

Naïve and ZFC-Axiomatic Set Theories

Laurent Dubois - 2004

*Mathematics without numbers nor figures!
When more fundamental elements than numbers arise.*

*From mathematics to mathematic,
When mathematics become a real language,
not a simple collection of theories.*

Legend:

ZFC Axiom	Logics formula	Logics matrices	Problematic sets	Naive theory demonstrations	ZFC demonstrations	Digressions

Here my introduction to the Zermelo-Fraenkel axiomatic set theory. This is a personal arrangement. Maybe will you experiment this agreeable sensation of being fit out to start to explore strange countries and to build serious foundations to mathematics.

This is an arrangement that focuses on the paradoxes contained in the naïve set theory, the iterative conception of set. The fact that what we have naïvely in mind when we think about sets, closed entity, is really dynamical, expansive. The term “set” itself, is it not moving, fuzzy ? On the other hand, it appears that an ontology cannot be satisfied with the restrictions established by the ZFC axiomatic.

Material : numbers and letters (sounds and fruit of observations) ;

Fundamental relations : relations

Tools/equipment : axioms

$\mathcal{L} \equiv \subseteq, \in, =, \equiv, \wedge, \vee, \neg, \rightarrow, \leftrightarrow, \forall, \exists, \#, (,),$ variables (x, y, z...),...

A Formula is a sentence written in the language \mathcal{L} .

If ϕ, ψ are formula, then $\phi \vee \psi, \phi \wedge \psi, \neg\phi, \phi \rightarrow \psi, \phi \leftrightarrow \psi, \forall x \phi, \exists y \psi$ are formula.

Linked variables are quantified : $\forall x, \exists y$

Parameters: non quantified/free variables : $\forall x \exists y x \in z \wedge z \in y \equiv \phi$

In this formula ϕ, z is a parameter, we cannot determine its truth.

$$\neg \forall x \phi(x, \dots) \equiv \exists x \neg \phi(x, \dots)$$

$$\neg \exists x \phi(x, \dots) \equiv \forall x \neg \phi(x, \dots)$$

$\phi(a, b, c)$ means that the set of the free variables of ϕ is a part of $\{a, b, c\}$. Anything with 2 variables can be with 3 or more variables : $x^2 + 3y^2 + 0z^2$

Sentence = complete phrase \equiv formula without parameters. / so a sentence asserts something, / it can be true or false

Γ = theory = collection/list of sentences.

Theorem of $\Gamma =$ sentence σ such that from Γ , one deduces $\sigma : \Gamma \vdash \sigma$.

Let's start with the **Null/Empty set**:

$$\exists y \forall x x \in y \leftrightarrow x \neq x$$

$x \neq x$ is a formula but any other impossible equality would function :

$$\begin{aligned} x = \emptyset \wedge x = \infty \\ 0 = 1 \end{aligned}$$

As no element can satisfy this condition/formula, the set y contains no element !

$$\begin{aligned} Y &= \{x \mid x \neq x\} \\ y &= \{\} \text{ or } \emptyset \end{aligned}$$

Why is it so ? In virtue of the principles of non-contradiction and excluded-middle:

$$\neg(p \wedge \neg p) \equiv p \vee \neg p$$

They have the same conditions of satisfaction :

$$\begin{aligned} \neg(p \wedge \neg p) &\equiv \neg(p) \vee \neg(\neg p) \\ &\equiv \neg p \vee p \\ &\equiv p \vee \neg p \end{aligned}$$

$$\begin{aligned} p \vee \neg p &\equiv \neg(\neg p \wedge p) \\ &\equiv \neg(p \wedge \neg p) \end{aligned}$$

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$	
0	1	0	1	1	
0	0	0	1	1	
1	1	1	0	0	
1	0	0	1	1	

p	-p	p ∧ -p	p ∧ -p	-(p ∧ -p)	p ∨ -p
0	1	0	1	1	
0	0	0	0	0	
1	1	1	0	0	
1	0	0	1	1	

Normally, “p ∧ -p” is true when the two propositions are true only; but here, the situation where they are both false is equivalent by virtue of the commutativity of the connector “∧” :

$$p \wedge -p \equiv -p \wedge p$$

In the same way, the situations where one is true and the other false can be reduced to one case.

Of course, we work in first order logic. And it is question here of the inclusive OR

(exclusive OR = XOR)

If we consider cases of presupposition, we can be tempted to establish a semantic/non-classical negation.

$$[\neg(p \wedge \neg p) \equiv p \vee \neg p] \equiv [\neg(p \wedge \neg p) \leftrightarrow p \vee \neg p] \leftrightarrow [\neg(p \wedge \neg p) \equiv p \vee \neg p]$$

$$\{[\neg(p \wedge \neg p) \equiv p \vee \neg p] \equiv [\neg(p \wedge \neg p) \leftrightarrow p \vee \neg p]\} \leftrightarrow \{[\neg(p \wedge \neg p) \equiv p \vee \neg p] \leftrightarrow [\neg(p \wedge \neg p) \leftrightarrow p \vee \neg p]\}$$

there is an inevitable disequilibria in the occurrences of the “**equivalence**” operators

$$S \cap \emptyset = \emptyset$$

$$S \cup \emptyset = S$$

$$\emptyset \cap \{\emptyset\} = \emptyset$$

$$\emptyset \cup \{\emptyset\} = \{\emptyset\}$$

$$\emptyset \in \{\emptyset\}$$

Really, the null set is the only non-set object admitted in the axiomatic.

No axiom of unconditional existence!

But let's come back to the formula, i.e. a sentence that can be determined true or false because it does not contain parameters, free variables :

$$\forall \xi \xi \in \{x \mid F(x)\} \equiv F(\xi)$$

with $F(x) =$

Now, in which measure is it legitimate to use such formula to define a set, were it by default? Is the null set more legitimate than the set of all sets ? On the other hand, why would it less legitimate than “0” ?

Now the **Infinite set** :

*From one extreme, \emptyset
to another one ∞ .*

$$\exists x (\emptyset \in x \wedge \forall y (y \in x \Rightarrow \{y\} \in x))$$

Thanks to the existence of the null set, it is possible to build an infinite set. It was funny to begin this tutorial with these seemingly two opposite sets!

$$0 = \emptyset \quad 1 = \{\emptyset\} \quad 2 = \{\emptyset, \{\emptyset\}\} \quad 3 = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\} \dots$$

or

$$0 = \{\} \quad 1 = \{\{\}\} \quad 2 = \{\{\}, \{\{\}\}\} \quad 3 = \{\{\}, \{\{\}\}, \{\{\{\}\}\}\} \dots$$

$$x = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\} \dots\} \equiv x = \{\{\}, \{\{\}\}, \{\{\{\}\}\} \dots\}$$

This is an illustration of the Induction principle. You show that the formula is correct for a minimal element, in general 0. After that you try to establish that if it is true for x, it must be true for x + 1.

Thanks to the **replacement axiom scheme** :

$$\forall u \forall v \forall w ((F(u, v) \leftrightarrow F(u, w)) \rightarrow v = w) \rightarrow \forall x \exists y \forall v (v \in y \leftrightarrow \exists u u \in x \wedge F(u, v))$$

we can build the **Naturals** :

$$\exists x (\emptyset \in x \wedge \forall y (y \in x \Rightarrow y \cup \{y\} \in x))$$

This is the translation of integers in set theory by Von Neumann, using the recursive algorithm :

$$0 := \emptyset$$

$$N + 1 := N \cup \{N\}$$

Zero, the smallest von Neumann integer, is defined as the empty set. The von Neumann integer N is defined as the finite set with N elements which are the von Neumann integers 0 to N-1.

$$0 := \emptyset$$

$$1 := 0 \cup \{0\} = \{\emptyset\}$$

$$2 := 1 \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$$

$$3 := 2 \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \dots$$

$$N + 1 := N \cup \{N\} = \{0, 1, 2, \dots, N\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \dots\} \dots$$

$$0 := \{\}$$

$$1 = \{\{\}\}$$

$$2 = \{\{\}, \{\{\}\}\}$$

$$3 = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}$$

$$N + 1 = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}, \dots, \{\{\}, \{\{\}\}\}, \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\} \dots\} \dots$$

$$x = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\} \dots\} \equiv x = \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\} \dots\}$$

von Neumann integers is infinite but every of its element N is finite.

The von Neumann integer transcription grows exponentially, for $N > 0$ it has $5 \cdot 2^{N-1} - 1$ characters (braces and commas).

Of course, this representation doesn't make sense, since N is infinite! This is the paradox of set theory.

:= := by definition

Axiom of foundation or regularity :

$$\exists x F(x) \rightarrow \exists x F(x) \wedge \forall y \neg(F(y) \rightarrow y \in x)$$

or

$$\exists x F(x) \rightarrow \exists x F(x) \wedge \neg(\exists y F(y) \wedge y \in x)$$

This axiom allows to avoid the circular inclusions (Heinlein auto generation) like :

$$x \in y \wedge y \in z \wedge z \in x$$

and infinitely descending chains of sets :

$$\dots x_3 \in x_2 \in x_1 \in x_0$$

In other words, increasing infinite allowed, descending infinite excluded.
So once again, we see the limits of this axiom in the frame of a universal ontology.

We consider now the **problematic sets**.

Sets that does not contain themselves :

$$\exists y \forall x x \in y \leftrightarrow x \notin x$$

$$y = \{x \mid x \notin x\}$$

With the **short comprehension axiom**,

$$\exists y \forall x x \in y \leftrightarrow F(x)$$

that gives :

$$x \in y \equiv x \notin x$$

If we **instantiate** y for x, we have :

$$y \in y \equiv y \notin y$$

which is, of course, absurd !

$$\forall \xi \xi \in \{x \mid x \in y \Rightarrow x \cup \{x\} \in y\} \equiv F(\xi)$$

Here, the **separation axiom scheme** will be useful, we can save :

$$\forall \vec{v} \forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge \varphi(z, \vec{v}))$$

Indeed we have now :

$$z \in y \leftrightarrow z \in x \wedge z \notin z$$

which gives, with the instantiation of y for z :

$$(y \in y \leftrightarrow y \in x \wedge y \notin y)$$

the condition to keep the validity of the axiom – otherwise an axiom would be false - is to consider that :

$$y \notin x \wedge y \notin y$$

which shows that, for any set, there is something not contained by it ;

so there is **no set of all sets** !

With Zermelo, this axiom has two conditions to build sets on the basis of a property :

- to start from an existing set
- well-defined property

as this second condition itself is not “well-defined”, Skolem will precise that a property is well-defined if :

- it is expressed in a first-order predicate calculus language
- it uses logical constants
- it uses the two predicate symbols = and \in only.

Separation axiom scheme:

$$\forall \vec{v} \forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge \varphi(z, \vec{v}))$$

$$\forall \xi \quad \xi \in \{x \mid F(x)\} \equiv \varphi(\xi)$$

$$\forall \xi \quad \xi \in \{x \mid F(x)\} \equiv F(\xi)$$

$$\forall \xi \quad \xi \in \{x \mid x \in y \Rightarrow x \cup \{x\} \in y\} \equiv F(\xi)$$

Replacement axiom scheme :

$$\forall u \forall v \forall w ((F(u, v) \leftrightarrow F(u, w)) \rightarrow v = w) \rightarrow \forall x \exists y \forall v (v \in y \leftrightarrow \exists u u \in x \wedge F(u, v))$$

The open sentence $F(u, v)$ is a functional condition, a function that relates each member in set u to a unique member in set v .

It is necessary to prove the existence of a limit \aleph_0 of the increasing series of transfinite cardinals ($\aleph_0, \aleph_1, \aleph_2, \dots$) $\equiv \{\aleph_i : i \in \mathbb{N}\}$

Axiom of extensionality:

$$\forall x \forall y \forall z ((z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

Sets are uniquely defined by their members. There cannot be two different sets that have the same elements. As the identity of sets is treated extensionally and not intentionally, two different set definitions can lead to identical sets.

The notions of “set”, “element” and “membership” are indissociable !

Note that the converse,

$$x = y \rightarrow \forall x \forall y \forall z ((z \in x \leftrightarrow z \in y))$$

is an axiom of the predicate calculus. Hence we have,

$$x = y \leftrightarrow \forall x \forall y \forall z ((z \in x \leftrightarrow z \in y)).$$

Therefore the Axiom of Extensionality expresses the most fundamental notion of a set: a set is determined by its elements. This is the reason why this axiom is ordinarily the introductory axiom of the theory. But if there is an infinity of sets with one or more members, there is “only one” null set!

Where the use of the null set as fundamental element is justified !

Two examples of demonstration :

$$\begin{array}{l} \text{Let } \mathbf{A} = \{\mathbf{0}, \mathbf{1}\}, \text{ let } \mathbf{B} = \{\mathbf{1}, \mathbf{0}\} \\ \text{Let's show that } \mathbf{A} = \mathbf{B} \end{array}$$

- 1) $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$ / *Axiom or $\forall x \forall y (\forall z (z \in x \equiv z \in y) \rightarrow x = y)$ Axiom*
- 2) $x = A, y = B$ / *We have set A and set B*
- 3) $\forall z (z \in A \leftrightarrow z \in B) \rightarrow A = B$ / *1, 2 Instantiation*
- 4) $0 \in A \equiv 0 \in B$ / *set definition of A, B*
- 5) $1 \in A \equiv 1 \in B$ / *set definition of A, B*
- 6) $\forall z (z \in A \leftrightarrow z \in B)$ / *4, 5*
- 7) $A = B$ / *Modus ponens*

Let $\mathbf{A} = \{\mathbf{0}, \mathbf{0}\}$, let $\mathbf{B} = \{\mathbf{0}\}$

Let's show that $\mathbf{A} = \mathbf{B}$

- 1) $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$ / *Axiom or $\forall x \forall y (\forall z (z \in x \equiv z \in y) \rightarrow x = y)$ Axiom*
- 2) $x = A, y = B$ / *We have set A and set B*
- 3) $\forall z (z \in A \leftrightarrow z \in B) \rightarrow A = B$ / *1, 2 Instantiation*
- 4) Let's 0_1 stand for "the first element" in A, and 0_2 stand for "the second element" in A
- 5) $0_1 \in A \equiv 0 \in A \equiv 0 \in B$ / *set definition of A, B*
- 6) $0_2 \in A \equiv 0 \in A \equiv 0 \in B$ / *set definition of A, B*
- 7) $\forall z (z \in A \equiv z \in B)$ / *from 5, 6*
- 8) $A = B$ / *Modus ponens*

The principle of "anti-symmetry" leads to the same result:

Let $\mathbf{A} = \{\mathbf{0}, \mathbf{1}\}$, let $\mathbf{B} = \{\mathbf{1}, \mathbf{0}\}$

$A \subseteq B \wedge B \subseteq A \Rightarrow A = B$

Since $\subseteq \rightarrow \subset$, we can put a higher condition:

$A \subset B \wedge B \subset A \Rightarrow A = B$

In the same way, we have :

$A \leq B \wedge B \leq A \Rightarrow A = B$

and

$A < B \wedge B < A \Rightarrow A = B$

As the order of the elements of a set has no importance, it is necessary to elaborate a definition of

ordered elements.

A collection of elements in which multiplicity but not order is relevant is called a **multi-set**.

As for the order, it is taken into account in this way:

$$(x, y) \neq (y, x).$$

Indeed, by definition,

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

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

Let's prove that $(x, y) \neq (y, x)$ as long as x is different of y ;

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

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

If $\{x, y\}$ is equal to $\{x, y\}$,

$\{x\}$ is really different of $\{y\}$ by hypothesis,

otherwise, by axiom of extensionality, we would have a

singleton $\{x\}$ or $\{y\}$

in place of $\{x, y\}$,

hence (x, y) is really different of (y, x) .

If we make a demonstration in a constructive way, we have

$$(x, y) = (x', y') \text{ Iff } x = x' \ \& \ y = y'$$

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} \equiv (\{\{x\} = \{x'\} \vee \{x', y'\}\} \wedge \{x, y\} = \{x'\} \vee \{x', y'\})$$

$$\{x, \{x, y\}\} = \{x', \{x', y'\}\} \equiv (\{x\} = \{x'\} \wedge \{x, y\} = \{x', y'\}) \vee (\{x\} = \{x', y'\} \vee \{x, y\} = \{x'\})$$

$$\equiv (\{x\} = \{x'\} \wedge \{x, y\} = \{x', y'\})$$

$$\equiv (x = x' \wedge y = y') \text{ by Axiom of Extensionality.}$$

Since we are dealing with “orders”, let's consider triplets, quadruplets, n-uplets.

$$(x, y, z) = (x, (y, z))$$

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

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

$$(a_1, a_2, a_3, \dots, a_n) = (a_1, (a_2, a_3, \dots, a_n)) = (a_1, (a_2, (a_3, \dots, a_n))) = (a_1, (a_2, (a_3, (\dots, a_n))))$$

We immediately see the limits of the axiom of extensionality in the frame of an high-level ontology.

What does mean “to have the same elements” ?

This is a way of erasing the time factor.

We can introduce a relativity scale (// Russell types?) ; referential.

A set has the dimension of its elements (space-time matter continuum).

Axiom of the pairs :

$$\forall x \forall y \exists z \forall t (t \in z \leftrightarrow t = x \vee t = y) \text{ or } \forall x \forall y \exists z \forall t (t \in z \equiv t = x \vee t = y)$$

From sets x and y, one can build {x, y}, and from that, recursively, the sets

$$\{x, \{x, y\}\}, \{y, \{x, y\}\} \dots$$

One can also build {x, x} that, by virtue of the principle of extensionality, is reduced to the singleton {x}.

If $x = \emptyset \equiv x = \{\}$, we have $\{\{\}\}$, and by recursivity, $\{\{\dots\}\}$.

The way to build sets as big as one wants.

Axiom of the parts or Power axiom :

Divergent infinites.

$$\forall x \exists y \forall z (z \in y \leftrightarrow \forall u u \in z \rightarrow z \in x)$$

A way of expressing the inclusion, the potentiality.

The road to differences in cardinality between infinite sets !

Indeed, we will make the demonstration that the elements of a set and the elements of the set of its parts cannot be made in bijection.

Only constructive axiom with the axiom of the pair.

If we start from the null set, we can build the singleton :

$$\wp_{(\emptyset)} = \{\emptyset\}$$

by recursivity :

$$\wp(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$$

$$\wp(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$$

If $\#X = n$, then $\#\wp(X) = 2^n$.

The axiom of the parts allows, as that of the pairs, to build infinitely big sets.

In geometry, the line L is a set of points and the set \mathcal{L} is of the lines of a plane π is a set of sets.

If m is a point of the plane π and D a line getting over m , we have:

$$m \in \pi \quad m \in L \quad L \subseteq \pi \quad L \in \mathcal{L}$$

Induction principle :

it is the demonstration that it will function because it has to function !)

If E has n elements, then $\wp(E)$ has 2^n elements.

Demonstration: by recurrence on n .

Be P the above property to demonstrate.

$P(0)$ is true because then $E = \emptyset$ and $\wp(\emptyset) = \{\emptyset\}$ contains 1 element.

Let's suppose that $P(n)$ is true; be then E with $n + 1$ element;

Be a one of these elements that we fix. We can divide $P(E)$ in two parts:

parts of E that contain a

parts of E that does not contain a ;

let's compute the number of elements of each of these parts;

be A the parts of E that does not contain a

be B the parts of E that contain a

We have a bijection between A and $\wp(E - \{a\})$ defined by $\alpha(a) = A$ for each $A \in A$. So these two sets have the same number of elements;

Since $E - \{a\}$ has n elements, since $P(n)$ is true, the cardinality of A is 2^n .

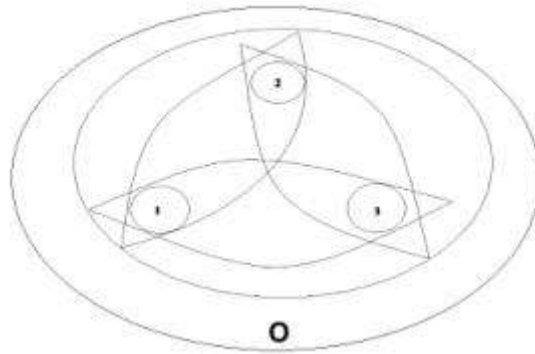
We also have a bijection between B and $\wp(E - \{a\})$ defined by $\beta(b) = B - \{a\}$.

So B has 2^n elements too. So $\wp(E)$ has $2^n + 2^n$ elements, i.e. 2^{n+1} elements.

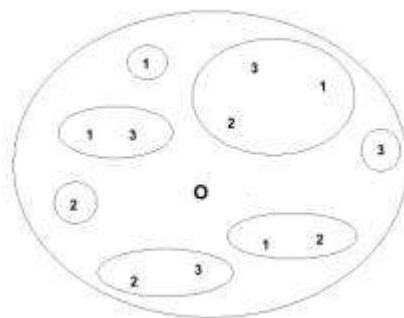
QED

If $n = 3$, \wp
(3) = 8





is it a legitimate translation of :



Axiom of union:

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists u u \in x \wedge z \in u)$$

If we apply the axiom of union to the Power set, we find the initial set ω . Really, as revealed by the Burali-Forti paradox, ω cannot be a set; it is a class !

Axiom of simplification in the same way as that of extensionality

Burali-Forti paradox :

ω cannot be a set, because it would be indexed by a type and would have to contain itself, because the definition of the ordinals

construction of ordinals each ordinal is constituted of its predecessors

maximal element

$$\xi_\gamma = f(\text{strict Maj.}\{\xi_\beta \mid \beta < \gamma\})$$

induction principle

How do the axioms play a role in the following developments ?

Injection, Bijection, Surjection

Be a function $f : E \rightarrow F$
 f is **injective** if we have

$$f(x) = f(y) \Rightarrow x = y$$

Of course, if f is a function,

$$x = y \Rightarrow f(x) = f(y)$$

is always true, which means that the graph is functional. So, for an injective application, we have :

$$x = y \Leftrightarrow f(x) = f(y)$$

f is **surjective** if $f(E) = F$.

It means that any element of F can be written $f(x)$ with $x \in E$.

$$f \text{ is surjective} \Leftrightarrow \forall y \in F \exists x \in E \mid y = f(x)$$

Bijection: f is bijective if it is both injective and surjective

Bijection \Rightarrow Injection (max. bij.)

Bijection \Rightarrow Surjection (min. bij.)

Injection : each element of target set has at most 1 antecedent in source set; or each element of source set is the only antecedent of an element of target set when it is an antecedent. Target set is at least as big as source set.

Surjection : each element of target set has at least 1 antecedent in source set; or each element of source set is the only antecedent of an element of target set when it is an antecedent. Target set is at

Be $A(\text{dom})$ and $B(\text{image})$.

Surjection : either B contains as many elements as A , and we have a bijection; either B contains

more elements than A. To have a proper identity, some elements of B have to have more than one antecedent in A ; but then $\varphi: A \rightarrow B$ is no more injective, which admits only one or 0 antecedent for each $b \in B$ in A.

$$\neg (\aleph \# \wp(\aleph))$$

*Transfinites: the institutionalisation of paradoxes in mathematics.
Set is infinitely far from infinite.
That doesn't prevent set and infinite to be very together.*

Demonstration :

$\wp(N)$ is infinite since we have an injection of N in $\wp(N): n \rightarrow \{n\}$; / indeed, $N \subset P \wp(N)$ consequently, it's not a finite set.

Now, we have to show that there is no bijection between N and P(N).

Be $\varphi: N \rightarrow \wp(N)$; let's show that φ cannot be a bijection. / there is an injection of N in $\wp(N) \equiv \varphi: N \rightarrow \wp(N) \equiv n \rightarrow \{n\} \equiv \varphi(n) = \{n\}$

Be $A = \{n \in N \mid n \notin \varphi(n)\}$.

Let's suppose there exists $a \in N$ such that $\varphi(a) = A$;

if $a \in A$, according to the definition of A, $a \notin \varphi(a) = A$; this is not possible;

if $a \notin A$, since $A = \varphi(a)$, $a \notin \varphi(a)$, so, by definition of A, $a \in A$, which is not possible either; consequently, that means that a doesn't exist and that φ is not surjective, thus not bijective. / since φ is injective, to show that it is not bijective, it is necessary to show that it is not surjective.

/ If $A \exists$, there must be free n in N and A must be in $\wp(N)$ since it is constituted of n only; A is obligatory a part of N.

/ If a doesn't exist, $A = \varphi(a)$ doesn't exist either, and there is no $n \in N$ such that $n \notin \varphi(n)$, and there is no possible surjection between n and $\wp(N)$ because of the lack of free elements in N.

It seems to be counter-intuitive that A doesn't exist because we can have, for example,,

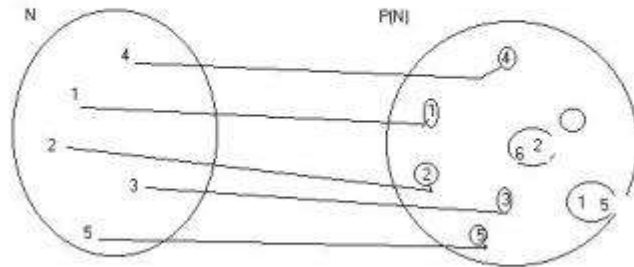
$\overline{\mathbb{N}}$

/ Since $N \in \wp(N)$, if we make a bijection between N and N in $\varphi: N \rightarrow \wp(N)$, we cannot use N for another bijection. If we make a bijection

/ between N and $N + (x, y)$, one cannot use N for another bijection. The problem is that there is an infinity of additional sets which we can make N in

/ correspondance with. So one cannot begin to attribute a n to all the parts/sets of $\wp(N)$.

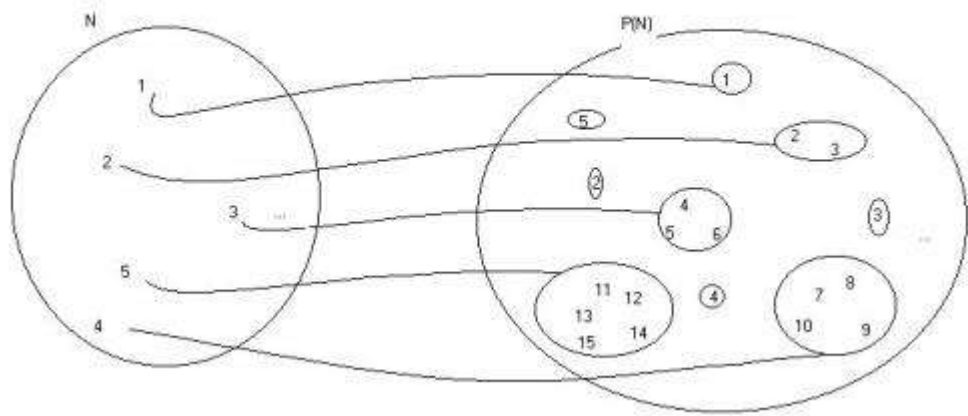
/ If there are $n \in N$ such that $n \notin \varphi(n)$, these n constituting the set A , they could be used for a surjection between N and $\wp(N)$. There must be enough elements in N such that each element of $\wp(N)$ has at least one specific antecedent.



of course, N and $\wp(N)$ are infinite, even in different ways:

$$\#N = \aleph_0$$

$$\#\wp(N) = 2^{\aleph_0} = \aleph_1$$



Complementary demonstration of the unaccountability of $\wp(E)$ that will be useful to establish that R is not countable.

Proposition : no injection from $\wp(E)$ in N .

Demonstration :

Be $\omega: \wp(N) \rightarrow N$. Let's show it is not injective.

We define $A = \{n \in N | \forall E \in \wp(N), \text{ if } n \in E, \text{ then } \omega(E) \neq n\}$. / *the formula says that N must be as big as $\wp(N)$ in order to have unused n in N.*

$\omega(a) \notin A$; indeed, if $\omega(a) \in A$ (thus in N), then $\forall E \in \wp(N)$, if $\omega(a) \in E$, then $\omega(E) \neq \omega(A)$; since we suppose $\neq \omega(A) \in A$, we can have $E = A$, consequently $\omega(A) \neq \omega(A)$; consequently, $\omega(A) \notin A$.

From an other point of view, the image of E must be different of the elements of E; thus different of $\omega(A)$, which is an element of E. Now, A is a E, then,

thus $\omega(E) \neq \omega(E)$.

From the definition of A, $\omega(A) \notin A$ means that $\exists E \in \wp(N) | \omega(A) \in E \wedge \omega(A) = \omega(E)$.

Thus we have $\omega(A) = \omega(E)$, though $A \neq E$ since $\omega(A) \notin A \wedge \omega(A) \in E$;

so ω is not injective.

Remark :

This demonstration would be acceptable for any set X, so there is no injection from $\wp(X)$ in X.

$$\forall E \in \wp(N) \quad n \in e \Rightarrow \omega(E) \neq n \Rightarrow n \in N$$

$$n \in E \wedge \omega(E) \neq n \Rightarrow n \in N$$

$$-(n \in N) \Rightarrow -(n \in E \wedge \omega(E) \neq n)$$

$$n \notin N \Rightarrow \neg \forall E \in \wp(N) (n \in E \wedge \omega(E) \neq n)$$

$$n \notin N \Rightarrow (\exists E \in \wp(N) (n \in E \wedge \omega(E) = n)) \vee (\exists E \in \wp(N) (n \notin E \wedge \omega(E) \neq n))$$

and we consider $\omega(A) \in E$, so...

Target set bigger than N? This is not a problem if we can make a finite choice of elements that allows a recursive process in the correspondence with the naturals. This is the case with Q but not with $\wp(N)$.

Nevertheless there is a difference between $\wp(E)$ and R, even if they have the same cardinality, because $\wp(E)$ allows a choice, even though infinite, while R doesn't even allow to select a first element.

$$\omega: \wp(N) \rightarrow N \neq \text{inj.} \equiv \varphi: N \rightarrow \wp(N) \neq \text{surj.}$$

Thus by recursivity, P(n) is true for any $n \in N$.

$\mathfrak{S} \neq \emptyset$

$\in \rightarrow \subset$

\subseteq (inclusion) is the membership in a large sense, i.e. real and potential

Axiom of choice well-ordering principle Zorn lemma are equivalent

Axiom of choice \equiv well-ordering principle \equiv Zorn lemma

Well-ordering principle = total order on a set E with the property that every non empty subset of E has a least element in this ordering. The set E with the well-order is then called a standard ordering of natural numbers, yes, but standard ordering of integers and positive real numbers, no !

Well-ordered set.

A **total order** has the following properties:

- Reflexivity: $E \leq E$
- Anti-symmetry: $E \leq F \wedge F \leq E \Leftrightarrow E = F$
- Transitivity: $E \leq F \wedge F \leq G \Rightarrow E \leq G$
- Totalness: $E \leq F$ or $F \leq E$

Theorems implying the axiom of choice are non-constructive, i.e. mathematical proofs that purport to demonstrate the existence of something, but not how to construct it! Frequent use of contraposition.

Banach-Tarski paradox

By use of the axiom of choice, cut a solid ball in 3-dimensional space into a finite number of pieces, re-assemble the pieces to get two balls, both of equal size to the first and using only rotation and translation, moving the pieces and reassemble them into two balls of the same radius as the original.

Axiom of choice:

=

If set x is constituted of non empty subsets disjointed two to two, there exists at least one set y that contains exactly one element of each of the subsets of x.

$$\forall X \exists f \text{ fct.}: X \rightarrow \cup X \mid \forall t \in X \setminus \{0\} f(t) \in t$$

f defined on X such that for each set S in X, f(t) is an element of t.

or

For any X without nul set, there exists a choice function f with arguments domain t , such that for any t belonging to X , $f(t)$ belongs to t .

Good order: $\forall x \exists$ relation \leq on $x \mid (x, \leq)$ G.O.

Zorn lemma :

Any inductive admits at least one maximal element.

Inductive: an order (X, \leq) is inductive iff $X \neq \emptyset \wedge$ any chain is majored

A chain is a totally ordered part by $\leq_{\wedge c}$

Be (X, \leq) an inductive, we have to show that there is a maximal element.

Let's take f a choice fct. over $\wp_x \setminus \{\emptyset\}$ (this parenthesis has not the same meaning as that of set)

$$\xi_0 = f(x)$$

either ξ_0 is maximal and then, stop.

either ξ_0 is not maximal, then strict Maj. $\{\xi_0\} \neq \emptyset$

ξ_α : ξ_α maximal? OK, stop!

If not, then

$$\text{strict Maj. } \{\xi_\alpha\} \neq \emptyset \Rightarrow \alpha + 1 = f(\text{strict Maj. } \xi_\alpha)$$



A totally ordered chain $\xi_0 \xi_1 \xi_\alpha \quad \alpha < \gamma$ limit ordinal

$\{\xi_\beta \mid \beta < \gamma \text{ limit}\}$ is an increased chain

to build

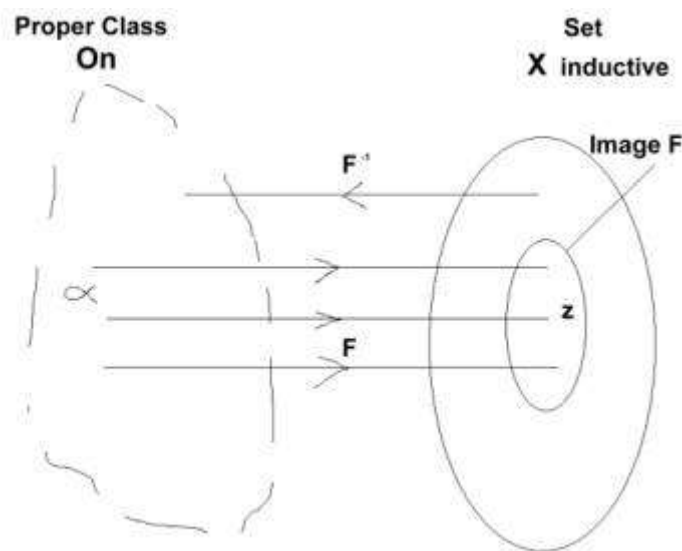
$$\xi_\gamma = f(\text{strict Maj. } \{\xi_\beta \mid \beta < \gamma\})$$

$\alpha \mapsto \xi_\alpha$ F fct. Defined by induction over O_n

2 possible cases :

- a) stop: there exist a maximal
- b) no stop: \rightarrow f injective fct. We never have two α sent on the same point. $O_n \rightarrow X$ set Now a fct. can never send a class on a set: $\neg \exists$ F injective fct. proper class \rightarrow set
So the case b) is impossible.

Let's show this :



We reverse the arrows. We build a F^{-1} . it will be functional since it is sufficient to say how it works.

$$F^{-1}(z) = \alpha \Leftrightarrow (z \in \text{image } F \wedge F(\alpha) = z) \vee (z \notin \text{image } F \wedge \alpha = 0)$$

So O_n is the image of F^{-1} : $O_n = \text{image } F^{-1}(X)$.

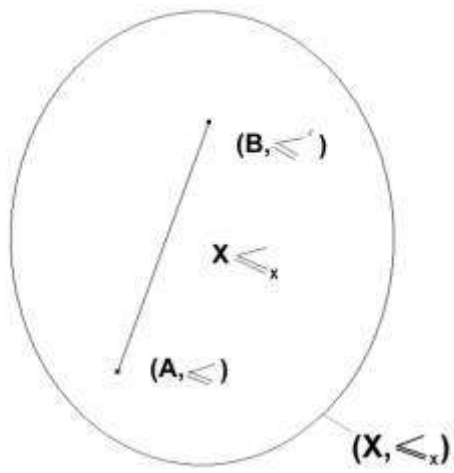
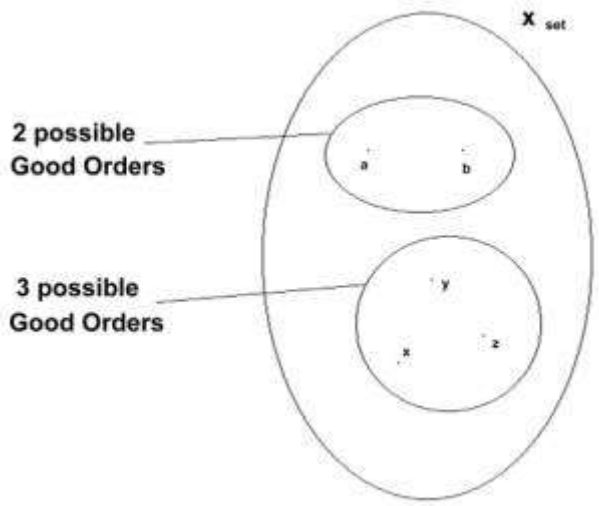
So O_n must be a set by virtue of axiom of replacement.

But it is impossible since O_n is a class.

Conclusion : any chain is increased ; any inductive admits at least one maximal element.

Demo : $3 \rightarrow 2$

$$X = \{(A, \leq) \mid A \subset X \wedge \leq \text{ is a good order on } A\}$$



X, \leq_X is an inductive, and we have X, \leq_X iff $A \subset B \wedge \leq$ is \leq'_A

“ ” in (B, \leq') because the order is not the same as in (A, \leq)

what is needed is to see “where” the chain goes, to build a raising element to the chain

$$\bigcup_{i \in I} A_i \quad \bigcup_{i \in I} \leq_i$$

$(B, \leq') \rightarrow$ Raising $i \in I$, $i \in I$
 (A_i, \leq_i)

OK ? Then, $\in X$

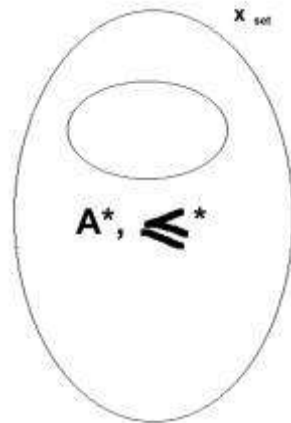
It is to verify that Good Order are OK.

Binary relations are seen as set of couples.

By Zorn: $\exists (A^*, \leq^*)$ maximal in X, \leq_X .

We would need a maximal part different of whole X.

But then there is an external point ξ and we could build a really bigger Good Order !



If $A^* \neq X$, then $(A^* \cup \{\xi\}, \leq^*$ followed by $\xi)$ is ~~\sum~~ (A^*, \leq^*) !!

But A^* is maximal, thus $A^* = X$

Conclusion, $A^* = X$ and \leq^* is a Good Order on X .

For any subset x of set y , there exists

Hyper sets or non-well-founded sets :

$$\exists x (x = \{x\})$$

proofs implying the axiom choice are non-constructive since they purport to demonstrate the existence of something without saying how to construct it.

Either ξ_0 is maximal and then, stop.

Either ξ_0 is not maximal, then strict Maj. $\{\xi_0\} \neq \emptyset$

In mathematics, a function is a relation such that each element of a set is associated with a unique element of another (possibly the same) set. The concept of a function is fundamental to virtually every branch of mathematics and every quantitative science.

The terms function, mapping, map, transformation and operator are usually used synonymously.

Another formulation of the axiom of choice (AC) states :

Given any set of mutually exclusive non-empty sets, there exists at least one set that contains exactly one element in common with each of the non-empty sets.

It seems obvious: if you've got a bunch of boxes lying around with at least one item in each of them, the axiom simply states that you can choose one item out of each box. Where's the controversy?

Well, the controversy was over what it meant to choose something from these sets. As an example, let us look at some sample sets.



In which measure extensionality and choice are in relation ?

1. Let X be any finite collection of non-empty sets : Then f can be stated explicitly (out of set A choose a , ...), since the number of sets is finite : Here the axiom of choice is not needed, you can simply use the rules of formal logic.
2. Let X be the collection of all non-empty subsets of the natural numbers $\{0, 1, 2, 3, \dots\}$: Then f can be the function that chooses the smallest element in each set : Again the axiom of choice is not needed, since we have a rule for doing the choosing.
3. Let X be the collection of all sub-intervals of $(0,1)$ with a length greater than 0 : Then f can be the function that chooses the midpoint of each interval : Again the axiom of choice is not needed.
4. Let X be the collection of all non-empty subsets of the reals : Now we have a problem. There is no obvious definition of f that will guarantee you success, because the other axioms of ZF.

The axioms are the result of work by Thoralf Skolem in 1922, based on earlier work by Adolf Fraenkel in the same year, which was based on the axiom system put forth by Ernst Zermelo in 1908 (Zermelo set theory).

The following set must exist, it gathers parts of \mathbb{N} :

$\{\{0, 2\}, \{1, 3\}, \{4, 5\}, \{6, 7\}, \{8, 11\}, \{9, 13\}, \{10, 17\}, \{12, 19\}, \{14, 23\}, \{15, 29\}, \{16, 31\}, \{18, 37\}, \{20, 41\}, \dots\}$

it is countable since there is a bijection: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

the choice axiom says that it functions but not “how” it functions.

(Zermelo set theory).

Cantor-Bernstein theorem

Let \mathbf{A} and \mathbf{B} be two sets. If there exists a one-to-one function f from \mathbf{A} to \mathbf{B} and another one-to-one function g from \mathbf{B} to \mathbf{A} , then $card(\mathbf{A}) = card(\mathbf{B})$.

$$\forall \mathbf{A} \forall \mathbf{B} (f: \mathbf{A} \rightarrow \mathbf{B} \leftrightarrow g: \mathbf{B} \rightarrow \mathbf{A}) \Rightarrow \# \mathbf{A} = \# \mathbf{B}$$

or

$$\forall \mathbf{A} \forall \mathbf{B} (f: \mathbf{A} \rightarrow \mathbf{B}: \text{inj.} \wedge g: \mathbf{B} \rightarrow \mathbf{A}: \text{inj.}) \Rightarrow \# \mathbf{A} = \# \mathbf{B} / h: \mathbf{A} \rightarrow \mathbf{B}: \text{bij.}$$

A total order always contains a co-final and well-ordered part, which means that any chain is raised/increased; so we have an inductive set E, \leq

The choice axiom allows to.

Contraposition :

Two main cases of use :

- when the conclusion to demonstrate is divided in numerous cases and sub cases, which corresponds to several "OR" between several propositions; then, it is better to start from the negation of this conclusion that will then be written as a conjunction of several propositions, i.e. with "AND" rather than "OR".

Example: to show that **if the prime number p divides all the numbers**

$$\sum_{i=0}^k a_i b^{k-i}$$

for $k = 0$ to n , either than p divides all the a_k either p divides all the b_i .

Demonstration :

p divides $a_0 b_0$; thus, p divides either a_0 either b_0 either both.

p divides $a_0 b_1 + a_1 b_0$; if p divides a_0 and b_0 , this gives us no info; if p divides a_0 only, then, it divides a_1 too.

p divides $a_0 b_2 + a_1 b_1 + a_2 b_0$; since p divides a_0 and a_1 and not b_0 , it divides a_2 too.

p divides $a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$; since p divides a_0, a_1 and a_2 and not b_0 , it divides a_3 too.

So we see it is possible to continue the demo by subdividing at each step according to the different cases, but it can become rather laborious.

So a contraposition demonstration seems to be judicious:

If p doesn't divide all the a_k nor all the b_i , then there exist a k such that p doesn't divide

$$\sum_{i=0}^n a_i b_{k-i}$$

Demonstration :

If p doesn't divide all the a_k , be r the first index such that p doesn't divide a_r (thus p divide all the previous k); / p divides a to a_{r-1}

in the same way, be s the first index such that p doesn't divide b_s ; / p divides b_0 to b_{s-1}

then, p doesn't divide $a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_r b_s + \dots + a_{r+s} b_0$ since it divides all the terms but $a_r b_s$.

QED

/ it is necessary that p divides at least all the a_k or all the b_i since there is a pair, a combination 2 by 2, of each a_k with b_i

- If a demonstration doesn't end in the direct sense or seems to be more and more complicated, contraposition is often salutary too.

Example : to show that

$$(\forall \epsilon > 0 \mid |a| \leq \epsilon) \Rightarrow a = 0$$

An attempt of direct demonstration could consist to show that:

$$|a| \leq \frac{1}{10}, |a| \leq \frac{1}{100}, \dots |a| \leq \frac{1}{1000000}$$

but we don't see how we can arrive to the conclusion $a = 0$; indeed, we cannot make a lead to 0 since the result we intend to demonstrate is precisely that that will all to justify such a passage to the limit !

Let's take the contraposition:

$$a \neq 0 \Rightarrow \exists \varepsilon > 0 |a| > \varepsilon$$

the demonstration is direct: if we have $a \neq 0$, we take $\varepsilon = \frac{|a|}{2}$ and we have indeed $\varepsilon > 0$ and a $\frac{|a|}{2} > \frac{|a|}{2} = \varepsilon$. QED

Ab absurdo Demonstration:

Principle : to demonstrate $A \Rightarrow B$

We demonstrate $A \Rightarrow \neg C$ and $(A \wedge \neg B) \Rightarrow C$

If B was false, and nevertheless A was true, we would deduce C ;

now $\neg C$ comes from A true; it is absurd since we cannot have C and $\neg C$ at the same time ; hence the two hypothesis A and $\neg B$ are incompatible ; consequently, B comes obligatory from A, in other words, A implies B, $A \Rightarrow B$.

Let's show that

$$\sqrt{2} \notin \mathbb{Q}$$

$$A \equiv x^2 = 2 \wedge x > 0$$

$$B \equiv x \notin \mathbb{Q}$$

$C \equiv$ any rational is written $\frac{p}{q}$ where p and q are prime between them.

$$A \Rightarrow B \quad | \quad x^2 = 2 \wedge x > 0 \Rightarrow x \notin \mathbb{Q}$$

Let's suppose that $x \in \mathbb{Q}$;

then $x = \frac{p}{q}$ where p and q are two integers with no common prime factors;

thus $x^2 = \frac{p^2}{q^2}$, which gives $p^2 = 2q^2$; / indeed, $x^2 = 2$; so $p = \sqrt{2q^2}$; $p = q\sqrt{2}$; now, $x = \frac{p}{q}$;

thus $\sqrt{2} = \frac{p}{q} \Rightarrow q = 1$; in any case $p (=q\sqrt{2})$ is not an integer !

so 2 is a prime factor of p^2 ; / indeed, 2 is a prime number

but the prime factor of p^2 are at an even power because it is a square, thus the power of 2 in p^2 is at least 2 ;

thus there is 2^2 in factor in $2q^2$, thus there is 2 in factor in q^2 ;

which causes that there is 2 in factor in q ;

but then 2 is a common factor to p and q , which is not possible given the choice of p and q ;

thus the demonstration is achieved by absurd.

$$A \cap B = B \Rightarrow B \subset A$$

This is a true demonstration by absurd.

$A \Rightarrow (B \Rightarrow C)$ Schema above.

Even if not obvious, it is a sentence of the type considered ; indeed,

$$(A \cap B = B \Rightarrow B \subset A) \equiv A \cap B = B \Rightarrow (x \in B) \Rightarrow (x \in A)$$

The demonstration must begin with the middle sentence, i.e. here by $x \in B$; the validity of this way of proceeding is justified by the rule that says that

$$A \Rightarrow (B \Rightarrow C) \equiv B \Rightarrow (A \Rightarrow C).$$

First, let's consider the transformation of $A \Rightarrow B$ into $B \vee \neg A$

$\neg (A \Rightarrow B) \equiv A \wedge \neg B$ / as we can see in the matrix below, the only case where the implication is false is when the antecedent is true and the conclusion false.

$$\neg (\neg (A \Rightarrow B)) \equiv \neg (A \wedge \neg B)$$

$$(A \Rightarrow B) \equiv \neg A \vee \neg (\neg B)$$

$$A \Rightarrow B \equiv \neg A \vee B$$

$$A \Rightarrow B \equiv B \vee \neg A$$

p	q	$p \wedge q$	$\neg (p \wedge q)$	$\neg p \vee \neg q$	$p \rightarrow q$
0	1	0	1	1	1
0	0	0	1	1	1
1	1	1	0	0	1
1	0	0	1	1	0

If we come back to $A \Rightarrow (B \Rightarrow C)$, we have :

$$A \Rightarrow (B \Rightarrow C) \equiv (B \Rightarrow C) \vee \neg A$$

$$\equiv (C \vee \neg B) \vee \neg A$$

$$\equiv C \vee \neg B \vee \neg A$$

$$\equiv C \vee \neg (B \wedge A)$$

$$\equiv (B \wedge A) \Rightarrow C$$

$$\equiv B \Rightarrow (A \Rightarrow C) / \text{by commutativity of } (B \wedge A)$$

To demonstrate a sentence of the type $A \Rightarrow (B \Rightarrow C)$, it is simpler to start from the middle proposition B and to use, in the process of the demonstration, the premise A in order to come to the conclusion C. Contrary to what we could think at first look, we don't have to write A first !/ *this would deserve a demonstration !*

So here, we have $x \in B$;

We use the premise that says : $A \cap B = B$

So we have $x \in A \cap B$

Thus, $x \in A$

So we have $x \in B \Rightarrow x \in A$

Another example :

P divides q $\Rightarrow qZ \subset pZ$ (nZ being the set of the multiple of n in Z)

$$q \Rightarrow qZ \subset pZ \equiv x \in qZ, \Rightarrow x \in pZ,$$

We start from the middle sentence :

Be $x \in q\mathbb{Z}$, then by definition, this means that x is written qk ;

Now, p divides q

Thus $q = rp$

Thus $x = rpk$

Consequently, x is a multiple of p .

/ $q \leq p$ because p contains all the possible divisors, thus the prime numbers too, while q doesn't. But q can contain 0 while p cannot !

About \subseteq (inclusion in its extended meaning as opposed to the strict inclusion \subset) : this relation is :

- reflexive : $E \subseteq E$
- transitive : $E \subseteq F \wedge F \subseteq G \Rightarrow E \subseteq G$
- antisymmetrical : $E \subseteq F \wedge F \subseteq E \Leftrightarrow E = F$ / *double inclusion method*

\cup and \cap are dual notions

$\cup \rightarrow \cap$

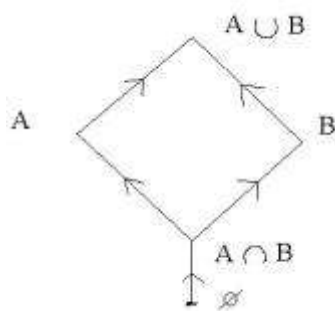
$\forall \rightarrow \exists$

set \subseteq set

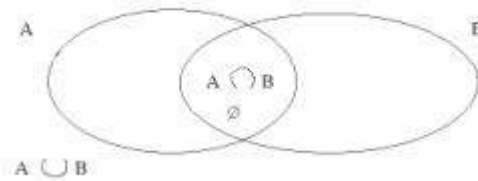
element \in set

Linear diagrams:

$$\emptyset \subseteq A \cap B \subseteq A \subseteq A \cup B \wedge \emptyset \subseteq A \cap B \subseteq B \subseteq A \cup B$$



is the translation of the following Euler Diagram :



Symmetrical difference :

$A \Delta B = (A \cup B) - (A \cap B)$
--

$A \Delta B$	\subseteq	$A \cup B$
XOR (exclusive OR)		OR (inclusive OR)

Properties of the symmetrical difference :

- associativity : $A \Delta (B \Delta C) = (A \Delta B) \Delta C$
- neutral element \emptyset : $A \Delta \emptyset = A$ / no common element to exclude
- any set is its own symmetric : $A \Delta A = \emptyset$ / all the elements are obviously common, thus to be excluded
- commutativity: $A \Delta B = B \Delta A$.

With these four properties, the symmetrical difference is a **law of commutative group over $\wp(E)$**
 or **$\wp(E)$ fit with this law is a commutative group.**

$p \Rightarrow q$

can be read :

- p is a sufficient condition for q
- q is a necessary condition for p

The sentence “this sentence is false” is true if it is false !

Short history

Frege Peano Russell Zermelo Fraenkel Zorn

Part of mathematics and of computer science (property).

Logic : classes, property $\rightarrow \in$ (comprehension) : if the element has the property, it belongs to “class”.

Math : $\in \rightarrow$ sets if the element belongs to the “set”, it has the property extension iterative conception of set belongs to the naïve set theory cardinality : extension of the notion of equality with Zermelo, a set is anything that makes true an axiom

Ordinal type of a well-ordered set. Sets with the same ordinal type, in other words identical good orders, whose respective members are linked by an univocal relation respecting the order, have the same ordinal type.

Null set extensionality (null set is unique) pairs (to build bigger and bigger sets) infinite foundation parts comprehension/separation scheme choice replacement scheme.

References

Bouvier, Alain, **La théorie des ensembles**, Que sais-je, PUF, 1972

Falquet, G., University of Geneva

Gochet, Paul, Gribomont, Pascal, **Logique**, Hermès, 1994

Krivine, Jean-Louis, **Théorie des ensembles**, Cassini, 1998

Pichon, Jacques, **Théorie des ensembles, Logique, Les Entiers**, Ellipses, 1989

Hinnion, Roland, **ZFC lessons**, Université Libre de Bruxelles, 2004

If “if” then “then”

$\Leftrightarrow \subset$

f: $\emptyset \longrightarrow \{\emptyset\}$