. *A set* S *is said to be* ***non denumerable*** *if* $\text{card}(S) > \aleph_0$.

Def. 140. *(Cardinal of* $\mathbb{R}$. $-$ ***Continuum***). *The cardinal of* $\mathbb{R}$ *is denoted* $\mathfrak{c} : \text{card}(\mathbb{R})$, *where* $\mathfrak{c}$ *is called the continuum.*

The term "continuum" has at least two distinct meanings in mathematics. The first is the non denumerable set of real numbers, denoted $\mathfrak{c}$ and the second is a compact connected metric space.

Aleph-0: The symbol $\aleph_0$ belongs to the set theory, and refers to a set having the same cardinal number as the "small" infinite set of integers. $\aleph_0$ is pronounced aleph-null rather than aleph-zero, due to the Cantor's native language. Algebraic numbers belong also to $\aleph_0$. Some properties of $\aleph_0$ are:

(1) $\aleph_0^p = \aleph_0 \qquad$ for $p > 0$
(2) $p\aleph_0 = \aleph_0 \qquad$ for $p \neq 0$
(3) $\aleph_0 + \Phi = \aleph_0$

where Φ is any finite set. Furthermore,

(4) $\aleph_0^{\aleph_0} = \mathfrak{c}$

where $\mathfrak{c}$ is the "*continuum*". The continuum $\mathfrak{c}$ is the non denumerable set of real numbers, which satisfies:

(5) $\aleph_0 + \mathfrak{c} = \mathfrak{c}$
(6) $\mathfrak{c}^i = \mathfrak{c}$
(7) $y^{\aleph_0} = \mathfrak{c} \quad$ for $y \geqslant 2$
(8) $\mathfrak{c}^{\mathfrak{c}} = \Omega$.

where i is a positive integer, and $\mathfrak{c}^{\mathfrak{c}} = \Omega$ represents *a set larger than the continuum.* Aleph-0, $\aleph_0$, is the smallest infinite cardinal, because any infinite set contains a denumerable infinite part, and because any subset of a denumerable set is at most denumerable. First proposed by Cantor, the continuum hypothesis enunciates that $(\mathfrak{c})$ is the smallest cardinal which is greater than $\aleph_0$ $(\mathfrak{c} > \aleph_0)$. This hypothesis was proved as undecidable.

Aleph-1: $\aleph_1$ is the set theory symbol for the smallest infinite set larger than $\aleph_0$ $(\aleph_1 > \aleph_0)$. As seen before, the continuum hypothesis asserts that $\aleph_1 = \mathfrak{c}$, where $\mathfrak{c}$ is the cardinality of the large infinite set of real numbers, called the continuum in set theory. An n-dimensional space has the same number of points $\mathfrak{c}$ as one-dimensional space, or any finite interval of one-dimensional space, a line segment, as was first understood by Cantor.

Considering the concepts of denumerability and non denumerability, we can describe an interesting operation on cardinals. Indeed, considering that if E is a *non denumerable set* and F a *numerable set*, we write $E \cup F \sim E$, then the following essential rule can be deduced: $|E| \geqslant \aleph_0 \wedge |F| \leqslant \aleph_0 \Rightarrow |E \cup F| = |E|$, i.e. $|E| + n = |E| + \aleph_0 = |E|$.

Rem. 3. *Given* $\mathbb{Q}^n = \mathbb{Q} \times \cdots \times \mathbb{Q}$ *and* $\bigcup_{i=1}^n E_i$, *then the cardinalities are the same* $|E_i| = |\mathbb{N}|$.

Rem. 4. *(Non denumerability of the set* $\mathbb{R}$*). Consider non-denumerable sets, the set of real numbers* $\mathbb{R}$ *is a famous example. A demonstration of the non denumerability of* $\mathbb{R}$ *is proved on a subset of* $\mathbb{R}$, *then is proved on* $\mathbb{R}$. *Such a subset can be denoted for example by* I. *Thus, consider a bijection:* $f : I \to \mathbb{R}$ *such that:* $x \mapsto f(x) = \frac{x-1/2}{x(x-1)}$, *with* $I = \{x : 0 < x < 1, x \in \mathbb{R}\}$, $\mathbb{R}$ *and* I *are equipotent:* $\boxed{\mathbb{R} \sim I}$. *The non denumerability of* $\mathbb{R}$ *is proved first on* I *and is demonstrated by the absurd. Indeed,* $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$, *has the same cardinality than* $\mathbb{R}$, *as also the complex number set* $\mathbb{C}$ *and the quaternion set. Then the set of points of a straight line and the set of points of a 3-dimension euclidian space are equipotent, which means that the dimension is not invariant under any bijective map. Proof by the absurd can be written:*

Proof. The initial hypothesis is: "I *is denumerable*". Then, there exists a bijective map $\mathbb{N} \to I$, such that (with $z_{ij} \in \{0,1,..,9\}$):

$$\begin{array}{ccccccccccc}
0 & \leftrightarrow & r_0 & = & 0. & z_{00} & z_{01} & z_{02} & z_{03} & \cdots \\
1 & \leftrightarrow & r_1 & = & 0. & z_{10} & z_{11} & z_{12} & z_{13} & \cdots \\
2 & \leftrightarrow & r_2 & = & 0. & z_{20} & z_{21} & z_{22} & z_{23} & \cdots \\
3 & \leftrightarrow & r_3 & = & 0. & z_{30} & z_{31} & z_{32} & z_{33} & \cdots \\
4 & \leftrightarrow & r_4 & = & 0. & z_{40} & z_{41} & z_{42} & z_{43} & \cdots \\
\vdots & & \vdots & & & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

The number $r = 0.\hat{z}_0\hat{z}_1\hat{z}_2...$, with $\hat{z}_i = 2$ if $z_{ii} = 1$ and $\hat{z}_i = 1$ if $z_{ii} \neq 1$ is not reached. There is *contradiction.* □

Quaternion (or "hypercomplex" number): It is the division algebra over the real numbers generated by the elements i, j, k subject to the relations $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$. Quaternion is also known as the *hypercomplex* number.

6. Cardinals

6.1. Induction (noetherian induction).

1) Noetherian induction. We say that at $n_0 \in \mathbb{N}$ a sequence (u_n) is stationary (at n_0) if it is constant from n_0 (rank), i.e. if $\forall n \geq n_0$, $u_n = u_{n_0}$. Now, introduce this proposition (which is also a definition):

Prop.1 *Let* E *be an ordered set. Following properties are equivalent:* (i) *Any increasing sequence of* E *is stationary.* (ii) *There is not strictly increasing sequence in* E. (iii) *Any nonempty part of* E *has a maximal element. We say that the ordered set* E *is noetherian.*

Proof. Assume the property (i) true. If there was in E a strictly increasing sequence, it would be increasing and not stationary, contradicting (i). This shows that $(i) \Rightarrow (ii)$. Now, assume the property (ii) true. We prove (iii) by the absurd. Let $A \subset E$ be a nonempty part that does not admit maximal element. From these hypotheses, we construct a strictly increasing sequence in A, so in E. Since A is nonempty, we can choose $u_0 \in A$, and we can choose $u_1 \in A$ such that $u_0 < u_1$. Iterating this process, we construct a strictly increasing sequence, contradicting (ii). This shows that $(ii) \Rightarrow (iii)$. Now, assume the property (iii) true. Let $(u_n)_{n\in\mathbb{N}}$ be an increasing sequence in E. The image $\{u_n | n \in \mathbb{N}\}$ of this sequence is an nonempty part of E, which thus admits (by assumption) a maximal element u_{n_0}. Since the sequence is increasing, then it is stationary (at n_0). □

The reasoning by induction (i.e. by recurrence) generalizes in $\mathbb{N}$, this is the "*Noetherian induction principle*", but it is based rather on the existence of minimal elements. We will call *artinian* an ordered set in which every nonempty part admits a minimal element; equivalently, every deceasing sequence is stationary; or also, there is no strictly deceasing sequence; e.g. every finite ordered set is smultaneously *artinian* and *noetherian.*

Th. 28. *(Noetherian induction principle). Let* E *be an artinian set. Let* $P(x)$ *be a property defined on* E *and verifying the hereditary property:* $\forall x \in E$, $(\forall y < x, P(y)) \Rightarrow P(x)$. *Then* P *is true on the whole of* E: $\forall x \in E$, $P(x)$.

PROOF. Let A be the set of $x \in E$ that does not satisfy $P(x)$. Assume A nonempty. Then it has a minimal element x. Thus, for every $y < x$, $y \notin A$, in other words $P(y)$. According to the hereditary property, we have then $P(x)$, which is not possible since $x \in A$. Thus A is empty, which is the sought condition. □

Ex. 47. *The set of monic polynomials (also called unit polynomials, or unitary polynomials) over a field K, ordered by the relation of divisibility, is artinian. In fact, If $P|Q$, then $\deg P \leq \deg Q$ and we know that there is not strictly decreasing sequence of natural numbers. Show by noetherian induction that every monic polynomial (unit polynomial) is product of irreducible polynomials; here we underly that the empty product is 1. It suffices to show the hereditary of this property. Therefore, let P be a monic polynomial (unit polynomial) such that every strict divisor of P is product of irreducibles. If P is irreducible, we have nothing to show. Otherwise, $P = QR$ where Q and R are monic polynomials (or unit polynomials) and strictly divide P. By noetherian induction assumption, they are product of irreducibles, so $P = QR$ is also. The property is therefore hereditary, therefore true for every monic polynomial (unit polynomial).*

2) Well-ordered sets. The general (non totally ordered) noetherian or artinian sets mainly appear in commutative algebra.

Def. 141. *(Well-ordered set). We say that the set E is well-ordered if every nonempty part of E admits a smallest element. We also say that its order is a well-order (or well-ordering).*

Ex. 48. *$(\mathbb{N}, \leq)$ is a classic example of well ordered set. Since a smallest element is minimal, every well-ordered set is artinian. If we consider a pair $\{a, b\}$, we see that the order is moreover total (if a is the smallest element, $a \leq b$, if b is the smallest, $b \leq a$). Conversely, every artinian total order is a well order: indeed, every nonempty part admits a minimal element, which is necessarily minimum (since the order is total). Zermelo's theorem states that every set can be endowed with a well order. This is clearly true for a finite order: it suffices to endow it with any arbitrary total order, which is not difficult. For a denumerable set, this is still possible; we use any aribitrary bijection $\phi : E \to \mathbb{N}$ and we set $x \leq y$, if and only if $\phi(x) \leq \phi(y)$. Note that we have to take care that the denumerable totally ordered sets $\mathbb{Z}$ and $\mathbb{Q}$ are not well ordered. (As an exercise we could also try to look for a well order on $\mathfrak{P}(\mathbb{N})$ or on $\mathbb{R}$ to understand the meaning of Zermelo's theorem.)*

3) Zorn lemma. First, consider a set S endowed with a law $\star$, and $(X_i)_{i\in I}$ a family of *stable* parts of S. The union X of the X_i has no reason to be stable. Indeed if $x, y \in X$ then there are indexes i,j such that $x \in X_i$ and $y \in X_j$, but (except if i=j) we have nothing to deduce. But if we suppose that two any arbitrary parts X_i are comparable for the inclusion, we have either $X_i \subset X_j$, or $X_j \subset X_i$; in the first case, x,$y \in X_j \Rightarrow x \star y \in X_j \Rightarrow x \star y \in X$, and similarly for the second case.

Def. 142. *(Chain of an ordered set).* (1) *We call "chain" of an ordered set E a nonempty family of elements of E that are pairwise comparable.* (2) *We say that E is inductive if any chain of E is bounded from above.*

Consequently, the union of a chain of stable parts of E is stable. The set of stable parts ordered by inclusion, is therefore an inclusion.

Lem. 3. *(Zorn lemma). Any inductive set admits a maximal element. More precisely, in an inductive set, any element is bounded from above by a maximal element.*

(The proof is not given here.) This lemma/theorem is essentially equivalent to Zermelo theorem and the axom of choice. Zorn lemma will be applied in the next heading, and in other headings of the present book.

6.2. Equipotence. We have already stated the definition of equipotence (in heading "*Number, equipotence and cardinality*"); indeed, we know that the set E and F are *equipotent* if there exists a bijection from E to F. Any set is equipotent to itself (by taking as bijection the identity); if E is equipotent to F and F to G, then E is equipotent to G (by taking the composition of two bijections); finally, if E is equipotent to F, then F is equipotent to E (by taking the inverse of the bijection). Equipotence is thus an *equivalence relation*. For finite sets, the equipotence is the relation "have the same number of elements". What is common between all sets equipotent to a given finite set is therefore an integer. For abitrary set, the general notion is that of cardinal, but its definition requires (an axiom which is also) a definition:

Def. 143. *We can associate with each set E an object called cardinal of E, denoted $\mathrm{card}(E)$, satisfying the following rule: two sets E and F have same cardinal if and only if they are equipotent.*

We write $0 := \mathrm{card}(\varnothing)$. The sets equipotent to a given singleton (resp. to a given pair) are the singletons (resp. the pairs), and we write $1 := \mathrm{card}\{a\}\ \forall a$ and $2 := \mathrm{card}\{a, b\}\ \forall\ a, b$ distinct, etc. Some presentations of set theory call "power" what we call "cardinal" and call "cardinal of E" a set selected in the class of E.

Def. 144. *We have $\mathrm{card}(E) \leqslant \mathrm{card}(F)$ ("less than or equal to") if there exists an injective map from E to F.*

Prop.A *If $E \neq \varnothing$, the relation $\mathrm{card}(E) \leqslant \mathrm{card}(F)$ is equivalent to the existence of a surjection from F to E.*

PROOF. It results from this proposition: □

Prop.B *Given E,F two nonempty sets. (i) Let $f : E \to F$ an injective map. There exists then a map $r : F \to E$ such that $r \circ f = Id_E$. The map r is surjective. We say that this is a **retraction** of f. (ii) Let $g : F \to E$ a surjective map. There exists then a map $s : E \to F$ such that $g \circ s = Id_F$. The map s is injective.*

PROOF. (*i*) For any element $y \in \mathrm{Im}\, f$, we define $r(y)$ as the unique antecedent of y by f (this antecedent exists because $y \in \mathrm{Im}\, f$, it is unique because f is supposed to be injective). For any $y \in F \backslash \mathrm{Im}\, f$, we define $r(y)$ as an arbitrary element of E (it's possible because E is nonempty). We verify easily that we have indeed $r(f(x)) = x$ for any $x \in E$. Implying in particular that any $x \in E$ admits at least an antecedent by r, that is $f(x)$. The map r is surjective indeed. (*ii*) $\forall x \in E$, we define $s(x)$ as (arbitrary) one of antecedents of x by g (it's possible since this one is surjective). We easily check that we have indeed $g(s(x))$=x,$\forall x \in E$. If we have $s(x)$=$s(x')$, then x=$g(s(x))$=$g(s(x'))$=x', and the map s is indeed injective. □

Th. 29. *(Cantor-Schröder-Bernstein th.). If there exist an injection from E to F and an injection from F to E, then E and F are equipotent.*

PROOF. Let us write $f : E \to F$ and $g : F \to E$ these injections. The map $h := g \circ f$ forms a bijection from E to $h(E)$ and the set $E' := g(F)$ (which is therefore in bijection with F) is such that $h(E) \subset E' \subset E$. It suffices to find a bijection from E to E'. The iterated images $h^n(E)$ (defined by $h^0(E) := E$ and $h^{n+1}(E) := h(h^n(E))$ form a decreasing sequence of parts of E. Given R their intersection. We verify that h induces a bijection from R to itself. Let us set $A_0 := E\backslash h(E)$ ("\" denotes the difference of E and F), then, by induction (by recurrence), $A_{n+1} := h(A_n) = h^n(E)\backslash h^{n+1}(E)$. Thus, h induces a bijection from A_n to A_{n+1} and the A_n are pairwise disjoint. We can write $E = (A_0 \cup \cdots \cup A_n \cup \cdots) \cup R$, the union being disjoint. The effect of h is therefore to send bijectively A_n to A_{n+1} and R bijectively to itself. Write now $A_0 := E\backslash h(E)$ as disjoint union of $B_0 := E\backslash E'$ and of $C_0 := E'\backslash h(E)$. Similarly, introduce the iterated images $B_{n+1} := h(B_n)$ and $C_{n+1} := h(C_n)$ so that each A_n is disjoint union of B_n and of C_n. Now we have two writings in disjoint union:
$E = (B_0 \cup C_0 \cup B_1 \cup C_1 \cup \cdots \cup B_n \cup C_n \cup \cdots) \cup R$,
$E' = (C_0 \cup B_1 \cup C_1 \cup \cdots \cup B_n \cup C_n \cup \cdots) \cup R$.
Now it is easy to construct the bijection from E to E': on the C_i and in R, this is the identity; on each B_n, this is the bijection $h : B_n \to B_{n+1}$. □

Cor. 5. *The relation $\leqslant$ between cardinals is an order relation.*

PROOF. Since the identity is injective and since the composition of two injective maps is injective, this relation is reflexive and transitive. The antisymmetry is a consequence of the previous theorem. □

Th. 30. *It is a total order.*

PROOF. Given E and F two arbitrary sets. We have to show that there exists an injection from the one to the other. We are going to show that there exists a bijection from the one to a part of the other, which is equivalent. To this end, introduce the set $\mathcal{E}$ whose elements are the triplets (A, f, B) consisting of a part A of E, of a part B of F and of a bijection f from A to B. This set is nonempty, since it contains $(\varnothing, f, \varnothing)$ (where f is the unique bijection from $\varnothing$ to itself). Let us set $(A, f, B) \preceq (A', f', B')$ if and only if $A \subset A'$, $B \subset B'$, and $f'_{|A} = f$. We verify easily that this an order relation on $\mathcal{E}$. We are going to this one is inductive. Given $\mathcal{C} = (A_i, f_i, B_i)_{i\in I}$ a chain of $\mathcal{E}$ (cf. def. of a *chain*). Let us set $A = \cup_{i\in I} A_i$ and $B = \cup_{i\in I} B_i$. Given $x \in A$; whatever $i \in I$ such that $x \in A_i$, $f_i(x) \in B$ has the same value. Indeed, if $x \in A_j$, we have for example $(A_i, f_i, B_i) \preceq (A_j, f_j, B_j)$ (because $\mathcal{C}$ is a chain), therefore f_i is the restriction of f_j, so $f_j(x) = f_i(x)$. Therefore we can write $f(x) = f_i(x)$ for any $i \in I$ such that $x \in A_i$. We see easily that $f : A \to B$ is a bijection, and that (A, f, B) is an element of $\mathcal{E}$

by which $\mathcal{C}$ is bounded from above: the set $\mathcal{E}$ is inductive. According to Zorn lemma (cf. heading "*Zermelo and Zorn theorems*") it admits a maximal element (A, f, B). Let us show that $A = E$ or $B = F$. It were not the case, there would be elements $a \in E\backslash A$ and $b \in F\backslash B$. By setting $A' = A \cup \{a\}$, $B' = B \cup \{b\}$ and by defining $f' : A' \to B'$ by $f'_{|A} = f$ and $f'(a) = b$, we would construct an element (A', f', B') of $\mathcal{E}$ by which (A, f, B) is strictly bounded from above, contredicting thus the maximality of this last. Thus we have indeed $A = E$ or $B = F$. In the first case, $\text{card}(E) \leqslant \text{card}(F)$; in the second case, $\text{card}(F) \leqslant \text{card}(E)$. □

Ex. 49. *The map $x \mapsto \{x\}$ is injective from E to $\mathfrak{P}(E)$. According to Cantor theorem (cf. heading "Images and antecedents"), there exists no surjection from E to $\mathfrak{P}(E)$, and therefore no injection from $\mathfrak{P}(E)$ to E (cf. **prop.B**). We have thus* $\text{card}(E) < \text{card}(\mathfrak{P}(E))$.

We will define (although the cardinals do not form a set) operations on them (while using vocabulary/notation of the section "*Laws of composition*"). Let E, F be two sets. To definition the *sum of two cardinals* E and F, we choose arbitrarily a set E' equipotent to E and a set F' equipotent to F, in a such way that E' and F' are disjoint; e.g. $E' := E \times \{0\}$ and $F' := F \times \{1\}$ are disjoint and we have bijections $E \to E'$, $x \mapsto (x, 0)$ and $F \to F'$, $y \mapsto (y, 1)$. This method (due to von Neumann) is analogous to the "renaming" used in computer science. We set then $\text{card}(E) + \text{card}(F) = \text{card}(E' \cup F')$; indeed, it is clear that with another choice E'', F'', we would have a bijection from $E' \cup F'$ to $E'' \cup F''$, hence the equality $\text{card}(E' \cup F') = \text{card}(E'' \cup F'')$. Then it is easy to show that the addition of cardinals is an associative law, commutative, with neutral element 0. In contrast, no cardinal is cancellable.

To define the *product of two cardinals*, we check (as above) that $\text{card}(E \times F)$ depends only on $\text{card}(E)$ and on $\text{card}(F)$. It is denoted by $\text{card}(E) \times \text{card}(F)$. It is also an associative law, commutative, with neutral element 1. Moreover, it is distributive with respect to the addition. It follows that if k is a nonzero integer (a finite cardinal), and if $\aleph$ (aleph) is an arbitrary cardinal, the product $k\aleph$ is equal to the sum of k terms $\aleph + \cdots + \aleph$.

Note that $\text{card}(\mathcal{F}(E, F))$ (recall: $\mathcal{F}(E, F)$ the set of maps from E to F) depend only on $\text{card}(E)$ and on $\text{card}(F)$. It is denoted $(\text{card}(F))^{\text{card}(E)}$ (read "$\text{card}(F)$ power $\text{card}(E)$"). This is a natural notation in the sense that if E and F are finite and respectively have n and p elements, then $\mathcal{F}(E, F)$ is finite and has p^n elements. Many rules on the power numbers hold; e.g. if k is a nonzero natural number (a finite cardinal), and $\aleph$ an arbitrary cardinal, the power $\aleph^k$ is equal to the product of k factors $\aleph \cdots \aleph$. Here is an important statements:

Th. 31. (*i*) *For any set E, we have* $\text{card}(\mathfrak{P}(E)) = 2^{\text{card}(E)}$. (*ii*) *For any cardinal $\aleph$, we have $\aleph < 2^{\aleph}$.*

Proof. We already proved (cf. theorem (†) in the heading "*Family of parts of a set*") that $\mathfrak{P}(E)$ and $\mathcal{F}(E, \{0, 1\})$ were equipotent, hence the first statement. (*ii*) results from the previous example. □

These operations are increasing functions of each arguments.

6.3. Finite and infinite cardinals.

Def. 145. *(Finite set; infinite set). A set E is called finite if there is no bijection from E to a part of E other than itself. Otherwise, it is called infinite.*

By induction we show that each of sets of the sequence $E_0 = \varnothing$, $E_{k+1} = E_k \cup \{E_k\}$ is finite, then that every finite set is equipotent to one and only one of these sets. At this stage, we cannot prove the existence of infinite sets, this is the role of the "*axiom of infinity*". We state below the axiom of infinity in a somewhat special form (which is also written as a definition):

Axiom of infinity. *The von Neumann integers E_k form a set, which is denoted* $\mathbb{N}$.

A von Neumann integer is not an integer, but instead a construction of a natural number using some basic set notation. The von Neumann integers are defined inductively. The von Neumann integer zero is defined to be the empty set $\emptyset$ and there are no smaller von Neumann integers. The von Neumann integer N is then the set of all von Neumann integers less than N . The set of von Neumann integers is the set of all finite von Neumann ordinals. This form of construction from very basic notions of sets is applicable to various forms of set theory (e.g. Zermelo-Fraenkel set theory). While this construction suffices to define the set of natural numbers, a little more work is needed to define the set of all integers. Ex. 0=$\emptyset$, 1={0}={$\emptyset$}, 2={0,1}={$\emptyset$,{$\emptyset$}}, 3={0,1,2}={$\emptyset$,{$\emptyset$},{{$\emptyset$,{$\emptyset$}}}},.., N={0,1,..,N-1}.

Return to the above axiom of infinity; having assumed its existence we can indeed prove this set is infinite. Conversely, we can show that, if there exists an infinite set E, the E_k form a set $\mathbb{N}$ and there exists an injective map from $\mathbb{N}$ to E.

(1) The set $\mathbb{N}$ of natural integers is infinite. Its cardinal is denoted by $\aleph_0$ (Aleph-0).

(2) Any finite set plunges injectively in $\mathbb{N}$. We have therefore for any natural integer n, considered as a cardinal: $n < \aleph_0$.

(3) For any infinite set E, there exists an injection from $\mathbb{N}$ to E. Therefore, for any infinite cardinal $\aleph$, $\aleph_0 \leqslant \aleph$.

Thus $\aleph_0$ is the smallest of infinite cardinals. We will say that a set E is denumerable (countable) if there exists an enumeration (counting) of E, i.e. a **bijection** from $\mathbb{N}$ to E. This is equivalent to say that E is equipotent to $\mathbb{N}$, i.e. $\text{card}(E) = \aleph_0$. We will show some formulas about $\aleph_0$ (by being partially based on explicit bijections; make explicit mutual bijections are left to reader as an exercise).

Beforehand, let us start with the following: *Exercise*: Identify the set {0,1,-1,2,-2,..}. *Solution*: It's obviously $\mathbb{Z}$. It can be described by the sequence $(u_n)_{n\in\mathbb{N}}$ defined by the formulas: $u_{2_p} = -p$ and $u_{2p+1} = -p + 1$. This exercise highlights an enumeratiion of $\mathbb{Z}$. We deduce that $\text{card}(\mathbb{Z}) = \aleph_0$. But $\mathbb{Z}$ is the disjoint union of $\mathbb{N}$ and $-\mathbb{N}^*$, and the last set is enumerated by $n \mapsto -n - 1$. We have therefore (by definition of the sum of cardinals) the formula: $\aleph_0 + \aleph_0 = \aleph_0$.

It is possible to enumerate $\mathbb{N} \times \mathbb{N}$ by successively running through the following sets: {(0,0)}, then, {(1,0),(0,1)}, then, {(2,0),(1,0),(2,2)},.. The reader will can show that the image of n is obtained as follows: We bound n by $\frac{k(k+1)}{2} \leq n < \frac{(k+1)(k+2)}{2}$, this comes down to write: $n = \frac{k(k+1)}{2} + \mu$, with $0 \leq \mu \leq k$. This writing is unique. Then we associate with n the pair $(k - \mu, \mu) \in \mathbb{N} \times \mathbb{N}$. We deduce from this enumeration that $\text{card}(\mathbb{N} \times \mathbb{N}) = \aleph_0$. Thus, we have (by definition of the product of cardinals) the following formula: $\aleph_0\aleph_0 = \aleph_0$.

As application, calculate $\text{card}(\mathbb{Q})$. Since $\mathbb{N} \subset \mathbb{Q}$, we have $\aleph_0 \leq \text{card}(\mathbb{Q})$. Moreover, define an injective map by associating with every $x \in \mathbb{Q}$ the unique pair $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ such that $\frac{a}{b} = x$ and a, b are relatively primes. Therefore $\text{card}(\mathbb{Q}) \leq \aleph_0\aleph_0 = \aleph_0$. Since $\leq$ is an order relation, we have $\text{card}(\mathbb{Q}) = \aleph_0$.

It is also possible to show that the set $\mathfrak{P}_f(\mathbb{N})$ of finite parts of $\mathbb{N}$ is denumerable (not shown here).

In order to state the next theorem, first state some rules:

(1) Let $\aleph_1$ and $\aleph_2$ be two cardinals. Then $\aleph_1 \leq \aleph_2 \Leftrightarrow \exists\aleph_3 : \aleph_2 = \aleph_1 + \aleph_3$. Indeed, write $\aleph_1 \leq \aleph_2$ is equivalent to say that there exists sets E_1, E_2 of cardinals $\aleph_1, \aleph_2$ and such that $E_1 \subset E_2$, i.e. such that E_2 is the disjoint union of E_1 and of a set E_3.

(2) Let $\aleph$ be a cardinal. Then $\aleph_0 \leq \aleph \Leftrightarrow \aleph = \aleph_0 + \aleph$. Indeed, if $\aleph_0 \leq \aleph$ we can write $\aleph = \aleph_0 + \aleph_1$, hence $\aleph+\aleph_0=\aleph_0+\aleph_0+\aleph_1=\aleph_0+\aleph_1$. The converse is evident.

(3) Let A be a denumerable set included in a set B non denumerable. Then $B\backslash A$ is equipotent to B. The set $B\backslash A$ is infinite, otherwise B would be denumerable.

Th. 32. *The cardinal of $\mathbb{R}$ is $2^{\aleph_0}$. We say that a set equipotent to $\mathbb{R}$ has the **power of the continuum**.*

Proof. The numbering (base 2) of real numbers garantees that any $x \in]0,1[$ admits a unique writing in the form $\sum_{n\geqslant 0} \varepsilon_n 2^{-n}$, where the sequence $(\varepsilon_n)_{n\in\mathbb{N}}$ is an element of $\{0, 1\}^{\mathbb{N}}$ such that: the ε_n are not all zero; they are not equal to 1 starting from a certain rank. We get thus a bijection from $]0,1[$ to $\{0,1\}^{\mathbb{N}}\backslash A$, where A is a denumerable part of $\{0,1\}^{\mathbb{N}}$. According to the last rule, $\text{card}(]0, 1[)=2^{\aleph_0}$. We conclude by any bijection from $\mathbb{R}$ to $]0, 1[$, e.g. the map $x \mapsto \frac{1}{2}(1+\frac{x}{\sqrt{1+x^2}})$. □

A famous problem of set theory was for a long time to know if there were a cardinal between the power of countable (or denumerable) and that of continuum, in other words, such that $\aleph_0 < \aleph < 2^{\aleph_0}$. The hypothesis of the continuum, formulated by Cantor, stated that it was impossible. Theorems due to softwares of Gödel (1939) and Cohen (1963) imply that neither the hypothesis of the continuum nor its negation are denumerable in the framework of (usual) set theory.

7. Structures

7.1. Fundamental structures. Bourbakist conception of mathematics has allowed to erase the compartmentalization existing between the different mathematical disciplines. Study of axiomatic constructions of the various theories reveals common fundamental structures. Traditional disciplines develop then based on these fundamental structures and on the multiple structures constructed from these fundamental structures before using supplementary axioms and definitions.

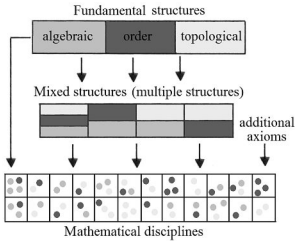


Fig. Construction of disciplines from structures.

Fundamental structures: The three *fundamental structures* are: *algebraic structure*, *structure of order* and *topological structure*. *Multiple structures* (or *mixed structures*) consists of several of the three fundamental structures. Examples of *multiple structures* are *topological groups*, *topological vector spaces*, *ordered fields*.

(1) *Algebraic structure:* A set can be endowed with an *algebraic structure* if one or several composition laws (internal or external) are defined on this set (such as addition and multiplication in the set of numbers, or multiplication of a vector with a scalar). Most important algebraic structures are *semigroup*, *group*, *ring*, *field*, *module* and *vector space*. *A module is a vector space in which scalars are a ring rather than a field.*
(2) *Order structure:* A set can be endowed with an *order structure* if an order relation is defined on this set; meaning in this set that there exists comparable elements in accordance with a predefined rule, such as in the set of reals by using the relation "$\leqslant$". (Examples of order structures: *partially ordered sets (ordered sets), totally ordered sets, well ordered sets, inductive sets.*)
(3) *Topological structure:* A set can be endowed with a *topological structure* if we have chosen in this set a subsets system $\mathfrak{F}$ verifying differentes properties. The topological structure is very important to define the concept of *convergence*. A set which has a topological structure is called a *topological space*.

7.2. Multiple structures. A *multiple structure* (also known as *mixed structure*) is composed from several of the three fundamental structures. Examples of multiple structures are: *Topological groups*, *Topological vector spaces* and *Ordered fields* (Fig.).

Field	**Totally ordered set**	**Particular topological space**
$(\mathbb{R};+,\cdot)$	$(\mathbb{R};\leq)$	$(\mathbb{R};\mathfrak{R})$
Composition of elements	Composition of elements	Convergence of sequences
Algebraic structure	Order structure	Topological structure

Fig. Structure of the set $\mathbb{R}$ of reals.

7.3. System of relations.
The fundamental structures can be reduced to the relations which produce these structures. Then, a structured set is a set S on which is defined a family of relations $\{R_i\}$. If S is provided with the relations R_1,...,R_n, then the associated space is written $\{S; R_1,...,R_n\}$. And the pair consisting of S and R_1,...,R_n is called a *system of relations*. For $n \geqslant 2$, the relations which provide the structures must be mutually compatible. The conditions of compatibility must be carrefully chosen to construct a theory (cf. distributivity to construct rings).

7.4. Derived structures.
From fundamental structures, we can construct the three main types of structure:
(1) *Substructure:* A substructure is a "subsystem of relations". Indeed the relations, which belong to a *subset*, generate a *substructure*. Examples of substructures are: the *subgroups*, *subrings*, *subfields*, *submodules*, *topological subspaces*, *induced orders*.
(2) *Product structure:* A product structure is a system of "product relations". Let be the similarly structured spaces $(S_1, R_1), ..., (S_n, R_n)$, for example by means of relations R all p-connected, then $S = S_1 \times \cdots \times S_n$ will be provided with the product structure by the relation R statisfied by p elements of S if and only if, for all i=1,..,n their p components of the index i satisfy R_i.
(3) *Quotient structure:* A quotient structure is a system of "quotient relations". Indeed, when the structure of S is transported to a quotient space $S/\mathfrak{R}$, then a quotient structure is generated, by using the equivalence relation $\mathfrak{R}$ and byusing the relations which generate this structure. Examples of quotient structures are: *quotient groups, quotient rings*, *quotient fields*, quotient m*odules*, *topological quotient spaces*.

7.5. Structures, maps, morphisms. The *maps* also allow to construct links between the elements of sets equipped with *analogous structures*. As seen before, the relations which provide the structures must be *compatible* between them. It is essential that the maps are compatible with the structures of sets that they link. Such maps (Ex. infra) are called *morphisms* (cf. infra); and generally create a *reduced* image of the starting structure (i.e. *domain* of definition) in the structure of the codomain. Essential characteristics of structures are conserved, e.g. the "*group*" by the *group homomorphisms*, the "*ordered sets*" by the *increasing maps*, the "*convergence*" by the *continuous maps* (cf. heading: "*Sequence Convergence and Filter Base*" in *Topology*).

Ex. 50. *Ilustrations of maps compatible with the structures (morphisms).*

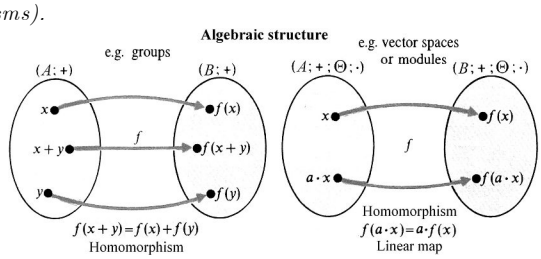


Fig. Algebraic structure.

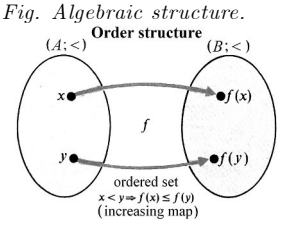


Fig. Order structure.

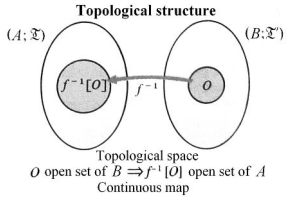


Fig. Topological structure.

When we face multiple structures, the morphisms must be compatible with each of the fundamental structures contained in these multiple structures. Morphisms of topological groups are continuous homomorphisms.

Morphisms: A *morphism* is a *map* between two *objects* in an *abstract category*. A category consists of a *collection of objects*, or, for each pair of *objects*, a *collection of morphisms* from one to another. An *object* is a *mathematical structure* (e.g. a group, vector space, differentiable manifold) *in a category. Homomorphisms*, *monomorphisms, epimorphisms*, *automorphisms* are types of *morphisms*.
(1) A general morphism is called a *homomorphism*.
(2) A morphism $f : F \to E$ in a category is a *monomorphism* if, for any two morphisms $\varphi, \psi : G \to F$, $f\varphi = f\psi$, implies that $\varphi = \psi$.
(3) A morphism $f : F \to E$ in a category is an *epimorphism* if, for any two morphisms $\varphi, \psi : E \to G$, $\varphi f = \psi f$, implies $\varphi = \psi$.
(4) A bijective morphism is called an *isomorphism,* if there is an isomorphism between two objects, then we say they are isomorphic.
(5) A surjective morphism from an object to itself is called an *endomorphism*.
(6) An isomorphism from an object to itself is called an *automorphism*.

7.6. Isomorphisms. 2 spaces of similar structures are regarded as equivalent with respect to the structures considered, if there exists a bijective morphism between them, whose inverse map is also a morphism. The isomorphisms of a structured set on itself is called *automorphism*. The set of all automorphisms of a structured set, provided with the composition of maps, is a *group* (group of automorphisms). This group is fundamental, especially in Galois theory.

8. Algebraic Structures

.In elementary algebra, we "calculate", i.e. we perform "operations". Thus 4+5=9 is an addition. As for the addition of natural numbers, it is the map associating with any pair of natural numbers their sum (and not the addition of two particular integers): the addition becomes a map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, i.e. a *internal composition law* on $\mathbb{N}$. Later, we will also consider *external composition laws*. Let us consider sets

with one or several laws of composition (such as the addition and the multiplication on $\mathbb{Z}$). When we require that these laws verify certain properties (called "axioms"), we get an "algebraic structure". Such structures are those of "groups", "rings", "fields", and "vector spaces". The "group" structure involves a law. The "axioms" of groups were chosen, especially, because of the many applications obtained by Galois (1811-1832) to solve algebraic equations. Groups play a central role in many branches of mathematics and physics, they are involved in the ring, field, and vector space.structures. A prototypical *group* is $\mathbb{Z}$ with the addition. Important thing in a group is not the nature of its elements nor the notation used, but the *calculation rules*, resulting from the axioms of groups (group axioms). Thus the elements of the "group of permutations of a set" are not numbers at all. A *ring* is provided with two laws of composition. A prototypical ring is $\mathbb{Z}$; the polynomial ring is close to $\mathbb{Z}$ for its "arithmetic", but there are very different examples of ring. The "*field*" structure, important in linear algebra, is connected with that of ring. In general, the most useful fields are $\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$ with their usual laws.
.We can perform the *sum* or the *product* of two reals; these two operations (i.e. sum and product) are "internal composition laws" in $\mathbb{R}$; this is the subject of the present section.

8.1. Internal composition law (general).

Internal composition laws have already been introduced in the heading "*Laws of Composition*". In the present heading, we group the properties of these laws that will be useful to study groups, rings and fields. A law on the set E is thus a map from $E \times E$ to E. With any pair $(x, y) \in E \times E$, this law associates an element, for example, denoted by z of E (it can be denoted in different ways). The most common notations are:

▪ The **additive notation**: the element z is denoted $x + y$ (*sum* of x and y), the law is called *addition* and denoted $+ : E \times E \to E$.

▪ The **multiplicative notation**: the element z is denoted xy or $x \times y$ (*product* of x and y), the law is called *multiplication* and denoted $\times : E \times E \to E$.

We can also use the notations such as: $x \star y$, $x \top y$, $x \circ y$, $x \cdot y$, or $x * y$. When we'll use $(E, \top)$, this will mean that $\top$ is a composition law on the set E.

Ex. 51. (1) *The addition (resp. multiplication) is a law on* $\mathbb{N}$ *(*$\mathbb{Z}$,$\mathbb{Q}$*).*
(2) *Let E be a set and $\mathcal{F}(E, E)$ be the set of maps from E to E. Let us associate with any pair (f, g) of elements of $\mathcal{F}(E, E)$ the composition $f \circ g$. This law on $\mathcal{F}(E, E)$ is the composition of maps.*
(3) *Let $\mathfrak{P}(E)$ be set of the parts of a set X. The intersection $(A, B) \mapsto A \cap B$ and the union $(A, B) \mapsto A \cup B$ are laws on $\mathfrak{P}(E)$.*
(4) *On the set $\mathbb{N}^*$, you have at your disposal the law* $\gcd : (a, b) \mapsto \gcd(a, b)$ *and the* $\mathrm{lcm} : (a, b) \mapsto \mathrm{lcm}(a, b)$.
(5) *Let $\star$ be a law on X. With any pair (A, B) of parts of X, let us associate $A \star B := \{x \star y | (x, y) \in A \times B\}$. This defines a law $(A, B) \mapsto A \star B$ on $\mathfrak{P}(X)$. If the law of X is $+$ (resp. $\times$), we write $A + B$ (resp. AB).*

Certain properties of the law have already been seen in the heading "*Laws of Composition*", especially, *associativity* and *commutativity*. In the examples (1) to (4), the laws are associatives. In the example (5), if the law $\star$ on X is associative, the law $\star$ on $\mathfrak{P}(X)$ is also associative. The *subtraction* in $\mathbb{Z}$ is not associative (check it as exercise).

Ex. 52. *We can define a law on a finite set by its table: on E=$\{a, b\}$, the table below define a non-associative multiplication. Indeed: aa=b, ab=a, ba=a, bb=a, so $(aa)b$=bb=$a \neq b$=aa=$a(ab)$.*

	a	b
a	b	a
b	a	a

$a \times b = a$

If a law is associative, we can *omit* the parentheses: if $x, y, z \in E$, the element $(x \star y) \star z = x \star (y \star z)$ can be denoted (without any ambiguity) by $x \star y \star z$ (or xyz, or $x + y + z$, etc.). By induction on n (i.e. by recurrence), we define in general maps $(x_1, ..., x_n) \mapsto x_1 \star \cdots \star x_n$ from E^n to E: for $n = 1$, we start with the identity map of E, then we use the inductive formula:

$$x_1 \star x_2 \star \cdots \star x_n := (x_1 \star x_2 \star \cdots \star x_{n-1}) \star x_n,\ n \geqslant 2.$$

If $x_1, ..., x_n \in E$ and $y_1, ..., y_m \in E$ $(n, m \geqslant 1)$, we have:
(1) $(x_1 \star x_2 \star \cdots \star x_n) \star (y_1 \star y_2 \star \cdots \star y_m) = x_1 \star x_2 \star \cdots \star x_n \star y_1 \star y_2 \star \cdots \star y_m$, (this is proved by induction on m). In additive notation, $x_1 + x_2 + \cdots + x_n$ is also denoted $\sum_{i=1}^{n} x_i$. In multiplicative notation, $x_1 x_2 \cdots x_n$ is also denoted by $\prod_{i=1}^{n} x_i$. Consider the important case where all the x_i are equal to a same element x:

Def. 146. *Let E be a set provided with a multiplication and $x \in E$. The sequence $(x^n)_{n \geqslant 1}$ of powers of x is defined by $x^1 := x$ and the recurrence relation $x^{n+1} := x^n \times x$. In additive notation, the sequence $(nx)_{n \geqslant 1}$ of multiples of x is defined by $1x := x$ and the relation $(n + 1)x := nx + x$.*

For an associative law, we have:

$$nx = \underbrace{x + x + \cdots + x}_{n \text{ terms}}, \text{ and } x^n = \underbrace{x \times x \times \cdots \times x}_{n \text{ factors}}.$$

Prop.1 *Let E be a set provided with an associative law and $x \in E$. For all integers $m, n \geqslant 1$, we have:*
(2) $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$
(3) $mx + nx = (m + n)x$ and $m(nx) = (mn)x$
The identities of (2) *are* ***in multiplicative notation****, and those of* (3) ***in additive notation****.*

Proof. 1st identity in (3) (e.g.) comes from (1), and we infer then the second (by induction on n). □

Consider $(E, \star)$. We say that $x, y \in E$ commute if $x \star y = y \star x$. If it is true far all $x, y \in E$, we say then that the law is *commutative*.

Rem. 5. (†). *Let us consider an associative law, denoted multiplicatively for example on a set E. Given $x, y_1, ..., y_n \in E$ $(n \geqslant 1)$. If x commutes with each of y_i, it commutes with $y_1 y_2 \cdots y_n$. This is true if $n = 1$ and, if it is true for $n - 1$ $(n \geqslant 2)$, we have $x(y_1 y_2 \cdots y_n) = (xy_1)(y_2 \cdots y_n) = (y_1 x)(y_2 \cdots y_n) = y_1(x(y_2 \cdots y_n)) = y_1((y_2 \cdots y_n)x) = (y_1(y_2 \cdots y_n))x = (y_1 y_2 \cdots y_n)x$.*

Preferably, we reserve the *additive notation* for *commutative laws*.
In the examples (1),(3),(4) the laws are comuutaive. In the example (5), if the law $\star$ on X is commutative, the law $\star$ on $\mathfrak{P}(X)$ is also commutative. The subtraction in $\mathbb{Z}$ is not commutative. The law $\circ$ (example (2)) is not either, when E has two distinct elements a, b: the maps $x \mapsto a$ and $x \mapsto b$ do not commute.

Prop.2 *Let E be a set provided with an associative multiplication (resp. addition). If x,$y \in E$ commute (e.g. for a commutative law), then for any integer $n \geqslant 1$:*
(4) $(xy)^n = x^n y^n$ *(resp.* $n(x + y) = nx + ny$*).*

Proof. In the multiplicative case, $\forall k \geqslant 1$, $xy^k = x^k y$ (given remark (†)). We prove by induction on n the above (4). The case $n = 1$ is immediate. If the expression is true at rank n, then: $(xy)^{n+1} = (xy)^n(xy) = (x^n \underbrace{y^n)(x}\, y) = (x^n \underbrace{x)(y^n}\, y) = x^{n+1} y^{n+1}$. □

For an associative and commutative addition, the sum of several elements does not depend on the order in which we perform the additions:

Prop.3 *Let E be a set provided with an associative and commutative addition, $x_1, ..., x_n \in E$ $(n \geqslant 1)$ and s a permutation of $[1, n] \in \mathbb{Z}$ (i.e. interval of integers $1 \leqslant s \leqslant n$). Then:*
(5) $x_1 + x_2 + \cdots + x_n = x_{s(1)} + x_{s(2)} + \cdots + x_{s(n)}$.

Proof. By induction on n (i.e. by recurrence), the case $n = 1$ is immediate. Assume $n \geqslant 2$ and the result is valid at the order $n - 1$. If $s(n) = n$, the induction hypothesis (hypothesis of recurrence) applies. Otherwise, $n = s(k)$ for a certain $k \in [1, n - 1] \in \mathbb{Z}$. Given the above remark (†), the right-hand side is equal to: $x_{s(1)} + x_{s(2)} + \cdots + x_{s(k-1)} + [x_n + (x_{s(k+1)} + \cdots + x_{s(n)})]$, i.e., $x_{s(1)} + x_{s(2)} + \cdots + x_{s(k-1)} + [(x_{s(k+1)} + \cdots + x_{s(n)}) + x_n]$, which reduces to the previous case. □

With the same assumptions. Let I be a finite set of cardinal $n \geqslant 1$ and $(x_i)_{i \in I}$ be a family of elements of E. If f is a *bijection* of $[1, n] \in \mathbb{Z}$ on I (numbering of the elements of I), let us $T(f) := x_{f(1)} + \cdots + x_{f(n)}$. If $g : [1, n] \in \mathbb{Z} \to I$ is another bijection, $s := f^{-1} \circ g \in \mathfrak{S}$ (the set $\mathfrak{S}$ of bijections from E to E (called *permutations of* E)), and $g = f \circ s$, therefore $T(f) = T(g)$, since $x_{f(1)} + x_{f(2)} + \cdots + x_{f(n)} = x_{f(s(1))} + x_{f(s(2))} + \cdots + x_{f(s(n))}$ given the proposition. Thus $T(f)$ *does not depend on* f, it is called the *sum* of the family $(x_i)_{i \in I}$, and is denoted by $\sum_{i \in I} x_i$. The index i is *dummy*, that is, can be changed $(\sum_{i \in I} x_i = \sum_{k \in I} x_k)$. In multiplicative notation, we write $\prod_{i \in I} x_i$ instead of $\sum_{i \in I} x_i$.
The above sums obey the following calculation rules:

Th. 33. $(*)$ *Let E be a set provided with an associative and commutative addition. Let I,J be nonempty finite sets. We can state then:*
1) *Given $(x_i)_{i \in I}$ a family of elements of E and $I_1, ..., I_m$ the nonempty finite parts of I which form a partition of I. If $u \in [1, m] \in \mathbb{Z}$, given S_u the sum of the family $(x_i)_{i \in I_u}$. The associativity formula is given by:*
(6) $\sum_{i \in I} x_i = S_1 + \cdots + S_m$, *i.e.* $\sum_{i \in I} = \sum_{u=1}^{n} (\sum_{i \in I_u} x_i)$.
2) *Let $(x_{i,j})_{(i,j) \in I \times J}$ a family of elements of E. Then:*

(7) $$\sum_{(i,j)\in I\times J} x_{i,j} = \sum_{i\in I}(\sum_{j\in J} x_{i,j}) = \sum_{j\in J}(\sum_{i\in I} x_{i,j}).$$

3) *Given $(x_i)_{i\in I}$ a family of elements of E and h a bijection from J to I. Then:*

(8) $$\sum_{j\in J} x_{h(j)} = \sum_{i\in I} x_i \text{ (index change formula).}$$

Proof. The first statement is left to the reader as exercise. The second statement results from the first: when $i \in I$, the part $\{i\} \times J$ form a partition of $I \times J$, hence the first identity. The second is similar. For the third statement, given $n := \text{card}(J)$, f a bijection from $[1, m] \in \mathbb{Z}$ to J, and $g := h\circ f$. For any $j \in J$, set: $y_j := x_{h(j)}$. In (8), the right-hand side is equal to $x_{g(1)} + \cdots + x_{g(n)} = x_{h(f(1))} + \cdots + x_{h(f(n))}$, i.e., $y_{f(1)} + \cdots + y_{f(n)}$, and l.h.s is equal to $\sum_{j\in J} y_j = y_{f(1)} + \cdots + y_{f(n)}$. □

Consider $(E, \top)$. An element e of E is *neutral element* for $\top$ if we have $\forall x \in E$, $x\top e = x = e\top x$. Such an element is unique, if it exists. It is denoted by 0 for an addition, and by 1 for a multiplication. Thus, in each of sets of usual numbers, 0 is neutral for the addition and 1 is neutral for the multiplication. In $\mathbb{N}^*$, 1 is neutral for the law "lcm". Check that there is no neutral element for the law "gcd".

Let E be a set. The identity map Id_E from E to E is neutral element for the "composition of maps" on $\mathcal{F}(E, E)$ (set of maps from E to E). On $\mathfrak{P}(E)$, the set of the parts of E, E is neutral for the law $\cap$ and the empty part $\varnothing$ is neutral for the law $\cup$.

Let E be a set provided with an associative law $\star$ and with a neutral element e. For a finite family $(x_1, ..., x_n)$ of elements of E ($n \geqslant 1$), the element $x_1 \star \cdots \star x_n$ has been defined. If $n = 0$, that is, if the family is nonempty, we agree that $x_1 \star \cdots \star x_n := e$ (i.e. $x_1 + \cdots + x_n := 0$ in additive notation, $x_1 \cdots x_n := 1$ in multiplicative notation). Thus, given $x \in E$. If the law is multiplicative (resp. additive), we have $x^0 := 1$ (resp. $0x := 0$) (note that the 0 on the left is an integer, the second member is the neutral of E). Endowed with these conventions, the formulas (1) to (4) are still valid for two integers $m, n \geqslant 0$ (the reader can check it).

Moreover, assume that the law is additive and *commutative*. Let $(x_i)_{i\in I}$ be a finite family of elements of E. The sum $\sum_{i\in I} x_i$ is defined if $I \neq \varnothing$. If $I = \varnothing$, we agree that this sum is 0. The formulas (6),(7),(8) remain true if some of the sets of involved indexes are empty. Let us generalize: instead assume I finite, assume that $I' = \{i \in I | x_i \neq 0\}$ is finite; I' is called **support** *of the family*. By definition, $\sum_{i\in I} x_i$ is then equal to $\sum_{i\in I'} x_i$. The previous theorem $(*)$ remains true, assuming for example in the formula (7) that the family $(x_{i,j})_{(i,j)\in I\times J}$ is a *finite support*.

Start with $(E, \top)$, E has a neutral element e for $\top$, and given $x \in E$. Recall that an element x' of E is called "*symmetric element*" (or "symmetric") of x if:

(9) $$x\top x' = e = x'\top x.$$

If such an element x' exists (in this case it is unique when the law is associative), we say that x is "*symmetrizable*"; For example, $\forall x \in E$ such that $x\top x = e$ is symmetrizable, (its own symmetric). Important examples are the "symmetries".

In additive notation, the symmetric element x' of an element x is called *opposite* of x and denoted by $-x$. Thus, $x + (-x) = 0 = (-x) + x$.

In multiplicative notation, x' is called *inverse* of x and denoted by x^{-1}. Thus, $x \times x^{-1} = 1 = x^{-1} \times x$; an element that has an inverse is said to be "*invertible*", instead of "*symmetrizable*". (Note that a transformation that is its own inverse is called an *involution.*)

Th. 34. *(Cancellation property, or Regularity). Let E be set admitting a neutral element e for an associative law $\top$ and x a symmetrizable element of E. Then x is cancellable or regular, meaning that for all $y, z \in E$:*

$$(x\top y = x\top z) \Rightarrow (y = z) \text{ and } (y\top x = z\top x) \Rightarrow (y = z).$$

(Cf. section "*Laws of Composition*", especially the heading "*General vocabulary, notation*".)

Prop.4 *Let E be a set that has a neutral element e for an associative multiplication, and $(x_1, ..., x_n)$ be invertible elements of E ($n \geqslant 0$). Then $x_1x_2 \cdots x_n$ is invertible, and its inverse is given by the formula:*

$$(x_1x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1}x_1^{-1}.$$

Proof. The cases n=0, n=1 are immediate; by induction (by recurrence), we are reduced to the case of two invertible elements x, y. Then: $(x, y)(y^{-1}x^{-1}) = (x(yy^{-1}))x^{-1} = (xe)x^{-1} = xx^{-1} = e$, and similarly we check $(y^{-1}x^{-1})(xy) = e$, the conclusion follows. □

Therefore, in one of the sets $\mathbb{Z}$, $\mathbb{Q}$ provided with its addition, every element x has an *opposite* $-x$. For the addition in $\mathbb{N}$, only 0 has an opposite. Every $x \in \mathbb{Q}^*$ has as multiplicative *inverse* $\frac{1}{x}$, also denoted x^{-1}. For the multiplication in $\mathbb{Z}\backslash\{0\}$, only -1 and 1 are invertible.

Ex. 53. *Let E be a set. If f is a $\mathcal{F}(E, E)$ (set of maps from E to E) has a symmetric f' for the law $\circ$, we have $f' \circ f = Id_E = f \circ f'$. The first identity (resp. second identity) proves that f is injective (resp. surjective). Thus, f is bijective. Conversely, given a bijection f from E to E and f^{-1} the inverse bijection of f. Since $f^{-1} \circ f = Id_E = f \circ f^{-1}$, f^{-1} is symmetric of f. The symmetrizable elements, preferably called "invertible elements", of $\mathcal{F}(E, E)$ for the law $\circ$ are thus exactly the permutations of E.*

From a law, we can define other laws (cf. section "*Laws of composition*"). Let's start from $(E, \top)$, let F be a *stable* part of E *for the law* $\top$: for all $x, y \in F$, $x\top y$ also belongs to F, that is, $F\top F \subset F$ (cf. Ex.(5) at the beginning of heading). Then $(x, y) \mapsto x\top y$ is a law on F, called *law induced by* $\top$. If F is stable for an associative law (resp. commutative), the law induced has the same property. Empty part and E are stable for $\top$. (About notion of "stable" part, see heading "*General vocabulary, notation*", in section "*Laws of Composition*", in chapter "*Relations and Structures*".)

Prop.5 *Let $\top$ be a law on the set E. If $(F_i)_{i\in I}$ is a family of stable parts of E for $\top$.*

In $\mathbb{Z}$, $\mathbb{N}$ is stable by addition and multiplication (in short, additively and multiplicatively stable), similarly for $n\mathbb{Z}$ if $n \in \mathbb{Z}$. By contrast, the *union* $F = 2\mathbb{Z}\cup 3\mathbb{Z}$ is not stable by addition (additively stable): $2 \in F$, $3 \in F$, but $5 \notin F$, 5 is not multiple of 2 nor of 3.

The set $\mathfrak{S}(E)$ of permutations of a set E is stable for the composition of maps on $\mathcal{F}(E, E)$ (set of maps from E to E): the composition of two bijections from E to E is a bijection from E to E.

A *product law can be defined by:*

Def. 147. *(Product law). Let $E_1, ..., E_n$ ($n \geqslant 2$) be sets, each of them is provided with a law $\top_i$. Given $F := E_1 \times E_2 \times \cdots \times E_n$. We call product of the laws $\top_1, ..., \top_n$ the law $\top$ defined on F by the expression:*

$$(x_1, ..., x_n)\top(y_1, ..., y_n) := (x_1\top_1 y_1, ..., x_n\top_n y_n),$$

where $i = 1, ..., n$, and $x_i, y_i \in E_i$. If each $\top_i$ is additively (resp. multiplicatively) denoted, then the law $\top$ is additively (resp. multiplicatively) denoted. If each $\top_i$ is associative (resp. commutative), then this is the same for $\top$. If each $\top_i$ has a neutral element e_i for the law $\top_i$, $e := (e_1, ...e_n) \in F$ is neutral element for the law $\top$. Moreover, suppose $x := (x_1, ...x_n) \in F$. If each x_i has a symmetric element x_i' for the law $\top_i$, then $x' := (x_i', ..., x_n')$ is symmetric of x for the law $\top$. (The term "product law" follows from the product $E_1 \times E_2 \times \cdots \times E_n$, it has nothing to do with the additive or multiplicative or other notations.)

Assume that the E_i are all equal to a same set E and the laws $\top_i$ are all equal to a same law $\top$. The product law on $F := E^n$ is still denoted $\top$. (Thus, the addition of vectors of the plane is a product law.)

More generally, let's start with $(E, \top)$, and consider an arbitrary set X. On the set $\mathcal{F}(X, E)$ of maps from X to E, we can define a law, also denoted by $\top$, as follows: Given $f, g \in \mathcal{F}(X, E)$, $f\top g$ is given $\forall x \in X$ by

(10) $$(f\top g)(x) := f(x)\top g(x).$$

It follows a "natural" addition and multiplication on the set $\mathcal{F}(\mathbb{R}, \mathbb{R})$ of functions defined on $\mathbb{R}$. The law $\top$ on $\mathcal{F}(X, E)$ is associative (or commutative) if the law $\top$ on E is also associative (or commutative; if $e \in E$ is neutral for the law $\top$, the map $x \mapsto e$ from X to E is neutral for the law $\top$ on $\mathcal{F}(X, E)$..

Exer. 1. (•). *Problems: Given $X := \mathbb{N}\backslash\{0\}$. Let us define on $\mathcal{F}(E, \mathbb{Z})$ (set of maps from E to $\mathbb{Z}$) a law $\star$ as follows: Let $f, g \in \mathcal{F}(E, \mathbb{Z})$, $f \star g : E \to \mathbb{Z}$ is given by $(f \star g)(n) := \sum_{(a,b)\in E^2, ab=n} f(a)g(b)$, $\forall n \in E$.* **1)** *Check that the function $\delta : E \to \mathbb{Z}$, which is 1 at 1 and is 0 elsewhere, is neutral element for the law $\star$.* **2)** *Show that the law $\star$ is associative (use previous formulas (6),(8) of theorem $(*)$), since $(\mathcal{F}(E, \mathbb{Z}), +, \star)$ is a commutative ring.* **3)** *Let $\mu : E \to \mathbb{Z}$ be* ***Möbius function*** *defined as follows. Given $n \in \mathbb{N}$; $\mu(n) := (-1)^r$ if n is product of r distinct prime numbers ($r \geqslant 0$), and $\mu(n) := 0$. Let $c : E \to \mathbb{Z}$ be the constant function equal to 1. Show that μ and c are inverse in $(\mathcal{F}(E, \mathbb{Z}), +, \star)$.* **4)** *Given the abelian group $(X, +)$ and two functions $f, g : E \to X$. Establish the equivalence: $(\forall n \in E, g(n) = \sum_{d|n} f(d)) \Leftrightarrow (\forall n \in E, f(n) = \sum_{d|n} \mu(n/d)g(d))$:* ***Möbius inversion formula****. In the above sums, d is the set of positive divisors of n.*

Solutions: Note first that if $n \in E$, $d \mapsto (d, n/d)$ is a bijection from the set of divisors $d \geqslant 1$ of n to the set of pairs $(a, b) \in E^2$ such that $ab = n$. The formula defining the $\star$ can therefore be written as follows: $(f \star g)(n) = \sum_{d|n} f(d)g(n/d)$, for any $n \in E$. Moreover, note that the law $\star$ is commutative (because the multiplication of $\mathbb{Z}$ is commutative). Finally, if $f, g \in \mathcal{F}(E, \mathbb{Z})$, clearly $(f \star g)(1) = f(1)g(1)$. **1)** *Given $f \in \mathcal{F}(E, \mathbb{Z})$. We have for every $n \in E$, $(\delta \star f)(n) = \delta(d)f(n/d)$. In*

*the right hand side member, the only d such that $\delta(d)$ is nonzero is $d=1$, then $(\delta\star f)(n)=\delta(1)f(n)=f(n)$. **2)** Given $f,g,h\in\mathcal{F}(E,\mathbb{Z})$, and $n\in E$. By definition $((f\star g)\star h)(n)=\sum_{(a,b)\in E^2,ab=n}(f\star g)(a)h(b)$. The second member of this identity can also be written as: $\sum_{(a,b)\in E^2,ab=n}(\sum_{(u,v)\in E^2,uv=a}f(u)g(v)h(b))$. Given $I:=\{(u,v,b)\in E^3|uvb=n\}$. For every $(a,b)\in E^2$ such that $ab=n$, denote by "$I_{(a,b)}$" the set of triplets (u,v,b), where $(u,v)\in E^2$ verifies the identity $uv=a$. The $I_{(a,b)}$ form a partition of I. The expression (6) of the theorem (∗) gives thus: $\sum_{(u,v,b)\in I}f(u)g(v)h(b))=\sum_{(a,b)\in E^2,ab=n}(\sum_{(u,v)\in E^2,uv=a}f(u)g(v)h(b))$. That is, $((f\star g)\star h)(n)=\sum_{(u,v,b)\in I}f(u)g(v)h(b)$. Considering the commutativity of the ring $\mathbb{Z}$, this can be written: $((f\star g)\star h)(n)=\sum_{(u,v,b)\in I}g(v)h(b)f(u)$. Since the function $(u,v,b)\mapsto(b,u,v)$ is a permutation of I, then the index change formula (8) of theorem (∗) gives: $((f\star g)\star h)(n)=\sum_{(u,v,b)\in I}g(u)h(v)f(b)$. In fact, the second member of this identity is $((g\star h)\star f)(n)$. Thus $(f\star g)\star h=(g\star h)\star f=f\star(g\star h)$, because of the commutativity of the law ⋆. The law ⋆ is thus associative. Of course, we could directly calculate $(f\star(g\star h))(n)$ and obtain:*
$(f\star(g\star h))(n)=\sum_{(a,b)\in E^2,ab=n}f(a)(g\star h)(b)=$
$=\sum_{(a,b)\in E^2,ab=n}(\sum_{(u,v)\in E^2,uv=b}f(a)g(u)h(v))$. *Using the same reasoning as in previous calculations, we get then: $(f\star(g\star h))(n)=\sum_{(a,u,v)\in I}f(a)g(u)h(v)=\sum_{(u,v,b)\in I}f(u)g(v)h(b)$. Now, the last property to be checked is the distibutivity of ⋆ with respect to +. This is much easier than the associativity of the law ⋆. Given $f,g,h\in\mathcal{F}(E,\mathbb{Z})$, and $n\in E$. Then $((f+g)\star h)(n)$ is equal by definition to the identities: $\sum_{(a,b)\in E^2,ab=n}(f+g)(a)h(b)=\sum_{(a,b)\in E^2,ab=n}(f(a)+g(a))h(b)=\sum_{(a,b)\in E^2,ab=n}f(a)h(b)+\sum_{(a,b)\in E^2,ab=n}g(a)h(b)=(f\star h)(n)+(g\star h)(n)=[(f\star h)+(g\star h)](n)$, and thus $(f+g)\star h=(f\star h)+(g\star h)$. **3)** We must show the identity $\mu\star c=\delta$. First, $(\mu\star c)(1)=\mu(1)c(1)$ is indeed equal to $\delta(1)=1$. Now, we finally have to show that for the integer $n\geqslant 2$ we have: $\sum_{d|n}\mu(d)=\delta(n)$, i.e. $\sum_{d|n}\mu(d)=0$. Let $p_1,..,p_r$ be the different prime factors of n (so distinct). Since $\mu(k)=0$ for any integer k having a multiple prime factor p ($v_p(k)\geqslant 2$), the divisors d of n such that $\mu(d)\neq 0$ are the product of some of p_i. In other words, for any part I of $[1,r]\in\mathbb{Z}$, denote by "p_I" the product the p_i, where i runs through I. Then according to the factorization theorem (also called "Fundamental Theorem of Arithmetic") stated in the heading "Primes, integer factorization" (section "Divisibility", chapter "Arithmetic", Part I Foundations of Mathematic"), $I\mapsto p_I$ is a bijection from the set of parts of $[1,r]\in\mathbb{Z}$ to the set of divisors d of n such that $\mu(d)\neq 0$. In addition, for any part I of $[1,r]$, the definition of μ shows that $\mu(p_I)=(-1)^{|I|}$, where $|I|$ denotes here the cardinal of I. We get then: $\sum_{d|n}\mu(d)=\sum_I(-1)^{|I|}$. Since we know that in a non-empty finite set, there are as many parts of even cardinal as parts of odd cardinal (cf. example (♢) in heading "Ring, calcularion rules", in section "Rings and Fields", in chapter Algebra). Thus, as sought we have $\sum_{d|n}\mu(d)=0$. **4)** It is important to mention that f and g are with values in X, but not in $\mathbb{Z}$. Actually, we can generalize ⋆ as follows: First, recall that if $k\in\mathbb{Z}$ and $x\in X$, kx has been defined in the definition (♢) of the heading "Group, group properties" (in section "Group Theory", in chapter "Algebra. See also Prop.C in the same heading), Then, given $\phi\in\mathcal{F}(E,\mathbb{Z})$ and $\psi\in\mathcal{F}(E,X)$. We define $\phi\star\psi\in\mathcal{F}(E,X)$ by the formula: $(\phi\star\psi)(n):=\sum_{(a,b)\in E^2,ab=n}\phi(a)\psi(b)$, $\forall n\in E$. Clearly, for example, for every function $\psi\in\mathcal{F}(E,X)$, $\delta\star\psi=\psi$. For every function $\phi,\phi'\in\mathcal{F}(E,\mathbb{Z})$, and $\psi\in\mathcal{F}(E,X)$, then, we show that $(\phi\star\phi')\star\psi=\phi\star(\phi'\star\psi)$, i.e. mixed associativity. It suffices to take again the proof given in 2), more specifically the direct proof (and not the one that used the commutativity of the law ⋆ on $\mathcal{F}(E,\mathbb{Z})$, this commutativity no longer makes sense here). With the above, come back to f,g. The following property $(\forall n\in E,g(n)=\sum_{d|n}f(d))$ means that $g=c\star f$, while the property $(\forall n\in E,f(n)=\sum_{d|n}\mu(n/d)g(d))$ means that $f=\mu\star g$. If $g=c\star f$, the mixed associativity and 4) give: $\mu\star g=\mu\star(c\star f)=(\mu\star c)\star f=\delta\star f=f$. Similarly, if $f=\mu\star g$, we have: $c\star f=c\star(\mu\star g)=(c\star\mu)\star g=\delta\star g=g$. Hence the equivalence of the initial statement.*

8.2. Internal composition law. In a nonempty set E, the symbol used to express an internal composition law is "$\top$"; it can mean "+" or "·", or any other operation. First, define the notion for two elements, the extension will be given subsequently.

Def. 148. *(Internal composition law on E). $\top$ is called internal composition law on a set E if for any pair $(a,b)\in E\times E$ there is a unique $c\in E$ verifying $a\top b=c$ (Fig.). A set, on which is defined an internal composition law, is denoted $(E;\top)$ and is called "Magma".*

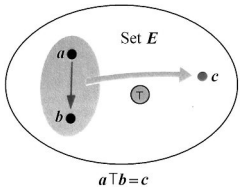


Fig. Internal composition law.

Rem. 6. *If there exists an operation $\top$ which is not possible for all $(a,b)\in E\times E$, we say "law of composition in E", (e.g. the division in $\mathbb{R}$).*

Rem. 7. *Any internal composition law can be defined as a map. Let be $F\subseteq E\times E$; then it is possible to define $\top:F\to E$ by $(a,b)\mapsto a\top b$. If we consider the case of an internal composition law on E, then $F=E\times E$.*

Operation table: In case of a finite set, a law of composition is represented by an "*operation table*"; For $E=\{a_0,a_1,a_2,a_3\}$, we have:

⊤	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

where $a_i\top a_i=a_0$ with $i\in\{0,1,2,3\}$, $a_0\top a_i=a_i=a_i\top a_0$ with $i\in\{1,2,3\}$, $a_2\top a_3=a_1=a_3\top a_2$, $a_3\top a_1=a_2=a_1\top a_3$.

Ex. 54. *(Law of composition on E).* (1) "+" or "·" on $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$. (2) *The composition of rotations around a point in an Euclidean plane (Fig.).* ***Composition of rotations (and rotation group):***

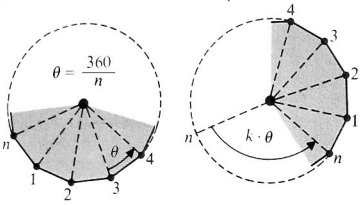


*Fig. **Rotation group**. Rotation of a regular polygon with n sides of a multiple of θ; ($n\in\mathbb{N}$, $n\geq 3$);*
$R_k:=$ *rotation of* $k\cdot\theta$ $(k\in\mathbb{N})$
$R_n=R_0$; $R_{n+1}=R_1$; ....; $R_{n+m}=R_m$.
Definition of an internal composition law $\circ:G_n\times G_n\to G_n$ by $R_j\circ R_i=R_{i+j}$ (i.e. perform first a rotation of $i\cdot\theta$, then a rotation of $j\cdot\theta$).

∘	R_0	R_1	⋯	R_{n-i}	⋯	R_j	⋯	R_{n-1}
R_0	R_0	R_1						
R_1	R_1	R_2						
⋮			⋱					
⋮				⋱				
⋮					⋱			
R_i				R_0		R_{i+j}		
⋮							⋱	
R_{n-1}								⋱

- *Associativity* $R_k\circ(R_j\circ R_i)=R_k\circ R_{i+j}=R_{(i+j)+k}$
$=R_{i+(j+k)}=R_{j+k}\circ R_i$
$=(R_k\circ R_j)\circ R_i$.
- *Commutativity* $R_j\circ R_i=R_{i+j}=R_{j+i}=R_i\circ R_j$.

(3) *Addition, vector product on an euclidean vector space in dimension 3.* (4) $\cap$, $\cup$ *on* $\mathfrak{P}(E)$ (5) "+" *on the set of (n,m)-matrices.* (4) "·" *on the set of (n,n)-matrices.*

Ex. 55. *(Law of composition in E).* (6) "−" *or* ":" *in* $\mathbb{N}$. (7) ":" *in* $\mathbb{Z}$. (8) "+" *or* "·" *in* $\{1,.,10\}$.

8.3. Associativity, associative law. In above definition, internal composition law was defined for only two elements; it can be extended to several elements.

Def. 149. *(Internal composition law for (a_1, a_2, ..., a_n)). Let us set in $(E;\top):\forall a_i\in E$:*
. $a_1\top a_2\top a_3:=(a_1\top a_2)\top a_3$
. $a_1\top...\top a_n:=(a_1\top...\top a_{n-1})\top a_n;n\in\mathbb{N},n\geqslant 3$

If we set $a_1\top a_2\top a_3:=a_1\top(a_2\top a_3)$, the results could be different. Thus, we are led to state the associativity.

Def. 150. *(Associativity of the internal composition law). $\top$ is said to be associative on E if for any a_1,a_2,a_3, we have $(a_1\top a_2)\top a_3:=a_1\top(a_2\top a_3)$. ($(E;\top)$ is also called an associative magma).*

The parentheses can be placed anywhere or are not necessary when the composition is associative.

8.4. Semigroup or Monoid.

Def. 151. *(Semigroup or Monoid).* $(E;\top)$ *is called monoid or semigroup if* $\top$ *is associative on* E.

Ex. 56. *In the heading "Internal composition law", examples* (1)-(5) *are semigroups, except* (3) *for the vector product.*

8.5. Neutral element. When $a \in \mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$, then, we have $a+0=a$, $a\cdot 1=a$, for the vectors $\vec{a}+\vec{0}=\vec{a}$, for $A\in\mathfrak{P}(E)$ $A\cup\varnothing=A$ and $A\cap E=A$. Then, $0,1,\vec{0},\varnothing$ et E are "neutral" for their respective laws, because the composition of an element with one of them gives this element.

Def. 152. *(Neutral element).* $e\in E$ *is a left-neutral element (resp. right-neutral element) of* $(E;\top)$ *if it verifies* $\forall a\in E, e\top a=a$ *(resp.* $\forall a\in E, a\top e=a$*). e is a neutral element if it is left-neutral and right-neutral.*

Rem. 8. *If the neutral element exists, it is unique.*

Rem. 9. *In a group the distinction between left-neutral and right-neutral elements are unnecessary, since a left-neutral element is necessarily right-neutral and conversely.*

Rem. 10. *(Neutral element: Identity element, Zero element). Roughly speaking, an element e is a neutral element for a "binary operation"* $\circ$ *on a set S if, for all a in S,* $a\circ e=e\circ a=a$*. If the operation is called "multiplication", a neutral element is normally called an "**identity element**" and may be denoted by* 1*. If the operation is called "addition", such an element is normally denoted by* 0*, and is often called a "zero element". However, there is a case for preferring the term "neutral element, as there is an alternative definition for the term "zero element" (cf. remark hereafter).*

Rem. 11. *(Zero element).* ▪ *An element z is a zero element for a binary operation* $\circ$ *on a set S if, for all a in S,* $a\circ z=z\circ a=a$*. Thus the real number* 0 *is a zero element for multiplication since, for all a,* $a0=0a=0$. ▪ *The term "zero element", also denoted* 0*, may be used for an element such that* $a+0=0+a=a$ *for all a in S, when S is a set with a binary operation + called addition. Strictly speaking, this is a "neutral element" for the operation +.*

Rem. 12. *(Identity element for a Group or related mathematical structure S). The identity element I (denoted I, e,* 1*, or E) of a group or related mathematical structure S is the unique element such that* $I\,a=a\,I=a$ *for every element* $a\in S$*. (The symbol "E" derives from the German word for unity, "Einheit"). An identity element is also called a "unit element".*

8.6. Inverse of an element. The differences between algebraic structures are mainly due to the possible existence of $a^{-1}\in E$, for $a\in E$, which verifies $a\top a^{-1}=a^{-1}\top a=e$, where e is the *neutral element.*

Def. 153. *(Inverse element).* $a^{-1}\in E$ *is a left-inverse element of* $a\in E$ *in* $(E;\top)$ *which has a neutral element e, if it verifies* $a^{-1}\top a=e$*.* ($a^{-1}\in E$ *is a right-inverse element of* $a\in E$ *in* $(E;\top)$ *which has a neutral element e, if it verifies* $a\top a^{-1}=e$*). Furthermore,* $a^{-1}\in E$ *is an inverse element of a, if it is a left-inverse and right-inverse element.*

Rem. 13. *If the law* $\top$ *is associative (e.g. in a group), this inverse is unique if an inverse exists.*

Rem. 14. ($+$*, neutral element* 0)*:* (1) *Only* 0 *has an opposite (i.e.* $\mathbb{N}$*).* (2) *Any number has an opposite (i.e.* $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$*).* ($\cdot$*, neutral element* 1)*:* (3) *Only* 1 *has an inverse (i.e.* $\mathbb{N}$*).* (4) *Only* 1 *and* -1 *have an inverse (i.e.* $\mathbb{Z}$*).* (5) *Except* 0*, every number has an inverse (the inverse), (i.e.* $\mathbb{Q},\mathbb{R},\mathbb{C}$*).*

Rem. 15. *The definition of an inverse law is possible because of the existence of neutral elements (e.g. the subtraction and division in* $\mathbb{N}$*, in* $\mathbb{Q}$*).*

Def. 154. *(Additive identity). In a mathematical system with an operation of addition, denoted +, an element* 0 *such that* $0+e=e+0=e$ *for any element e in the system.*

Def. 155. *(Additive inverse). In a mathematical system with an operation of addition, denoted +, an additive inverse of an element e is an element* $-e$ *such that* $e+(-e)=(-e)+e=0$*, where* 0 *is the additive identity.*

In an additive group G, the additive inverse of an element a is the element a' such that $a+a'=a'+a=0$, where 0 is the additive identity of G. Usually, the additive inverse of a is denoted $-a$, as in the additive group of integers $\mathbb{Z}$, of rationals $\mathbb{Q}$, of real numbers $\mathbb{R}$, and of complex numbers $\mathbb{C}$, where $-(x+iy)=-x-iy$. The same notation with the minus sign is used to denote the additive inverse of a vector, of a polynomial, of a matrix, and in general, of any element in an abstract vector space or a module.

Def. 156. *(Multiplicative identity). In a mathematical system with an operation of multiplication, denoted* $\cdot$*, an element* 1 *such that* $1\cdot e=e\cdot 1=e$ *for any element e in the system.*

Def. 157. *(Multiplicative inverse). In a mathematical system with an operation of multiplication, denoted* $\cdot$*, the multiplicative inverse of an element e is an element* $\overline{e}$ *such that* $e\cdot\overline{e}=\overline{e}\cdot e=1$*, where* 1 *is the multiplicative identity.*

8.7. Group. Sets provided with an internal composition law (for which *the existence of inverse elements is verified*) possess particular algebraic structures.

Def. 158. *(Group).* $(E;\top)$ *is called a group if :*
(i) $\top$ *is associative,*
(ii) there exists a neutral element,
(iii) any element has an inverse (Fig.).

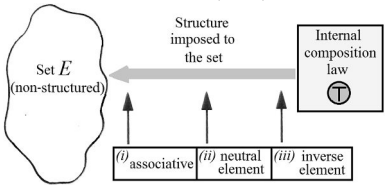


Fig. Group structure.

As seen before, we know that a semigroup (or monoid) is defined by the associativity on E. Thus a group is a semigroup also verifying the conditions *(ii),(iii).*

Def. 159. *(Abelian group). A group* $(E;\top)$ *is called an Abelian group (or commutative group) if* $\top$ *is commutative, i.e. if* $\top$ *verifies* $\forall a,b\in E$, $a\top b=b\top a$.

Ex. 57. *The groups:* $(\mathbb{Z};+)$,$(\mathbb{R};+)$,$(\mathbb{C};+)$,$(\mathbb{Q};+)$,$(\mathbb{R}\backslash\{0\};\cdot)$, $(\mathbb{C}\backslash\{0\};\cdot)$, $(\mathbb{Q}\backslash\{0\};\cdot)$*. Another example is the set of all rotations of a regular* n*-sided polygon* ($n\geqslant 3$*) (cf. Illustration of composition of rotations in heading "Internal composition law") is an example of finite group. Another example is the Klein group (see previous remark about "operation table" and internal composition law). Each one of these groups are Abelian.*

Def. 160. *(Group order). The number of elements in a group G, denoted* $|G|$ *(or also for a finite group:* ord$G$*). If the order of a group is a finite number, the group is said to be a finite group.*

The order of an element g of a finite group G is the smallest power of n such that $g^n=I$, where I is the identity element.
We can also define a group via the notion of "closure" (which is described subsequently in another section).

8.8. Ring, integral domain (entire ring).
Algebraically structured sets possessing two laws are particularly important. These laws can be denoted "+" and "·" using the same symbols as the addition and multiplication in the set of numbers. To get a homogeneous structure, we need that these laws are compatible. The compatibility condition is given below, rings afterwards:

Def. 161. *(Distributive law). We say that "·" is left-distributive with respect to "+" in* $(E;+,\cdot)$ *if we have* $\forall a,b,c\in E, a\cdot(b+c)=a\cdot b+a\cdot c$*. We say that " ·" is right-distributive with respect to "+" in* $(E;+,\cdot)$ *if we have* $\forall a,b,c\in E, (a\cdot b)+c=a\cdot c+b\cdot c$*. Moreover, we say that " ·" is distributive with respect to "+" if it is left and right distributive.*

There is an equivalence between the left and right distributivity, if the multiplication is commutative.
The set $\mathbb{Z}$ has an interesting structure: indeed $(\mathbb{Z},+)$ is an Abelian group, $(\mathbb{Z},\cdot)$ is a commutative semigroup having a neutral element 1. The doublestruck capital letter Z, $\mathbb{Z}$, denotes the ring of integers $\ldots,-2,-1,0,1,2,\ldots$. The symbol derives from the German word Zahl, meaning "number" and first appeared in Bourbaki's Algebra. The ring of integers is sometimes also denoted using the doublestruck capital I,$\mathbb{I}$.

Def. 162. *(Ring).* $(E;+,\cdot)$ *is called a ring if (Fig.):*
(i). $(E;+)$ *is an Abelian group,*
(ii). $(E;\cdot)$ *is a semigroup,*
(iii). " ·" is distributive with respect to "+".

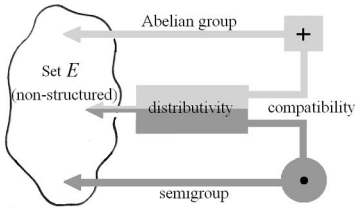


Fig. Ring structure.

The neutral element of the law "+" is called the "zero element". When the neutral element exists, this element is called the "*unit element*[1]", then the ring is "unitary". Furthermore, a ring is "commutative" if the multiplication is commutative.

Ex. 58. *The simplest rings are the integers $\mathbb{Z}$, polynomials $\mathbb{R}[x]$and $\mathbb{R}[x,y]$ in one and two variables, and square $n \times n$ real matrices. ($\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ provided with the laws - also called binary operators - "+" or "·", are respectively: ring of matrices (n,n), quotient ring, ring of polynomials).*

Rem. 16. 0 *plays a particular role by the distributivity, indeed we can write in the rings: $a=0 \vee b=0 \Rightarrow a \cdot b = 0$. If the converse $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ is also true, the ring is said to be* ***with no zero divisors***[2] *(or with no divisors of zero). In the opposite case, there exists $a \neq 0$ and $b \neq 0$ such that $a \cdot b = 0$. Then a and b are called "divisors of zero".*

A definition of a *unit ring* can be given by using *basic binary operators* as follows:

Def. 163. *(**Unit ring**). A unit ring is a ring with a multiplicative identity. It is thus sometimes also known as a "**ring with identity**". It is given by a set endowed with two binary operators $(E;+,\cdot)$ satisfying the following conditions:*
1. *Additive associativity: For all $a,b,c \in E$, $(a+b)+c = a+(b+c)$,*
2. *Additive commutativity: For all $a,b \in E$, $a+b=b+a$,*
3. *Additive identity: There exists an element $0 \in E$ such that for all $a \in E : 0+a=a+0=a$,*
4. *Additive inverse: For every $a \in E$, there exists a $-a \in E$ such that $a+(-a)=(-a)+a=0$,*
5. *Multiplicative associativity: For all $a,b,c \in E$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,*
6. *Multiplicative identity: There exists an element $1 \in E$ such that for all $a \in E$, $1 \cdot a = a \cdot 1 = a$,*
7. *Left and right distributivity: For all $a,b,c \in E$, $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$, and $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$.*

Rem. 17. *A* ***unit ring*** *is also called* ***ring with identity***, ***ring with unity***, ***unitary ring***, ***ring with*** 1 *(or* 1_R*) sometimes* ***unital ring*** *(for short, a ring with "any" unit is always a unital ring).*

Def. 164. *(Integral domain, or Entire ring). A unit ring (with $1 \neq 0$) with no divisor of zero, and which is commutative, is said to be an "**entire ring**" or an "**integral domain**" (sometimes known as a "**domain**").*

Integral domain (or Entire ring): A commutative ring with identity where the product of nonzero elements is never zero. Also known as entire ring. In other words, A ring that is commutative under multiplication, has a multiplicative identity element, and has no divisors of 0; (e.g. the integers form an integral domain).

Def. 165. *(Quotient ring). Quotient ring (also called residue-class ring, or factor ring) is a ring that is quotient of a ring R and one of its ideals $\mathfrak{a}$, denoted $R/\mathfrak{a}$.*

Def. 166. *(Ideal). An ideal is a subset $\mathbb{I}$ of elements in a ring R that forms an additive group and has the property that, whenever x belongs to R and y belongs to $\mathbb{I}$, then xy and yx belong to $\mathbb{I}$. For example, the set of even integers is an ideal in the ring of integers $\mathbb{Z}$. Given an ideal $\mathbb{I}$, we can define a factor ring $R/\mathbb{I}$. (Ideals are commonly denoted using a Gothic typeface)*

Ex. 59. *(Quotient ring). When the ring R is $\mathbb{Z}$ and the ideal is $6\mathbb{Z}$ (multiples of 6), the quotient ring is $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$. Usually, a quotient ring is a set of equivalence classes where $[[x]] = [[y]]$ if and only if $x-y \in \mathfrak{a}$. The quotient ring is an integral domain iff the ideal $\mathfrak{a}$ is prime. A stronger condition occurs when the quotient ring is a field, which corresponds to when the ideal $\mathfrak{a}$ is maximal.*

[1] *Unit element*: An element in a ring which acts as a multiplicative identity. *Unit*: An element of a ring with identity that has both a left inverse and a right inverse.
Identity element: The identity element I (also denoted e, 1, or E) of a group or related mathematical structure S is the unique element such that $Ia=aI=a$ for every element $a \in S$. An identity element is also called a *unit element*.

[2] *Divisor of zero*: A nonzero element x of a commutative ring such that $xy=0$ for some nonzero element y of the ring. Also known as zero divisor.

8.9. Field.

Structures stronger than "unitary rings" are structures where each element has also an inverse according to the multiplication (except for the zero element which does not have an inverse, due to $\forall a \in E$, $0 \cdot a = 0 \neq 1$). Thus, if E is provided with a *unit ring* structure, it is possible to find an element having an inverse, according to the multiplication, only in $E\backslash\{0\}$.

Def. 167. *(Field). $(E;+,\cdot)$ is called a field if:*
(i). $(E;+,\cdot)$ is a ring,
(ii). $(E\backslash\{0\};\cdot)$ is a group.

Rem. 18. *When $(E\backslash\{0\};\cdot)$ is an Abelian group, E is a commutative field. The fields considered in practice are commutative. (The inverse of a according to "·" is denoted a^{-1}).*

Ex. 60. *$\mathbb{R},\mathbb{Q},\mathbb{C}$ provided with "+" or "·"; Quotient field; Fields with two elements (Fig.)*

(1) $E=\{h,w\}$ (2) (3) $E\backslash\{h\}=\{w\}$

+	h	w
h	h	w
w	w	h

$(E;+)$
Abelian group

·	h	w
h	h	h
w	h	w

$(E;\cdot)$
Abelian semigroup

·	w
w	w

$(E\backslash\{h\};\cdot)$
Abelian group

Fig. Fields with two elements: (1) $(E;+)$ Abelian group with neutral element h. (2) $(E;\cdot)$ Abelian semigroup with neutral element w. (3) $(E\backslash\{h\};\cdot)$ Abelian group. [E is a field with two neutral elements; (E is isomorphic to $\mathbb{Z}/2\mathbb{Z}$)].

In each field, by analogy with the set of numbers, it is possible to define a subtraction and a division except for zero $0 : a-b=a+(-b)$, $c/d = c \cdot d^{-1}$.
Briefly, a field is any set of elements that satisfies the field axioms for both addition and multiplication and is a commutative division algebra. An archaic name for a field is "rational domain". The French term for a field is "*corps*" and the German word is "*Körper*". A field with a finite number of members is called a *finite field* or *Galois field*.

8.10. External composition law.

External composition laws allows also to construct important algebraic structures. Let act on a nonempty set E another set, called "set of operators". The elements of the set of operators are formed by elements of E. Let us denote the external composition law by "$\perp$".

Def. 168. *(External composition law). $\perp$ is called external composition law on a set E provided with Θ the set of operators if to any pair $(\alpha,a) \in \Theta \times E$ corresponds one and only one $b \in E$ such that $\alpha \perp a = b$. If b does not exist for any pair (α,a), we say that $\perp$ is an external composition law in E (Fig.)*

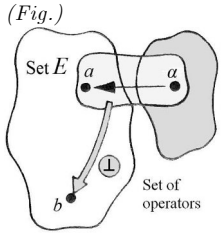


Fig. External composition law. ($\alpha \perp a$)

A set on which is defined an external composition law is denoted $(E,\Theta;\perp)$.

Rem. 19. *(Map). Any external composition law can be regarded as a map. Let be $T \subseteq \Theta \times E$; then, it is possible to define $\perp : T \to E$ by $(\alpha,a) \mapsto \alpha \perp a$. For an internal composition law on E, $T = \Theta \times E$. Rings and Fields can be used as sets of operators.*

Rem. 20. *By setting Θ=E, any internal composition law can be regarded as an external composition law.*

Ex. 61. *The multiplication of a vector by a scalar ($\Theta = \mathbb{R}$), the multiplication of matrices by a scalar ($\Theta = \mathbb{R}$), a repeated rotation or its inverse ($\Theta = \mathbb{Z}$).*

8.11. Module, vector space.

In the previous examples, it is easy to observe that E and Θ can have each one internal laws. The modules and vector spaces are exemplifications of these cases.

Def. 169. *(Module). Let be $(E;+)$ an Abelian group, $(\Theta;+,\cdot)$ an unitary ring and "$\bullet$" an external composition law on E whose Θ is the set of operators. Then $(E;+,\Theta;\bullet)$ is called module on the ring Θ (denoted "Θ-module") if we have for all $a,b \in E$ and $\alpha,\beta \in \Theta$ (Fig.): (i). $\alpha \bullet (a+b) = \alpha \bullet a + \alpha \bullet b$,*

(ii). $(\alpha+\beta)\bullet a=\alpha\bullet a+\beta\bullet a$,
(iii). $(\alpha\bullet\beta)\bullet a=\alpha\bullet(\beta\bullet a)$,
(iv). $1\bullet a=a$.

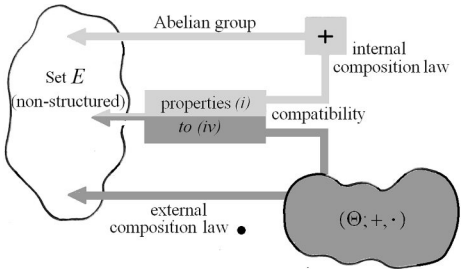


Fig. Θ-module structure.

Ex. 62. *The set of rotations (see ill. in heading "Internal composition law") provided with the internal law " ∘" (replacing +) and the external law "." (replacing •) is a $\mathbb{Z}$-module. $G_n=\{R_k|k\in\{0,1,...,n-1\}\subset\mathbb{N}\}$. Define an external composition law whose set of operators is $\mathbb{Z}$. $\mathbb{Z}\times G_n\to G_n$ map defined by $(z,R_k)\mapsto z\cdot R_k$, where $z\cdot R_k=\begin{cases}R_{z\cdot k} & \text{if } z\geq 0\\ R_{|z|\cdot(n-k)} & \text{if } z<0\end{cases}$. $R_{z\cdot k}$ can be thought of as a rotation of a multiple of $k\cdot\theta$.*

Ex. 63. *Any ring (and so any field) is a module on itself; the multiplication of the ring can be taken as external law.*

Thus, a module is defined as a mathematical object in which elements can be added together commutatively by multiplying coefficients and in which most of the rules of manipulating vectors hold. *A module is very similar to a vector space*, although in modules, coefficients are taken in the rings that are much more general algebraic objects than the fields used in vector spaces. A module which takes its coefficients in a ring R is called a module over R, or a R-module. Modules are the basic tool of homological algebra. Examples of modules: the set of integers $\mathbb{Z}$, the cubic lattice in d dimensions $\mathbb{Z}^d$, and the group ring of a group. $\mathbb{Z}$ is a module over itself. It is closed under addition and subtraction, although it is sufficient to require closure under subtraction.
In short, it is also possible to say that a module is a vector space in which the scalars are a ring rather than a field.

Def. 170. *(Vector space). If the set of operators Θ of a module is a field, which is not necessarily commutative, then this module is called "vector space" over the field (denoted Θ-vector space or Θ-v.s.).*

Ex. 64. *The set of continuous functions from $\mathbb{R}$ into $\mathbb{R}$ is a vector space over $\mathbb{R}$. Any commutative field is a vector space on itself.*

9. Order Structure

9.1. Comparability of sets.

In the sets $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$, the relation "$\leq$" always allows to compare two numbers; this relation establishes an *order* in the these sets. The relation "$\subseteq$" allows to compare sets in a system consisting of sets, but two sets are not necessarily *comparable* (Fig.). The two relations "$\leq$" and "$\subseteq$" have the fundamental properties, necessary and sufficient, which allow a comparison:
(1) *Reflexivity*: any element is a relation with itself,
(2) *Antisymmetry*: if x is in relation with y and y is in relation with x then $x=y$,
(3) *Transitivity*: if x is in relation with y and y is in relation with z then x is in relation with z.
These properties are the fundament of the *generalisation* of the notion of *order* about numbers. We give up the property that garantees that two elements are always comparable.

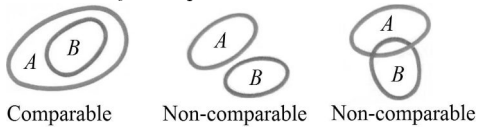


Fig. Comparison of sets; (A and B).

9.2. Order relation, ordered set.

Def. 171. *(Order relation). A relation $\preccurlyeq\subseteq S\times S$ is called an order relation if $\preccurlyeq$ is reflexive, antisymmetric and transitive. $(S;\preccurlyeq)$ is known as an ordered set; ("$\preccurlyeq$" means "less than or equal to"). Order relation is also known as order or ordering.*

Ex. 65. *$(\mathfrak{P}(S);\subseteq)$ is an ordered set, as well as every set systems provided with $\subseteq$; as well as $(\mathbb{N},\leq),(\mathbb{Z},\leq),(\mathbb{Q},\leq),(\mathbb{R},\leq)$. Divisibility is also an order relation over $\mathbb{N}$.*

The relation $<$ is not reflexive, thus this relation is not an order relation in the number sets. It is the same for the relation $\subset$ in any set system. But, instead of the reflexivity, the relations $<$ and $\subset$ have the following property: $x<y\Rightarrow\neg(y<x)$, this means that these relations are asymmetric. This observation leads to define the strict order relation.

Def. 172. *(Strict order relation). A relation $\prec\subseteq S\times S$ is called a strict order relation if $\prec$ is asymmetric and transitive. $(S;\prec)$ is known as a strict ordered set ($\prec$ means "strictly less than").*

Ex. 66. (1) *The relation $\leq$ on $\mathbb{R}$ is a total order relation (note that a relation on a totally ordered set is called a "total order", see heading "Totally ordered set"). The relation induced on $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ also. The strict order associated with the strict inequality relation $<$.* (2) *The relation $\leq$ on the set $\mathcal{F}(\mathbb{R},\mathbb{R})$ of numerical functions on $\mathbb{R}$ is an order relation. This is not a total order: for example the functions $x\mapsto x$ and $x\mapsto 0$ are not comparable. Here, $f<g$ means: $\forall x\in\mathbb{R}$, $f(x)\leq g(x)$ and $\exists x\in\mathbb{R}:f(x)<g(x)$. Therefore, it should not make the mistake to infer that: $\forall x\in\mathbb{R}$, $f(x)<g(x)$.* (3) *The relation $\subset$ on the set $\mathfrak{P}(\mathbb{N})$ is an order relation. This is not a total order since for example $\{0\}$ and $\{1\}$ are not comparable (none of both is included in the other).* (4) *The relation | (divisibility) on the set $\mathbb{N}$ is an order relation. This is not a toral order, since for example 2 and 3 are not comparable (none of both divides the other).* (5) *The relation | (divisibility) on the set $\mathbb{Z}$ is not an order relation, since it is not antisymmetric: the elements a and $-a$ divide each other.* (6) *Let $(S_1,\leq)$,..,$(S_n,\leq)$ be ordered sets,. The "product" order on $S:=S_1\times\cdots\times S_n$ is defined by: $(x_1,..,x_n)\preccurlyeq(y_1,..,y_n)$ if and only if $x_1\leq y_1,..,x_n\leq y_n$. This is not generally a total order. For example, on $\mathbb{R}\times\mathbb{R}$, $(0,1)$ and $(1,0)$ are not comparable for the "product" order. The lexicographic order on S is defined by: $(x_1,..,x_n)\preccurlyeq(y_1,..,y_n)$ if and only if $(x_1,..,x_n)=(y_1,..,y_n)$, or, i being the smallest index such that $x_i\neq y_i$, we have $x_i<y_i$. We can show that if the S_i are totally ordered, this is a total order. For example, on $\mathbb{R}\times\mathbb{R}$ endowed with the lexicographic order, $(0,1)\preccurlyeq(1,0)$. If $A=\{a,b,c\}$ is endowed with the alphabetic order (such as $a\leq b\leq c$) the lexicographic order on $A\times A$ is given by the relations: $(a,a)\leq(a,b)\leq(a,c)\leq(b,a)\leq(b,b)\leq(b,c)\leq(c,a)\leq(c,b)\leq(c,c)$.*

9.3. Contruction of order structures.

A strict order relation cannot be an order relation, due to the *absence of reflexivity.* Nevertheless, we can choose indiscriminately one or the other in order to construct the *order structures,* because any order relation induces a strict order relation on the same set and conversely. The bridge between both relations is garanteed by the diagonal $D:=\{(x,x)|x\in S\}$ expressing the reflexivity. Indeed, we can write: $\preccurlyeq\Rightarrow\preccurlyeq\setminus D$ (i.e. the order relation implies the strict order relation by the exclusion of the diagonal) and it is also possible to write: $\prec\Rightarrow\prec\cup D$ (i.e. the strict order relation implies the order relation by the inclusion of the diagonal which expresses the reflexivity). This can be expressed by means of following elements: $x\preccurlyeq y\Leftrightarrow x\prec y\vee x=y$ and respectively $x\prec y\Leftrightarrow x\preccurlyeq y\wedge x\neq y$. Thus $\preccurlyeq,\prec$ can be used simultaneously or indiscriminately. All remarks above are true for the following inverse relations: $\succcurlyeq,\succ$, their writings are stated easily.
The (strict or not) order relations $\subseteq,\subset,\leq,<$, "is divisor of", have inverse correpondences, i.e. the inverse order relations $\supseteq,\supset,\geq,>$,"is multiple of".

9.4. Totally ordered set.

When two elements of a set are always comparable, then such a characteristic defines total relations. Thus, we can define totally ordered sets:

Def. 173. *(Totally ordered set; Chain). $(S;\preccurlyeq)$ is known as a totally ordered set (also called linearly ordered set, simply ordered set, chain) if $\preccurlyeq$ is a total order relation (also called total order).*

A relation on a totally ordered set is called a "*total order*", or a "total order relation".

Def. 174. *(Totally ordered set; Chain)'. A totally ordered set (also called linearly ordered set, simply ordered set, chain) is a set plus a relation "$\preccurlyeq$" on the set (called total order) that satisfies the conditions for a partial order plus an additional condition known as the comparability condition. A relation "$\preccurlyeq$" is a total order on a set S ("$\preccurlyeq$ totally orders S") if the following conditions hold:*
1) $a\preccurlyeq a$ for all $a\in S$ (reflexivity)
2) $a\preccurlyeq b$ and $b\preccurlyeq a$ implies $a=b$ (antisymmetry)
3) $a\preccurlyeq b$ and $b\preccurlyeq c$ implies $a\preccurlyeq c$ (transitivity)
4) $\forall a,b\in S$, either $a\preccurlyeq b$ or $b\preccurlyeq a$ (comparability).
The first three are the axioms of a partial order, while addition of the comparability (also called "totality" or trichotomy law) defines a total order.

Antisymmetry eliminates uncertain cases when both a precedes b and b precedes a. A relation having the property of "comparability" (or "totality") means that any pair of elements in the set of the relation are comparable under the relation. This also means that the set can be diagrammed as a line of elements, giving it the name linear. Totality also implies reflexivity ($a \preccurlyeq a$). Thus, a total order is also a partial order. As seen above, the partial order has a weaker form of the fourth condition (it only requires reflexivity, not totality or comparability).
An **extension** of a given partial order to a total order is called a *linear extension* of that partial order.
Every *finite totally ordered set* is *well ordered*. Any two totally ordered sets with n elements (for n a nonnegative integer) are order isomorphic, and therefore have the same order type (which is also an ordinal number).

Rem. 21. *A total order is also called linear order, simple order, or non-strict ordering.*

Ex. 67. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *provided with* $\leq$ *are totally ordered sets, however* $(\mathfrak{P}(S); \subseteq)$ *and* $(\mathbb{N}; |)$ *are not a totally ordered set.*

While *chain* is merely a synonym for totally ordered set, it can also refer to a totally ordered subset of some partially ordered set. The latter definition has a central role in Zorn's lemma.

9.5. Partially ordered set.

Def. 175. *(Partially ordered set). a partially ordered set (or poset) is a set plus a relation on the set (called partial order) that satisfies the conditions for a partial order. The relation "$\preccurlyeq$" is a partial order on a set S if the following conditions hold:*
1) $a \preccurlyeq a$ *for all* $a \in S$ *(reflexivity)*
2) $a \preccurlyeq b$ *and* $b \preccurlyeq a$ *implies* $a = b$ *(antisymmetry)*
3) $a \preccurlyeq b$ *and* $b \preccurlyeq c$ *implies* $a \preccurlyeq c$ *(transitivity).*
A partially ordered set is also called a poset.

9.6. Order diagram. In simple cases, the order structure of a finite set can be clearly represented by an *order diagram*, also salled *Hasse diagram* (cf. Hasse diagram in heading "*Lattices and order relations*"). In such a diagram, each element is represented by a point in the plane; using the convention to draw b above a and link it with a if $a \prec b$, $a \preccurlyeq b$ respectively . The number of line segments is reduced by adding the convention of not linking b with a if b is located above another point linked with a (i.e. transitivity).
In the picture below (Fig.(I)) we have has placed b as the neighbor immediately above a if we have $a \preccurlyeq b \wedge \forall x(a \preccurlyeq x \preccurlyeq b \Rightarrow a{=}x \vee b{=}x)$. The elements of a *totally ordered set* are then depicted using the form of a "**chain**" (cf. def. of *Totally ordered set*; *Chain*). For subsets of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ the use of the numerical straight-line also allows a good rendering of the induced order of which we can endow them.

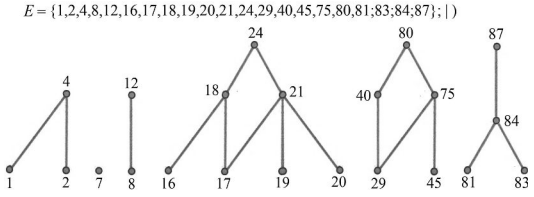


Fig.(I) Order diagram.

Hasse Diagram (order diagram): Graphical rendering of a partially ordered set (*poset*) displayed by the cover relation of the partially ordered set with an implied upward orientation. A point is drawn for each element of the poset, and line segments are drawn between these points according to the following two rules: (1). If $a < b$ in the poset, then the point corresponding to a appears lower in the drawing than the point corresponding to b. (2). The line segment between the points corresponding to any 2 elements a and b of the poset is included in the drawing iff a covers b or b covers a.

9.7. Induced order. If we restrict the *order structure* of a set E to one of its *subsets* S, here the order is then called "*induced order*" (Fig.); the *structure* of E is then transmitted to S. Moreover, the induced order may have additional properties compared to the order of the initial set (in Fig.(I), e.g. the subset {4,7,12,24,80,87} is a totally ordered set, while the initial set E is not a totally ordered set). If needed, we can examine the structure of the initial order using induced orders, e.g. using *Zorn theorem*; in this process the notions below are central.

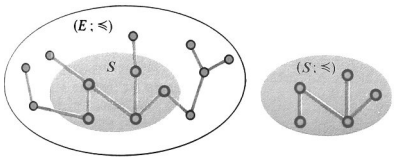


Fig. Induced order (partial order).

9.8. Greatest element, maximal element.
Thereafter, S is an **ordered set**.

Def. 176. *(Greatest element, or maximum element). a is the greatest element (or maximum element) of* $S :\Leftrightarrow a \in S \wedge \forall x(x \in S \Rightarrow x \preccurlyeq a)$.

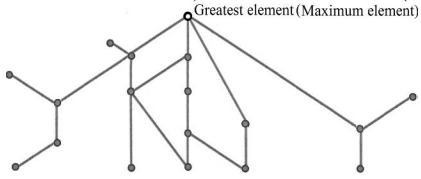


Fig. Greatest element (maximum element).

As we can see in previous Fig.(I), there does not necessarily exist a greatest element in a set, but if it exists it is unique. In contrast, in the same set, each of the elements 4,7,12,24,80,87 is the greatest element of the subset of those that are comparable to it. Such elements are said to be maximal.

Def. 177. *(Maximal element). a is a maximal element in* $S :\Leftrightarrow a{\in}S \wedge \forall x((x{\in}S \wedge a \preccurlyeq x) \Rightarrow (x{=}a))$.

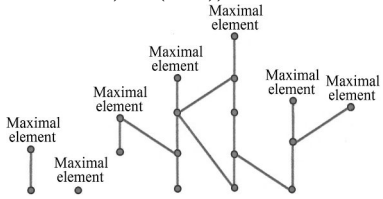


Fig. Maximal element.

An ordered set can have several maximal elements, but a totally ordered set can have at most one: this is the greatest element if it exists.
Zorn theorem concerns the existence of **maximal elements** (cf. heading "*Zermelo and Zorn theorems*").
In order theory, the *greatest element* of a subset U of a partially ordered set (poset) is an element of U which is greater than or equal to any other element of U. The term *least element* is defined dually. A bounded poset is a poset that has both a greatest element and a least element. The g*reatest elements* of a partially ordered subset must not be confused with *maximal elements* of such a set which are elements that are not smaller than any other element. A poset (partially ordered set) can have several maximal elements without having a greatest element. In a totally ordered set both terms coincide; it is also called *maximum*; in the case of function values it is also called the *absolute maximum*, to avoid confusion with a *local maximum*. The dual terms are *minimum* and *absolute minimum*. Together they are called the *absolute extrema*. A *maximal element* of a subset U of some partially ordered set is an element of U that is not smaller than any other element in U. A *minimal element* of a subset U of some partially ordered set is defined dually as an element of U that is not greater than any other element in U. The notions of maximal and minimal elements are weaker than those of greatest element and least element which are also known, respectively, as maximum and minimum.
Minimum element (*least element*) and *minimal element* are dualy defined as in the above definitions.
While a partially ordered set can have at most one each maximum and minimum it may have multiple maximal and minimal elements. Zorn's lemma states that every partially ordered set for which every totally ordered subset has an upper bound contains at least one maximal element. This Zorn's lemma is equivalent to the well-ordering theorem and the axiom of choice and implies crucial results in other areas of mathematics (such as Hahn-Banach theorem, Tychonoff's theorem, the existence of an algebraic closure for every field...)

9.9. Upper bound, least upper bound (supremum).
Here are two general definitions of an upper bound (sometimes called majorant).
Upper bound: **1.** If Q is a subset of an ordered set P, an upper bound b for Q in P is an element b of P such that $x \leq b$ for all x belonging to P. **2.** An upper bound on a function f with values in a partially ordered set E is an element of E which is larger than every element in the *range* of f.

In a set, the concept of the greatest element can be applied to subsets provided with the induced order. When in the subset A of a set S there is not a greatest element, then it is sometimes possible to find in the set S an element u which is upper (higher) or equal to all elements of A, i.e. u is the greatest element of $A \cup \{u\}$.

Ex. 68. *For a subset $G := \{x | x = 1 - \frac{1}{n} \wedge n \in \mathbb{N}\backslash\{0\}\}$ of $(\mathbb{Q}; \leq)$, such an element can be:* $1, 3/2, 2$.

Def. 178. *(Upper bound). u is an upper bound of $A :\Leftrightarrow A \subseteq S \wedge u \in S \wedge \forall x(x \in A \Rightarrow x \preccurlyeq u)$. If such an element u exists, then A is said to be "bounded from above" (Fig.*(1)).

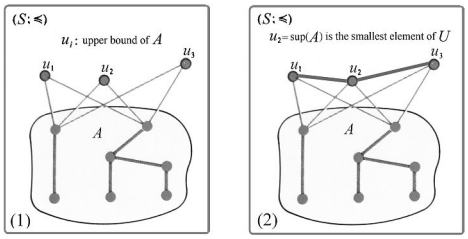


Fig. (1) Upper bound. (2) Least upper bound.

Rem. 22. *"u is an upper bound of A" is equivalent to " u is the greatest element of $A \cup \{u\}$".*

Since the subset which is "bounded from above", it is possible to consider the set U of all its upper bounds, and we can ask ourselves if it possesses a least element. Thus for the subset G defined previously, the set $U = \{x | x \in \mathbb{Q} \wedge x \geqslant 1\}$ admits 1 as the least element. The existence of such a "least upper bound" is not insured in the general case.

Def. 179. *(Least upper bound, or Supremum). The least upper bound of A (denoted s) is such that $s = \sup(A) :\Leftrightarrow A \subseteq S \wedge U = \{u |$ u upper bound of $A\} \wedge s$ least element of U. Also called "supremum" (*sup*).*

Given this definition, we can immediately deduce that if the least upper bound exists for such a subset, this least upper bound is unique, since it is the least element.

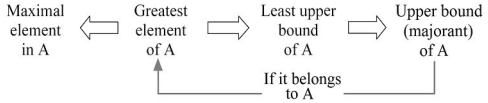


Fig. Relationship between greatest element, maximal element, upper bound and least upper bound.

Rem. 23. *The least upper bound (or supremum) plays a significant part in many "completion" processes, for example the completion of $\mathbb{Q}$ by means of the irrational numbers to get the field of real numbers $\mathbb{R}$. In $(\mathbb{Q}; \leq)$, a subset "bounded from above" does not necessarily have a least upper bound (Ex. infra), while this property is true in $(\mathbb{R}; \leq)$ by the introduction of irrational numbers.*

Ex. 69. *(Bounded subset of $\mathbb{Q}$ that does not admit least upper bound): Given $(\mathbb{Q}; \leq)$ and $X := \{x | x \in \mathbb{Q}^+ \wedge x^2 \leqslant 2\}$;*

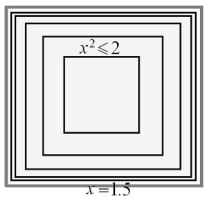


Fig. Illustration.

x can be considered as the length of the side of a square of area $x^2 \leqslant 2$. There exist upper bounds of X in $\mathbb{Q}$, e.g. 1.5*;* 1.42*;* 1.415*; etc., so X is bounded. There is no least upper bound of X in $\mathbb{Q}$,because $\sqrt{2} \notin \mathbb{Q}$ (see irrationality of $\sqrt{2}$ in heading "Default of order structure of $\mathbb{Q}$"). If we consider $(\mathbb{R}; \leq)$, then X admits $\sqrt{2}$ as least upper boun in $\mathbb{R}$. In a general way, we have the result: "Any bounded part of $\mathbb{Q}$ has a least upper bound in $(\mathbb{R}; \leq)$ (cf. theorem of the least upper bound in the heading "Construction of $\mathbb{R}$").*

Def. 180. *(Majorant). Let A be a part of a set E, where E is endowed with an order relation $\leq$. We say that an element M of E is a majorant of A in E, if every $x \in A$ verifies $x \leq M$. Attention, it is important to note that a majorant of A in E is an element of E but not necessarily an element of A. A* ***majorant*** *identifies with an* ***upper bound****.*

Def. 181. *(Least upper bound -Using the set of majorants). Let* $\mathrm{Maj}(A)$ *be the set of majorants. If there exists a smallest element b_s of* $\mathrm{Maj}(A)$*, then it is unique, it is a majorant of A, and more precisely the smallest majorant of A, in that sense that any other majorant M of A verifies $b_s \leq M$. We say then that b_s is the least upper bound of A in E.*

Attention, the least upper bound b_s can exist without being element of A. We show that A admits a greatest element if and only if it admits a least upper bound which is element of A; this least upper bound is then the greatest element of A.
We say that the order, defined on a set E, by a given order relation, is inductive if every totally ordered part A of E (i.e. such that for all x and $y \in A$ we have either $x \leq y$ or $y \leq x$) admits a majorant (i.e. upper bound) in E.
The order, defined on a set E, by a given order relation, is said *inductive* if any totally ordered part A of E (i.e. such that for all x and $y \in A$ we have either $x \leq y$ or $y \leq x$) admits a majorant (i.e. upper bound) in E.

9.10. Lower bound, greatest lower bound (infimum).

Here are both general definitions of a lower bound (sometimes called *minorant*).
Lower bound: **1.** A lower bound of a subset A of a set S is a point of S which is smaller than every element of A. **2.** A lower bound of a function f with values in a partially ordered set S is an element of S which is smaller than every element in the range of f.

Def. 182. *(Greatest lower bound). The greatest lower bound of a set of numbers S is the largest number among the lower bound of S. Abbreviated glb. Also known as "infimum" (inf).*

Def. 183. *(Minorant). Let A be a part of a set E, where E is endowed with an order relation $\leq$. We say that an element m of E is a minorant of A in E, if every $x \in A$ verifies $m \leq x$. Attention, it is important to note that a minorant of A in E is an element of E but not necessarily an element of A. A minorant identifies with a lower bound.*

Def. 184. *(Greatest lower bound -Using the set of majorants). Let* $\mathrm{Min}(A)$ *be the set of minorants. If there exists a greatest element b_g of* $\mathrm{Min}(A)$*, then it is unique, it is a minorant of A, and more precisely the greatest minorant of A, in that sense that any other minorant m of A verifies $m \leq b_g$. We say then that b_g is the greatest lower bound of A in E.*

Attention, the greatest lower bound b_g can exist without being element of A. We show that A admits a smallest element if and only if it admits an greatest lower bound which is element of A; this greatest lower bound is then the smallest element of A.

9.11. Well ordered set.

A relation on a totally ordered set is called a "*total order*". The property of a total order relation is equivalent to those which guarantees that any subset, constituted by two elements (and therefore any nonempty subset), has a least element: $a \preccurlyeq b \vee b \preccurlyeq a \Leftrightarrow \exists c\,(c \in (a, b) \wedge c$ least element of $(a, b))$. Starting from this analysis $(\mathbb{N}; \leq)$ and $(\mathbb{Z}; \leq)$ are considered as different, because in $(\mathbb{N}; \leq)$, any infinite subset (including $\mathbb{N}$) possesses also a least element, whereas this is not true in $(\mathbb{Z}; \leq)$, for example for $\mathbb{Z}$ or {0,-1,-2,...} does not possess a least element. Thus, $(\mathbb{N}; \leq)$ has a particular total order.

Def. 185. *(Well-ordered set). An ordered set $(E; \preccurlyeq_{w.o})$ is said to be well-ordered if any nonempty subset of E possess a least element. Then, we say that $\preccurlyeq_{w.o}$ is a well order (also said well ordering).*

Well-ordering principle: Every nonempty set of positive integers contains a smallest member.

A totally ordered set $(A; \leq)$ is said to be well ordered (or have a well-founded order) iff every nonempty subset of A has a least element. Every finite totally ordered set is well ordered. The set of integers $\mathbb{Z}$, which has no least element, is an example of a set which is not well ordered. An ordinal number is the order type of a well ordered set.
A well order is necessarily a total order, so, any well ordered set is totally ordered. The converse is false, since $(\mathbb{Z}; \leq)$ is totally ordered but it is not well ordered.
An important property resulting from all the above is the property that guarantees that any element of a well ordered set, if it is not the greatest element of the set, possesses one and only one *successor*[3] in the sense of the order relation (cf. heading "*Construction of* $\mathbb{N}$" in *Construction of Number System*).

[3] *Successor:* For any ordinal number a, the successor of a is $a \cup \{a\}$ (Ciesielski 1997). The successor of an ordinal number a is therefore the next ordinal, $a + 1$.

Ex. 70. $(\mathbb{N};\leq)$ *and any totally ordered finite set, are well ordered.* $\mathbb{Z}$ *can be well ordered by means of the introduction of another order relation, which is deduced from the sequence (0,1,-1,2,-2,...) by* $z_i \preccurlyeq_{w.o} z_k :\Leftrightarrow i \leq k$. $(\mathbb{Q};\leq)$ *and* $(\mathbb{R};\leq)$ *are not well ordered because they contained* $(\mathbb{Z};\leq)$. *Furthermore,* $\mathbb{Q}$ *can be well ordered by means of a sequence, i.e. the one of the diagonal method (see section about the denumerability). By contrast this method fails regarding* $\mathbb{R}$, *because* $\mathbb{R}$ *is not denumerable. Indeed, a well order for* $\mathbb{R}$ *could not be clarified until now. However, if we admit the axiomatic construction leading to the Zermelo theorem, then, any set can be well ordered, including* $\mathbb{R}$.

9.12. Zermelo and Zorn theorems.

Mathematics uses *transfinite induction (or recurrence*) and Zermelo theorem for demonstrations regarding *infinite sets.* Let us recall (1) the principle of transfinite induction and (2) the Zermelo theorem.

Principle of transfinite induction: Given A a *well ordered set* and B a subset of the nonnegative integers $\mathbb{Z}^*$ with the properties that the set B contains the least element 0 of A and any time that $[0,x) \subset B$, we can show that x belongs to A. Under these conditions, B=A.

Th. 35. (**Zermelo**). *"Any set can be well ordered".*

Zermelo theorem results from the *axiom of choice* in the *set theory.* Furthermore, the *axiom of choice* can be deduced from the property of the Zermelo theorem, taken as an axiom. Thus, there is an equivalence between the Zermelo theorem and axiom of choice. It is important to mention that they have been either criticized. Indeed, Zermelo theorem does not guarantee that the existence of a well order for any set A, but the relation defining it usually has nothing to do with an order structure that we could know on A. Finally, after the Zermelo theorem and axiom of choice, there is a third statement (in connection with the two first) which involves the concept of *inductive ordered set*, i.e. ordered set in which any totally ordered subset (for the induced relation) admits a least upper bound. This is the Zorn lemma. First, recall the meaning of an inductive set.

Inductive set: A set-theoretic term having a number of different meanings (according to Fraenkel, Bourbaki, Russel, Pinter, Lang, Jacobson, Roitman,..). Fraenkel (1953, p 37) used the term as a synonym for "*finite set*". However, according to Russell's definition (Russell 1963, p 21-22), an inductive set is a *nonempty partially ordered set* in which every element has a *successor.* An example is the set of natural numbers $\mathbb{N}$, where 0 is the first element, and the others are produced by adding 1 successively. For many other authors (e.g. Bourbaki 1970 p 20-21, or Pinter 1971), an *inductive set* is a partially ordered set in which every totally ordered subset has an upper bound, i.e. it is a set fulfilling the assumption of Zorn lemma.

Lem. 4. *(Zorn - Version n° 1). "Any inductive ordered set admits at least a maximal element".*

(Recall: *Chain* (also called *totally ordered set*): Given E a finite partially ordered set; a *chain* in E is a set of pairwise comparable elements (i.e. a *totally ordered subset*). The partial order length of E is the maximum cardinality of a chain in E. For a partial order, the size of the longest chain is called partial order length.)

Lem. 5. *(Zorn - Version n° 2). If E is any nonempty partially ordered set in which every chain has an upper bound, then E has a maximal element. This statement is equivalent to the axiom of choice.*

The corollary of this lemma is written:

Cor. 6. *If* $(E;\preccurlyeq)$ *is an inductive well ordered set, then* $\forall x \in E$ *there is a maximal element* α *such that* $x \preccurlyeq \alpha$.

Ex. 71. *A basis for an arbitrary vector space* $\neq\{0\}$ *containing a given free part.*

10. Ordinals

The concept of cardinal highlights the numbers of elements of a set. This concept is based on the comparison of *non-structured sets* by means of *bijective maps.* As regard this method, the infinite sets create problems, unlike finite sets. The denumerable sets are simplest examples, i.e. the sets which are in a bijective relation with $\mathbb{N}$. Moreover, $\mathbb{N}$ has a remarkable "order structure"; Two of its elements can always be compared; one element has always a *successor* (or a following element) and any nonzero element has an *antecedent.* About $\mathbb{N}$, a case which cannot be *in a bijective relation with* $\mathbb{N}$, is the infinite set of real numbers $\mathbb{R}$ which is a field. Indeed, two real numbers can be always compared by means of the natural order relation of $\mathbb{R}$, by contrast, no real number has a successor or antecedent. The taking into account of the elements of a set S can use a good order structure on S, this structure can be defined either directly or by bijection starting from an ordered set. Thus, we are led to compare ordered sets by using bijective maps compatible with the ordered structures. This is the purpose of the next heading.

10.1. Isomorphisms of ordered sets.

Def. 186. *(Isomorphism of ordered sets). Given* $(A;\preccurlyeq_1)$,$(B;\preccurlyeq_2)$ *two ordered sets, and* $f : A \to B$ *a map. Then*
(i) f *increasing* $:\Leftrightarrow \forall x\forall y(x \preccurlyeq_1 y \Rightarrow f(x) \preccurlyeq_2 f(y))$
(ii) f *isomorphism of ordered sets* $:\Leftrightarrow f$ *bijective* $\wedge f$, f^{-1} *increasing.* $(A;\preccurlyeq_1)$ *and* $(B;\preccurlyeq_2)$ *are "similar" if there is an isomorphism of ordered sets from the one to the other; written* $(A;\preccurlyeq_1) \cong (B;\preccurlyeq_2)$.

[Remember that the statement *"A is isomorphic to A′"* is denoted $A \cong A'$, see section about "Lattices and order relations"]. We can say that two similar ordered sets have *equivalent orders* (i.e. isomorphic), thus, they cannot be differentiated according to their order structure (in Ex. infra, only (5) and (6) are similar).

Ex. 72. *(Order structures and equipotence):* (1) $(\mathbb{N};\leq) := (0,1,2,...)$*; no greatest element,* 0=*smallest element.* (2) $(\mathbb{N};\preccurlyeq_1) := (..,2,1,0)$*; no smallest element,* 0=*greatest element.* (3) $(\mathbb{N};\preccurlyeq_2)$:=$(.,5,3,1,0,2,4,.)$*; no smallest element, no greatest element.*
(4) $(\mathbb{N}\cup\{-1\};\preccurlyeq_3) := (0,1,2,...,-1)$*;* 0=*smallest element,* -1=*greatest element, the greatest element has no antecedent.* (5) $(\mathbb{N}\cup\{-1,-2\};\preccurlyeq_4) := (0,1,2,..,-1,-2)$*;* 0=*smallest element,* -2=*greatest element, whose antecedent is* -1. (6) $(\mathbb{N};\preccurlyeq_5) := (2,3,4,..,0,1)$*;* 2=*smallest element,* 1=*greatest element, whose antecedent is* 0.

Def. 187. *(Order isomorphic). Two totally ordered sets* $(A;\preccurlyeq)$ *and* $(B;\preccurlyeq)$ *are order isomorphic iff there is a bijection f from A to B such that for all* α_1,$\alpha_2 \in A$, $\alpha_1 \leq \alpha_2$ *if and only if* $f(\alpha_1)\leq f(\alpha_2)$, *meaning that A and B are equipollent ("the same size") and there is an order preserving mapping between the two. (This property is called "similar". Def. is valid for partially ordered sets).*

Rem. 24. *Two similar ordered sets are equipotent, since an isomorphism of ordered sets is a bijection, but the converse is not true. Indeed, two ordered equipotent sets are not necessarily similar.*

Equivalents sets (equipotent sets): Sets with *same cardinal number*; set whose elements can be put into one-to-one correspondence with each other; also called equinumerable sets; *equipotent sets.*

10.2. Order type.

The relation $\cong$ (seen before) is an equivalence relation in any set of ordered sets $\mathfrak{E}$:
(1) 1_A is an isomorphism of ordered sets,
(2) f isomorphism of ordered sets $\Rightarrow f^{-1}$ isomorphism of ordered sets,
(3) f isomorphism of ordered sets $\wedge g$ isomorphism of ordered sets $\Rightarrow g \circ f$ isomorphism of ordered sets.
Thus, the quotient set denoted $\mathfrak{E}/\cong$ is composed of classes of similar ordered sets.

Def. 188. *(Order type).An element of the quotient set* $\mathfrak{E}/\cong$ *is called order type.*

Every totally ordered set $(A;\preccurlyeq)$ is associated with a so-called *order type.* Two sets A and B are said to have the same *order type* if and only if they are *order isomorphic.* Thus, an *order type* categorizes totally ordered sets in the same way that a cardinal number categorizes sets. The term dates back Georg Cantor and the definition is valid for partially ordered sets.
It is possible to assign to any ordered set of $\mathfrak{E}$ an order type by means of a map that we name "orty" (see "Equivalence relation, quotient set" about canonical surjection), orty : $\mathfrak{E} \to \mathfrak{E}/\cong$ defined as follows: orty(A;$\preccurlyeq$)$\mapsto$ orty(A;$\preccurlyeq$)=[[(A;$\preccurlyeq$)]]. Then we can check:
orty$(A;\preccurlyeq_1)$= orty$(B;\preccurlyeq_2)\Rightarrow$ card(A)=card(B);
note that the converse is not true.

Rem. 25. *The property of well order is preserved by an isomorphism of ordered sets, then* $\mathfrak{E}/\cong$ *can be splitted among two disjoint subsets,* $\mathfrak{E}_{w.o.}/\cong$ *containing all the order types of well ordered sets, and* $\mathfrak{E}_{n.w.o.}/\cong$ *containing these order types of non-well-ordered sets.*

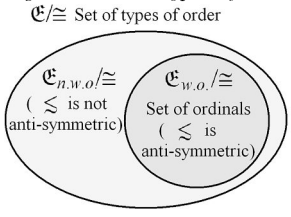


Fig. Partition into 2 subsets of the quotient space of order types. $((E_1;\preccurlyeq_1) \cong (E_2;\preccurlyeq_2) \wedge \preccurlyeq_1$ *well order* $\Rightarrow \preccurlyeq_2$ *well order.)*

10.3. Comparison of order type. We know that two similar ordered sets are also equipotent then an order relation $\leq$ for the order types must be compatible with those on the cardinals. Thus, a def. can by given by: $\text{orty}(E;\preccurlyeq_1) \lesssim \text{orty}(F;\preccurlyeq_2) :\Leftrightarrow \exists G(G \subseteq F \wedge G \cong E)$, where G is a subset of F provided with the induced order (cf. heading). The relation thus defined is reflexive and transitive but *non-antisymmetric, therefore it is not an order relation* (see Ex. below). By contrast, when we restrict the selected set to the subset of well-ordered sets ($\mathfrak{E}_{w.o.}/\cong$), then the *antisymmetry* is verified, this results from the prop.1 in the next heading.

Ex. 73. *(Set of the non-antisymmetry of $\lesssim$): $A = \{x | x \in \mathbb{Q} \wedge -2 < x \leq -1\}$; $B = \{x | x \in \mathbb{Q} \wedge 1 \leq x < 2\}$; $f : C \to A$ defined by $x \mapsto f(x) = 2x - 4$; $g : D \to B$ defined by $x \mapsto g(x) = 2x + 4$. $(A;\leq)$ and $(B;\leq)$ are not similar, since B does not have greatest element. Given $C = \{x | x \in \mathbb{Q} \wedge 1 < x \leq \frac{3}{2}\}$ and $D = \{x | x \in \mathbb{Q} \wedge -\frac{3}{2} \leq x < -1\}$; We have $C \subset B$ and $(C;\leq) \cong (A;\leq)$ respectively $D \subset A$ and $(D;\leq) \cong (B;\leq)$, that is,* $\text{orty}\, A \leq \text{orty}\, B$ *and* $\text{orty}\, B \leq \text{orty}\, A$ *but* $\text{orty}\, A \neq \text{orty}\, B$ *(Fig.).*

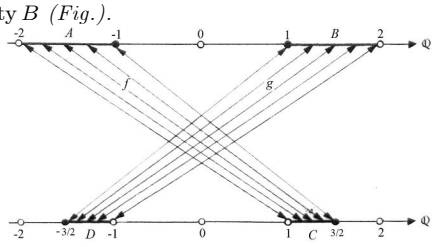


Fig. Illustration.

10.4. Ordinals. *Ordinal number:* In common usage, an ordinal number is an adjective describing the *numerical position* of an object (e.g. 1st, 2nd, 3rd, etc). In set theory, an ordinal number, sometimes called an "ordinal", is one of the numbers in Cantor's extension of the whole numbers. An ordinal number is defined as the order type of a well ordered set.

Def. 189. *(Ordinal). The order type of a well ordered set is called ordinal, written* $\text{ord}(E;\preccurlyeq_{w.o.})$ *(Fig. in heading "Order type").*

A *standard representation of ordinals* is:

Symbol	*Elements*	*Characterization*
0	$\varnothing$	empty set
1	{0}	set of one element
2	{0,1}	set of two elements
3	{0,1,2}	set of three elements
⋮		
ω	{0,1,2,...}	set of all finite ordinals
ω+1	{0,1,2,..,ω}	
⋮		
ω_1		set of all countable ordinals
⋮		
ω_2		set of all countable and $\aleph_1$ ordinals
⋮		
ω_ω		set of all finite ordinals and $\aleph_k$ ordinals for all nonnegative integers k
⋮		

Rem. 26. *We can consider that the map "*ord*" is a restriction of the map "*orty*" to the subset $\mathfrak{E}_{w.o.}$ of well ordered sets of $\mathfrak{E}$.*

If the relation previously defined $\lesssim$ is restricted to ordinals, this relation becomes an order relation, denoted $\leq$. In addition, this relation is total and is also a well order on any set of ordinals because of the particular structure of well ordered sets.

Rem. 27. *(Initial segment). We introduce the notion of initial segment in a totally ordered set S. If $x \in S$, the part $E_x := \{y \in S \mid y < x\}$ is the open initial segment defined by x, whereas $E_x := \{y \in S \mid y \leq x\}$ is the closed initial segment defined by x. Thus, we obtain the important proposition:*

Prop. 1. *Given two well ordered sets. Then either they are similar or one well ordered set is similar to an initial segment of the other.*

Cor. 7. *A well ordered set is similar to none of its beginning sections.*

We know that every finite totally ordered set is well ordered. Any two totally ordered sets with k elements (k: nonnegative integer) are order isomorphic and therefore have the same order type, which is also an ordinal number. The ordinals for finite sets are denoted $0, 1, 2, 3$, ..., i.e. the integers one less than the corresponding nonnegative integers. The first transfinite ordinal, denoted ω, is the order type of the set of nonnegative integers. This is the "smallest" of *Cantor's transfinite numbers*[4], defined to be the smallest ordinal number greater than the ordinal number of the whole numbers. It is denoted $\omega = \{0, 1, ..|\}$. From the definition of ordinal comparison, it follows that the ordinal numbers are a well ordered set. In order of increasing size, the ordinal numbers are $0, 1, 2$, ..., ω, $\omega + 1$, $\omega + 2$, ..., $\omega + \omega$, $\omega + \omega + 1$, ... The notation of ordinal numbers can be a bit counterintuitive, e.g. even though $1 + \omega = \omega$, $\omega + 1 > \omega$. The cardinality of the set of countable ordinal numbers is denoted $\aleph_1$ (i.e. aleph-1). If $(S;\leq)$ is a well ordered set with ordinal number α, then the set of all ordinals $< \alpha$ is order isomorphic to S. Thus it is possible to define an ordinal as the set of all ordinals less than itself.

Rem. 28. *John von Neumann defined a set to be an ordinal number if and only if:*
1. *If β is a member of α, then β is a proper subset of α*
2. *If β,γ are members of α then one of the following is true: β=γ, β is a member of γ, or γ is a member of β.*
3. *If β is a nonempty proper subset of α, then there exists a γ member of α such that the intersection $\gamma \cap \beta$ is empty.*

10.5. Finite ordinals. Let us recall that $(\mathbb{N};\leq)$ is well ordered, and therefore any finite subset of $\mathbb{N}$ is also well ordered. When the following subsets $\varnothing, \{0\}, \{0,1\}$,... are non structured they represent the finite cardinals. If they are provided with the induced order, they represent the finite ordinals. Indeed, let be a well ordered set $(A;\preccurlyeq_{w.o})$ such that $\text{card}(A) = n$: we can represent it in the form of a sequence, since $a_0 \preccurlyeq_{w.o} a_1 \preccurlyeq_{w.o} \cdots \preccurlyeq_{w.o} a_{n-1}$. The map $f : A \to \{0, 1, ..., n-1\}$, defined by $a_i \mapsto i$ is then an isomorphism of ordered sets, this means that $\text{ord}(A;\preccurlyeq_{w.o}) = \text{ord}(\{0, 1, ..., n-1\};\leq)$.
The case of finite sets show that several well orders can be defined on a same set. Any permutation different from the identity applied to elements of the sequence creates a new well order; if $\text{card}(A) = n$ then there exist $n!$ pairwise different well orders on A. However, for finite sets, the different well orders are associated with the same ordinal, i.e.

$$\text{card}(A) = \text{card}(B) \Leftrightarrow \text{ord}(A) = \text{ord}(B).$$

Thus, finite ordinals can be confused with finite cardinals $0, 1, 2, ...$ By contrast, we know that there exists a crucial difference between infinite ordinals and infinite cardinals: see ordinal classes.

10.6. Infinite ordinals. The smallest infinite ordinal is denoted ω, and is such that $\omega := \text{ord}(\mathbb{N};\leq)$. If $ord(A;\preccurlyeq_{w.o}) < \omega$ then $(A;\preccurlyeq_{w.o})$ is necessarily similar to an initial segment of $(\mathbb{N};\leq)$, which is a finite subset of $\mathbb{N}$. This implies that A is also finite, and therefore $ord(A;\preccurlyeq_{w.o})$ is a finite ordinal. Moreover, we can describe other infinite ordinals by the proposition below:

Prop. 2. *If we add to a set representing an ordinal α an element as the greatest element of the new set thus formed, we obtain a set which is a representative of the ordinal β, an immediate successor of α ($\beta := \alpha + 1$) (cf. Ex below).*

Ex. 74. *(Successor of an ordinal): Consider* $(A;\preccurlyeq_{w.o.}) := (a, b, ...)$, *we have* $\alpha := \text{ord}(A;\preccurlyeq_{w.o.})$; *consider now* $(A \cup \{x\};\preccurlyeq_{w.o.}) := (a, b, ..., x)$, *we have* $\beta := \text{ord}(A \cup \{x\};\preccurlyeq_{w.o.})$. *We have:* $\alpha < \beta \wedge \neg\exists\gamma(\alpha < \gamma < \beta)$.

Thus, the well ordered sets (0,1,..,−1), (0,1,..,−1,−2), ..., (0,1,...,−1, ...,−n), etc. are representatives of ordinal successors of ω: $\omega + 1 = \{0, 1, 2, ..., \omega\}$, $\omega+2 = \{0, 1, 2, ..., \omega, \omega+1\}$,..., $\omega+n = \{0, 1, 2, ..., \omega, \omega+1, .., \omega + n - 1\}$, etc... The previous proposition makes possible to build the successor $\alpha + 1$ of any ordinal α. However this process by finite ordinals does not make possible to reach all ordinals; e.g. the ordinal associated with $(0, 1, ..., -1, -2, ...)$ which is denoted $\omega + \omega = \{0, 1, 2, ..., \omega, \omega+1, \omega+2, ...\}$, cannot be reach because this set does not possess a greatest element. This is also true if we apply this process to finite ordinals in order to build ω. More generally, an ordinal (different from zero) which is not successor of another ordinal is called a "limit ordinal" (ω and $\omega + \omega$ are examples).

Def. 190. *(Limit ordinal). An ordinal number $\alpha > 0$ is called a limit ordinal if and only if it has no immediate "predecessor", i.e. if there is no ordinal number β such that $\beta + 1 = \alpha$.*

[4] *Transfinite number:* Any ordinal or cardinal number equal to or exceeding aleph null. (One of Cantor's ordinal numbers $\omega, \omega+1, \omega+2, ..., \omega+\omega, \omega+\omega+1$,... which is "larger" than any whole number).

Def. 191. *(Predecessor). α is called a predecessor if there is no ordinal number β such that $\beta+1=\alpha$.*

Then it is possible to repeat the previous process by starting from a limit ordinal. Indeed, from $\omega+\omega$ (or $\omega\cdot 2$), we obtain the limit ordinal which is immediately superior, $\omega+\omega+\omega$ (or $\omega\cdot 3$), etc.. Thus, an (infinite) sequence of ordinals is constructed, which is called the *Cantor sequence (Ex. below)*, for which one of properties is given by:

Prop. 3. *The ordinal of any open initial segment Ω_α of the well ordered set, generated by the Cantor sequence, is.α.*

Ex. 75. *(A sequence of ordinals):*

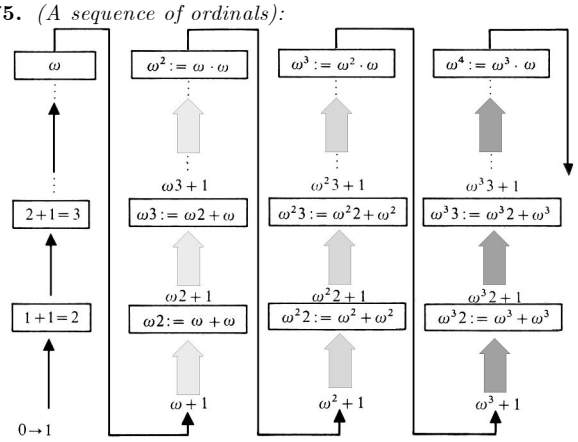


Fig. A sequence of ordinals (Cantor).

10.7. Burali-Forti paradox. If we suppose the existence of the set Ω of all ordinals, then it can be well ordered (i.e. there exists an ordinal α : ord$(\Omega;\leq)$, with $\alpha\in\Omega$, α makes it possible to define an open initial segment Ω_α of $(\Omega;\leq)$, which verifies ord$(\Omega_\alpha;\leq)=\alpha$ since Ω is supposed contain all the ordinals (the ordinal associates with the closed initial segment is $\alpha+1$). Therefore $(\Omega_\alpha;\leq)$ and $(\Omega;\leq)$ are similar, which is contradictory with the **Prop 1.** Another way to present this paradox is as follows:

Def. 192. *(Burali-Forti paradox). In the theory of transfinite ordinal numbers,*
(1) *Every well ordered set has a unique ordinal number,*
(2) *Every segment of ordinals (i.e. any set of ordinals arranged in natural order which contains all the predecessors of each of its elements) has an ordinal number which is greater than any ordinal in the segment, and*
(3) *The set Φ of all ordinals in natural order is well ordered. Then by statements* (3) *and* (1)*, Φ has an ordinal β. Since β is in Φ, it follows that $\beta<\beta$ by* (2)*, which is a contradiction.*

10.8. Ordinal comparison.

Def. 193. *(Ordinal comparison). Let $(E;\leq)$,$(F;\leq)$ be well ordered sets with ordinal numbers α and β. Then $\alpha<\beta$ if and only if E is order isomorphic to an initial segment of F. We can then easily show that the ordinal numbers are totally ordered by the relation. In fact, they are well ordered by the relation.*

10.9. Ordinal classes. A non-structured set can be well ordered by using different ways. In the case of infinite sets, we can generate different ordinals. Let be a a cardinal, then "$Z(a)$" denotes the set of all ordinals, whose representatives are the cardinal of a. Then: Finite $a\Rightarrow \text{card}\,(Z(a))=1$; Infinite $a\Rightarrow \text{card}\,(Z(a))\geqslant a$.

Ex. 76. *An example is $Z(\aleph_0)$, where $\aleph_0=\text{card}(\mathbb{N})$ is a non denumerable set, whose cardinal is denoted $\aleph_1$. We can show that there is no cardinal between $\aleph_0$ and $\aleph_1$. If we accept the "continuum hypothesis" (cf. section: "Denumerability, Non-denumerability", and def. of Continuum), then we deduce: card($\mathbb{R}$)=$\aleph_1$.*

Continuum hypothesis: ■ The notion dates back to *Cantor* who shown that there is no infinite set with a cardinal number between the *small* infinite set of integers $\aleph_0$ and the *large* infinite set of real numbers c, i.e. the "continuum". The continuum hypothesis is such that $\aleph_1=c$. ■ *Gödel* proved that no contradiction would appear if the continuum hypothesis were added to classical *Zermelo-Fraenkel* set theory. Furthermore, *Cohen* (by using a method named *forcing*) proved that no contradiction would appear if the negation of the continuum hypothesis was added to set theory. The *Gödel* and *Cohen* works established that the validity of the continuum hypothesis depends on the version of set theory being used, and is therefore undecidable (assuming the *Zermelo-Fraenkel axioms* together with the axiom of choice). ■ *Conway* and *Guy* relate a generalized version of the continuum hypothesis which dates back *Hausdorff* and is also undecidable: The problem is to know if $2^{\aleph_\alpha}=\aleph_{\alpha+1}$ exists for every α. The continuum hypothesis results from *generalized continuum hypothesis*, ZF+GCH+CH. ■ *Woodin* formalized a *new "axiom"* whose acceptance (in addition to the *Zermelo-Fraenkel axioms* and *axiom of choice*) would imply that the continuum hypothesis is *false*. Such an approach became widespread among the theoreticians.

Rem. 29. *Using the concept of "ordinal class" and the well order $\leq$ on ordinals, we can show that the relation $\leq$ on cardinals is also a well order.*

10.10. Operations on ordinals. The *ordered union of ordered sets* allows to define a *non-commutative addition* on the ordinals. Indeed by means of the *lexicographic product* of ordered sets, it is possible to introduce a noncommutative multiplication on ordinals (see I below); By the *lexicographic product* of an ordered set, we introduce *a non commutative multiplication* of ordinals (see II below). These laws, addition and multiplication are associative, but the multiplication is only left distributive with respect to the addition (cf. also heading "*Operations on cardinals*").

Sum and product of ordinals:
Given $(X;\prec_1):=(x_0,x_1,...)$; $(Y;\prec_2):=(y_0,y_1,...)$;
I) $X\cap Y=\emptyset$, $(X\cup Y;\prec_0):=(x_0,x_1,...,y_0,y_1,...)$

Def. 194. ord$(X;\prec_1)+$ord$(Y;\prec_2)$:=ord$(X\cup Y;\prec_0)$

II) *Lexicographic product, product of ordinals*:
$(X\times Y;\prec_p):=((x_0,y_0),(x_0,y_1),...,(x_1,y_0),(x_1,y_1),...)$

Def. 195. ord$(Y;\prec_2)\cdot$ord$(X;\prec_1)$:=ord$(X\times Y;\prec_p)$

Ex. 77. $\begin{cases}(X;\prec_1):=(0,1,2,...); & \text{ord}\,X=\omega.\\ (Y;\prec_2):=(y_0,y_1); & \text{ord}\,Y=2.\end{cases}$

I) $(X\cup Y;\prec_0)=(0,1,2,...,y_0,y_1)$; ord$(X\cup Y)=\omega+2$
$(Y\cup X;\prec_0)=(y_0,y_1,0,1,2,...)$; ord$(Y\cup X)=\omega$
i.e.: ord $X+$ ord $Y\neq$ ord $Y+$ ord X

II) $(X\times Y;\prec_p)=((0,y_0),(0,y_1),(1,y_0),(1,y_1),..)$; ord$(X\times Y)=\omega$.
$(X\times Y;\prec_p)=((y_0,0),(y_0,1),..,(y_1,0),(y_1,1),..)$; ord$(Y\times X)=\omega\cdot 2$
i.e.: ord $X\cdot$ ord $Y\neq$ ord $Y\cdot$ ord X.

10.11. Spotting of elements of a set. The cardinal α of a nonempty set S can be defined as smallest ordinal number equipotent to S. We can transport to S a well order $\preccurlyeq_{w.o}$by the bijection associated with this equipotence. $\alpha:=\text{ord}(S;\preccurlyeq_{w.o})\cdot\text{ord}(S;\preccurlyeq_{w.o})$ is similar to the (open) initial segment Ω_α constituted by ordinals $\beta<\alpha$. $\forall x\in S$, the (open) initial segment $S_x:=\{y\in S|y<x\}$ defines the ordinal number ord(S_x). If $x'\neq x''$ we have ord$(S_{x'})\neq$ ord$(S_{x''})$. Thus, we can spot the elements of S through these ordinals whose set constitutes α. If S is denumerable, we find again a numbering of S by $\mathbb{N}$.

10.12. Transfinite induction. *Transfinite induction:* In short, the transfinite induction is a reasoning by which if a theorem holds true for the first element of a well ordered set E and is true for an element n whenever it holds for all predecessors of n. then the theorem is true for all members of E.
The principle of transfinite induction can also be written: "Let E be a well ordered set and F be a subset of the nonnegative integers $\mathbb{Z}^*$ with the properties that (first) the set F contains the least element 0 of E and (second) any time that $[0,x)\subset F$, one can show that x belongs to E. Under these conditions, $F=E$."
5th Peano axiom: $\forall S((S\subseteq\mathbb{N}\wedge 0\in S\wedge\forall n(n\in S\Rightarrow succ.(n)\in S))\Rightarrow S=\mathbb{N})$. It is generalized to *open initial segments* of ordinal numbers. This allows an extension of the *principle of mathematical induction,* namely, the *transfinite induction.*

Prop. 4. *Given $\Omega_\alpha=\{\beta|\beta<\alpha\}$ an "open" initial segment of an ordinal and $S\subseteq\Omega_\alpha$. If $0\in S$ and for any "open" initial segment $\Omega_\beta\subseteq S(\beta<\alpha)$ we have also $\beta\in S$ then $S=\Omega_\alpha$.*

If $\Omega_\alpha=\mathbb{N}$ we obtain the *5th Peano axiom.* The above proposition allows the extension of the mathematical induction (principle of recurrence) to infinite ordinals. Then we can show properties of the form: $\forall\beta(\beta\in\Omega_\alpha\Rightarrow A(\beta))$. In fact it would be necessary to prove:
(i) $A(0)$,
(ii) $(\forall\gamma(\gamma<\beta\Rightarrow A(\gamma)))\Rightarrow A(\beta)$.
If $\Omega_\alpha=\mathbb{N}$, the 2nd condition is equivalent to $\forall n(A(n)\Rightarrow A(n+1))$. Since we have previously stated the 5th Peano axiom, let us briefly present the *Peano's Axioms* (Peano axioms will give Peano arithmetic - i.e. a version of number theory). In short, **Peano axioms** are:
(1) Zero is a number.
(2) If α is a number, the successor of α is a number.

(3) zero is not the successor of a number.
(4) Two numbers of which the successors are equal are themselves equal.
(5) If a set S of numbers contains zero and also the successor of every number in S, then every number is in S. (It is the *induction axiom*).

11. Topological Structures

Topological structure: A set can be provided with a *topological structure* if one selected in this set a subsets system $\mathfrak{F}$ verifying differentes properties. The topological structure is very important to define the concept of *convergence*. A set which has a topological structure is called a *topological space*.

As shown before (cf. particular maps), we know that a *sequence* can be regarded as a *particular map*. Besides, sequences are analytic tools and allow to provide fundamental constructions. Despite the foregoing, the algebraic structures and the order structures do not allow to define the crucial concept of "*convergence of a sequence*". In short, we can say that the existence of a limit for a sequence means that in any neighborhood of this limit we always find all elements of the sequence except a finite number of them (Fig.). This intuitive approach will be formalized by using particular subsets of the initial set. Indeed, this initial set will be provided with a structure which is called *topological structure* and will become then a *topological space* in which the concept of neighborhood is axiomatically defined.

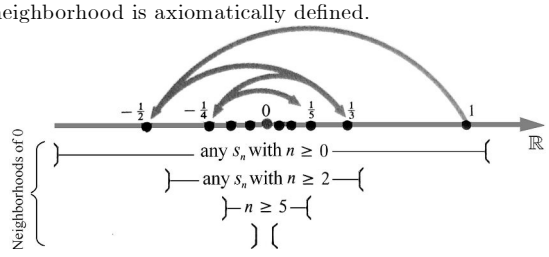


Fig. Convergence of a sequence.
$(s_n) := ((-1)^n \frac{1}{n+1})$=$(1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, ..)$.

11.1. Topological space.

Def. 196. *(Topological space). $(E, \mathfrak{T})$ is a topological space if $\mathfrak{T}$ is a subset of $\mathfrak{P}(E)$ having the properties:*
$(i) : \varnothing \in \mathfrak{T}, E \in \mathfrak{T}$,
$(ii) : O_1, O_2 \in \mathfrak{T} \Rightarrow O_1 \cap O_2 \in \mathfrak{T}$,
$(iii) : \mathfrak{T}' \subseteq \mathfrak{T} \Rightarrow \bigcup_{O \in \mathfrak{T}'} O \in \mathfrak{T}$.
$\mathfrak{T}$ is called topology on E. The elements of $\mathfrak{T}$ are called open sets, and those of E are called points.

Open set: A set included in a topology; equivalently, a set which is a neighborhood of each of its points; a topology on a space is determined by a collection of subsets which are said *open*.

Def. 197. *(Open set). A set consisting only of interior points is called an open set (e.g. a disc without its circumference).*

Neighborhood notion can be defined by open sets:

Def. 198. *(Set of all neighborhoods of x: $\mathfrak{B}(x)$). V is called neighborhood of x if $V \subseteq E$ and if there exists one $O \in \mathfrak{T}$ such that $x \in O \subseteq V$. One denotes by $\mathfrak{B}(x)$, "the set of all neighborhoods of x". Moreover it is known that $\mathfrak{B}(x) \neq \varnothing$, since $E \in \mathfrak{B}(x)$.*

Rem. 30. *A topological space can also be defined by using axioms on the neighborhood; the concept of open set results from this approach. By the notion of neighborhood we can define the convergence of a sequence:*

Def. 199. *(Convergence of a sequence). Let $(a_0, a_1, ...)$ be a sequence in a topological space $(E, \mathfrak{T})$. We say that the sequence converges to $a \in E$ (denoted $\lim_{n\to\infty} a_n = a$) if for any neighborhood $V \in \mathfrak{B}(x)$ there exists one $n_0 \in \mathbb{N}$ such that $n \geqslant n_0 \Rightarrow a_n \in V$.*

In a topological space, the limit is not necessarily unique. However if for any pair of distinct points of E we can find two disjoint open sets contaning them (separated space in the Hausdorff sense), then the limit is unique. Metric spaces are separated spaces.

Metric spaces: Metric spaces are a generalization of the Euclidean spaces. Like Euclidean spaces they admit a "topology" defined by a metric.

11.2. Metric space.

Def. 200. *(Metric space). A set E is a metric space if we define a distance on E, i.e. if there is a map $d : E \times E \to \mathbb{R}_+$ verifying the properties:*
$(i) : d(x, y) = 0 \Leftrightarrow x = y$,
$(ii) : d(x, y) = d(y, x)$,
$(iii) : d(x, y) + d(y, z) \geq d(x, z)$.

Ex. 78. *In the Euclidean plane $\mathbb{R}^2$, we can defined a metric by: $d(X, Y) := XY$; that is, by using the distance between the points X and Y; thus we obtain the properties: (a) $XY = 0 \Leftrightarrow X = Y$. (b) $XY = YX$, i.e. symmetry. (c) $XY + YZ \geq XZ$, called triangular inequality. (In cartesian coordinates, if $X : (x_1, x_2)$ and $Y : (y_1, y_2)$ we have*

$$XY = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}).$$

Ex. 79. *$\mathbb{Q}$ and $\mathbb{R}$ are metric spaces for the distance def. by the absolute value $d(x, y)$:=$|x-y|$.*

Any metric space can be made topological; to this end, we define an *open ball* of center m and radius $\varepsilon > 0$ by: $B(m, \varepsilon) := \{x \mid x \in E \wedge d(x, m) < \varepsilon\}$ (i.e. E is provided with a distance $d(x, m) < \varepsilon$) (Fig.) and it is said that a non-empty subset of E is open if it contains at least an open ball centered at each one of its points.

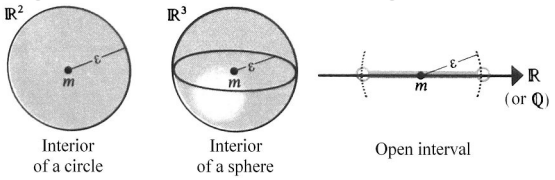


Fig. Open balls of center m and radius ε.

Rem. 31. *(Topological spaces, Balls, Neighborhoods): Open balls have a special property in such a space, indeed they are themselves open sets, and thus we can say that: "Any non-empty open set is a union of open balls". Consequently, rather than the set of neighborhoods of a point, it suffices to consider the set of open-balls centered at this point. Taking into account what was just stated, we can rewrite the definition of the convergence of a sequence in terms of balls.*

Def. 201. *(Convergence of a sequence in terms of balls). Let $(a_0, a_1, ..)$ be a sequence in a topological space $(E, \mathfrak{T})$. It is said that sequence converges to $a \in E$, as soon as for any open ball $B(a, \varepsilon)$ there exists a $n_0 \in \mathbb{N}$ such that $n \geqslant n_0 \Rightarrow a_n \in B(a, \varepsilon)$, i.e. if we have: $\forall \varepsilon (\varepsilon \in \mathbb{R}_+^* \Rightarrow \exists n_0 \forall n (n \geqslant n_0 \Rightarrow d(a_n, a) < \varepsilon))$.*

Furthermore, it would be possible to prove that any *metric space* is *separated*.

11.3. Continuous maps.

Maps compatible with the topological structure must be defined by using open sets; we are led to define a continuous map.

Def. 202. *(Continuous map). Let $(A, \mathfrak{T})$,$(B, \mathfrak{T}')$ be topological spaces and $f : A \to B$ a map, f is said to be continuous on A if $\forall O (O \in \mathfrak{T}' \Rightarrow f^{-1}[O] \in \mathfrak{T})$ (cf. 3^{th} Fig in "Structures, maps, morphisms").*

f is said to "*ontinuous at $a \in A$* (local continuity) if $\forall V\ (V \in \mathfrak{B}(f(a))) \Rightarrow \exists U\ (U \in \mathfrak{B}(a) \wedge f[U] \subseteq V)$.

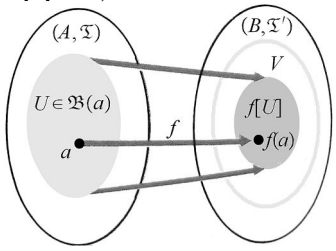


Fig. Continuity at a point. For any $V \in \mathfrak{B}(f(a))$ there exists a $U \in \mathfrak{B}(a)$ such that $f[U] \subseteq V$.

Moreover, we can show that f is continuous on A if and only if it is continuous at every point of A.

Rem. 32. *Two topological spaces are indiscernible from a topological point of view if there is a homeomorphism (i.e. a bicontinuous bijection whose inverse f^{-1} is continuous) between them. Continuous maps are maps compatible with the topological structure.*

The local continuity in continuous maps can be proved in terms of open balls:

Def. 203. *(Local continuity -in terms of open balls). f is continuous at a iff any open ball centered at $f(a)$ contains the image of an open ball centered at a.*

Then,we can provide a definition of the local continuity by using the limit of sequences, which is an usual continuity condition in analysis:

Def. 204. *(Local continuity -in terms of sequences). f is continuous at a iff for any sequence (a_n) converging to a, we have* $\lim_{n\to\infty} f(a_n) = f(\lim_{n\to\infty} a_n) = f(a)$.

11.4. Particular topological structures. Separated space and metric space are two topological structures. The study of derived structures (i.e. subset, product space, quotient space) and particular topological structures, having additional properties (e.g. connectivity, compactness), will be done in Topology.

Chapter 4

Arithmetic

The arithmetic is the science of numbers and more specifically that of *whole numbers*, whether *natural* (0,1,2,...) or *integer* (...,-2,-1,0,1,2,...). It studies thus the sets $\mathbb{N}$ and $\mathbb{Z}$ (see also heading "*Construction of Number System*"). The main tools are the four operations, addition, multiplication, subtraction, division, to which we have to add the order relation $\leqslant$. In this chapter, the objective is not to study $\mathbb{N}$ and $\mathbb{Z}$ for themselves but in connection with many areas of mathematics (or applications) in which they operate.
The present chapter is, of course, closely related to the chapters "*Construction of Number System*" and "*Number Theory*"; there are many correspondences between them but the treatment differs. Note that in the following, the theorems are always given with proofs.
Branch of mathematics known as number theory is sometimes known as *higher arithmetic*; but number theory is also simply called *arithmetic*.

1. Set of Natural Numbers $\mathbb{N}$

This section uses headings concering sets, and the notions of injective (surjective, bijective) maps, and order relation, are supposed to be known. (1) A fully intuitive approach can not suffice. (2) So far, we do not give a rigorous construction of $\mathbb{N}$, contrary to what we will do later for the sets $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$. (3) Consequently, we will admit that there exists a set, that we will denote by $\mathbb{N}$, having three simple properties; these properties will be taken as axioms (or axiomatic rules). Here, the key is to understand how we deduce from these axioms the properties of integers that will be useful. Of course, the axioms are not arbitrary.

1.1. Order relation and natural numbers. Consider an *ordered set* Φ, that is, a set endowed with an order relation, denoted by $\leq$ This binary relation between elements of Φ is thus reflexive, antisymmetric and transitive; we deduce the relations denoted: $<$, $\geq$, and $>$. Let A be a part of Φ and $\alpha \in \Phi$. We know what means "t is an upper bound (or a lower bound) of A" (or equivalently, "t is a majorant (or a minorant) of A"), "t is the smallest element of A", what we denote $t = \min(A)$, "t is the greatest element of A", what we denote $t = \max(A)$. We also know what means "t is bounded from above, bounded from below, or bounded".
From the relation $\leq$ we can speak of intervals. Let a, b be two given elements of Φ. We denoted by $[a, b]$ the set of elements of Φ such that $a \leq x \leq b$ and $]a, b[$ the set of elements of Φ such that $a < x < b$. Analogous definitions can be given for $]a, b]$ and $[a, b[$. The set of elements of Φ such that $x \geq a$ (resp. $x > a$) is denoted here by $[a, \rightarrow [$ (resp. $]a, \rightarrow [$). The definitions of $] \leftarrow, a[$ (resp. $[\leftarrow, a[$) are analogous. These various intervals can potentially be empty.
First, we admit the *existence of a nonempty ordered set* $\mathbb{N}$ verifying three properties:
(N1) Any nonempty part of $\mathbb{N}$ has a smallest element.
(N2) Any nonempty part of $\mathbb{N}$, which is bounded from above, has a greatest element.
(N3) The set $\mathbb{N}$ itself is not bounded from above, in particular it does not have greatest element.
The elements of $\mathbb{N}$ are called *natural numbers*.
In practice, the reader can admit that the natural numbers $\mathbb{N}$ form a set that satisfies the properties (N1), (N2), (N3). (Note that we can wonder if two ordered sets verifying the above conditions lead to equivalent theories; the anwser is positive.)

If $P(n)$ is defined only on an interval $[n_0, n]$, we change (R2) as follows: "If $P(n)$ is true for a certain integer $n \in [n_0, n_1 - 1]$, $P(n+1)$ is also true. Keeping (R1)

1.2. Recurrence (induction). Here, we give important consequences of the properties (N1),(N2),(N3) of the previous heading. We will speak of "*integers*" instead of "*natural numbers*" as long as there is no risk of confusion. A first consequence of (N1) is that $\mathbb{N}$ is totally ordered, that is, two arbitrary elements x, y of $\mathbb{N}$ are always *comparables*: we have either $x \leqslant y$ or $y \leqslant x$ (or both). This is obvious if $x = y$. Otherwise, $\{x, y\}$ is a nonempty part of $\mathbb{N}$, it has a smallest element, either equal to x or to y, and we have $x \leqslant y$ (resp. $y \leqslant x$) in the first (resp. in the second) cas. Then, the set $\mathbb{N}$ itself being nonempty, the property (N1) shows that it has a smallest element, denoted by 0: the integers others than 0 are said to be strictly positive, they form a part of $\mathbb{N}$ denoted by $\mathbb{N}^*$. Now, consider $n \in \mathbb{N}$. The set $A := \{k \in \mathbb{N} | k > n\}$ is not empty, since n is not upper bound (majorant) of $\mathbb{N}$, considering the property (N3). Thus A has a smallest element, denoted $n+1$ and called *successor* of n. The successor of 0 is denoted 1. Likewise, if $n \in \mathbb{N}^*$, $B := \{k \in \mathbb{N} | k < n\}$ is not empty, since $0 \in B$. Of course, n is an upper bound (a majorant) of B; the property (N2) shows then that B has a greatest element, denoted $n-1$ and called *predecessor* of n. Temporarily, the notation $n+1$ is not related to the addition, and $n-1$ is not related to the subtraction. However, we have $(n-1)+1 = n = n+1 = -1$ for any integer $n > 0$ (this can be checked as exercise, as well as the equality $[0, n[= [0, n-1[$). For two naturals m, n, we have the following equivalences (resulting from definitions): $(m > n) \Leftrightarrow (m \geqslant n+1)$, $(m < n) \Leftrightarrow ((n > 0)$ and $(m \leqslant n-1))$.
Here is an important result (recurrence theorem), giving logical foundations to reasoning by recurrence, also known as reasoning by induction; (reasoning by recurrence and reasoning by the absurd are two major tools).

Th. 36. (I). (**Recurrence th.**). *Let n_0 be a integer. For any integer $n \geqslant n_0$, let us denote by $P(n)$ a special property of the integer n. We have the following assumptions:*
(R1) *The property $P(n_0)$ is true.*
(R2) *If the property $P(n)$ is true for a certain integer $n \geqslant n_0$, the property $P(n+1)$ is also true.*
Under these assumptions, the property $P(n)$ is true for any integer $n \geqslant n_0$.

Proof. Reasoning by the absurd: suppose that there exists at least a integer $m \geqslant n_0$ such that $P(m)$ is false. The set A of integers $k \geqslant n_0$ such that $P(k)$ is false being then nonempty, it has a smallest element n. According to the assumption (R1) $n \neq n_0$, then $n \geqslant n_0$ and then $n - 1 \geqslant n_0$ (definition of $n-1$). Thus $n_0 \leqslant n-1 < n$, thus $n - 1 \neq A$ (since $n = \min(A)$), i.e. $P(n-1)$ is true. Since n is the successor of $n-1$, (R2) makes that $P(n)$ is true , this is absurd since $n \in A$. Thus there no longer exists integer $m \geqslant n_0$ such that $P(m)$ is false. This completes the proof.. □

In this proof, (R1) and (R2) can be replaced by the assumption (R3) given below, without changing the conclusion of the theorem (check it); this is what we call the "*strong recurrence*" (or "*strong induction*"). It is sometimes easier to check (R3) rather than (R1) and (R2).
(R3) "*If an integer $n \geqslant n_0$ is such that $P(k)$ is true for all the integers k verifying $n_0 \leqslant k < n$, the property $P(n)$ is true.*"
If $P(n)$ is defined only on the interval $[n_0, n_1]$, we change (R2) as follows: If $P(n)$ is true for a certain integer $n \in [n_0, n_1 - 1]$, $P(n+1)$ is also true. Keeping (R1) we get the following conclusion: $P(n)$ is true for all $n \in [n_0, n_1]$ (finite recurrence). A useful consequence of the recurrence theorem (I). Let A be a part of $\mathbb{N}$ including 0. Suppose that the successor of any element of A also belongs to A. Then $A = \mathbb{N}$. (for $P(n)$, take the relation $n \in A$) .
. Another side of the recurrence (induction) is a type of construction that uses the recurrence (induction), i.e. construction by induction (construction by recurrence). Let E be a set, g a map from E to E and a a given element of E. There exists a unique sequence (u_n) of elements of E such that $u_0 = a$ and $u_{n+1} = g(u_n)$ for any integer n. We say that we have constructed this sequence starting from its first term $u_0 := a$ and from the "*recurrence relation*" $u_{n+1} := g(u_n)$.

Ex. 80. *For example the sequence (2^n) of powers of 2 is defined by its first term 1 and the recurrence relation $2^{n+1} := 2 \times 2^n$. Likewise, the sequence $(n!)$ of factorials is defined by its first term $0! := 1$ and the recurrence relation $(n+1)! := (n+1)n!$.*

Recall that a sequence of elements of E is simply a map from $\mathbb{N}$ to E.

The justification of this type of construction (by induction) results from the following theorem:

Th. 37. (II). *Let E be a set, and g a map from E to E, and a a given element of E. There exists a unique map f from $\mathbb{N}$ to E such that $f(0) = a$ and $f(n+1) = g(f(n))$ for any integer n.*

PROOF. If f exists, its restriction f_n to $[0, n]$ is such that: $f_n(0) = a$ and $f_n(m+1) = g(f_n(n))$ for any $m < n$. Conversely, let us show by induction (recurrence) that a map such that f_n exists and is unique. This is true for $n = 0$. If it's true for n, it is necessary that f_n is the restriction of f_{n+1} to $[0, n]$ and that $f_{n+1}(n+1) = g(f_{n+1}(n)) = g(f_n(n))$. Conversely, these two relations imply that f_{n+1} is appropriate. It follows, if f exists it is unique, since defined for any n by $f(n) := f_n(n)$. This map is appropriate since $f(0)=f_n(0)=a$ and for any n we have $f(n+1)=f_{n+1}(n+1)=g(f_n(n))=g(f(n))$. □

Ex. 81. (1) *Let X be a set, $b \in X$ and b a map from $\mathbb{N} \times X$ to X. We can define a sequence (u_n) by its first term $u_0 := b$ and the recurrence relation $u_{n+1} = h(n, u_n)$. As an exercise we check that it suffices to apply the above theorem* (II) *by replacing E by the set $\mathbb{N} \times X$, and replacing g by the map $(n, x) \mapsto (n+1, h(n, x))$ from E to E, and replacing a by the pair $(0, b)$. The map f is then of the form $n \mapsto (n, u_n)$, and the sequence answers the question. Take for example $X := \mathbb{N}$, $b := 1$, and define $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by the formula $h(k, x) := (k+1)x$. The sequence (u_n) is then the sequence $(n!)$ of factorials, whose definition is thus justified. We have used here the multiplication of integers, whose definition is given in the next heading, the reader will observe that there is not vicious circle.* (2) *Let X be a set, and $f : X \to X$ be a map. We define the sequence (f_n) of iterations of f by its first term, which is the identity map Id_X of X, and the recurrence relation $f_{n+1} := f \circ f_n$. If this does not cause confusion, f_n will be denoted by f^n (thus $f^0 = Id_X$, $f^1 = f$, $f^2 = f \circ f$,...). Because of the associativity of the composition of maps, we have $f^3 = f \circ f^2 = f \circ (f \circ f) = (f \circ f) \circ f = f^2 \circ f$.*

The following theorem will be used in the next heading.

Th. 38. (III). *Let X and Y be two sets and $u : X \to Y$, $v : Y \to Y$, be two maps. There exists a unique map F from $\mathbb{N} \times X$ to Y verifying the following conditions:*
(1) *For any element $x \in X$, $F(x, 0) = u(x)$.*
(2) *For any $x \in X$, and any integer n, $F(x, n+1) = v(F(x, n))$.*

PROOF. Define $F : \mathbb{N} \times X \to Y$, thus: $F(x,n) := (v^n \circ u)(x)$ for all $x \in X$, $n \in \mathbb{N}$. Then F verifies the condition (1) since $v^0 \circ u = u$. If $n \in \mathbb{N}$ and $x \in X$, we have $v^{n+1} \circ u = (v \circ v^n) \circ u = v \circ (v^n \circ u)$ (associativity of the composition of maps), and we infer that F verifies the condition (2): $F(x,n+1) = (v \circ (v^n \circ u))(x) = v((v^n \circ u)(x)) = v(F(x,n))$. Let $F' : \mathbb{N} \times X \to Y$ be another map, veifying the conditions (1) and (2). Denote $P(n)$ the following property of an integer n: For any $x \in X$, $F(x,n) = F'(x,n)$. Given the condition (1) (for F and F'), $P(0)$ is true. Then, $P(n) \Rightarrow P(n+1)$ for any n (by the condition (2)). According to recurrence theorem, $P(n)$ is true for any integer n, that is, $F = F'$. □

Th. 39. (IV). *There is not strictly decreasing map from $\mathbb{N}$ to $\mathbb{N}$.*

PROOF. Reasoning by the absurd: suppose that such a map f exists. Let $m := \min(f(\mathbb{N}))$; there is $k \in \mathbb{N}$ such that $m = f(k)$. Then $f(k+1) < f(k) = m$, since f strictly decreases. But $f(k+1) \in f(\mathbb{N})$, so $m \leqslant f(k+1)$, by definition of m. Which is a contradiction. □

An application of this theorem is as follows: let $P(n)$ be a certain property depending on an integer n. Now, suppose that we know how to construct, from any integer n such that $P(n)$ is true, an integer $n' < n$ such that $P(n')$ is true. Then *for any integer k, $P(k)$ is false.* This is called the "*Fermat's principle of infinite descent*", or "*Fermat's method of infinite descent*", or simply "*Fermat infinite descent*"

1.3. Addition and multiplication in $\mathbb{N}$. Previous results allow to introduce a definition of two elementary operations in $\mathbb{N}$, and to show their main properties. Here, we just state the results and sketch the proofs. The following theorem is also taken as definition:

Th. 40. (V). *There is a unique map "+" from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ such that:*
(1) *For every integer n, $n+0=n$, and $n+1$ is the successor of n.*
(2) *For every integers m,n, we have $m+(n+1)=(m+n)+1$.*
The map $+$ is called the addition and, if a,b are two integers, $a+b$ is called sum of a and b.

PROOF. If s is the map from $\mathbb{N}$ to $\mathbb{N}$ associating with any integer its successor. Apply theorem (III) (previous heading), set: $X := \mathbb{N}$, $Y := \mathbb{N}$, u equal to the identity map of $\mathbb{N}$ and $v := s$. There is a unique map F from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ such that, for all integers a, b, we have $F(a, 0) = a$ and $F(a, s(b)) = s(F(a, b))$, hence $F(a, 1) = s(a)$. Then to conclude it suffices to define $+$ by the formula $m+n = F(m, n)$ (the reader will check it). □

Some standard properties of addition:
(i) For any integer a, $a + 0 = a = 0 + a$.
(ii) (Associativity): for all the integers a, b, c we have $(a + b) + c = a + (b + c)$.
(iii) (Commutativity): for all the integers a, b we have $a + b = b + a$.
(iv) (Compatibility with the order): for all the integers a, a', b, b' the inequalities $a \leqslant a'$ and $b \leqslant b'$ imply $(a + b) \leqslant (a' + b')$.
(v) for all the integers a, b, c, $(a \leqslant b) \Leftrightarrow (a + c \leqslant b + c)$.
(vi) (Regularity): for all the integers a, b, c, $a + c = b + c$ implies $a = b$.
(vii) for all the integers a, b, the equality $a + b = 0$ implies $a = b = 0$.
The property (i) is immediate, by induction on a (by recurrence). Fot the associativity, denote $P(c)$ the following property of an integer c: for *all* $a, b \in \mathbb{N}$, $(a + b) + c = a + (b + c)$. The property $P(0)$ is true, considering the condition (1) of theorem (V). If $P(c)$ is true for a certain c and if $a, b \in \mathbb{N}$, we see that $P(c+1)$ is true, using several times the condition (2) of theorem (V): $(a+b)+(c+1) = ((a+b)+c)+1 = (a+(b+c))+1 = a+((b+c)+1) = a+(b+(c+1))$. Proofs of the other properties is left to the reader.

Ex. 82. ($\diamond$). *Exercise: Let X be a set and $f : X \to X$ be map. Show that $f^m \circ f^n = f^{m+n}$ for all integers m,n. Solution: Denote $P(m)$ the following property of an integer m: $\forall n \in \mathbb{N}$ we have $f^m \circ f^n = f^{m+n}$. The property $P(0)$ is true:$\forall n \in \mathbb{N}$ we have $f^0 \circ f^n = Id_X \circ f^n = f^{0+n}$. Let m be an integer such that $P(m)$ is true. $\forall n \in \mathbb{N}$ the associativity of the composition of maps gives: $f^{m+1} \circ f^n = (f \circ f^m) \circ f^n = f \circ (f^m \circ f^n) = f \circ f^{m+n} = f^{(m+n)+1}$. But $(m+n)+1 = (m+1)+n$, and so $P(m+1)$ is true. The composition of two injective (resp. surjective) maps is injective (resp. surjective). Thus if f is injective (resp. surjective), we infer by induction on n (by recurrence) that each f^n (resp. surjective) is also injective (resp. surjective).*

Here is a theorem (also taken as definition):

Th. 41. *Let a, b be two integers. To get $a \leqslant b$, it is necessary and sufficient that there exists an integer c such that $b = a + c$. Such an integer c is then unique, we denote it by $b-a$, and we call it difference of b and a. In other words, the map $x \mapsto a + x$ is a bijection from $\mathbb{N}$ to $[a, \to [$.*

Here, only the surjectivity of the map t_a (i.e. translation of the vector a) considered needs proof, immediate by induction on a.

Th. 42. *There exists a unique map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, denoted by $\times$, verifying the following properties:*
(1) *For any integer m, we have $m \times 0 = 0$.*
(2) *For all integers m, n, we have: $m \times (n+1) = (m \times n) + m$.*
The map $\times$ is called multiplication and, if $a, b \in \mathbb{N}$, $a \times b$ is called product of a and b, and just written ab if this does not cause confusion (e.g. $2 \times x$ can be written $2x$ but 2×3 cannot be written 23!).

PROOF. For all integers m, n, set $m \times n := t_m^n(0)$, where t_m^n is the nth iteration of the translation of vector m. The property (1) is obvious. For (2), let $m, n \in \mathbb{N}$. The commutativity of the addition gives: $m \times (n+1) = t_m^{n+1}(0) = (t_m \circ t_m^n)(0) = t_m(m \times n) = m + (m \times n) = (m \times n) + m$, proving the "existence" (of the statement). The "uniqueness" is left to the reader. (Note that the multiplication thus appears as a succession of additions ($x \times 3 = x + (x + x)$, ..) □

Some standard properties of multiplication:
(i) For any integer a, $1 \times a = a = a \times 1$.
(ii) (Associativity): for all the integers a, b, c we have $(ab)c = a(bc)$.
(iii) (Commutativity): for all the integers a, b we have $ab = ba$.
(iv) (Distributivity of the multiplication with respect to the addition): for all the integers a, b, c, we have $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$.
(v) (Compatibility with the order): for all the integers a, a', b, b' the inequalities $a \leqslant a'$ and $b \leqslant b'$ imply $ab \leqslant a'b'$. In particular, the product of two strictly positive integers is strictly positive.
(vi) For all the integers a, b, c, where c is nonzero, the inequalities $a \leqslant b$ and $ac \leqslant bc$ are equivalent.
(vii) (Regularity): for all the integers a, b, c, where c is nonzero, $ac = bc$ implies $a = b$.
(viii) For all the integers a, b, the equality $ab = 0$ is equivalent to ($a = 0$ and $b = 0$), and the equality $ab = 1$ is equivalent to $a = b = 1$.

Prop.1 (**Archimedean property**). *Let a, b be two integers, and suppose $a > 0$. There exists an integer n such that $na > b$.*

PROOF. According to property (N3) of $\mathbb{N}$, b is not an upper bound (majorant) of $\mathbb{N}$. Thus, there exists an integer n such that $n > b$. But $a > 0$, so $a \geqslant 1$ (def. of 1), hence $na \geqslant n \times 1 = n > b$, and so $na > b$. □

From the multiplication, we define the sequence (a^n) of powers of a fixed integer a, by $a^0 := 1$ and the recurrence relation $a^{n+1} := a^n \times a$. Beyond obvious equalities $0^n{=}0$ for any integer $n > 0$ (but $0^0{=}1$) and $1^n{=}1$ for any integer n, the classical formulas to remember are:

Prop.2 *For any integers a, b, m, n, we have $a^m \times a^n = a^{m+n}$, $(a^m)^n = a^{mn}$, $(ab)^n = a^n \times b^n$.*

PROOF. Let a be an integer, and denote by ϑ_a the map $x \mapsto ax$ from $\mathbb{N}$ to $\mathbb{N}$. For any integer n, we have $a^n = \vartheta_a^n(1)$, hence (cf. Ex.($\diamond$) above) the first formula. It follows the second, with the definition of the multiplication starting from the addition. The last formula is shown simply by induction on n (by recurrence), using the commutativity of the multiplication. □

Lem. 6. *Given two integers m, t such that $m > 1$ and $1 \leqslant t \leqslant m$. Then there exists a bijection u of from set $T = [1, m]\backslash\{t\}$ (complement of the singleton $\{t\}$ in $[1, m]$) to $[1, m-1]$.*

PROOF. The map s from $[1, m]$ to $[1, m]$ defined by $s(t) := m$, $s(m) := t$ and $s(k) := k$ if $k \notin \{m, t\}$ is a bijection from $[1, m]$ to $[1, m]$ (for example the identity if $t = m$). The map u from T to $[1, m-1]$ defined by $u(k) := s(k)$ is appropriate. □

Prop.3 *Let n,p be two strictly positive integers.*
(1) *There exists an injection from $[1, n]$ to $[1, p]$ if and only if $n \leqslant p$.*
(2) *There exists a surjection from $[1, n]$ to $[1, p]$ if and only if $n \geqslant p$.*

PROOF. The map f from $[1,n]$ to $[1,p]$ defined by $f(k){:=}\min(k,p)$ is injective if $n{\leqslant}p$ and surjective if $n{\geqslant}p$, hence the sufficient condition in (1),(2). Consider now the necessary condition. We prove by induction on $n{\geqslant}1$ the property $P(n)$ according to which the existence of an injection from $[1,n]$ to $[1,m]$ implies $n{\leqslant}m$. Property $P(1)$ is evident. Suppose $P(n)$ true for an integer $n \leqslant 1$, and let us show $P(n{+}1)$. Given f an injection from $[1,n{+}1]$ to $[1,m]$ and $t{=}f(n{+}1)$; the restriction g of f to $[1,n]$ is an injection from $[1,n]$ to $[1,m]\backslash\{t\}{\neq}\varnothing$. Then $u \circ g$ is an injection $[1, n]$ to $[1, m{-}1]$, hence $n{\leqslant}m{-}1$ and $n{+}1{\leqslant}m$ (u is such as in previous lemma). Proof of the other necessary condition is analogous. Given f a surjection from $[1,n{+}1]$ to $[1,m]$; the equalities $[1,m]{=}f([1,n{+}1]){=}f([1,n])\cup\{f(n{+}1)\}$ make that either $f([1,n]){=}[1,m]$, then $n{+}1{>}n{\geqslant}m$ by the hypothesis of recurrence (induction hypothesis) or there is a t such that $f([1,n]){=}[1,m]\backslash\{t\}$. Then $u \circ g$ is a surjection from $[1,n]$ to $[1,m{-}1]$, hence $n{\geqslant}m{-}1$ and $n{+}1{\geqslant}m$. □

Prop.3 will be useful in the next section.

2. Denumerability (Counting)

2.1. Finite sets, denumerable sets. Finite sets and denumerable sets (consideed here) have already been approached before. Here the point of view adopted is slightly different, it specifies the intuitive definition: "*A finite set is a set that has a finite number of elements.*"

Def. 205. *(Finite and infinite sets). A set E is said to be finite if it is empty or it is in bijection with $[1, n]$, for a certain integer $n \geqslant 1$. If it is not finite, E is said to be infinite.*

Th. 43. *Let E be a finite set. If E is nonempty there exists a unique integer $n \geqslant 1$ such that E is in bijection with $[1, n]$. This integer n is called **cardinal** of E, denoted by $\mathrm{card}(E)$, and we say that E is a set of n elements. If E is empty we write $\mathrm{card}(E) = 0$.*

PROOF. Let $n, p \geqslant 1$ be two integers, g be a bijection from E to $[1, n]$, and h a bijection from E to $[1, p]$. We have to prove that $n = p$. However $v := h \circ g^{-1}$ is a bijection from $[1, n]$ to $[1, p]$. Thus $n \leqslant p$ since v is injective (statement (1) of **prop.3** of previous heading "*Addition and multiplication in $\mathbb{N}$*") but also $n \geqslant p$ since v is surjective (statement (2) of **prop.3** of previous heading). Hence $n = p$. □

The previous **prop.3** can now be written as follows:

Th. 44. (†). *Let E and F be two finite sets, of respective cardinals n and p.*
(1) *There exists an injection from E to F iff $n \leqslant p$.*
(2) *There exists a surjection from E to F iff $n \geqslant p$.*
(3) *There exists a bijection from E to F if $n = p$.*

PROOF. It is immediate from **prop.3**. There exists a bijection u from $[1, n]$ to E and a bijection v from F to $[1, p]$. Given $f : E \to F$ and $\Psi : [1, n] \to [1, p]$ two maps. The equalities $\Psi = v \circ f \circ u$ and $f = v^{-1} \circ \Psi \circ u^{-1}$ are equivalent. If they are verified, f will be injective (resp. surjective) iff Ψ is it also, hence the result. □

Here is a consequence of previous results. Given n, p two integers such that $n > p$. No map from a finite set of n elements to a finite set of p elements is injective. Indeed, the existence of an injection from a set of n elements to a set of p elements would contredict the statement (1) of the previous theorem. The above result is called *Dirichlet box principle (or also Dirichlet Pigeonhole principle)* due to the following interpretation. If we distribute n objects in p boxes, and if $n > p$, one of boxes would contain at least two objects. Indeed, given E the set of objects, F the set of boxes and $f : E \to F$ the map associating with any object x the box $f(x)$ in which x is placed. The conclusion translates the non-injectivity of f.

Th. 45. (‡). *Let E be a finite set and A a part of E. The set A is finite, $\mathrm{card}(A) \leqslant \mathrm{card}(E)$, and this inequality is an equality only if $A = E$.*

PROOF. Proceed by induction on $n{=}\mathrm{card}(E)$ since the case $n{=}0$ is evident. Suppose E of cardinal $n \geqslant 1$, the conclusion being true for any finite set of cardinal strictly less than n. Given A a part of E. If $A{=}E$, there is nothing to prove. Otherwise, given $x \in E\backslash A$. There exists a $q \in [1, n]$ and a bijection from $E\backslash\{x\}$ to $[1, n]\backslash\{q\}$. Since $[1, n]\backslash\{q\}$ is of cardinal $n{-}1$, $E\backslash\{x\}$ is it also. However $A \subset E\backslash\{x\}$. According to hypothesis of recurrence (induction hypothesis), A is thus finite, of cardinal at least $n{-}1$, hence the result. □

Th. 46. (▷). *Let E, F be two sets of same finite cardinal n. A map $f : E \to F$ is bijective if and only if it is injective (resp. surjective).*

PROOF. Via bijections from $[1, n]$ to E and F, we reduce the case to the case where $E = F = [1, n]$. If f is bijective, it is injective and surjective. If f is injective, the map $x \mapsto f(x)$ is a bijection from $[1, n]$ to $f([1, n])$. Thus $f([1, n])$ is a part of $[1, n]$ of n elements, so $f([1, n]) = [1, n]$ given the previous theorem: f is surjective, therefore bijective. Suppose f surjective. If $k \in [1, n]$, denote by $g(k)$ the smallest antecedent of antecdents of k by f. Thus we define a map g from $[1, n]$ to itself, and $f \circ g$ is, by construction, the identity map of $[1, n]$. It follows that g is injective, since the identity map is it also. Considering the above, g is bijective, thus f is also bijective (inverse of g). □

The problem of enumeration (counting) consists in computing the cardinal (or number of elements) of a finite set E, which can be defined by various processes. The first method, called *bijective method*, is to establish a bijection between E and a finite set F of which we know already the cardinal; if we succeed, we will have $\mathrm{card}(E){=}\mathrm{card}(F)$, according to previous theorem (†). As example: if $a, b \in \mathbb{N}$ and if $a \leqslant b$, the cardinal of $[a, b]$ is $b{-}a{+}1$ (do not forget the 1), since $x \mapsto x{+}a{-}1$ is a bijection from $[1, b{-}a{+}1]$ to $[a, b]$ (as the reader can verify). Here are two fundamental theorems:

Th. 47. (∗). *Let F be a set, $n \geqslant 1$ an integer and $A_1, ..., A_n$ of finite parts of E pairwise disjoint. The union of these parts is finite, and: $\mathrm{card}(A_1 \cup A_2 \cup \cdots \cup A_n) = \mathrm{card}(A_1) + \mathrm{card}(A_2) + \cdots + \mathrm{card}(A_n)$.*

PROOF. By induction on n (by recurrence) we are easily reduced to the case $n{=}2$. Let us set $m_i := \mathrm{card}(A_i)$, $i{=}1, 2$. Let f_i be a bijection from A_1 to $[1, m_1]$. Since $J := [m_1 + 1, m_1 + m_2]$ is the cardinal m_2, there exists a bijection f_2 from A_2 to J. Define a map $f : A_1 \cup A_2 \to [1, m_1 + m_2]$ as follows: if $x \in A_1 \cup A_2$, we write $f(x) := f_1(x)$ if $x \in A_1$ and $f(x) := f_2(x)$ if $x \in A_2$; this definition is lawful since $A_1 \cap A_2$ is empty. Clearly f is a bijection from $A_1 \cup A_2$ to $[1, m_1 + m_2]$, hence the result. □

Def. 206. *(Fiber). Let E, F be two sets and $f : E \to F$ a map. If $y \in F$, given $f^{-1}(\{y\})$ the preimage of $\{y\}$ by f, i.e. the set of antecedents of y by f; such a set is called a **fiber** of f.*

When this does not cause confusion, $f^{-1}(\{y\})$ will be simply denoted $f^{-1}(y)$. Thus, a variant is given:

Def. 207. *(Fiber)'. A fiber of a map $f : E \to F$ is the preimage of an element $y \in F$; that is, $f^{-1}(y) = \{x \in E : f(x) = y\}$.*

(*Preimage:* Given $f : E \to F$, the image of x is $f(x)$. The preimage of y is then $f^{-1}(y) = \{x | f(x) = y\}$, or all x whose image is y. Preimages are subsets (possibly empty) of the domain.)

Ex. 83. *Let E, F be two finite sets and $f : E \to F$ is a map. When $y \in F$, the fibers $f^{-1}(y)$ form a partition of E: if $x \in E$, the only element y of F such that $x \in f^{-1}(y)$ is $f(x)$. Hence*
$(*)$ $\quad \mathrm{card}(E) = \sum_{y\in F} \mathrm{card}(f^{-1}(y))$.
Given now A, B two finite sets and U a part of $A\times B$. We can compute the cardinal of U in two ways, by the Fubini's formula: $\mathrm{card}(U) = \sum_{a\in A} \mathrm{card}(\{b \in B|(a, b) \in U\}) = \sum_{b\in B} \mathrm{card}(\{a \in A|(a, b) \in U\})$. *Given indeed $p : U \to A$ the map defined by $(x, y) \mapsto x$ (does not forget that U is a part of $A \times B$). If $a \in A$, the fiber $p^{-1}(a)$ is the intersection $U \cap (\{a\} \times B)$, in bijection with the set of the $b \in B$ such that $(a, b) \in U$. The first equality result thus from the previous equality $(*)$, applied to p. The second equality is analogous (exchange the roles of A and B).*

Th. 48. *The union of two finite parts A, B of a set E is finite, and:* $\mathrm{card}(A \cup B) + \mathrm{card}(A \cap B) = \mathrm{card}(A) + \mathrm{card}(B)$.

Proof. Let us set $A' := A\backslash B$ and $B' := B\backslash A$. These are finite parts of E (see theorem (‡)). Since A is disjoint union of $A \cap B$ and A', the above theorem shows that $\mathrm{card}(A) = \mathrm{card}(A \cap B) + \mathrm{card}(A')$. Likewise $\mathrm{card}(A \cup B) = \mathrm{card}(B) + \mathrm{card}(A')$, since $A \cup B$ is disjoint union of B and of A'. The announced equality follows: $\mathrm{card}(A \cup B) + \mathrm{card}(A \cap B) + \mathrm{card}(A') = \mathrm{card}(A) + \mathrm{card}(B) + \mathrm{card}(A')$. □

(Note that the two last theorem are used especially in what we call the "*inclusion-exclusion principle*", or also "sieve formula".)

Th. 49. (♦). *Given $n \geqslant 1$ an integer and $E_1, ..., E_n$ finite sets. The product set $E_1 \times E_2 \times ... \times E_n$ is finite, and we have:* $\mathrm{card}(E_1 \times E_2 \times ... \times E_n) = \mathrm{card}(E_1) \times \mathrm{card}(E_2) \times ... \times \mathrm{card}(E_n)$.

Proof. It suffices to study n=2, observing for example that if E, F, G are three sets, $(x, y, z) \mapsto ((x, y), z)$ is a bijection from $E\times F\times G$ to $(E \times F) \times G$. Let us write E, F instead of E_1, E_2, and let us set $m := \mathrm{card}(E)$, $p := \mathrm{card}(F)$. If $x \in E$, $A_x := \{x\} \times F$ is a part of p elements of $E \times F$, since $y \mapsto (x, y)$ is a bijection from F to A_x. When $x \in E$, the A_x form a partition of $E \times F$: these parts are pairwise disjoint and their union is $E \times F$. According to previous theorem $(*)$, the cardinal of $E \times F$ is thus $\underbrace{p + p + \cdots + p}_{n \text{ terms}}$, i.e., *mp*. (Multiplication appears here as a succession of additions.) □

Let us introduce some results on infinite sets. The *existence* of infinite sets is not evident; in fact, in certain theoretical presentations, this existence is taken as axiom. Here the existence will result from properties of $\mathbb{N}$, already admitted and established.

Th. 50. *For a set E, these conditions are equivalent:*
(i) There exists an injection from $\mathbb{N}$ to $\mathbb{N}$.
(ii) There exists a bijection from E to a part of E distinct of E.
(iii) The set E is infinite.
In particular, the set $\mathbb{N}$ is infinite.

Proof. For the implication $(i) \Rightarrow (ii)$, given $f : \mathbb{N} \to E$ an injection and $a = f(0)$. Define a map $g : E \to E\backslash\{a\}$ thus: if $x \in E\backslash f(\mathbb{N})$, let us set $g(x) := x$; if x belongs to $f(\mathbb{N})$, there exists a unique integer n such that $x = f(n)$ (injectivity of f), let us set $g(x) := f(n + 1)$. We check easily that g is a bijection from E to $E\backslash\{a\}$. The implication $(ii) \Rightarrow (iii)$ results trivially (by contraposition) from the theorem (‡). Since $n \mapsto n+1$ is a bijection from $\mathbb{N}$ to $\mathbb{N}^*$, a consequence of this implication is that $\mathbb{N}$ is infinite. For the implication $(iii) \Rightarrow (i)$, we will only outline the proof. Thus, suppose E infinite, and given $a \in E$ (E nonempty). Define a sequence (u_n) of elements of E by its first term $u_0 := a$ and the following "recurrent process": if $n \in \mathbb{N}$ and if $u_0, ..., u_n$ have already been defined and are pairwise distinct, the part $\{u_0, ..., u_n\}$ of E is finite, therefore is not equal to E. We select therefore an element u_{n+1} of E not belonging to this part. The sequence (u_n) being thus constructed, the map $n \mapsto u_n$ from $\mathbb{N}$ to E is obviously injective. This construction can be *justified* by certain axioms of set theory. □

A set E is finite if and only if there does not exist bijection from E to a part of E *distinct* from E; *This property no longer refers to* $\mathbb{N}$. The infinite sets can be more or less large. Like in the finite case, we say that two arbitrary sets have **same cardinal**, or are **equipotent**, *if there exists a* **bijection** from one to the other. Thus, $\mathbb{N}^*$ has the same cardinal as $\mathbb{N}$, it is as large as $\mathbb{N}$; this points out the limits of the "natural" intuition concerning the notion of infinity. Here is another definition of a denumerable set (see other def. in heading "*Denumerability, non denumerability*"):

Def. 208. *(Denumerable set)'. A set is said to be denumerable if it is in bijection with* $\mathbb{N}$.

If E is a denumerable set, *choose a bijection* from $\mathbb{N}$ to E comes down to *number* all the elements of E, exhaustively and wihout repetition. Let us mention three important results concerning the denumerable sets.

Th. 51. (◊). *Any part of a denumerable set is finite or denumerable.*

Proof. It suffices to see that any infinite part A of $\mathbb{N}$ is denumerable. First, A is not bounded from above: otherwise we would have $A \subset [0, \max(A)]$, thus A would be finite. Given $a := \min(A)$. We define a sequence (u_n) of integers by $u_0 := a$ and the recurrence relation $u_{n+1} := \min(A\cap]u_n, \to [)$. The reader will check that $n \mapsto u_n$ is a bijection from $\mathbb{N}$ to A. □

A set E is *finite or denumerable* if and only if there exists an injection from E to $\mathbb{N}$.

Th. 52. (1) *If E, F are two denumerable sets, $E\times F$ is denumerable.*
(2) *More generally, given denumerable sets E_1,...,E_p ($p \geqslant 1$), their product $E_1 \times E_2 \times \cdots \times E_p$ is denumerable.*

Proof. (2) results from (1), (induction on p). For (1), it suffices to show that $\mathbb{N} \times \mathbb{N}$ is denumerable. Let us outline *two methods* to achieve this: (A) It consists in enumerating the elements of $\mathbb{N} \times \mathbb{N}$: (0,0), (0,1) ,(1,0), (0,2), (1,1), (2,0), (0,3), (1,2), (2,1), (3,0),.. Thus we successively write for n=0,1,2,.. all the pairs $(a, b) \in \mathbb{N} \times \mathbb{N}$ such that $a + b = n$, ranked by order of increasing a. The reader will be able to explicit the corresponding bijection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$ and the inverse bijection, then, give the graphical interpretation via the grid of the plane. (A) Second method: Any strictly positive integer can be written in a unique way as product of a power of 2 and of an odd integer; the map $(n, p) \mapsto 2^n(2p + 1) - 1$ is thus a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. □

Th. 53. *Let E be a set, I a finite or denumerable set and $(A_i)_{i\in I}$ a family of finite or denumerable parts of E. The union of the A_i is finite or denumerable.*

Proof. Sketch of the proof. Let A be the union of the A_i. First, by an injection from I to $\mathbb{N}$, and (possibly by adding empty A_i) the case is reduced to the case $I = \mathbb{N}$. For each $i \in \mathbb{N}$ there exists an injection f_i from A_i to $\mathbb{N}$. Define thus a map $f : A \to \mathbb{N} \times \mathbb{N}$. Given $x \in A$ and i the smallest integer such that $x \in A_i$. Let us set: $f(x) := (i, f_i(x))$. We show easily that f is injective, therefore in bijection with its image $f(A)$. This last one is a part of $\mathbb{N} \times \mathbb{N}$, which is denumerable, so $f(A)$ is finite or denumerable, according to theorem (◊). □

Th. 54. *Let f be a map from a set E to the set F.*
(1) *Assume f injective. If F is finite, E is it also. If F is denumerable, E is finite or denumerable.*
(2) *Assume f surjective. If E is finite, F is it also. If E is denumerable, F is finite or denumerable.*

Proof. For (1), since E is in bijection with $f(E)$, the conclusion results from theorem (‡) and theorem (◊). For (2) we can refer to the fact that there exists an injection from F to E, and apply the statement (1). □

We will see later (and again) that the sets $\mathbb{Z}$ and $\mathbb{Q}$ are denumerable, but that the set $\mathbb{R}$ is not denumerable.

2.2. Combinatorial analysis.

Combinatorial analysis (or combinatorics) studies finite or countable discrete structures, enumeration (meaning counting in combinatorics), combination and permutation of sets of elements; and also helps to solve certain enumeration problems of finite sets, whether in geometry, number theory, graph theory or in probability.
The objective of this heading is to solve classical problems of counting, which point out the effectiveness of statements of the previous heading. We use here rational, real, and complex numbers, although the rigorous construction of the sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ has not yet been given. Recall that the sequence of factorials $(n!)$ is defined by its first term 0!=1 and the recurrence relation $(n + 1)! := n! \times (n + 1)$. Thus, 0!=1, 1!=1, 2!=2, 3!=6, 4!=24, 5!=120, 6!=720. The sequence $(n!)$ increases very quiclky (its increasing is "ultra-exponential").

Th. 55. (¥). *Let E and F be two finite sets of cardinals $n, p \geqslant 1$. The set $\mathcal{F}(E, F)$ of maps from E to F is of cardinal p^n.*

PROOF. We number the elements of E : $x_1, ..., x_n$, this comes down to choose a bijection $i \mapsto x_i$ from $[1,n]$ to E. We then define a map $\Psi : f \mapsto (f(x_1), ..., f(x_n))$ from $\mathcal{F}(E,F)$ to $\underbrace{F \times F \times \cdots \times F}_{n \text{ factors}} = F^n$. Consider $v = (y_1, ..., y_n) \in F^n$. The only antecedent of v by Ψ is the map $f : E \to F$ defined by $f(x_i) := y_i$, $i = 1, .., n$. Thus Ψ is bijective. According to theorem (♦) of the previous heading "*Finite sets, denumerable sets*", F^n is of cardinal p^n, this completes the proof. □

Now, introduce the notion (important in probability theory) of characteristic function of a part of a set.

Def. 209. *(Characteristic function). Let E be a set, and A be a part of E. We call characteristic function of A the map χ_A from E to $\{0,1\}$ taking the value 1 on A and the value 0 on $E\backslash A$, complement of A in E.*

Prop.4 *Let E be a set. The map $A \mapsto \chi_A$ is a bijection from the set $\mathfrak{P}(E)$ of the parts of E to $\mathcal{F}(E,\{0,1\})$.*

PROOF. With every function $f \in \mathcal{F}(E,\{0,1\})$ associate the part $f^{-1}(\{1\})$ of E. Clearly, the map $A \mapsto \chi_A$ from $\mathfrak{P}(E)$ to $\mathcal{F}(E,\{0,1\})$ and $f \mapsto f^{-1}(\{1\})$ from $\mathcal{F}(E,\{0,1\})$ to $\mathfrak{P}(E)$ are two inverse bijections (see compositions in both directions). □

Th. 56. (♣). *Let E be a finite set of n elements. The set $\mathfrak{P}(E)$ of the part of E is finite, of cardinal 2^n.*

PROOF. Given Prop.4, it suffices to apply the theorem (¥), by setting $F := \{0,1\}$ and $p := 2$. □

Let n, p be integers, with $0 \leqslant p \leqslant n$. An "*arrangement*" of n elements taken p by p is a sequence of p *distinct* elements taken among the n given elements. Here, we denote by A_n^p (we could also use the notation $a(n,p)$) the number of arrangements of n elements taken p by p. Thus, an arrangement of 26 letters of the alphabet taken 3 by 3 is the word consisting of three *distinct* letters. We wonder how many such words there are. There are 26 possibilities for the 1st letter; once chosen this letter, it remains 25 possible choices for the 2nd, then, this 2nd letter being chosen, it remains 24 possible choices for the 3rd. The number obtained is thus: $A_{26}^3 = 26 \times 25 \times 24$. This example can be generalized. Let F be a finite set, of cardinal n. A sequence $(y_1,..,y_p)$ of p elements of F is by definition a map $f : [1,p] \to F$ ($f(i)=y_i$ for $i=1,..,p$), and $y_1,..,y_p$ are distinct if and only if f is *injective*. Thus an arrangement of n elements of F taken p by p is just an *injective map* from $[1,p]$ to F. The determination of numbers A_n^p results from the theorem:

Th. 57. (ð). *Let E and F be two finite sets. $p := \text{card}(E)$, $n := \text{card}(F)$. Let $\mathcal{I}(E,F)$ be the set of injections from E to F. If $p \leqslant n$, the cardinal of $\mathcal{I}(E,F)$ is: $A_n^p := \underbrace{n(n-1)\cdots(n-p+1)}_{p \text{ factors}} = \frac{n!}{(n-p)!}$. If $p > n$, there is no injections from E to F.*

PROOF. Consider the first equality as definition of A_n^p. The second equality is evident. For every integer p, let us denote by $P(p)$ the following property: "for *every* set E of cardinal p, and *every* finite set F of cardinal $n \geqslant p$, the cardinal of $\mathcal{I}(E,F)$ is A_n^p." The property $P(0)$ is true: for every set G, there is only one map from the emty set to G, and it is injective (ref. to definitions). Let $p \geqslant 1$ be an integer such that $P(p-1)$ is true. It suffices to show that $P(p)$ is true. If therefore E, F, n are consistent with the statement, we must show that the cardinal of (E,F) is A_n^p. Fix an element $a \in E$, and given $E' := E\backslash\{a\}$, which is the cardinal $p-1$. With any injection f of $\mathcal{I}(E,F)$ we can bijectively associate the pair (g,b) where g is the restriction of f to E' and b is $f(a)$, which does not belong to $g(E')=f(E')$ which is of cardinal $p-1$. It follows: $\text{card}(\mathcal{I}(E,F))=\text{card}(\mathcal{I}(E',F))(n-p+1)=A_n^{p-1}(n-p+1)=A_n^p$. Thus we have shown that $P(p)$ is true. The last statement of the theorem follows from theorem (†) of the heading "*Finite sets, denumerable sets*". □

Thus the number A_n^p is indeed the *number of arrangement* of n elements taken p by p. A direct consequence of the above theorem (and of theorem (▷) of heading "*Finite sets, denumerable sets*") is:

Th. 58. *Let E, F be two finite sets of same cardinal n. The number of bijections from E to F is $n!$. Specifically, the set $\mathfrak{S}$ of bijections from E to E (called permutations of E) is of cardinal $n!$.*

Let p be an natural number. For any complex number a, we set $\binom{a}{p} := \frac{a(a-1)\cdots(a-p+1)}{p!}$. Numerator is the product of p factors, and for $p=0$ its value is 1 (by convention). A priori $\binom{a}{p}$ is then a complex number; e.g. $\binom{a}{0}=1$, $\binom{a}{1}=a$, $\binom{a}{2}=\frac{a(a-1)}{2}$, $\binom{a}{3}=\frac{a(a-1)(a-2)}{6}$. Let n, p be two integers such that $0 \leqslant p \leqslant n$ and E a set of cardinal n. We call "*combination*" of n elements of E taken p by p every part of E of p elements. The theorem below shows that the number of these combinations is $\binom{n}{p}$. Fix $p=3$, with E the set of 26 letters of the alphabet. Each part of E of 3 elements (e.g. {k,p,u}) corresponds to $3!=6$ words consisting of three distinct letters (kpy, kyp, pky, pyk, ykp, ypk). The number of parts of E of 3 elements is therefore $\frac{A_{26}^3}{3!} = \binom{26}{3}$.

Th. 59. (▲). *Let E be a finite set, of cardinal n, and $p \in [0,n]$ be an integer. The number of parts of p elements of E is given by:*

$$(**) \qquad \binom{n}{p} := \frac{n(n-1)\cdots(n-p+1)}{p!} = \frac{n!}{p!(n-p)!} = \frac{A_n^p}{p!}.$$

PROOF. The first equality gives the definition of the number $\binom{n}{p}$, the two last comes from the previous theorem (ð). We must show that the cardinal of the set $\mathfrak{P}_p(E)$ of the parts of p elements of E is $\frac{A_n^p}{p!}$. Let $f : [1,p] \to E$ be an injection, $f([1,p])$ is a part of p elements of E. it follows a map $t : f \mapsto f([1,p])$ from $\mathcal{I}([1,p],E)$ to $\mathfrak{P}_p(E)$. Let S be a part of E. The fiber $t^{-1}(\{S\})$ consists of injections $f : [1,p] \to E$ whose image is S, i.e., bijections from $[1,p]$ to S. According to the last theorem, the cardinal of this fiber is thus $p!$. The theorem (ð) and the formula (∗) (that is, $\text{card}(E) = \sum_{y \in F} \text{card}(f^{-1}(y))$) leads to write: $A_n^p = \text{card}(\mathcal{I}([1,p],E)) = \sum_{S \in \mathfrak{P}_p(E)} p! = p!\,\text{card}(\mathfrak{P}_p(E))$. □

Let E be a set of finite cardinal n (e.g. $[1,n]$). The $\mathfrak{P}_p(E)$, for $p = 0, 1, .., n$ form a partition of $\mathfrak{P}(E)$. The previous theorem and theorem (∗) of the heading "*Finite sets, denumerable sets*" give the equality:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

(As example, give another proof of this formula (without the binomial formula). The coefficient $\binom{n}{p}$ are known as the *binomial coefficients*.

Ex. 84. (1) $\binom{50}{3} = \frac{50!}{47!3!}$, *we do not have to compute* $50!$, *actually* $\frac{50!}{47!3!} = \frac{50 \times 49 \times 48}{6} = 50 \times 49 \times 8 = 19600$. (2) *If n, p are natural numbers, we can write then* $\binom{-(n+1)}{p} = \frac{(-n-1)(-n-2)\cdots(-n-p)}{p!} = (-1)^p \frac{(n+p)(n+p-1)\cdots(n+1)}{p!} = (-1)^p \binom{n+p}{p}$.

In the only previous formula (∗∗), it is not obvious that the number $\binom{n}{p}$ is an integer. In fact, this is true because of theorem (▲) itself; but this also results from the important formula: $\binom{a+1}{p+1} = \binom{a}{p} + \binom{a}{p+1}$ ($a \in \mathbb{C}$, $p \in \mathbb{N}$). Let us prove this formula. Multiplying the two members by $(p+1)!$, it suffices to observe that $(p+1)a(a-1)\cdots(a-p+1)+a(a-1)\cdots(a-p+1)(a-p)$ is equal to $(a+1)a(a-1)\cdots(a-p+1)$. In particular, we have the **Pascal's relation**:

$$\binom{n+1}{p+1} = \binom{n}{p} + \binom{n}{p+1} \ (n,p \in \mathbb{N}, p \leqslant n-1) \quad \text{(Pascal's relation)}$$

This is the rule of construction of the *Pascal's arithmetical triangle*, shown in the table below for the binomial coefficients from 0 to 5. Observe the symmetry, $\binom{n}{p} = \binom{n}{n-p}$ when $0 \leqslant p \leqslant n$. This property of symmetry can be directly checked, then, using theorem (▲).

n \ p	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

3. Divisibility

The divisibility are studied in $\mathbb{N}$ and in $\mathbb{Z}$. Some results are proved in two different ways (especially, two fundamental theorems: Gauss theorem, and Euclid lemma). While in $\mathbb{N}$ the proofs are rather natural (although not necessarily easier), in $\mathbb{Z}$ the proofs are interesting and emphasize the *linear* nature of the divisibility.

3.1. Euclidean division, numeration.

For two integers a, b with $b \neq 0$, it is usually not possible to divide a by b, that is, to find an integer q such that $bq = a$. This is why rational numbers (fractions) are introduced. If q exists, it is unique (*regularity* of the multiplication). In this case we say that "b divides a", or "b is a divisor of a", or also "a is a multiple of b". An integer is said to be *even* if it is a multiple of 2, and *odd* otherwise. Moreover, if b divides two integers a, a', then b divides $ua + u'a'$, for all integers u, u', as well as $a - a'$ if $a \geqslant a'$. In $\mathbb{N}^*$, the sentence "x divides y" is an *order relation*, denoted by $x|y$. Moreover, 1 is the smallest element of $\mathbb{N}^*$, and for example, 2 and $3(=2+1)$ are not comparable for the divisbility: the order obtained is not a total order. If the exact division is not always possible, it is replaced by the Euclidean division, defined by the following theorem:

Th. 60. *(Euclidean division). Let a, b be two integers, with $b > 0$. There exists a unique pair of integers (q, r) verifying the conditions:*
(D1) : $a = bq + r$, *and*
(D2) : $0 \leqslant r \leqslant b$.
Integers q, r are respectively called quotient and remainder of the division of a by b, we denote them "a div b" and "a mod b", respectively.

PROOF. If X denote the set of the integers n such that $nb > a$. According to the archimedean property (cf. prop.1 in heading "*Addition and multiplication in* $\mathbb{N}$"), X is nonempty, given $m := \min(X)$, and $m \neq 0$. Set: $q := m-1$. By definition of m, we have $bq \leqslant a < b(q+1)$. Then we can set: $r := a\text{-}qb$, hence $a = bq+r$. Moreover, $bq+r < bq+b$, so $r < b$, with the property (ii) of the addition: the pair (q, r) verifies the conditions (D1), (D2) of the theorem above. If (q', r') is another pair of integers such that $a = bq' + r'$ and $r' < b$. Then $bq' \leqslant a$ but $b(q' + 1) > bq' + r' = a$, that is, $(q' + 1) \in X$ but $q' \notin X$. Thus $q' + 1 = m$, that is, $q' = m - 1 = q$, we infer r'=r. □

Exer. 2. *As this proof is not a "proof by construction" ("constructive proof"), consider this exercise: Denote by $q(a, b)$, $r(a, b)$ the quotient and the remainder of the division of a by b; then check that $(q(a, b), r(a, b))$ is equal to $(0, a)$ if $a < b$ and $(1+q(a-b, b), r(a-b, b))$ if $a \geqslant b$. "Proof by construction" ("constructive proof") the existence of the pair (q, r), and an algorithm allowing to compute q and r starting from a and b.*

Th. 61. *(Numeration in base b). Let b be an integer, $b > 1$. Any nonzero integer x can be written uniquely in the form:*
(1) $$x = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0,$$
where n is an integer, $a_0, a_1, ..., a_n$ are integers in the interval $[0, b-1]$, and $a_n \neq 0$. Then we say that $x = a_n a_{n-1} ... a_1 a_0$ is the writing of x in base b. Moreover, when the base b must be explicitely specified, we write $x = (a_n a_{n-1} ... a_1 a_0)_b$.

PROOF. Let $P(x)$ be the property: "x has a writing of the type (1)" (cf. theorem above). If $x < b$, $P(x)$ is true: take $n := 0$ and $a_0 := x$. Assume $P(v)$ is true for all the integers $v < x$, with $x > b$. Given $a_0 := x \bmod b$: there exists an integer q such that $x = bq+a_0$, and $q \neq 0$ since $x \geqslant b > a_0$. Moreover, $q < bq$ (since $b > 1$ and $q > 0$), so $q < bq \leqslant x$. Thus $P(q)$ is true: q is written $q = a_n b^{n-1} + \cdots + a_2 b + a_1$, where n is a nonzero integer and $a_1, ..., a_n \in [0, b-1]$, $a_n \neq 0$. In the theorem, the equality (3) comes then from the the equality $x = bq+a_0$; We conclude that $P(x)$ is true., and the recurrence theorem shows that $P(\mu)$ is true for every integer $\mu > 0$. For the uniqueness, the conclusion is immediate if $x < b$. Otherwise, from a writing of the type (1), set $q := a_n b^{n-1} + \cdots + a_2 b + a_1$; then $x = bq + a_0$ and $0 \leqslant a_0 < b$, so $a_0 = x \bmod b$. We conclude as above, by induction on x (recurrence), via the regularity of the addition and mltiplication. □

The *decimal numeral system* (also called *base ten* numeral system, or *base-10 numeral system*, or occasionally *denary*) has ten as its base (i.e. $b = 10$); it is the numerical base most widely used by modern civilizations. Binary numeral system (b=2) is used for computers, which also used *hexadecimal numeral system* (b=16).

Ex. 85. *There is a fast way to compute a power x^n. Let $n > 0$ be an integer, and x be an integer, or the element of an arbitrary ring (e.g. $\mathbb{Z}/u\mathbb{Z}$ where $u > 0$ is an integer). The key is the associativity of of the multiplication and the equality $x^0 = 1$. Normally, $n-1$ multiplications are required to compute x^n, so $x^4 = x \times (x \times (x \times x))$. There is a better way to do; e.g. $x^2 = x \times x$, $x^4 = x^2 \times x^2$, $x^8 = x^4 \times x^4$, $x^{13} = x^8 \times (x^4 \times x)$, so five multiplications suffice to compute x^{13} (instead of n-1=13-1=12). In this example we tacitly used the equality $13 = 1101_2$. Generalization: first, for any integer k, k multiplication (raise to square successively) allow to compute x^{2^k}. Then, in the binary writing of n, if we do not keep the number 1, we get an equality of the type: $n = 2^{k_p} + 2^{k_{p-1}} + \cdots + 2^{k_1} + 2^{k_0}$, where $(k_0, k_1, .., k_p)$ is a sequence of strictly increasing integers. Hence the calculation of x^n with $u := k_p + p$ multiplications: k_p to compute $x^{2^{k_p}}$ (which also gives the other $x^{2^{k_j}}$), then, p multiplications to compute the product of the $x^{2^{k_j}}$ for $j = 0, 1, .., p$. (Note that $p \leqslant k_p$, so $u \leqslant 2k_p$.) Moreover, $2^{k_p} \leqslant n$, i.e., $k_p \leqslant \log_2(n)$. Thus, $u \leqslant 2\log_2(n)$, this is more efficient than $n - 1$ (an example consists in checking that compute x^{10007} can be done with 20 multiplications). A variant of this technique does not really use the binary writing of n but only the (euclidean) division by 2 (e.g. $x^{13} = x \times x^{13}$, $x^{12} = (x^6)^2$, $x^6 = (x^3)^2$, $x^3 = x \times x^2$, $x^2 = x \times x$ gives again x^{13} by five multiplications).*

3.2. Primes, integer factorization.

Def. 210. *(Prime number). We call prime number every integer $p > 1$ that has exactly two divisors: 1 and p. We denote here by $\mathbf{P}$ the set of prime numbers.*

Prop.5 *To make that an integer $p > 1$ is prime, it is necessary and sufficient that it cannot be written as the product of two integers strictly higher than* 1.

PROOF. Assume that p is not prime: it has divisor $a \neq 1, p$. Given the integer b such that $p = ab$; $b \neq 1$, p, considering the assumption about a. Thus $p = ab$, and $a > 1$, $b > 1$. Conversely, assume that p can be written $p = xy$, where x, y are two integers strictly higher than 1. Then $x|p$, and $x \neq p$ (otherwise $y = 1$), i.e. x is a divisor of p different from 1 and p: p is not a prime. □

Th. 62. (Euclid th, n°1). *Any integer $n > 1$ is a (finite) product of prime numbers. In particular, n has at least a prime divisor.*

PROOF. For an integer n, denote by $P(n)$ the property: "n is the product of prime numbers". If $n > 1$ is an integer such that $P(k)$ is true for any integer k such that $1 < k < n$. It suffices to show that $P(n)$ is true (it is a case of strong induction (strong recurrence), cf. the assumption (R3) in the heading "*Recurrence (induction)*" (in section "*Set of Natural Numbers* $\mathbb{N}$"). If n is prime number, it is product of only one prime number, that is, itself. Otherwise, n=ab, where a, b integers strictly higher than 1. Since $a > 1$, $b < ab$=n, each of integers a, b is, by assumption, product of of prime numbers. Then n=ab is also product of prime numbers (juxtapose prime factors of a and b). □

Prime factor: A factor that is prime; i.e. one that cannot itself be factored.
Prop.6 *Given $n > 1$. If n is not prime number, it has a prime factor p such that $p^2 \leqslant n$.*

PROOF. By hypothesis n does not belong to the set $\mathbf{P}$ of prime numbers, then it can be written $n = ab$, where a, b are integers strictly higher than 1, assume that $a \leqslant b$. Given a prime factor p of a, whose existence is guaranteed by the previous theorem, then we have $p|n$, and $p^2 \leqslant ap \leqslant ab$=$n$. □

The numbers 2,3,5,7,11 are prime, but not 1. The following statement says how to know if an integer $N > 0$ is prime. "We list the primes p such that $p^2 \leqslant N$ (i.e. using the reals, $p \leqslant \text{Int}(\sqrt{N})$, where $\text{Int}(x)$ the *integer part* of a real x). Then N is also prime if and only if it is multiple of no prime numbers obtained."

Ex. 86. $N = 1789$ *is prime.* $\text{Int}(\sqrt{1789}) = 42 : 42^2 = 1764$, $43^2 = 1849$. *Primes less than* 42 *are:* 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41*; we check that none of these numbers divides* 1789*, using euclidean division.*

In practice, this approach is not used for large numbers (with more than one hundred figures), today there much faster techniques (not shown here).
The "Sieve of Eratosthenes gives a procedure that allows to find all the primes less than a given integer $N > 1$ (this procedure is shown in the heading "*Infinitude of prime numbers*", in the section "*Prime Numbers*", in *Number Theory*).

Th. 63. (Euclid th., n°2). *The set $\mathbf{P}$ of prime number is infinite.*

PROOF. Consider the set $\mathbf{P}$ of prime number is finite. Let $n \geqslant 1$ be the cardinal of $\mathbf{P}$. Denote the elements of $\mathbf{P}$ by $\mathbf{P} = \{p_1, p_2, .., p_n\}$. The integer $N := 1+p_1 p_2 \cdots p_n$ is strictly higher than 1. According to Euclid theorem n°1, this integer has a prime factor p. But $p \in \mathbf{P}$ must be one the p_i, so p divides $p_1, p_2, .., P_n = N - 1$. Since also divides N, it divides $1 = N - (N - 1)$; which is absurd since $p \neq 1$, and the only divisor of 1 is 1. □

Th. 64. (Euclid lemma). *If a prime number divides the product of two (strictly positive) integers, it divides at least one of these two integers. More generally, is a prime number divides a product of strictly positive integers, it divides one of these integers.*

PROOF. Let p be prime, dividing ab but not a. The set E of integers $n > 0$ such that p divides an contains p, b and $m := \min(E) > 0$, but not 1, so $m > 1$. $\forall n \in E$, we perform the euclidean division $n = mq + r$, with $0 \leqslant r < m$; then p divides $an - (am)q = ar$. Since $r < m$, we have $r \notin E$, so $r = 0$, which shows that m divides n. Specifically, m divides p and b. Moreover, p is prime and $m > 1$, so $p = m$, which thus divides b. The second statement comes from the first, by induction on the number of factors. □

Exer. 3. (◊). *Let p be a prime, and $\lambda \in [1, p-1] \in \mathbb{Z}$. Show that $\binom{p}{\lambda}$ is multiple of p. Since $\binom{p}{\lambda} = px$, where $x = (p-1)(p-2)\cdots(p-\lambda+1)/\lambda!$, we can say that $p|\binom{p}{\lambda}$ since $\binom{p}{\lambda} = px : p$ is in factor in $\binom{p}{\lambda}$; this is false; indeed, this would come down to say that $2|3$ because $3 = 2\cdot(\frac{3}{2})!$ The divisibility is about $\mathbb{N}$ or $\mathbb{Z}$, but not $\mathbb{Q}$. Thus remain in $\mathbb{N}$. Write $\lambda!\binom{p}{\lambda} = p(p-1)(p-2)\cdots(p-\lambda+1) = ph$, where here $h \in \mathbb{N}$. Thus p divides $\lambda!\binom{p}{\lambda}$. Euclid lemma shows that p divides either $\lambda!$ or $\binom{p}{\lambda}$; the first case is excluded: if p divides $\lambda!$ (product of $1, 2, .., \lambda$) the Euclid lemma implies the existence of an integer $k \in [1, \lambda]$ multiple of p; which does not make sense since $k \leqslant \lambda \leqslant p-1$. Therefore $p|\binom{p}{\lambda}$.*

Here is a "*factorization*" theorem, known as "*fundamental theorem of arithmetic*", or also "*unique factorization theorem*:

Th. 65. (Fundamental Theorem of Arithmetic). *Let n be an integer strictly higher than 1. We can factorize n, that is, we can write n in the form:*

$$n = p_1 p_2 \cdots p_r, \tag{2}$$

where r is a strictly positive integer and $p_1, p_2, .., p_r$ are prime numbers (not necessarily distinct). This factorization is unique, up to the order of factors, we also say that it is ***essentially unique****. This theorem is also known as the "unique factorization theorem", or sometimes "factorization theorem".*

Proof. The existence of a factorization of n of the type (2) above, results from Euclid theorem n°1. Let us show its uniqueness by strong induction (strong recurrence). Let $n>1$ be an integer such that the statement of the uniqueness holds for any integer m, with $1<m<n$. Given two factorizations of n: $n=p_1p_2\cdots p_r=q_1q_2\cdots q_s$. We have to check that they are essentially the same. If n is prime, $r=s=1$ and $p_1=n=q_1$. Suppose $r \geqslant 2$, $s \geqslant 2$. Since the prime p_1 divides $n=q_1q_2\cdots q_s$, Euclid lemma implies the existence of an index $j \in [1, s]$ such that $p_1|q_j$. By reordering the q_k, we can assume that $j=1$. The numbers p_1, q_1 are prime and $p_1|q_1$, so $p_1=q_1$. It follows by simplifying that $p_2\cdots p_r=q_2\cdots q_s$, let us denote this product by n'. Since $n'<n$ (since $n=p_1n'$), the two factorizations of n' we have are essentially the same. That is, first $r=s$, and in addition, $p_2\cdots p_r$ and $q_2\cdots q_s$ are the same, up to the order. Since $p_1=q_1$, the two factorizations of n differ only up to the order. □

In a factorization of the type (2), we get (by grouping equal prime factors) a new writing of n in the form

$$n = q_1^{u_1} q_2^{u_2} \cdots q_r^{u_s}, \tag{3}$$

where here $q_1q_2\cdots q_s$ are *pairwise distinct* prime numbers and the u_i are strictly positive integers. Such a factorization of n, or *decomposition of n into prime factors*, is unique, up to the order of the q_i, and it becomes truly unique if the q_i are ordered in ascending order (e.g. the factorization of 9000 is $2^3 \times 3^2 \times 5^3$). The factorization of an integer n starts with the determination of a prime factor p (see above), we write $n=pn'$, where n' is an integer such that $n'<n$, then, we have to factorize n', etc.

Notation: If n is written as in (3), and $i \in [1, s]$, the integer u_i is called the *exponent of the prime number q_i in the decomposition of n into prime factors*, and is denoted $v_{q_i}(n)$. If p is a prime number distinct from $q_1, .., q_s$, we set $v_p(n) := 0$. The equality (3) becomes:

$$n = \prod_{p \in \mathbf{P}} p^{v_p(n)}. \tag{4}$$

In this formula, the product is a *finite* product: if $p \in \mathbf{P}$ is not one of the q_i, which leads to say that p does not divide n; ($p^{v_p(n)}=p^0=1$ is left out in this product). The notation v_p is completed by setting $v_p(1) := 0$ for every $p \in \mathbf{P}$. If $n \in \mathbb{N}^*$ and $p \in \mathbf{P}$, the integer $v_p(n)$ is also called *valuation of n at p*.

Given $a, b \in \mathbb{N}^*$. By setting $a = \prod_{p\in\mathbf{P}} p^{v_p(a)}$ and $b = \prod_{p\in\mathbf{P}} p^{v_p(b)}$, clearly $ab = \prod_{p\in\mathbf{P}} p^{v_p(a)+v_p(b)}$. It follows the important formula, which holds for all $a, b \in \mathbb{N}^*$ and every prime number p:

$$v_p(ab) = v_p(a) + v_p(b). \tag{5}$$

This formula results from the uniqueness of a factorization of the type (4) above for ab.

Th. 66. (♭). *Let λ, γ be two strictly positive integers. In order that λ divides γ, it is necessary and sufficient that $v_p(\lambda) \leqslant v_p(\gamma)$ for every prime number p.*

Proof. If $\lambda|\gamma$, let us set $\gamma = \lambda\mu$, where $\mu \in \mathbb{N}^*$. For every $p \in \mathbf{P}$, the expression (5) gives $v_p(\gamma) = v_p(\lambda) + v_p(\mu) \geqslant v_p(\lambda)$. Conversely, assume $\forall p \in \mathbf{P}$, $v_p(\lambda) \leqslant v_p(\gamma)$. If $p \in \mathbf{P}$, let us set $v_p(\gamma) = v_p(\lambda) + \tau_p$, where $\tau_p \in \mathbb{N}$ (subtraction in $\mathbb{N}$). Then $\gamma = \lambda\mu$, where $\mu = \prod_{p\in\mathbf{P}} p^{\tau_p}$, so γ divides λ (note that the product $\mu = \prod_{p\in\mathbf{P}} p^{\tau_p}$ is finite). □

(It could be interesting for the reader to wonder why the product defining μ is finite.)

3.3. GCD, LCM, Euclid algorithm. The concept of *greatest common divisor* is central in the sets $\mathbb{N}$ and $\mathbb{Z}$ (as well as in polynomial rings). Here, integers will be supposed to be strictly positive when dealing with the divisibility. Moreover, note that for two integers a, b the relation $a|b \Rightarrow a \leqslant b$. Let $a_1, .., a_n$ be integers, an integer is called *common divisor* to $a_1, .., a_n$ if it divides thus each of the a_i. The set of these common divisor is bounded from above by a_1, there is therefore a greatest element (see property (N2) of $\mathbb{N}$ of the heading "*Set of Natural Numbers* $\mathbb{N}$"), which will be denoted: "gcd" (of the a_i). Formally, we have the following *theorem* (also taken as *definition*):

Th. 67. *(Greatest common divisor). Let $a_1, a_2, .., a_n$ be strictly positive integers, with $n \geqslant 1$. There exists a unique integer $d > 0$ verifying the following conditions:*
(i) The integer d is a common divisor to $a_1, a_2, .., a_n$.
(ii) Any other common divisor to $a_1, a_2, .., a_n$ divides d.
This integer d, called ***greatest common divisor****, or* gcd *of $a_1, a_2, .., a_n$, is denoted $\gcd(a_1, a_2, .., a_n)$, or $a_1 \wedge a_2 \wedge \cdots \wedge a_n$. It is explicitly given (in terms of factorizations of the a_i) by the following formula, $\forall p \in \mathbf{P}$:*

$$d = \prod_{p\in\mathbf{P}} p^{m_p}, \text{ where } m_p := \min(v_p(a_1), .., v_p(a_n)). \tag{6}$$

Proof. In the formula (6), the product is indeed a finite product: if $p \in \mathbf{P}$ does not divide a_1, $m_p = 0$. According to theorem (♭) of the previous heading "*Primes, integer factorization*", d divides each of a_i. Let h be a common divisor to a_i. For $p \in \mathbf{P}$, $v_p(h) \leqslant v_p(a_i)$ for $i=1,..,n$, hence $v_p(h) \leqslant m_p$. Thus $h|d$: d verifies 1 and 2. Finally, given an integer d' verifying the same properties (i) and (ii) as d, let us show that $d' = d$. Since d' is common divisor to a_i, the property (ii) (for d) shows that $d'|d$. Similarly $d|d'$, so $d = d'$. □

Thus, an integer h divides two integers a and b if and only if it divides their gcd.

Ex. 87. (A). *The* gcd *of $9000 = 2^3 \times 3^2 \times 5^3$ and $1575 = 3^2 \times 5^2 \times 7$ is $3^2 \times 5^2 = 225$.*

Def. 211. *(Relatively prime). Two integers are relatively prime if their* gcd *is 1, that is, if they have no common divisor other than 1. Similarly, the integers $a_1, a_2, .., a_n$ ($n \geqslant 1$) are relatively primes if their* gcd *is 1.*

Rem. 33. *Do not confuse (for the integers u, v, w) the two following writings: (1) $\gcd(u, v, w)=1$, and (2) $u\wedge v=v\wedge w=w\wedge u=1$. In (2), the integers u, v, w are said to be "pairwise relatively prime". In (1), the integers u, v, w are "relatively prime"; e.g. $4, 6, 9$ are relatively prime, but not pairwise relatively prime ($4 \wedge 6=2$).*

For the set $\mathbb{N}^*$, the formula (6) implies that the associativity and commutativity hold with respect to the operation $\gcd : (a, b) \mapsto a \wedge b$ is . Similarly, the distributivity of the multiplication holds with respect to $\gcd : a(b \wedge c) \mapsto ab \wedge c$.
The following Gauss's theorem is sometimes also called Euclid's lemma:

Th. 68. (Gauss th.). *Let a, b, c be three strictly positive integers. If $a|bc$, and a is relatively prime to b, then $a|c$. (In other words, if a divides bc and a is relatively prime to b. Then a divides c)*

Proof. By assumption $a\wedge b=1$. Thus $c=c(a\wedge b)=ca\wedge cb$. In fact, a divides ca and also cb, therefore it divides the gcd of ca and cb. □

Let us introduce the *Euler's totient function* (also refer to the heading "*Decimal expansion*", in "*Construction of Number System*"). In number theory, Euler's totient function, or Euler's totient or phi function, $\varphi(n)$ (also denoted by $\phi(n)$) is an arithmetic function that counts the totatives of n, i.e. the positive integers less than or equal to n that are *relatively prime* to n. Thus if n is a positive integer, then $\varphi(n)$ is the number of integers k in the range $1 \leqslant k \leqslant n$ for which $\gcd(n, k) = 1$. The totient function is a multiplicative function, meaning that if two numbers m and n are relatively prime (to each other), then $\varphi(mn) = \varphi(m)\varphi(n)$.

Def. 212. *(Euler's totient function). For a positive integer n, let $\varphi(n)$ be the number of positive integers less than n that are relatively prime to n. In other words, a function φ defined on the positive integers equal to or less than n and relatively prime to n. Also known as the totient function, the Euler totient, Euler's totient, totient, phi function, or indicator. ($\varphi(n)$ is sometimes denoted by $\phi(n)$.)*

Ex. 88. (1) $\varphi(12)=4$, *since four numbers* $1,5,7$ *and* 11, *are relatively prime to* 12. (2) *There are eight totatives of* 24 (1, 5, 7, 11, 13, 17, 19, *and* 23), *so* $\varphi(24)=8$. (3) $\varphi(n)$ *is always even for* $n\geq 3$ *and* $\varphi(0)$=1. *The first few values of* $\varphi(n)$ *for* n=1,2,...*are* 1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10,...

The function φ defined on the set of positive integers, is *Euler's function*. It can be shown that, if the prime decomposition of n is $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, we have then $\varphi(n)=p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_r^{\alpha_r-1}(p_1-1)(p_2-1)\cdots(p_r-1)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$.
There are several formulas for the totient (computing Euler's function); the *Euler's product formula* states $\varphi(n)=n\prod_{p|n}(1-\frac{1}{p})$, where the product is over the distinct prime numbers dividing n.
The totient function is important because it gives the order of the multiplicative group of integers modulo n (the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$).

Exer. 4. $(*)$. *For every integer* $m\geqslant 1$, *denote* $\varphi(m)$ *the number of integers* $k\in[1,m]$ *relatively prime to* m. *The function* $\varphi:\mathbb{N}^*\to\mathbb{N}$ *thus defined is called Euler's totient function (Euler's indicator, phi function, etc.). Prove for any integer* $n\geqslant 1$ *the following formula* $\sum_{d|n}\varphi(d)=n$, *where the sum is extended to all the divisors* $d>0$ *of* n. *Solution: The key is to sort the integers* $k\in[1,n]$ *based on the value of* $h=k\wedge n$. *Let* U *be the set of pairs* (d,w) *such that* $d>0$ *is a divisor of* n *and* $w\in[1,d]$ *is relatively prime to* d. *According to Fubini's formula (cf. Ex. in heading "Finite sets, denumerable sets"), the sum* $\sum_{d|n}\varphi(d)$ *is equal to* $\mathrm{card}(U)$. *Let* $f:U\to[1,n]$ *be the map associating with any pair* $(d,w)\in U$ *the product* hw, *where* h *is the only integer such that* $n=hd$. *It suffices to show that* f *i bijective. Given* $k\in[1,n]$. *A pair* $(d,w)\in U$, *with* $n=hd$ *as above, is an antecedent of* k *by* f *iff* $k=hw$. *If it is true,* $n\wedge k=hd\wedge hw=h$, *hence the uniqueness of* h, *and therefore that of* d *and* w. *Conversely, let us set:* $h:=k\wedge n$. *We can write* $k=hw$, $n=hd$, *where* $w,d\in\mathbb{N}^*$ *and* $w\wedge d=1$. *But* $hw=k\leqslant n=hd$, *so* $w\in[1,d]$; *then* $(d,w)\in U$ *is an antecedent of* k *under the map* f. *Thus* k *has a unique antecedent by the map* f, *so* f *is bijective.*

Note that the calculation of the gcd of two "large" integers by the formula (6) takes a lot of time (due to the factorization of these integers); but there is a faster procedure based on euclidean division:

Th. 69. (Euclid algorithm). *Let* $a,b\in\mathbb{N}^*$. *There exists a unique integer* $n\geqslant 1$ *and two sequences of integers* $(q_1,..,q_n)$ *and* $(r_1,..,r_n)$, *also unique, which verify the following conditions:*
(*i*) (Initialization)*:* $r_1:=a$ *and* $r_2:=b$.
(*ii*) *For* k=$1,..,n$, $r_k=q_kr_{k+1}+r_{k+2}$ *(we denote this equality by* E_k*).*
(*iii*) *We have* $r_2>r_3>\cdots>r_{n+1}>r_{n+2}:=0$.
gcd *of* a *and* b *is then* r_{n+1}, *last nonzero remainder.*

Proof. The existence is shown by induction on b. If $b|a$, we write a=bq_1 ($q_1\in\mathbb{N}^*$), it suffices to set: $n:=1$ and r_1:=a, r_2:=b, r_3:=0. Assume that b does not divides a and that the existence has been shown for every integer strictly less than b. Performing the euclidean division of a by b: a=bq+r, with $q\in\mathbb{N}$, $0\leqslant r<b$. Since b does not divides a, $r>0$. Now, replace the pair (a,b) by (b,r). Apply the induction to (b,r), there is an integer $n\geqslant 2$ and two sequences $(q_2,..,q_n)$, $(r_2,..,r_{n+2})$ for which r_2=b, r_3=0, 0=r_{n+2}<r_{n+1}<...<r_3, and the equality E_k is true for μ=2,..,n. Now, set: r_1:=a and q_1:=q. Thus, the equality E_1 is satisfied, and r_3=r<b=r_2. Thus the conditions hold for (a,b). Now, assume that the conditions (i),(ii),(iii) hold for the sequences $(q_1,..,q_n)$ and $(r_1,..,r_{n+2})$. Given $d:=a\wedge b$, let us show that $d=r_{n+1}$. It suffices to show for k=1,..,n that d=$r_k\wedge r_{k+1}$: for $k=n$ we have d=$r_n\wedge r_{n+1}$. Moreover, E_k is written r_n=q_nr_{n+1}, so $r_n\wedge r_{n+1}$=r_{n+1}, and so d=r_{n+1}. By induction on k. According to (i), $r_1\wedge r_2$=$a\wedge b$=d. Assume d=$r_k\wedge r_{k+1}$ for a certain integer $k\in[1,n-1]$. Let h be a divisor of r_{k+1}. Since $r_k=q_kr_{k+1}+r_{k+2}$, h divides r_k iff it divides r_{k+2}. Thus the common divisors to r_k and r_{k+1} are the same as the common divisors to r_{k+1} and r_{k+2}, hence $r_{k+1}\wedge r_{k+2}$=$r_k\wedge r_{k+1}$=d: the statement is true at the rank k+1. To complete the proof, we have to check that the sequences $(q_1,..,q_n)$ and $(r_1,..,r_{n+2})$ are unique (left to the reader). □

(The integer n is the number of euclidean divisions to perform $a\wedge b$ by the technique suggested by this proof.)

Exer. 5. (B).*Consider again the exercise that calculated the* gcd *of* 9000 *and* 1575. *We perform the euclidean divisions:* $9000=5\times1575+1125$, $1575=1\times1125\times450$, $1125=2\times450\times225$, $450=2\times225+0$. *The* gcd *sought is thus* 225, *last nonzero remainder.*

Now, let us introduce the notion of least common multiple, denoted by lcm. Formally, we have the following *theorem* (also taken as *definition*):

Th. 70. *(Least common multiple). Let* $a_1,a_2,..,a_n$ *be strictly positive integers, with* $n\geqslant 1$. *There exists a unique integer* $m>0$ *verifying the following conditions:*
(*i*) *The integer* m *is a common multiple of* $a_1,a_2,..,a_n$.
(*ii*) *Any other common multiple of* $a_1,a_2,..,a_n$ *is a multiple of* m.
This integer m *is called* ***least common multiple****, or* lcm *of* $a_1,a_2,..,a_n$, *and is denoted* $\mathrm{lcm}(a_1,a_2,..,a_n)$, *or* $a_1\vee a_2\vee\cdots\vee a_n$. *Moreover,* m *is explicitly given (in terms of factorizations of the* a_i*) by the following formula,* $\forall p\in\mathbf{P}$*:*
(7) $$m=\prod_{p\in\mathbf{P}}p^{h_p},\ \textit{where}\ h_p:=\max(v_p(a_1),..,v_p(a_n)).$$

Proof. It is analogous to the proof of "greatest common divisor" theorem, it is left to the reader. □

Rem. 34. lcm *and* gcd *are related for two integers.*

Prop.7 *Let* a,b *be two integers. If* m *is their* lcm, and d *is their* gcd, *then* $dm=ab$.

Proof. Note that if r,s are two integers, or even two reals, $r+s=\max(r,s)+\min(r,s)$. This simple statement suffices. Indeed, given $p\in\mathbf{P}$. Given the previous formulas (6), (7), and also the formula (5) (in previous heading "*Primes, integer factorization*"), we have $v_p(ab)=v_p(a)+v_p(b)=\min(v_p(a),v_p(b))+\max(v_p(a),v_p(b))=v_p(d)+v_p(m)=v_p(dm)$. Thus, for every $p\in\mathbf{P}$, the exponents of p in ab and dm are equal. Given the formula (4) (in "*Primes, integer factorization*") applied to ab and dm, hence the conclusion. □

Th. 71. *Let* $a_1,a_2,..,a_n\in\mathbb{N}^*$ $(n\geqslant 2)$ *be pairwise relatively prime integers. Their* lcm *is then equal to their product.*

Proof. Let m be the lcm, and Π the product of a_i. It suffices to consider $\forall p\in\mathbf{P}$, $v_p(m)$=$v_p(\Pi)$. Moreover, $v_p(\Pi)$ is the sum of the $v_p(a_i)$ (formula (7)). The key is that, among the integers $v_p(a_i)$, only one at most is nonzero (then the maximum and the sum are equal). Indeed, assume the opposite, and that $i,j\in[1,n]$ with $i\neq j$ and $v_p(a_i)\geqslant 1$, $v_p(a_j)\geqslant 1$ such that p divides a_i and a_j, contradicting the assumption $a_i\wedge a_j$=1. □

Exer. 6. *The product of* 4,6,9 *is* 216 *while their* lcm *is* 36. *Yet* 4,6,9 *are relatively prime. For what reason?*

4. Integers $\mathbb{Z}$

4.1. Operations. The subtraction (inverse operation to addition) in $\mathbb{N}$ is not always defined: indeed, $x-y$ makes sense in $\mathbb{N}$ only if $x\geqslant y$. The introduction of integers (...,-2,-1,0,1,2,...) overcomes this defect. The integers form a set, denoted by $\mathbb{Z}$, which contains $\mathbb{N}$. Here, the objectives are: (1) Recall (without proving) main properties of standard operations and of the order relation on $\mathbb{Z}$; (2) Give a *rigorous construction of the set* $\mathbb{Z}$ starting from $\mathbb{R}$, then, of the three operations and of the order relation on $\mathbb{Z}$.
The construction of $\mathbb{Z}$ is based on the notion of *quotient of a set by an equivalence relation.*
The addition in $\mathbb{Z}$ is a map $(a,b)\mapsto a+b$ from $\mathbb{Z}\times\mathbb{Z}$ to $\mathbb{Z}$. Its main properties are mentioned below. (Recall: $\mathbb{Z}$ contains $\mathbb{N}$).

Prop.8 *The addition in* $\mathbb{Z}$ *has the following properties:*
(1) *It is associative and commutative.*
(2) *For any* $u\in\mathbb{Z}$, $0+u=u$.
(3) *Given* $u\in\mathbb{Z}$. *There exists a unique element* $u'\in\mathbb{Z}$ *such that* $u+u'=0$. *This elements* u' *is denoted by* $-u$ *and called opposite of* u.
(4) *For all* $x,y\in\mathbb{Z}$, $-(-x)=x$ *and* $-(x+y)=(-x)+(-y)$.
(5) *The map* $n\mapsto-n$ *is a bijection from* $\mathbb{N}^*$ *to the complement of* $\mathbb{N}$ *in* $\mathbb{Z}$. *Clearly, any element of* $\mathbb{Z}$ *is either an element of* $\mathbb{N}$ *or in the form* $-n$, *with* $n\in\mathbb{N}^*$.
(6) *It extends that of* $\mathbb{N}$: *if* $x,y\in\mathbb{N}$, *the sum* $x+y$ *is the same, whether calculated in* $\mathbb{N}$ *or in* $\mathbb{Z}$.
(7) *For all* $a,b,c\in\mathbb{Z}$, $a+c=b+c$ *implies* $a=b$.
This is the property (3) that distinguishes $\mathbb{Z}$ from $\mathbb{N}$ about the addition. The properties (1),(2),(3) can be described by saying that $\mathbb{Z}$, *provided with the addition*, is a *commutative group.*
We define, from the addition, the subtraction in $\mathbb{Z}$: if $x,y\in\mathbb{Z}$, we set: $x-y:=x+(-y)$. Hence for example $-(x-y)=y-x$. Any integer x can be written in the form $x=a-b$, hence $a,b\in\mathbb{N}$ (for what reason), but this writing is not unique (-3=2-5=5-8).

Exer. 7. *Show that* $\mathbb{Z}$ *is denumerable (countable). Since the map* $(a,b)\mapsto a-b$ *from* $\mathbb{N}\times\mathbb{N}$ *to* $\mathbb{Z}$ *is surjective,* $\mathbb{Z}$ *is finite or denumerable (countable) because* $\mathbb{N}\times\mathbb{N}$ *is denumerable (countable) (cf. the last theorem of the heading "Finite sets, denumerable sets"). But* $\mathbb{Z}$ *is not finite since it contains* $\mathbb{N}$.

Prop.9 *The multiplication in $\mathbb{Z}$ has the properties:*
(1) *It is associative and commutative.*
(2) *It is distributive with respect to the addition:* $a(b+c)=ab+ac$ for all $a,b,c\in\mathbb{Z}$.
(3) $\forall u\in\mathbb{Z}$, $1\times u=u$.
(4) *It extends that of* $\mathbb{N}$: *if* $x,y\in\mathbb{N}$, *the product* xy *is the same, whether calculated in* $\mathbb{N}$ *or in* $\mathbb{Z}$.
(5) *Given* $a,b\in\mathbb{Z}$. *Then* $ab=0$, *iff* $a=0$ *or* $b=0$.
(6) *Given* $a,b\in\mathbb{Z}$. *Then* $ab=1$, *iff* $a=b=\pm1$.

Properties (1),(2),(3) together with the properties of the addition, mean that $\mathbb{Z}$, *provided with the addition and the multiplication, is a commutative ring*. The property (5) means that $\mathbb{Z}$ is an *integral domain* (*entire ring*).

The properties of the ordinary *order relation on* $\mathbb{Z}$ are:

Th. 72. *The order relation on $\mathbb{Z}$ has the properties:*
(1) *It is total: if* $x,y\in\mathbb{Z}$ *we have either* $x\leqslant y$ *or* $y\leqslant x$.
(2) *For any* $x\in\mathbb{Z}$, *we have* $0\leqslant x$, *iff* $x\in\mathbb{N}$.
(3) *It extends that of* $\mathbb{R}$: *if* $x,y\in\mathbb{N}$, $x\leqslant y$ *has the same meaning in* $\mathbb{Z}$ *and in* $\mathbb{N}$.
(4) *It is compatible with the addition: if* $a,a',b,b'\in\mathbb{Z}$ *and if* $a\leqslant a'$ *and* $b\leqslant b'$, *we have:* $a+b a\leqslant a'+b'$.
(5) *For two arbitrary elements* $x,y\in\mathbb{Z}$, $(x\leqslant y)\Leftrightarrow(-y\leqslant -x)$.
(6) *Given* $a,a',b\in\mathbb{Z}$. *If* $a\leqslant a'$ *and* $b\geqslant 0$, *we have:* $ba\leqslant ba'$. *In addition, if* $b>0$, $(a\leqslant a')\Leftrightarrow(ba\leqslant ba')$ *and* $(a<a')\Leftrightarrow(ba<ba')$.
(7) *Every nonempty part bounded from above of* $\mathbb{Z}$ *has at most a greatest element.*
(8) *Every nonempty part bounded from below of* $\mathbb{Z}$ *has at least a smallest element.*

Construction of $\mathbb{Z}$. Now, let's sketch the construction of $\mathbb{Z}$. On the set $\mathbb{N}\times\mathbb{N}=\mathbb{N}^2$, define the relation, denoted by $\sim$, as follows: $(a,b)\sim(c,d)$ if $a+d=b+c$. It is an equivalence relation on $\mathbb{N}^2$. Only the transitivity is worth to be shown. Assume $(a,b)\sim(c,d)$ and $(c,d)\sim(e,f)$ with $a,b,c,d,e,f\in\mathbb{N}$. Thus $a+d=b+c$ and $c+f=d+e$. Hence $(a+f)+c=a+(c+f)=a+(d+e)=(a+d)+e=(b+c)+e=(b+e)+c$. Therefore the *regularity of the addition* in $\mathbb{N}$ gives: $a+f=b+c$, that is, $(a,b)\sim(e,f)$.
By this equivalence relation, the set $\mathbb{Z}$ is (by definition) the quotient of $\mathbb{N}^2$. Denote (temporarily) $[[(a,b)]]$ the class of the pair $(a,b)\in\mathbb{N}^2$, note that it'll play (later) the role of *difference* of a and b. The map $(a,b)\mapsto[[(a,b)]]$ from $\mathbb{N}^2$ to the its quotient $\mathbb{Z}$ is thus surjective.
We can wonder what becomes $\mathbb{N}$ in this construction. The map $n\mapsto[[(n,0)]]$ from $\mathbb{N}$ to $\mathbb{Z}$ is *injective*: if $n,n'\in\mathbb{N}$ and if $[[(n,0)]]=[[(n',0)]]$, we have $n+0=n'+0$, that is, $n=n'$. Then it is natural to identify each $n\in\mathbb{N}$ with $[[(n,0)]]\in\mathbb{Z}$. From now on, we consider $\mathbb{N}$ as part of $\mathbb{Z}$. In particular, $0\in\mathbb{Z}$ since identified with $[[(0,0)]]$.
.We wonder how to define the **addition in** $\mathbb{Z}$. The purpose is simple: given $u,u'\in\mathbb{Z}$. If (a,b), $(a',b')\in\mathbb{N}^2$ are such that $u=[[(a,b)]]$ and $u'=[[(a',b')]]$, we set:
(†) $$u+u':=[[(a+a',b+b')]].$$
This expression is justified by checking that the second member depends only on u, u', and not on the choice of (a,b), (a',b'). Thus, let (c,d) (resp. (c',d')) be another representative of u (resp. u'). Thus $(a,b)\sim(c,d)$, that is $a+d=b+c$, likewise $a'+d'=b'+c'$. Then: $(a+a')+(d+d')=(a+d)+(a'+d')=(b+c)+(b'+c')=(b+b')+(c+c')$, so $(a+a',b+b')\sim(c+c',d+d')$. This justifies the above formula (†), which is thus valid *for any* choice of the representative (a,b) (resp. (a',b')) of u (resp. u'). Hence an *addition*: $\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ which is associative and commutative (like that of $\mathbb{N}$). It extends that of $\mathbb{N}$ since if $n,n'\in\mathbb{N}$, we have $[[(n,0)]]+[[(n',0)]]=[[(n+n',0)]]$.
Given $u\in\mathbb{Z}$, let us write it $u=[[a,b]]$, where $a,b\in\mathbb{N}$, and let us set $u'=[[b,a]]\in\mathbb{Z}$. Then $u+u'=[[(a+b,b+a)]]=[[(0,0)]]=0$, hence the property (3) of Prop.8. If $a\geqslant b$, $a-b$ makes sense in $\mathbb{N}$, and $(a-b)+b=a$, hence $[[a,b]]=[[a-b,0]]\in\mathbb{N}$. If $a<b$, $b-a$ makes sense in $\mathbb{Z}$, and $[[a,b]]=[[(0,b-a)]]=-[[(b-a,0)]]$, hence the property of Prop.8. The other properties of Prop.8 are left to the reader.
.We wonder how to define the **multiplication in** $\mathbb{Z}$. Given $u,u'\in\mathbb{Z}$. If (a,b), $(a',b')\in\mathbb{N}^2$ are such that $u=[[(a,b)]]$ and $u'=[[(a',b')]]$, we set:
(‡) $$uu':=[[(aa'+bb',ab'+ba')]].$$
The proof of validity of (‡) is left to the reader (in the same manner as (†)). Hence an *multiplication*: $\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, which indeed extends that of $\mathbb{N}$ since if $n,n'\in\mathbb{N}$, we have $[[(n,0)]]\times[[(n',0)]]=[[(nn',0)]]$.
As example, let's check the property (5) of Prop.9 (the other properties are left to the reader). Assume a,b nonzero. If $a,b\in\mathbb{N}^*$, the product ab in $\mathbb{Z}$ is the same as in that of $\mathbb{N}$, so it is nonzero. If $b\in\mathbb{N}^*$ and $a=-n$, $n\in\mathbb{N}^*$, we have $ab=(-n)b=-(nb)$ (comes from property (2)), so $ab\neq0$. We have an analogous result if $a\in\mathbb{N}^*$ and $b=-n'$, $b\in\mathbb{N}^*$. Finally, if $a=-n$ and $b=-n'$, where $n,n'\in\mathbb{N}^*$, $ab=(-n)(-n')=nn'\neq0$.
.We wonder how to define the order relation on $\mathbb{Z}$. Given $x,y\in\mathbb{Z}$. We say that $x\leqslant y$ if $y-x\in\mathbb{N}$. If $x\in\mathbb{Z}$, $x-x=x+(-x)=0$, so $x\leqslant x$: the reflexivity holds. If $x,y,z\in\mathbb{Z}$ and $x\leqslant y\leqslant z$, $(y-x)$ and $(z-y)$ are in $\mathbb{N}$, their sum $(y-x)+(z-y)=z-x$ also (property (6) of addition), so $x\leqslant z$: the transitivity holds. Finally, Given $x,y\in\mathbb{Z}$ such that $x\leqslant y$ and $y\leqslant x$: $a=y-x$ and $b=x-y$ are two elements of $\mathbb{N}$ of nonzero sum, they are both nonzero. Thus, $x=y$, hence the antisymmetry. We have thus defined an order relation on $\mathbb{Z}$.
In the above theorem about the order relation on $\mathbb{Z}$, the properties (1) to (6) are immediate. Let's prove (8). Thus, given a nonempty part A of $\mathbb{Z}$ and m a lower bound (minorant) of A. $\forall a\in A$, we have a $m\leqslant a$, i.e., $a-m\in\mathbb{N}$. Set: $B:=\{a-m|a\in A\}$. This is a nonempty part of $\mathbb{N}$, i.e. $b_0:=\min(B)$. Since $b_0\in B$, there is an element a_0 of A such that $b_0=a_0-m$. Then, given $a\in A$. $a-m\in B$ (by definition of B), so $b_0\leqslant a-m$. The property (4) gives $b_0+m\leqslant(a-m)+m=a$, i.e. $a_0\leqslant a$. Thus a_0 is the smallest element of A. The property (7) is deduced from (8) via the bijection $x\mapsto-x$ from $\mathbb{Z}$ to $\mathbb{Z}$ (check it).
The reader can check that $\mathbb{Z}$ has no smallest element nor greatest element; especially, the property (N1) of $\mathbb{N}$ does not hold in $\mathbb{Z}$.

4.2. Subgroups of $\mathbb{Z}$, divisibility in $\mathbb{Z}$. Euclidean division in $\mathbb{N}$ extends easily to $\mathbb{Z}$. Here is the analogue of "euclidean division" theorem (in heading "*Euclidean division, numeration*"):

Th. 73. *(Euclidean division in $\mathbb{Z}$). Given $a,b\in\mathbb{Z}$, with $b>0$. Given $q,r\in\mathbb{Z}$. There exists a unique pair of integers (q,r) verifying the following conditions:*
(D1) : $a=bq+r$, *and*
(D2) : $0\leqslant r\leqslant b$.
The integers q,r are respectively called quotient and remainder of the division of a by b, we denote them "a div b" and "a mod b", respectively.

Proof. Let's show the existence of (q,r). The initial "euclidean division" theorem (in heading "*Euclidean division, numeration*") guarantees the existence if $a\geqslant0$. Thus assume $a<0$. Then $-a\in\mathbb{N}$, so there is $(q',r')\in\mathbb{N}^2$ such that $-a=bq'+r'$ and $0\leqslant r'\leqslant b$. If $r'=0$, it suffices to take $q:=-q'$, $r:=0$. If $r'>0$, we take $r:=b-r'$ and $q:=-q'-1$. Assume $bq+r=a=bq'+r'$, where q,r,q',r' are integers and $0\leqslant r$, $r'<b$. If (for example) $r'\leqslant r$, we have $0\leqslant b(q'-q)=r-r'<b$ and so $0\leqslant q'-q<1$. Thus $q=q'$, hence $r=r'$. □

Like in $\mathbb{N}$, given two integers a,b we say that a *divides* b, or that b *is a multiple of* a, if there is an integers c such that $b=ac$ (denoted $a|b$). If moreover $b\neq0$, we have $|a|\leqslant|b|$. Note that 1 has two divisors: 1 and -1. Given $n\in\mathbb{Z}$, the set of multiples of n is denoted by $n\mathbb{Z}$:
$$n\mathbb{Z}:=\{kn|k\in\mathbb{Z}\}.$$
If $n\in\mathbb{Z}$ is nonzero, $k\mapsto kn$ is a bijection from $\mathbb{Z}$ to $n\mathbb{Z}$. (Note that $0\mathbb{Z}=\{0\}$.)

Prop.10 *Given $a,b\in\mathbb{Z}$, a divides b if and only if $b\mathbb{Z}\subset a\mathbb{Z}$. Moreover, $a\mathbb{Z}=b\mathbb{Z}$ if and only if $a=\pm b$.*

Proof. If $a|b$, given $c\in\mathbb{Z}$ such that $b=ca$. $\forall k\in\mathbb{Z}$, $kb=(kc)a\in a\mathbb{Z}$, hence $b\mathbb{Z}\subset a\mathbb{Z}$. If $b\mathbb{Z}\subset a\mathbb{Z}$, especially $b=b\times1\in a\mathbb{Z}$. Therefore there is an integer k such that $b=ka$, so $a|b$. This proves the first equivalence. The other is left to the reader. □

The "parts $n\mathbb{Z}$ of $\mathbb{Z}$" can be defined as follows:

Def. 213. *(Subgroup of $\mathbb{Z}$). A part Φ of $\mathbb{Z}$ is called (additive) subgroup of $\mathbb{Z}$ if the following conditions hold:*
(1) *It is nonempty.*
(2) *It is additively stable: the sum of two arbitrary elements of Φ belongs to Φ.*
(3) *The opposite of any element of Φ also belongs to Φ.*

Th. 74. (♮). (i) *For any integer n, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.* (ii) *Conversely, let Φ be a subgroup of $\mathbb{Z}$. There exists a unique integer $n\geqslant0$ such that $\Phi=n\mathbb{Z}$.*

Proof. The statement (i) is immediate. For (ii), let Φ a subgroup of $\mathbb{Z}$. It includes 0: indeed, given $a\in\Phi$. According to the property (3), $-a\in\Phi$, so $0=a+(-a)\in\Phi$ (property (2)). If $\Phi=\{0\}$, we only need to take $n:=0$. Otherwise, given $b\in\Phi$, $b\neq0$. We can assume $b>0$ (even if we may need to replace b by $-b$, which also belongs to Φ). Thus $\Phi\cap\mathbb{N}^*$ is a nonempty part of $\mathbb{N}^*$, it has a smallest element n. Let's show that $\Phi=n\mathbb{Z}$. Clearly, we have the inclusion $n\mathbb{Z}\subset\Phi$:

given $k \in \mathbb{Z}$. If $k = 0$, $kn = 0 \in \Phi$. If $k > 0$, $kn = n + n + \cdots + n$ belongs to Φ (repeatedly applying the stability of Φ by addition). If $k < 0$, kn is the opposite of $(-k)n$, which belongs to Φ (case above), so $kn \in \Phi$ (property (3)). The reverse inclusion $\Phi \subset n\mathbb{Z}$ comes from the "Euclidean division in $\mathbb{Z}$" theorem, Indeed, given $a \in \Phi$. Perform the euclidiean division of a by n : $a = nq + r$, where $q, r \in \mathbb{Z}$ and $0 \leqslant r < n$. First $nq \in n\mathbb{Z} \subset \Phi$, and $a \in \Phi$, so $r = a - qn \in \Phi$ (properties (2),(3)). Note that if r is nonzero, it belongs to $\Phi \cap \mathbb{N}^*$, and we have then $n = \min(\Phi \cap \mathbb{N}^*) \leqslant r$, which is false. Therefore $r = 0$, hence $a = nq \in n\mathbb{Z}$. □

Def. 214. *Let A, B be two parts of $\mathbb{Z}$. We call sum of A and B, the set of integers of the form $a + b$, where $a \in A$ and $b \in B$.*

Such a sum is associative and commutative.

Prop.11 *The sum of two subgroups of $\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.*

Proof. Let Φ, Φ' be two subgroups of $\mathbb{Z}$. First, $0 \in \Phi$ and $0 \in \Phi'$, so $0 = 0 + 0 \in \Phi + \Phi'$. Given $x \in \Phi + \Phi'$. There is $(a, a') \in \Phi \times \Phi'$ such that $x = a + a'$. Then $-x = (-a) + (-a') \in \Phi + \Phi'$, since $-a \in \Phi$ (property (3)) and likewise $-a' \in \Phi'$. The stability by addition of $\Phi + \Phi'$ is immediate. □

Note that $\Phi + \Phi'$ contains Φ (and Φ'): if $x \in \Phi$, $x = x + 0 \in \Phi + \Phi'$ since $0 \in \Phi'$. Conversely, every subgroup S of $\mathbb{Z}$ containing Φ and Φ' contains $\Phi + \Phi'$. Indeed, given $x \in \Phi + \Phi' : x = a + a'$, where $a \in \Phi$, $a' \in \Phi'$. Then a and a' belong to S, which is stable by addition, so $x = a + a' \in S$:

Property: *In the sense of the inclusion, the sum $\Phi + \Phi'$ is the smallest subgroup of $\mathbb{Z}$ containing Φ and Φ'.*

Th. 75. *(Greatest common divisor in $\mathbb{Z}$). For arbitrary $a, b \in \mathbb{Z}$.*
(1) *There exists a unique integer $d \geqslant 0$ such that $a\mathbb{Z} + b\mathbb{Z}$ is equal to $d\mathbb{Z}$.*
(2) *The integer d divides a and b. Conversely, any common divisor to a and b divides d.*
(3) *There exist two integers u, v verifying the following Bézout's identity: $au + bv = d$.*
(4) *If $a, b \in \mathbb{N}^*$, d is the* gcd *of a and b in the sense of the "Greatest common divisor" theorem stated in the heading "GCD, LCM, Euclid algorithm".*

Proof. (1) follows from the previous proposition and from theorem (♮). Then, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, then $d|a$, and $d|b$. Let λ be a common divisor to a and b. Thus, $\lambda\mathbb{Z}$ contains $a\mathbb{Z}$ and $b\mathbb{Z}$, and thus also their sum $d\mathbb{Z}$, that is, $\lambda|d$: hence (2). Since $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, d is the sum of an element of $a\mathbb{Z}$ and of an element of $b\mathbb{Z}$, hence (3). Finally, assume $a, b > 0$. First, $d > 0$ (since $a\mathbb{Z} + b\mathbb{Z} \neq \{0\}$). Then, there is $c \in \mathbb{Z}$ such that $a = cd$, hence $c > 0$, so that we have $d|a$ in $\mathbb{N}$, similarly, $d|b$ in $\mathbb{N}$. Let h be a common divisor to a and b in $\mathbb{N}$. Fom (2), h divides d in $\mathbb{Z}$, so in $\mathbb{N}$ (note the signs). Thus, (4) follows from the "Greatest common divisor" theorem (in heading "*GCD, LCM, Euclid algorithm*"). □

Given (4), we have the following definition:

Def. 215. *Let a, b be two arbitrary integers. We call greatest common divisor (or* gcd*) of a and b, the unique integer $d \geqslant 0$ such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, denoted here by $a \wedge b$. We say that a and b are relatively prime if $a \wedge b = 1$.*

Thus, $a \wedge b$ is characterized by the following property:

Property: *$a \wedge b \geqslant 0$ and $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.*

Note that, if $a \in \mathbb{Z}$, the gcd of 0 and a is $|a|$. Now, we can state three fundamental theorems:

Th. 76. (Bézout th.). *In order that two integers a and b are relatively prime, it is necessary and sufficient that there exist two integers u, v such that $au + bv = 1$.*

Proof. If $a \wedge b = 1$, the statement (3) of the previous "greatest common divisor in $\mathbb{Z}$" theorem gives the existence of two integers u, v such that $au + bv = 1$. Conversely, assume there exist $u, v \in \mathbb{Z}$ such that $au + bv = 1$, and given $d := a \wedge b$. Then $d|au$ and $d|bv$, so d divides $1 = au + bv$. Since $d \geqslant 0$, we necessarily have $d = 1$. □

Th. 77. (Gauss th.). *Given $a, b, c \in \mathbb{Z}$. If a divides a and bc and is relatively prime to b, it divides c.*

Proof. Since $a \wedge b = 1$, $\exists u \in \mathbb{Z}, \exists v \in \mathbb{Z}$ such that $au + bv = 1$. Moreover, $a|a(cu)$, $a|v(bc)$ (since $a|bc$), so $a|a(cu)+v(bc)=c(au+bv)=c$. □

Th. 78. (Euclid lemma). *If a prime number divides the product of two integers $a, b \in \mathbb{Z}$, it divides (at least) one of the two integers.*

Proof. Fix p prime, assume that p divides a product ab ($a, b \in \mathbb{Z}$). Assume: "p does not divide b", and show that p divides c. Given $d{:=}p \wedge b$. Then $d{>}0$, and d divides p in $\mathbb{N}$, so d is equal to 1 or p, since p is prime. We exclude $d{=}p$, indeed $d{=}p \Rightarrow$"p divides b", contracting the assumption. Thus, $d{=}1$, i.e. p is relatively prime to b. Gauss theorem allows to conclude. □

The above proofs are quite simple. In $\mathbb{Z}$, the Euclid lemma results from the Gauss theorem, while in $\mathbb{N}$ it was the reverse.
Given $a_1, .., a_n \in \mathbb{Z}$ (with $n \geqslant 3$). The definition of their gcd is easy: it is the unique integer $d \geqslant 0$ such that $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$. The associativity of the sum (addition) of subgroups of $\mathbb{Z}$ implies the associativity of the operation gcd. Like in $\mathbb{N}$, the concept "relatively prime" differs from that of "pairwise relatively prime".

Prop.12 *Let $a_1, .., a_n$* (with $n \geqslant 2$) *be integers, not all zero, and d their* gcd. *For $i = 1, .., n$, let us set $a_i = db_i$, where $b_i \in \mathbb{Z}$ (d divides a_i). Then $b_1, .., b_n$ are relatively prime.*

Proof. Clearly, $d \neq 0$. Given $h \geqslant 0$ the gcd of the b_i. Thus, $\forall i$, hd divides a_i. Thus, hd is a common divisor to the a_i, and it follows $hd|d$. Since $d \neq 0$, h divides 1, that is, $h = \pm 1$, and $h = 1$ since $h \geqslant 0$. □

Exer. 8. *Consider the following problem. Given $a, b \in \mathbb{Z}$ and $d := a \wedge b$. There exist two integers u, v (Bézout's coefficients) such that $au + bu = d$. We wonder how to find such a pair (u, v). We already have seen (*Ex.(A) *in heading "GCD, LCM, Euclid algorithm") that the* gcd *of* 9000 *and* 1575 *is* 225. *Now, we search for a solution (u, v) of the equation*

$$(*) \qquad 9000u + 1575v = 225$$

*with $(u, v) \in \mathbb{Z}$. The Euclid algorithm (*Exerc.(B) *in heading "GCD, LCM, Euclid algorithm") gives: $225 = 1125 - 2 \times 450$, $450 = 1575 - 1 \times 1125$, $1125 = 9000 - 5 \times 1575$, hence $225 = 1125 - 2(1575 - 1 \times 1125) = 3 \times 1125 - 2 \times 1575 = 3(9000 - 5 \times 1575) - 2 \times 1575 = 3 \times 9000 - 17 \times 1575$. The solution of $(*)$ is $(3, -17)$.*

The above is related to the resolution of certain equations of the first degree with integer coefficients. Formally, we have the statement:

Prop.13 *Let $a, b, c \in \mathbb{Z}$ be integers* (with a and b nonzero), *and $d \geqslant 1$ the* gcd *of a and b.* Let's set $a = da'$, $b = db'$, *where $a', b' \in \mathbb{Z}$. Now, let's consider the identity:*

$$(**) \qquad ax + by = c.$$

(1) *$(**)$ has a solution $(x, y) \in \mathbb{Z}^2$ iff $d|c$.*
(2) *If $(**)$ has a solution $(x_0, y_0) \in \mathbb{Z}^2$, its other solutions are given by $(x, y) = (x_0 + kb', y_0 - ka')$, with arbitrary $k \in \mathbb{Z}$.*

Proof. Given a solution $(x, y) \in \mathbb{Z}^2$ of $(**)$. We have then $d|c$, since $c = ax + by = dd(a'x + b'y)$. Conversely, assume $c = dc'$, where $c' \in \mathbb{Z}$. There exists $(u, v) \in \mathbb{Z}^2$ such that $au + bv = d$, hence $c = c'd = a(c'u) + b(c'v)$. Thus $(c'u, c'v) \in \mathbb{Z}^2$ verifies $(**)$, hence the statement (1). About (2), consider first $k \in \mathbb{Z}$. Since $ab' = da'b' = ba'$, it follows: $a(x_0 + kb') + b(y_0 - ka') = (ax_0 + by_0) + k(ab' - ba') = ax_0 + by_0 = c$, so $(x_0 + kb', y_0 - ka') \in \mathbb{Z}^2$ is solution of $(**)$. Conversely, given a solution $(x, y) \in \mathbb{Z}^2$ of $(**)$: $ax + by = c = ax_0 + by_0$, hence $a(x - x_0) = b(y_0 - y)$, i.e., $da'(x - x_0) = db'(y_0 - y)$, or $a'(x - x_0) = b'(y_0 - y)$, since d is nonzero. Since $a' \wedge b' = 1$, b' divides $x - x_0$ (Gauss th.): $\exists k \in \mathbb{Z}$, such that $x - x_0 = kb'$, i.e. $x = x_0 + kb'$. Then $b'(y_0 - y) = a'(x - x_0) = ka'b'$, so $y = y_0 - ka'$, or $y_0 - y = ka'$. The sought result is $(x, y) = (x_0 + kb', y_0 - ka')$. □

Now, consider the lcm. Let Φ and Φ' be two subgroups of $\mathbb{Z}$. Clearly, $\Phi \cap \Phi'$ is a subgroup of $\mathbb{Z}$. We infer then the following theorem (and definition):

Th. 79. *(Least common multiple in $\mathbb{Z}$). Given two arbitrary $a, b \in \mathbb{Z}$.*
(1) *There is a unique integer $m \geqslant 0$ such that $a\mathbb{Z} \cap b\mathbb{Z}$ is equal to $m\mathbb{Z}$. This integer is called* lcm *of a and b.*
(2) *The integer m is a multiple of a and b. Conversely, any common multiple of a and b is a multiple of m.*
(3) *Given $a, b \in \mathbb{N}^*$, m is* lcm *of a and b in the sense of the "least common multiple" theorem stated in the heading "GCD, LCM, Euclid algorithm".*

This statement can easily be generalized to n arbitrary elements of $\mathbb{Z}$ for $n \geqslant 2$.

5. Rational Numbers $\mathbb{Q}$

The inverse operation of the multiplication in $\mathbb{Z}$ (i.e. the division) is not always defined (e.g. $\frac{2}{3}$ does not make sense in $\mathbb{Z}$); the rational numbers overcomes this defect. The set $\mathbb{Q}$ contains $\mathbb{Z}$, and its elements are called *rational numbers*. Let's set: $\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}$. To every pair

$(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$ corresponds a rational number written in the form of a *fraction* $\frac{a}{b}$, and every rational number is written in the same way (e.g. if $a\in\mathbb{Z}^*$, $a=\frac{a}{1}$). Such a writing is not unique, let's consider:

Property A *If $a,c\in\mathbb{Z}$ and $b,d\in\mathbb{Z}^*$, $(\frac{a}{b}=\frac{c}{d})\Leftrightarrow(ad=bc)$.*

The addition in $\mathbb{Q}$ is a map $(x,y)\mapsto x+y$ from $\mathbb{Q}\times\mathbb{Q}$ to $\mathbb{Q}$. (Recall: "$\mathbb{Q}$ *contains* $\mathbb{Z}$.") The main properties of the addition in $\mathbb{Q}$ are given in the following proposition:

Prop.14 *The addition in $\mathbb{Q}$ has the properties:*
(1) *It is associative and commutative.*
(2) *For any $u\in\mathbb{Q}$, $0+u=u$.*
(3) *If $a,c\in\mathbb{Z}$ and $b,d\in\mathbb{Z}^*$, we have $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$.*
(4) *Given $u\in\mathbb{Q}$. There is a unique $u'\in\mathbb{Q}$ such that $u+u'=0$. It is denoted by $-u$ and called opposite of u. If $u=\frac{a}{b}$ $(a\in\mathbb{Z},b\in\mathbb{Z}^*)$, we have $-u=\frac{-a}{b}$.*
(5) *The addition in $\mathbb{Q}$ extends that of $\mathbb{Z}$: if $x,y\in\mathbb{Z}$, the sum $x+y$ is the same, whether calculated in $\mathbb{Z}$ or in $\mathbb{Q}$.*
(6) (Regularity): *$\forall x,y,z\in\mathbb{Q}$, $x+z=y+z$ implies $x=y$.*

Thus, $\mathbb{Q}$ *provided with the addition is a commutative group.* The subtraction can be defined similarly.

The multiplication in $\mathbb{Q}$ is a map $(x,y)\mapsto xy=x\times y$ from $\mathbb{Q}\times\mathbb{Q}$ to $\mathbb{Q}$. The main properties of the addition in $\mathbb{Q}$ are given below:

Prop.14 *The multiplication in $\mathbb{Q}$ has the properties:*
(1) *It is associative and commutative.*
(2) *It is distributive with respect to the addition: $a(b+c)=ab+ac$* for all $a,b,c\in\mathbb{Q}$.
(3) *For any $u\in\mathbb{Q}$, $1\times u=u$.*
(4) *If $a,c\in\mathbb{Z}$, and $b,d\in\mathbb{Z}^*$, we have: $\frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}$.*
(5) *The multiplication in $\mathbb{Q}$ extends that of $\mathbb{Z}$: if $x,y\in\mathbb{Z}$, the product xy is the same, whether calculated in $\mathbb{Z}$ or in $\mathbb{Q}$.*
(6) *Let $u\in\mathbb{Q}^*$. There is a unique $u'\in\mathbb{Q}^*$, called inverse of u, such that $uu'=1$. It is also denoted by u^{-1} or $\frac{1}{u}$. If $u=\frac{a}{b}$ $(a,b\in\mathbb{Z}^*)$, $u^{-1}=\frac{b}{a}$.*
(7) (Regularity): *For any $x,y,z\in\mathbb{Q}$. If $xz=yz$ and if $z\neq 0$, then $x=y$.*

The property (6) is the most important. $\mathbb{Q}^*$ *provided with the multiplication is a commutative group.* $\mathbb{Q}$ *provided with the laws $+$ and $\times$ is a commutative field.* The definition of the division starting from the multiplication results from the following property:

Property B *Let $h\in\mathbb{Q}$, $u\in\mathbb{Q}^*$. The identity $ux=h$ has a unique solution $x\in\mathbb{Q}$, called quotient of h by u and denoted by $\frac{h}{u}$, or h/u, or also hu^{-1}. If $h=\frac{a}{b}$ and $u=\frac{c}{d}$, where $a\in\mathbb{Z}$ and $b,c,d\in\mathbb{Z}^*$, we have $\frac{h}{u}=\frac{ad}{bc}$.*

Main properties of the *order relation* on $\mathbb{Q}$ are:

Th. 80. *The order relation on $\mathbb{Q}$ has the properties:*
(1) *It is total: if $x,y\in\mathbb{Q}$ we have either $x\leqslant y$ or $y\leqslant x$.*
(2) *It extends that of $\mathbb{Z}$: if $x,y\in\mathbb{Z}$, $x\leqslant y$ has the same meaning in $\mathbb{Z}$ and in $\mathbb{Q}$.*
(3) *It is compatible with the addition: if $x,x',y,y'\in\mathbb{Q}$ and if $x\leqslant x'$ and $y\leqslant y'$, we have: $x+y\leqslant x'+y'$.*
(4) *For two arbitrary elements $x,y\in\mathbb{Q}$, $(x\leqslant y)\Leftrightarrow(-y\leqslant -x)$.*
(5) *Given $u,x,y\in\mathbb{Q}$. If $u>0$, $(x\leqslant y)\Leftrightarrow(ux\leqslant uy)$ and $(x<y)\Leftrightarrow(ux<uy)$. If (by contrast) $u<0$, $(x\leqslant y)(ux\geqslant uy)$ and $(x<y)\Leftrightarrow(ux>uy)$.*
(6) *The "sign rule" hold: if $x,y\in\mathbb{Q}^*$, each of numbers xy, $\frac{x}{y}$ is strictly positive if x,y are of the same sign and strictly negative ortherwise.*

Using intervals, it is necessary to specify if it is an interval in $\mathbb{Z}$ or in $\mathbb{Q}$ or in $\mathbb{R}$.
The order relation on $\mathbb{Q}$ is much more complex than that of $\mathbb{Z}$. Indeed, consider the following theorem and especially its first statement.

Th. 81. (1) *Given $a,b\in\mathbb{Q}$ such that $a<b$. The interval $]a,b[$ is infinite. It is bounded from above and from below, and it has no maximum element nor minimum element.* (2) *Given $a,b\in\mathbb{Q}$, $b>0$. There is an integer $n\in\mathbb{N}$ such that $nb>a$ (Archimedean property).*

Proof. Note first that the interval $]a,b[$ is nonempty: it contains $\frac{a+b}{2}$ (while in $\mathbb{Z}$, $]0,1[$ is empty). If $]a,b[$ was finite, it would have a maximum element c, since the order of $\mathbb{Q}$ is total. This is absurd, since $a<c<\frac{b+c}{2}<b$. Likewise, $]a,b[$ has no minimum element, hence (1). For (2), the conclude is simple if $a\leqslant 0: n:=0$ is appropriate. Now, assume $a>0$. Let's set: $a=\frac{r}{c}$ and $b=\frac{s}{c}$, where $r,s\in\mathbb{Z}$ and $c\in\mathbb{Z}^*$ (reduce to the same denominator). We can assume (even if we potentially have to change the sign of c) $c>0$, hence $r>0$ since $a,b>0$. With the Archimedean property in $\mathbb{N}$, there is a $n\in\mathbb{N}^*$ such that $ns>r$, hence (2). □

Let us sketch the construction of $\mathbb{Q}$, then, the addition, the multiplication, and the order relation on $\mathbb{Q}$. The ways to do are similar to those of $\mathbb{Z}$. The set $\mathbb{Z}^*$ of nonzero integers is *stable by the multiplication*: the pproduct of two nonzero integers is nonzero. Define on the set $\mathbb{Z}\times\mathbb{Z}^*$ a relation, denoted by $\sim$, as follows: $(a,b)\sim(c,d)$ if $ad=bc$. This is an equivalence relation on $\mathbb{Z}\times\mathbb{Z}^*$ (the reader can check it). By definition, the set $\mathbb{Q}$ is the quotient of $\mathbb{Z}\times\mathbb{Z}^*$ by the relation $\sim$, and the elements of $\mathbb{Q}$ are called *rational numbers.* The class of a pair $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$ will be denoted by $\frac{a}{b}$, it'll play (later) the role of "quotient" of a by b. The map $(a,b)\mapsto\frac{a}{b}$ from $\mathbb{Z}\times\mathbb{Z}^*$ to its quotient $\mathbb{Q}$ is *surjective.* By definition, the property A is true (see beginning of section).
.We wonder how to define the addition and the multiplication in $\mathbb{Q}$. Let u,u' be two rational numbers, represented by $\frac{a}{b},\frac{a'}{b'}$ respectively $(a,a'\in\mathbb{Z},\ b,b'\in\mathbb{Z}^*)$. Let us set: $u+u':=\frac{a}{b}+\frac{a'}{b'}=\frac{ab'+a'b}{bb'}$ and $uu':=\frac{a}{b}\times\frac{a'}{b'}=\frac{aa'}{bb'}$. These formulas are valid whatever the choice of the representative $\frac{a}{b}$ (resp. $\frac{a'}{b'}$) of u (resp. u). It follows: a *addition*: $+:\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ and a *miltiplication*: $\times:\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$.
.We wonder what becomes $\mathbb{Z}$ in this construction. The map $a\mapsto\frac{a}{1}$ from $\mathbb{Z}$ to $\mathbb{Q}$ is injective: if $a,a'\in\mathbb{Z}$, and if $\frac{a}{1}=\frac{a'}{1}$, we have $(a,1)\sim(a',1)$, that is, $a=a'$. Theferore we identify each $a\in\mathbb{Z}$ with $\frac{a}{1}\in\mathbb{Q}$, and *henceforth $\mathbb{Z}$ can be considered as "part" of $\mathbb{Q}$.* In particular, 0 and 1 are identified with $\frac{0}{1}$ and $\frac{1}{1}$, respectively.
.*Proofs* of **prop.14** and **prop.15** consist of many *but trivial* checks; it is interesting to perform these checks to become familiar with the use of the relation $\sim$.

Ex. 89. *As an example, if $a\in\mathbb{Z}$, $b\in\mathbb{Z}^*$ we have: $\frac{a}{b}+\frac{-a}{b}=\frac{ab+b(-a)}{b^2}=\frac{0}{b^2}=\frac{0}{1}=0$ and $\frac{a}{b}\times\frac{b}{a}=\frac{ab}{ba}=\frac{1}{1}=1$.*

The *definition* of the order relation of $\mathbb{Q}$ is tricker. First, given $x\in\mathbb{Q}$. We say that x is positive $(x\geqslant 0)$ if it written $x=\frac{a}{b}$, where $a\in\mathbb{Z}$, $b\in\mathbb{Z}^*$, and $ab\geqslant 0$. In this case, if $x=\frac{c}{d}$ where $c\in\mathbb{Z}$, $d\in\mathbb{Z}^*$, we have $ad=bc$, hence $(ab)(cd)=a^2d^2\geqslant 0$ and it follows $cd\geqslant 0$. Thus the fact that x is positive applies to *any* representative of x. Set: $\mathbb{Q}_+:=\{x\in\mathbb{Q}|x\geqslant 0\}$, and $\mathbb{Q}_+^*:=\{x\in\mathbb{Q}|x>0\}$. We can easily check that $\mathbb{Q}_+$ is stable by the addition and multiplication: if $x,y\in\mathbb{Q}_+$, we have $x+y\in\mathbb{Q}_+$ and $xy\in\mathbb{Q}_+$. Moreover, $\forall x\in\mathbb{Q}^*$, we have either $x\in\mathbb{Q}_+^*$ or $-x\in\mathbb{Q}_+^*$, and these two options are mutually incompatible (the reader can check).
Now, consider $x,y\in\mathbb{Q}$. We say that $x\leqslant y$ if $y-x\in\mathbb{Q}_+$ (this is correct since $x\geqslant 0$ iff $x\in\mathbb{Q}_+$). It follows that we get thus an *order relation* on $\mathbb{Q}$ The statements of the previous theorem on "*the order relation on* $\mathbb{Q}$" can easily be checked and are trivial (left to the reader).

Ex. 90. *As an example, given $x,y\in\mathbb{Q}$, assume $x>0$, $y<0$. Then we can write: $x=\frac{a}{b}$, $y=\frac{c}{d}$, where $a,b,c,d\in\mathbb{Z}^*$ and $ab>0$, $cd<0$. We have $xy=\frac{ac}{bd}<0$ since $(ac)(bd)=(ab)(cd)<0$ (in $\mathbb{Z}$).*

Let us consider other properties of $\mathbb{Q}$.

Prop.15 *The set $\mathbb{Q}$ is denumerable.*

Proof. The map $(a,b)\mapsto\frac{a}{b}$ from $\mathbb{Z}\times\mathbb{Z}^*$ to $\mathbb{Q}$ is surjective and $\mathbb{Z}\times\mathbb{Z}^*$ is denumerable (countable) since $\mathbb{Z}$ is denumerable. Thus $\mathbb{Q}$ is finite or denumerable (cf. last th. in heading: "*Finite sets, denumerable sets*"): but $\mathbb{Q}$ is not finite since it contains $\mathbb{Z}$. □

The following statements show how the *arithmetic* (which concerns the integers) can be involved in *real numbers.* First, recall the important notion of *integer part,* denoted $\mathrm{Int}(x)$, or $[x]$. Here is a theorem (also taken as definition) about the *integer part*:

Th. 82. *(Integer part). Let x be a rational number.*
(1) *There exists an integer $n\in\mathbb{Z}$ such that $n\leqslant x<n+1$. This integer is called integer part of x, denoted* $\mathrm{Int}(x)$, *or* $[x]$. *Thus:*
$$\mathrm{Int}(x)\leqslant x<\mathrm{Int}(x)+1 \text{ and } \mathrm{Int}(x)\in\mathbb{Z},$$
and these properties characterize $\mathrm{Int}(x)$.
(2) *Write x in the form $x=\frac{a}{b}$ $(b\in\mathbb{N}^*,a\in\mathbb{Z})$. Then* $\mathrm{Int}(x)$ *is the quotient in the euclidean division of a by b.*

Proof. If x is expressed in the form $\frac{a}{b}$, perform the euclidean division of a by b: $a=bq+r$, where $q,r\in\mathbb{Z}$, $0\leqslant r<b$. Then $bq\leqslant bq+r\leqslant b(q+1)$ hence, dividing by $b: q\leqslant x<q+1$. The integer q is the only one for which such a bounding is true. Indeed, consider another integer q' such that $q'\leqslant x<q'+1$. Then $q\leqslant x<q'+1$, so $q-q'\leqslant 0$, *because $q-q'$ is an integer.* Symmetrically, $q'-q\leqslant 0$, hence $q=q'$. Proving (1) and (2) at the same time. □

Thus $\mathrm{Int}(\frac{13}{5})=2$, while $\mathrm{Int}(-\frac{13}{5})=-3$ (check it).
Actually, the integer part of a real number is the part of the number that appears before the decimal point. (For example, the integer part of π is 3, and the integer part of $-\sqrt{2}$ is -1.) More precisely, for $x\in\mathbb{R}$, the integer part of x, that we can denote $[x]$, is given by $[x]=\begin{cases}\lfloor x\rfloor & \text{if } x\geqslant 0\\ \lceil x\rceil & \text{if } x<0\end{cases}$, where $\lfloor x\rfloor$ and $\lceil x\rceil$ denote the *floor* and *ceiling* of x, respectively.

.The *floor* of a real number is the greatest integer less than or equal to the number. The floor of x is usually denoted by $\lfloor x \rfloor$. Also known as *floor function.*

.The *ceiling* of a real number is the smallest integer greater than or equal to the number. The ceiling of x is usually denoted by $\lceil x \rceil$. Also known as *ceiling function. (*Some examples: $\lceil 6.2 \rceil = 7$, $\lceil 0.4 \rceil = 1$, $\lceil 7 \rceil = 7$, $\lceil -5.1 \rceil = -5$, $\lceil \pi \rceil = 4$, $\lceil -4 \rceil = -4$. Note that this function is not the integer part ($\lfloor x \rfloor$), since $\lceil 3.5 \rceil = 4$ and $\lfloor 3.5 \rfloor = 3$.

Exer. 9. *Given two rational numbers a, b such that $b - a > 1$. Prove that the interval $]a, b[$ contains at least an integer. Solution: If b is integer, $b-1$ is appropriate. Otherwise, $m := \mathrm{Int}(b)$. By definition of the integer part, $m > b - 1 > a$, hence $m \in]a, b[$, and m is integer. In both cases, $-\mathrm{Int}(-b) - 1$ is appropriate.*

Rem. 35. *Let a, b be two integers with b nonzero. In order that b divides a (in $\mathbb{Z}$), it is necessary and it suffices that the rational number $\frac{a}{b}$ is integer. It is necessary, since if $b|a$, $a = \lambda b$ where $\lambda \in \mathbb{Z}$, and $\frac{a}{b} = \frac{\lambda}{1} = \lambda \in \mathbb{Z}$. Conversely, if $\frac{a}{b} = \gamma \in \mathbb{Z}$, then $a = \gamma b$, so b divides a.*

Th. 83. *(Irreducible form of a rational number). Let x be a rational number. There exists a unique pair of integers $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ such that*
- *The number x is equal to $\frac{a}{b}$.*
- *The integers a and b are relatively prime.*

Then we say that $x = \frac{a}{b}$ is the irreducible form of x. The other representatives of x are the $\frac{\lambda a}{\lambda b}$, where λ is an arbitrary nonzero integer.

Proof. Let's prove the existence of a pair (a, b) having the required properties. In any case there exist integers $h \in \mathbb{Z}$ and $u \in \mathbb{N}^*$ such that $x = \frac{h}{u}$ (if needed, after having change the sign of numerator and denominator). Given $d := h \wedge u$; set: $h = da$ and $u = db$, where $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Recall that $a \wedge b = 1$ (cf. **prop.12** in heading "*Subgroups of $\mathbb{Z}$, divisibility in $\mathbb{Z}$*"). In addition, $x = \frac{h}{u} = \frac{da}{db} = \frac{a}{b}$: the pair (a, b) is appropriate. Given $(a', b') \in \mathbb{Z} \times \mathbb{N}^*$ is another pair representating $x : x = \frac{a'}{b'} = \frac{a}{b}$. Thus, $ab' = a'b$. Since $a \wedge b = 1$ and $a|a'b$, the Gauss theorem shows that $a|a'$. Thus given $\lambda \in \mathbb{Z}$ such that $a' = \lambda a$. It follows $ab' = a'b = \lambda ab$, so $b' = \lambda b$. Proving the last statement of the theorem. Finally, assume that we also have $a' \wedge b' = 1$ and $b' > 0$. With above notations, λ is necessarily 1, hence $(a', b') = (a, b)$. □

Ex. 91. *Consider the case $1575 \wedge 9000 = 225$. Since $1575 = 7 \times 225$ and $9000 = 40 \times 225$, the irreducible form of $\frac{1575}{9000}$ is $\frac{7}{40}$.*

Moreover, consider a prime number p, and the real numbers; the following proposition shows that $\sqrt{p}$ is an *irrational number*:

Prop.16 *Prime number p is never the square of a rational number.*

Proof. Reductio ad absurdum (proof by contradiction): Assume $p = x^2$ with $x \in \mathbb{Q}$. Given $\frac{a}{b}$ the irreducible form of x. Then $p = (\frac{a}{b})^2$. From $a \wedge b = 1$, it follows that $a^2 \wedge b^2 = 1$ (the reader can check it in several ways). Thus $\frac{a^2}{b^2}$ is an irreducible form of p. But $p = \frac{p}{1}$ is also an irreducible form, so $b = 1$ and $p = a^2$. This is absurd, since a would be divisor of p different from 1 and p. □

Finally, recall the definition of the absolute value of a rational number.

Def. 216. *(Absolute value of rational number). We call absolute value of a rational number x, the number $|x| := \max(x, -x)$. Thus, $|x| = x$ if $x \geqslant 0$, otherwise $|x| = -x$.*

Recall the following properties (which will extend to real numbers):
- For any $x \in \mathbb{Q}$, $-|x| \leqslant x \leqslant |x|$ and $(|x|=0) \Leftrightarrow (x=0)$.
- For all $x, y \in \mathbb{Q}$, $|xy| = |x|\,|y|$.
- For all $x, y \in \mathbb{Q}$, $|x+y| \leqslant |x|+|y|$ (triangular inequality).
- For all $x, y \in \mathbb{Q}$, $|x - y| \geqslant ||x| - |y||$.

The last property follows from the triangular inequality as follows: The identity $x = (x-y)+y$ gives $|x| \leqslant |x-y|+|y|$, hence $|x-y| \geqslant |x|-|y|$. Swapping x and y, $|x-y| \geqslant |y|-|x|$. Then we have $|x-y| \geqslant \max(|x|-|y|, |y|-|x|) = ||x|-|y||$.

6. A General Exercise

Exer. 10. *Consider the following three natural numbers $m, p, q \in \mathbb{N}$, with $m \leqslant \min(p, q)$. Prove the following expression: $\sum_{\lambda=0}^{m} \binom{p}{\lambda}\binom{q}{m-\lambda} = \binom{p+q}{m}$. Take a set E with $p+q$ elements, divide it into two parts of respective cardinals p and q. Count the parts with m elements of E. We wonder how to modify the above expression by replacing the assumption $m \leqslant \min(p, q)$ by a weaker assumption $m \leqslant p+q$. Moreover, let n be an integer. Compute the sum $\sum_{p=0}^{n} \binom{n}{p}^2$. Solution: It is convenient to use the following notation: If Θ is a finite set and if $\lambda \in \mathbb{N}$, the set of parts with λ elements of Θ will be denoted by $\Theta^{|\lambda|}$. With the above, given then E a set of cardinal $p+q$, and consider a part A of E of cardinal p. Given $B := E \backslash A$. Fix the parts A and B. Let us set: $F := E^{|m|}$. Then, consider that λ belongs to an interval of integers such that $0 \leqslant \lambda \leqslant m$, written $\lambda \in [0, m] \in \mathbb{Z}$, and denote F_λ the set of parts $Z \in F$ such that $A \cap Z$ is of cardinal λ. The F_λ, $\lambda \in [0, m] \in \mathbb{Z}$ forms a partition of F, so that: $\binom{p+q}{m} = \mathrm{card}(F) = \sum_{\lambda=0}^{m} \mathrm{card}(F_\lambda)$. Given a fixed integer $\lambda \in [0, m] \in \mathbb{Z}$. Clearly, if $X \in A^{|\lambda|}$ and $Y \in B^{|m-\lambda|}$. $X \cup Y \in F_\lambda$; moreover, $(X, Y) \mapsto X \cup Y$ is a bijection from $A^{|\lambda|} \times B^{|m-\lambda|}$ to F_λ, the inverse bijection being defined by $Z \mapsto (A \cap Z, B \cap Z)$. Given the theorem (♦) of the heading "Finite sets, denumerable sets" (of the section "Denumerability (Counting)"), we can write: $\mathrm{card}(F_\lambda) = \mathrm{card}(A^{|\lambda|}) \times \mathrm{card}(B^{|m-\lambda|}) = \binom{p}{\lambda}\binom{q}{m-\lambda}$, the last identity follows from the theorem (▲) of the heading "Combinatorial analysis" (of the section "Denumerability (Counting)"). Hence:*

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

Now replace the assumption $m \leqslant \min(p, q)$ by a weaker assumption $m \leqslant p+q$. The above reasoning must be modified as follows: The integer λ must be such that $A^{|\lambda|}$ and $B^{|m-\lambda|}$ are nonempty, i.e. $0 \leqslant \lambda \leqslant p$ and $0 \leqslant m - \lambda \leqslant q$, i.e. $\max(0, m-q) \leqslant \lambda \leqslant \min(m, p)$. Then $\binom{p+q}{m} = \sum_{\max(0,m-q)}^{\min(m,p)} \binom{p}{\lambda}\binom{q}{m-\lambda}$. Applying the formula (1) by setting $m = p = q = n$. We get: $\binom{2n}{n} = \sum_{\lambda=0}^{n} \binom{n}{\lambda}\binom{n}{n-\lambda} = \sum_{\lambda=0}^{n} \binom{n}{\lambda}^2$, the last identity follows from the property of symmetry $\binom{n}{\lambda} = \binom{n}{n-\lambda}$.

Chapter 5

Construction of Number System

1. Semigroup of Natural Numbers

1.1. Construction of $\mathbb{N}$. The term "natural number" refers either to a member of the set of positive integers 1,2,3,... or to the set of nonnegative integers 0,1,2,3,... (Bourbaki). Unfortunately, there is no general agreement on whether 0 should be included in the list of natural numbers. The set of natural numbers (whatever the definition adopted) is denoted $\mathbb{N}$ (sometimes called whole numbers). The lack of standard terminology leads to recommend (cf. table) the following terms and notations in preference to *counting number*, *natural number*, and *whole number*.

Set	*Name*	*Symbol*
..,-2,-1,0,1,2,..	integers	$\mathbb{Z}$
1,2,3,4,..	positive integers	$\mathbb{Z}+$
0,1,2,3,4,..	nonnegative integers	$\mathbb{Z}^*$
0,-1,-2,-3,-4,..	nonpositive integers	
-1,-2,-3,-4,..	negative integers	$\mathbb{Z}-$

Natural numbers $\mathbb{N}$ are the result of an approach that consists (1) in arranging comparable population sets in a same class, i.e. equipotent sets, (2) in constructing axiomatically the set of natural numbers $\mathbb{N}$ which allows to specify a particular set of the precedent classes (i.e. classes of finite sets), by introducing the class of the nonempty set with which one associates the integer zero, denoted 0. The three following axioms (of Peano) define $\mathbb{N}$ (up to an isomorphism):

(1) Zero is an element of $\mathbb{N}$.

(2) There exists a bijection from $\mathbb{N}$ to $\mathbb{N} \backslash \{0\}$ also denoted $\mathbb{N}^* : x \mapsto S(x)$ ($S(x)$ successor of x).

(3) If a part P of $\mathbb{N}$ contains 0 and the successor of any element of P, then $P = \mathbb{N}$.

The 3rd axiom is the *induction axiom* and is the base of the reasoning by induction (recurrence). Let A be a statement depending on a natural number n. If $A(0)$ is true and for any $n \in \mathbb{N}$ we have ($A(n)$ *true* $\Rightarrow A(n')$ *true*), then, $A(n)$ is true for any $n \in \mathbb{N}$. From the natural number 0 we can construct all natural numbers.

Def. 217. [A] *(Construction of natural numbers).* $1 := 0'$, $2 := 1'$, $3 := 2'$, *etc.*

If we replace $\mathbb{N}$ by $\mathbb{R}$ in the previous two first axioms we find two properties of $\mathbb{R}$, but $\mathbb{R}$ is not isomorphic to $\mathbb{N}$ because $\mathbb{R}$ and $\mathbb{N}$ are not equipotent.

1.2. Operations.

Addition and multiplication of two natural numbers are based on the principle of induction (principle of recurrence).

Def. 218. [B] *(Operations of natural numbers).* $\forall n \in \mathbb{N}$ $n + 0 = n$, $n \cdot 0 = 0$, $0 = 0$ *and* $(n, m) \in \mathbb{N}^2$ $n + m' := (n+m)'$, $n \cdot m' = n \cdot m + n$.