Axiom of infinity and construction of N

F Portal

Axiom of infinity and construction of $\mathbb{N}$

F. Portal*

February 11, 2015

Abstract

The aim of the present note is to show that it is possible, in the construction of numbers sets, to replace axiom of substitution and the standard Axiom of infinity (there exists an infinite ordinal) by one simple axiom "there exists an infinite set". Then the Axiom of choice will ensure the existence of a well-ordered set without maximal element with only one hereditary set. We then show that all these sets are isomorphic, and can then be called "naturel integer sets".

1 Introduction

The axioms of the ZFC set theory are precisely described in(Cori and Lascar, 1993) in(HALMOS, 1974) (KRIVINE., 1998)and (KURATOWSKI, 1977)

AE Axiom of extension

AS Axiom of specification

AP Axiom of pairing

AU Axiom of union

AR Axiom of substitution

AI Axiom of infinity (There exist an infinite ordinal)

APO Axiom of power set

AC Axiom of choice

The axioms of the ZFC set theory imply the existence of the empty set $\varnothing$: there exists a set $\varnothing$ such that $x \in \varnothing$ is always false.
The Axiom of Infinity is classically formulated as follows.

Axiom 1.1 (Axiom of Infinity (AI).) *There exists a set X such that $\varnothing \in X$ and, for all $y \in X$, then $y \cup \{y\} \in X$.*

That axiom is equivalent to the existence of an infinite ordinal (see (KRIVINE., 1998) by example). Then the set $\mathbb{N}$ is defined as the minimal set satisfying this axiom. We recall that without an infinite ordinal **all** the sets are finites (because by AR each well ordered set is isomorphe to a unique ordinal (see (HALMOS, 1974) page 80 and (KRIVINE., 1998) page 22), so without an infinite ordinal we have to process without the axiom of substitution AR . We prove that the axioms AR and AI may be replaced by one very simple axiom :

Axiom 1.2 (Naive Axiom of Infinity (NAI).) *There exists an infinite set.*

*Frédéric Portal, `frederic.portal@univ-mlv.fr`

Let us examine the set theory issued from the axioms [AE], [AS],[AP],[AU],[APO],[AC],[NAI], this set theory will be denote by ZFC\ (AI , AR). Without Axiom AI and Axiom AR the set $\mathbb{N}$ remains to be constructed. We remark that the notion of finite/infinite can be easily introduced without the help of the set $\mathbb{N}$:

Definition 1.1 (Finite set.) *A nonempty set X is finite if the only element of $\mathfrak{P}(X)$ (the set of all subsets of X) which is one-to-one with X is X.*

Definition 1.2 (Infinite set.) *A nonempty set X is infinite if it is not finite, that means that there exists $A \in \mathfrak{P}(X)$ such that $A \neq X$ and A is one-to-one with X.*

Remark 1.1 *Note that the above definitions ensure that a finite set or an infinite set is always nonempty. In particular, there is no sense to the question whether $\varnothing$ is finite or infinite.*

Therefore, a naive question is the following. Why the Axiom of infinity is not stated as NAI ?
Our aim is to remark that the set theory ZFC\ (AI , AR) allows as well to construct the set $\mathbb{N}$. The line which is followed consists in using the Axiom of choice, for the existence of well-ordered sets, and the Naive Axiom of Infinity, for obtaining the existence of a well-ordered set without maximal element. Then the set $\mathbb{N}$ is defined as the minimal set (up to an isomorphism) satisfying this property.

2 Well-ordering and Axiom of choice

We consider the set theory ZFC\ (AI , AR).

Let us first recall the definition of a well-ordered set.

Definition 2.1 *[Order.] An order O on a given nonempty set X is a subset of $X \times X$ such that*

1. $\forall x \in X, (x,x) \in O$,
2. $\forall (x,y) \in X \times X,\ (x,y) \in O$ *and* $(y,x) \in O \Rightarrow x = y$,
3. $\forall (x,y,z) \in X \times X \times X,\ (x,y) \in O$ *and* $(y,z) \in O \Rightarrow (x,z) \in O$.

We denote $(x,y) \in O$ by $x \le y$, and we say that (X,O) is an ordered set.

Definition 2.2 *[Well-ordered sets, minimal element.] An ordered set, denoted by (X,O), is well-ordered if any nonempty subset A of X contains a minimal element, in the following sense:*

$$\forall A \in \mathfrak{P}(X),\ A \neq \varnothing \Rightarrow (\exists x \in A, \forall y \in A, x \le y).$$

Since this element is unique, it is denoted $\min(A)$.

We recall the following theorem, which is equivalent to the assumption of the Axiom of choice:

Theorem 2.1 *Assuming ZFC\(AI , AR), for all nonempty set X, there exists an order O such that (X,O) is well-ordered.*

3 Construction of $\mathbb{N}$

Let us first prove the following lemma, which looks straightforward, but which must be rigorously handled using the notions of finite and infinite sets.

Lemme 3.1 *Let X be a nonempty set. Let $A \in \mathfrak{P}(X)$ such that $A \neq X$ and A is finite, and let $b \in X \setminus A$. Then*

1. there exists no injective mapping from $A \cup \{b\}$ to A,

2. $A \cup \{b\}$ is finite.

Proof The full item of this lemma wil be proved by contradiction. Let i be an injective mapping from $A \cup \{b\}$ to A. Then i is one-to-one from A to $i(A) \subset A$ defined by

$$i(A) = \{y \in A / \exists x \in A : i(x) = y\}.$$

Since A is finite, we have $i(A) = A$. Therefore, for all $y \in A$, there exists $x \in A$ such that $i(x) = y$. Since $i(b) \in A$,there exists $x \in A$ such that $i(x) = i(b)$. Since i is assumed to be injective, we get that $x = b$, which is in contradiction with $b \in X \setminus A$.

We now turn to the proof of the second item of the lemma. Let $C \subset A \cup \{b\}$ and g be a one-to-one mapping from C to $A \cup \{b\}$. Let us prove that $C = A \cup \{b\}$, which concludes the proof that $A \cup \{b\}$ is finite. Let us first assume that $b \notin C$. Then $C \subset A$ and g^{-1} is injective from $A \cup \{b\}$ to A. The proof of the preceding item shows that it is not possible. Therefore $b \in C$. Let us construct a one-to-one mapping f from C to $A \cup \{b\}$ such that $f(b) = b$.

- If $g^{-1}(b) = b$, we let $f = g$.
- Otherwise, we define the mapping φ from C to C by

$$\varphi(x) = \begin{cases} x & if \quad x \notin \{b, g^{-1}(b)\} \\ b & if \quad x = g^{-1}(b) \\ g^{-1}(b) & if \quad x = b \end{cases}$$

  Since φ is one-to-one from C to C, we define the one-to-one mapping f by $f = g \circ \varphi$, from C to $A \cup \{b\}$. It then satisfies $f(b) = g(g^{-1}(b)) = b$

Since f is a one-to-one mapping from C to $A \cup \{b\}$ such that $f(b) = b$, we get that $f(C \cap \{b\}^c) = A$ as well as the fact that there exists a one-to-one mapping from $C \cap \{b\}^c \subset A$ to A. Since A is finite, we get $C \cap \{b\}^c = A$, and therefore

$$C = (C \cap \{b\}^c) \cup \{b\} = A \cup \{b\},$$

which concludes the proof. ■

Let us now state the following lemma, which concerns a few properties of the succession operator.

Lemme 3.2 *Let (X, O) be a well-ordered set with more than one element. Then*
(i) the set $\mathrm{Max}(X)$, defined by

$$\mathrm{Max}(X) = \{m \in X,\ \forall x \in X,\ x \le m\},$$

cannot contain more than one element, and its complementary $(\mathrm{Max}(X))^c$ is such that

$$\forall x \in (\mathrm{Max}(X))^c, \exists y \in X, (x \le y \text{ and } x \ne y).$$

We then define, for all $x \in X$, the sets $]\leftarrow, x] = \{y \in X, y \le x\}$ and $]x, \rightarrow[= \{y \in X, x \le y \text{ and } x \ne y\}$.
(ii) The mapping s defined from $(\mathrm{Max}(X))^c$ to X by

$$\forall x \in (\mathrm{Max}(X))^c,\ s(x) = \min(]x, \rightarrow[)\},$$

is such that s is strictly increasing and

$$\forall x \in (\mathrm{Max}(X))^c,]\leftarrow, s(x)] =]\leftarrow, x] \cup \{s(x)\}.$$

Proof

(i)

Let $m \in \text{Max}(X)$ and $m' \in \text{Max}(X)$. We get, since m is maximal and $m' \in X$, $m' \leq m$ and similarly $m \leq m'$. Therefore $m = m'$.

(ii)

We first notice that, thanks to the assumption that X contains more than one element

$$(\text{Max}(X))^c \neq \varnothing.$$

Let x and y be elements of $(\text{Max}(X))^c$ such that $x \leq y$. Then, if $y = x$, $s(y) = s(x)$. If $x \neq y$, then $y \in]x, \rightarrow [$ and therefore $s(x) \leq y$. Since $y \leq s(y)$ and $y \neq s(y)$, we get $s(x) \leq s(y)$ and $s(x) \neq s(y)$. This proves that s is strictly increasing.
Let $x \in (\text{Max}(X))^c$ be given. Let $y \in] \leftarrow, x]$. Then $y \leq x$. Since $x \leq s(x)$, $y \leq s(x)$ and therefore $y \in] \leftarrow, s(x)]$. Since $s(x) \in] \leftarrow, s(x)]$, we have proved that $] \leftarrow, x] \cup \{s(x)\} \subset] \leftarrow, s(x)]$.
Reciprocally, let $y \in] \leftarrow, s(x)]$. First assume that $x \leq y$ and $x \neq y$. We then have $y \in]x, \rightarrow [$ and therefore $s(x) \leq y$. If $y \leq s(x)$, we get $y = s(x)$ and therefore $y \in \{s(x)\}$. Otherwise, $y \leq x$ and therefore $y \in] \leftarrow, x]$. This proves that $] \leftarrow, s(x)] \subset] \leftarrow, x] \cup \{s(x)\}$, and we conclude that $] \leftarrow, s(x)] =] \leftarrow, x] \cup \{s(x)\}$.
■

We may now state the following theorem, which concludes to the existence of a well-ordered set without extremal element.

Theorem 3.1 *Let us assume Axiom NAI. Let X be an infinite set, O be an order on X such that (X, O) is well-ordered in the sense of Definition 2.2. Let us denote, for all $(a, b) \in X \times X$ such that $a \leq b$, $[a, b] = \{x \in X, a \leq x \text{ and } x \leq b\}$. We denote by $\mathcal{F}(X) \subset \mathfrak{P}(X)$ the family of all finite subsets of X. We then define the set*

$$H = \{x \in X / [\min(X)\ ,\ x] \in \mathcal{F}(X)\}.$$

Then H satisfies the following properties:

a *H is nonempty and $H \cap \text{Max}(X) = \varnothing$. (Hence, $H \subset (\text{Max}(X))^c$),*

b *$s(H) \subset H$: $x \in H \Rightarrow s(x) \in H$*

c *$(\ H\ , O \cap (H \times H)\ )$ is a well-ordered set without maximal element.*

Proof
We have that $\min(X) \in H$ so that H is nonempty.
Let $x \in \text{Max}(X)$. Then, for any $y \in X$, $y \in [\min(X)\ ,\ x]$. This proves that $X \subset [\min(X)\ ,\ x]$. Since $[\min(X)\ ,\ x] \subset X$, we get that $X = [\min(X)\ ,\ x]$. Hence $[\min(X)\ ,\ x]$ is infinite, and $x \notin H$. This proves Item a.
Now suppose $x \in H$. Thanks to Lemma 3.2, we have

$$[\min(X)\ ,\ s(x)] = [\min(X), x] \cup \{s(x)\}.$$

Therefore, applying Lemma 3.1, we get that $[\min(X)\ , s(x)]$ is finite. Therefore $s(x) \in H$, which proves item b.
The set $(H\ ,\ O \cap (H \times H))$ is well-ordered, since (X, O) is well ordered. Let us denote $\text{Max}(H)$ the set of the maximal elements of $(H\ ,\ O \cap (H \times H))$. Let $x \in H$. Since $x \leq s(x)$, $x \neq s(x)$ and $s(x) \in H$, we obtain that $\text{Max}(H) = \varnothing$. This proves item c.

■

Let us now characterize the well-ordered sets without maximal elements.

Theorem 3.2 *Let us assume Axiom NAI. Let (X,O) be a well ordered set without maximal element . Then there exists $Y \in \mathfrak{P}(X)$ such that, for all $A \subset Y$ such that $\min(Y) \in A$ and $s(A) \subset A$ (in the sense $x \in A \Rightarrow s(x) \in A$), then $A = Y$.*
Moreover Y is infinite and $s(Y) = Y \setminus \{\min(Y)\}$.

Proof Let $\mathcal{H}$ be the set defined by

$$\mathcal{H} = \{A \in \mathfrak{P}(X)/\min(X) \in A \text{ and } s(A) \subset A\}.$$

Since (X,O) has no maximal element, we have $X \in \mathcal{H}$, which allows to define

$$Y = \bigcap_{H \in \mathcal{H}} H.$$

Then $(Y,\ O \cap (Y \times Y))$ is well-ordered and such that $s(Y) \subset Y$. Moreover, the succession for the order $O \cap (Y \times Y)$ is identical to that of the order (X,O). Indeed, temporarily denoting this succession by $\widetilde{s}$, we have, for all $x \in Y$, since $s(x) \in Y$, $\widetilde{s}(x) \leq s(x)$, and, since $(x, \widetilde{s}(x)) \in O$ and $x \leq \widetilde{s}(x)$, $s(x) \leq \widetilde{s}(x)$. This proves that $\widetilde{s}(x) = s(x)$. We have as well $\min(Y) = \min(X)$.

Let $A \subset Y$ such that $\min(Y) \in A$ and $s(A) \subset A$. Then $A \in \mathcal{H}$. Therefore $Y \subset A$. This concludes that $Y = A$.
Finally, let us denote $Y^\star = Y \backslash \{\min(Y)\}$, and prove, thanks to Lemma 3.2, that s is a one-to-one mapping from Y to $Y^\star$. Firstly, for any $x \in Y$, we get that $s(x) \neq \min(Y)$, since $\min(Y) \leq x$. Hence $s(Y) \subset Y^\star$. Secondly, s is injective, since it is strictly increasing. Thirdly, for any $y \in Y^\star$, the set $[\min(Y), y[\subset Y$ defined by $[\min(Y), y[= \{x \in Y, x \leq y \text{ and } x \neq y\}$ contains $\min(Y)$.
First assume that $s([\min(Y), y[) \subset [\min(Y), y[$. Then $[\min(Y), y[\in \mathcal{H}$ and therefore $Y \subset [\min(Y), y[$. Since $y \in Y$, there is a contradiction. Therefore $[\min(Y), y[$ contains some element x such that $s(x) \notin [\min(Y), y[$. Since $x \leq y$ and $x \neq y$, we have $y \in]x, \rightarrow[$ and therefore $s(x) \leq y$. Since $s(x) \notin [\min(Y), y[$, then ($s(x) \leq y$ and $s(x) \neq y$) is false. Therefore, since $s(x) \leq y$, we get $s(x) = y$. This proves that s is a one-to-one mapping from Y to $Y^\star$ and concludes the proof of of item *2.*. ■

We now define any set of natural integers, following the classical Peano's axioms.

Definition 3.1 *We call "a naturel integers set" any pair $(\mathbb{N}, O)$, where $\mathbb{N}$ is a well-ordered set by the order O, in the sense of Definition 2.2, such that*

1. $\text{Max}(\mathbb{N}) = \varnothing$
2. *For all $A \subset \mathbb{N}$ such that*
   (a) $\min(\mathbb{N}) \in A$
   (b) $s(A) \subset A$ *(in the sense $x \in A \Rightarrow s(x) \in A$),*

   then $A = \mathbb{N}$.

Applying theorems 2.1, 3.2, and 3.1, the existence of at least one natural integers set follows from the assumption of Axiom NAI.
Let us now show that all natural integers set are isomorphic.

Theorem 3.3 *Let $(\mathbb{N}, O)$ and $(\mathbb{N}', O')$ be two natural integers sets in the sense of Definition 3.1. Then there exists an increasing one-to-one mapping from $(\mathbb{N}, O)$ to $(\mathbb{N}', O')$.*

Proof Let us denote by s (resp. s') the succession in $(\mathbb{N}, O)$ (resp. $(\mathbb{N}', O')$) and

$$0 = \min_O\{n : n \in \mathbb{N}\}\ ,\ 0' = \min_{O'}\{n : n \in \mathbb{N}'\}.$$

Let $\mathcal{G} \subset \mathfrak{P}(\mathbb{N} \times \mathbb{N}')$ defined by

$$\mathcal{G} = \{R \in \mathfrak{P}(\mathbb{N} \times \mathbb{N}')/(0, 0') \in R \text{ and } [(n, x) \in R \Rightarrow (s(n), s'(x)) \in R]\}.$$

Hence $\mathcal{G}$ is the set of all graphs from $\mathbb{N}$ to $\mathbb{N}'$ such that $0' \in R(\{0\})$ and $s'(x) \in R(\{s(n)\})$ if $x \in R(\{n\})$. Let us prove that the graph g from $\mathbb{N}$ to $\mathbb{N}'$ defined by

$$g = \bigcap_{R \in \mathcal{G}} R = \{(n, x) \in \mathbb{N} \times \mathbb{N}' / \ (n, x) \in R, \ \forall \ R \in \mathcal{G}\},$$

satisfies $g \in \mathcal{G}$ and that g is a one-to-one mapping from $\mathbb{N}$ to $\mathbb{N}'$.

1. Let us prove $g \in \mathcal{G}$. Indeed, since for all $R \in \mathcal{G}$, we have $(0, 0') \in R$, we get $(0, 0') \in g$. Moreover, if $(n, x) \in g$, then for all $R \in \mathcal{G}$, $(n, x) \in R$ and therefore, $(s(n), s'(x)) \in R$. Therefore $(s(n), s'(x)) \in g$, which shows that $g \in \mathcal{G}$.
2. Let us prove $\text{im}(g) = \mathbb{N}'$. Thanks $(\mathbb{N}', O')$ is a natural integer set we have to look $0' \in \mathbb{N}'$ and $n' \in \text{im}(g) \Rightarrow s'(n') \in \text{im}(g)$. But by consruction $(0, 0') \in g$ et $(p, n') \in g \Rightarrow (s(p), s'(n')) \in g$
3. Let us prove $\text{dom}(g) = \mathbb{N}$. Thanks $(\mathbb{N}, O)$ is a natural integer set we have to look $0 \in \text{dom}(g)$ and $n \in \text{dom}(g) \Rightarrow s(n) \in \text{dom}(g)$. But by consruction $(0, 0') \in g$ et $(n, p) \in g \Rightarrow (s(n), s'(p)) \in g$
4. Let us prove that g is a function. We then define the set H by

   $$H = \{n \in \mathbb{N}/(\exists x \in \mathbb{N}', (n, x) \in g) \text{ and } (\forall (x, x') \in \mathbb{N} \times \mathbb{N}', ((n, x) \in g \text{ and } (n, x') \in g) \Rightarrow x = x')\}.$$

   Hence, H is the set of all $n \in \mathbb{N}$ such that $g(\{n\})$ contains one and only one $x \in \mathbb{N}'$.

   Let us prove that $0 \in H$. We first have $(0, 0') \in g$. Assume that $y \in \mathbb{N}'$ is such that $y \neq 0'$ and $(0, y) \in g$. We define

   $$g' = \{(n, x) \in \mathbb{N} \times \mathbb{N}'/(n, x) \in g \ et \ (n, x) \neq (0, y)\}.$$

   Then we have $g' \in \mathcal{G}$. Indeed, $(0, 0') \in g'$ since $(0, 0') \in g$ and $0' \neq y$. For any $(n, x) \in g'$, then $(n, x) \in g$, and therefore $(s(n), s'(x)) \in g$. Since $s(n) \neq 0$, we get $(s(n), s'(x)) \neq (0, y)$, and therefore $(s(n), s'(x)) \in g'$.

   Since $g' \in \mathcal{G}$, we get $g \subset g'$, which is in contradiction with $(0, y) \in g$.

   Let us now prove that $[n \in H \Rightarrow s(n) \in H]$. Let $x \in \mathbb{N}'$ be such that $(n, x) \in g$. Then $(s(n), s'(x)) \in g$. Assume that there exists $y \in \mathbb{N}'$ with $y \neq s'(x)$ and $(s(n), y) \in g$. We define

   $$g'' = \{(m, z) \in g/(m, z) \neq (s(n), y)\}.$$

   We again have $g'' \in \mathcal{G}$. Indeed, $(0, 0') \in g''$ since $s(n) \neq 0$. Let $(m, z) \in g''$. Since $(s(m), s'(z)) \in g$, assume that $(s(m), s'(z)) = (s(n), y)$. By the injectivity of s, we deduce $m = n$ and $y = s'(z)$. Since $n \in H$, this proves that $z = x$. Therefore $y = s'(x)$. This contradiction implies that $(s(m), s'(z)) \neq (s(n), y)$, and therefore $g'' \in \mathcal{G}$.

   We then get that $g \subset g''$, which is in contradiction with $(s(n), y) \notin g''$.

   Hence, we obtain $[n \in H \Rightarrow s(n) \in H]$.

   The set $H \subset \mathbb{N}$ being such that $0 \in H$ and $s(H) \subset H$, we get from Definition 3.1 that $H = \mathbb{N}$.
5. Morever the equality $s'(g(n)) = g(s(n))$ implies :

   $$g(]n \ , \rightarrow [\subset]g(n) \ , \rightarrow [)$$

   we get that g is one-to-one and strictly increasing from $(\mathbb{N}, O)$ to $(\mathbb{N}', O')$, this concludes the proof that $(\mathbb{N}, O)$ and $(\mathbb{N}', O')$ are isomorphic

■

References

Cori, R. and Lascar, D. (1993). *Logique mathématique. Cours et exercices. II.* Axiomes. Collection de Logique Mathématique. [Axioms. Collection in Mathematical Logic]. Masson, Paris. ISBN 2-225-84080-6. Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles. [Recursive functions, Gödel's theorem, set theory, model theory], With a preface by J.-L. Krivine.

HALMOS, P. R. (1974). *Naive set theory.* Springer-Verlag, New York-Heidelberg. Reprint of the 1960 edition, Undergraduate Texts in Mathematics.

KRIVINE., J. L. (1998). *Théorie des ensembles.* Paris :Cassini.

KURATOWSKI, K. (1977). *Introduction to set theory and topology.* PWN—Polish Scientific Publishers, Warsaw; Pergamon Press, Oxford-New York-Toronto, Ont. Containing a supplement, "Elements of algebraic topology" by Ryszard Engelking, Translated from the Polish by Leo F. Boroń, International Series of Monographs in Pure and Applied Mathematics, 101.