A fourth course on Algebra: Set Theory

Adiel González

Introduction

Índice general

1
First order logic

§ Introduction

§ Formal languages

$\wedge \vee \rightarrow \leftrightarrow \Rightarrow \Leftrightarrow$

2
Axioms of set theory

§ **Class-set theory**

§ **Zermelo-Fraenkel**

3
Set algebra

§ Common results

4
Relations and functions

§ **Relations**

§ **Functions**

5
Natural numbers

To begin the construction of natural numbers we want them to satisfy their usual properties. For starters, we want to define every natural number in a way that lets us obtain the following one. We also want to derive its order properties, like the tricotomy property. We want them to satisfy Peano axioms, one property in particular is to have a succesor function that is injective and for them to be inductive. We'll explore what all this means by shortly exploring Zermelo's construction and then Von Neumann's. Other constructions along with a full Zermelo's construction is found in [Qui09].

§ Notions and constructions

Zermelo's construction

Von Neumann's construction

The principal idea of this construction is to have a natural defined by its precedent numbers. This representation is actually pretty intuitive since here any natural number n has exactly n elements. But we do not use this property to define them since it is circular. But we can formally identify any set resembling this idea of having n elements so it's clear that we can choose a representative for these sets.

Definición (Cardinality)***:*** Let X, Y be classes, we say that X has the same cardinality as Y or that X is equipotent to Y if there is a bijective function $f : X \longrightarrow Y$.
$x \mapsto f(x)$

Notice that we can define equipotent in terms of a function that instead is defined from Y to X.

Proposición 5.1: *Let $X, Y \in \mathcal{V}$. Define $X \sim Y \longleftrightarrow X$ is equipotent to Y. Then $\sim$ is an equivalence relation in $\mathcal{V}$.*

Demostración. The identity function $\underset{x \mapsto x}{\mathrm{Id} : X \longrightarrow X}$ is bijective.

If $X \sim Y$ then there is a bijective function $\underset{x \mapsto f(x)}{f : X \longrightarrow Y}$, that is, it's inverse $\underset{y \mapsto f^{-1}(y)}{f^{-1} : Y \longrightarrow X}$ also is bijective.

Finally, if $X \sim Y$ and $Y \sim Z$ then there are bijective functions $\underset{x \mapsto f(x)}{f : X \longrightarrow Y}$ and $\underset{y \mapsto f(y)}{g : Y \longrightarrow Z}$. Its composition $\underset{x \mapsto (g \circ f)(x)}{g \circ f : X \longrightarrow Z}$ is bijective.

Q.E.D.

So now we can choose a convenient representative for the sets that have n elements. And we did not use that notion to define the concept, so there should be no contradictions.

Definición (Natural number)***:*** A set n is a natural number if it satisfies:

i) n is transitive.

ii) $\in_n$ is an strict linear ordering in n.

iii) $\forall m \subset n$, m has a minimum and a maximum under $\in_n$.

Let $\mathbb{N}$ denote the class of natural numbers. We now have a way to find natural numbers. For instance, $\varnothing$ is a natural number. Then, we can find the following as $1 := \{\varnothing\}$. And now we can find $2 := \{\varnothing, \{\varnothing\}\}$. These sets satisfy the definition (prove it), and inspire the next definition and results.

Definición (Succesor of a set)***:*** If $x \in \mathcal{V}$ the succesor of x is defined to be the set $x \cup \{x\}$ and is denoted x^+.

From here on, we begin to develope our theory using these definitions.

Properties

Proposición 5.2: *If $n \in \mathbb{N}$ and $y \in n$ then $y \in \mathbb{N}$.*

Demostración. Let $x \in n$, $y \in x$ and $z \in y$. Since n is transitive, $y, z, w \in n$. Because $\in_n$ is a total order in n we have that $z \in_n y \longrightarrow z \in_n x$ so $y \subset x$.

Let $u, v \in x$. Then, since $\in_n$ is a total ordering in n, $u, v \in n$ are $\in_n$-comparable. In particular, $v, u \in x$, are such that $v \in u$ or $u \in v$, that is (v, u) or $(u, v) \in$ are in $\in_x$, so $v, u \in x$ are $\in_x$-comparable.

Let $w \subset x$. Since $w, x \in n$, w has a minimum and a maximum under $\in_n$. Since in particular $t \in w \longrightarrow t \in x$ then w has a minium and a maximum under $\in_x$.

Q.E.D.

Lema 5.1: $\forall n \in \mathbb{N}$, *n is ordinary, in other words,* $n \notin n$.

Demostración. If $n \in n$ then there is an element in n such that $n \in_n n$ which contradicts that $\in_n$ is a strict linear ordering.

Q.E.D.

Proposición 5.3: $\forall n, m \in \mathbb{N}$, *it cannot be that both* $n \in m$ *and* $m \in n$.

Demostración. If $n \in m$ and $m \in n$ then by transitivity $m \subset n$, therefore $n \in n$ which contradicts the preceeding Lema 5.1

Q.E.D.

Proposición 5.4: *If* $n \in \mathbb{N}$ *then* $n^+ \in \mathbb{N}$.

Demostración. Let $x \in n^+$ and $y \in x$. Then $x \in n$ or $x \in \{n\}$. If $x \in n$ then $x \in \mathbb{N}$, so $y \in n$ and therefore $y \in n^+$. If $x = n$ then $x \subset n$. So n^+ is transitive.

If $u, v \in n^+$ then $u, v \in n$, $u \in n \wedge v \in \{x\}$, $v \in n \wedge u \in \{n\}$ or $u, v \in \{n\}$. If $u, v \in n$ then trivially $u, v \in n^+$ so u, v are $\in_{n^+}$-comparable. If $u \in n \wedge v \in n^+$ then $v = n$ so $u \in v$ so $u, v \in n^+$ are $\in_{n^+}$-comparable. The same results of $v \in n \wedge u \in n^+$. If $u, v \in \{n\}$ then $u = v$. So by Lema 5.1, we have that $\in_{n^+}$ is an estrict linear ordering in n^+.

Let $w \subset n^+$. If $n \notin w$ then $w \subset n$ has a minimum and a maximum under $\in_n$, in particular $t \in w \longrightarrow t \in n^+$ so w has a minimum and a maximum under $\in_{n^+}$. If $n \in w$ then for any $x \in w \setminus \{n\}$, $x \in n$ so n is the maximum of w under $\in_{n^+}$, and if $w = \{n\}$ then n is both minimum and maximum, otherwise the minimum of $w \setminus \{n\}$ under $\in_n$ is also the minimum of w under $\in_{n^+}$.

Q.E.D.

Let us state an axiom from which will be derived the known Axiom of Infinity.

Axioma 1 (Alternative Axiom of Infinity)**:** Not every set is a natural number.

Definición (Inductive class)***:*** A class A is said to be inductive if

i) $\varnothing \in A$.

ii) If $x \in A$ then $x^+ \in A$.

Then we can derive the following theorem, also stated in some books as an axiom.

Teorema 5.1: *There is an inductive set.*

Demostración. Assume that no set in $\mathcal{V}$ is inductive. If there was an $x \in \mathcal{V}$ that was not a natural number then there would be an inductive set A such that $x \notin A$, thus, every $x \in \mathcal{V}$ is a natural number. This contradicts Axiom 1, thus there is an inductive set.

Q.E.D.

Teorema 5.2: *If $n \in \mathbb{N}$, n is in every inductive set.*

Demostración. Let A be an inductive set. Assume that there is $n \in \mathbb{N}$ such that $n \notin A$. Then, $n \in n^+ \setminus A$, and $n^+ \in \mathbb{N}$ so we can define $x := \min n^+ \setminus A$ under $\in_{n^+}$. Now $x \in \mathbb{N}$ and $x \subset n^+$. Moreover, because of the election of x, if $t \in x$ then $t \in A$, so $x \subset A$. $x \neq \varnothing$ since $\varnothing \in A$, so let be $y := \max x$ under $\in_x$. Now, $y \in A$ so $y^+ \in A$ and $y^+ \subset x$. If there was a $t \in x \setminus y^+$ then $t \notin y$ and $t \neq y$ so, since $\in_x$ is a total strict ordering, $y \in_x t$ so y is not maximum. So $x \setminus y^+ = \varnothing$, therefore $x \subset y^+$ and then $x = y^+$ so $x \in A$. Thus $n \in A$.

Q.E.D.

From this, we can prove the usually accepted axiom (now theorem):

Teorema 5.3 (Theorem of infinity)**:** $\mathbb{N} \in \mathcal{V}$.

Demostración. Let A be an inductive set. Then by Theorem 5.2 and Axiom **??**

$$\mathbb{N} = \{n \in A \mid n \text{ is a natural number}\} \subset A$$

so $\mathbb{N} \in \mathcal{V}$.

Q.E.D.

Having established that $\mathbb{N}$ is a set, now we can treat our construction of its properties and operations as in ZF.

From Theorem 5.3 follows the known principle of induction.

Teorema 5.4 (Induction Principle)**:** *Let* P(x) *be a property of x. If*

i) $\mathbf{P}(0)$,

ii) $\forall k \in \mathbb{N}$, $\mathbf{P}(k) \implies \mathbf{P}(k^+)$,

then $\mathbf{P}(n)$ $\forall n \in \mathbb{N}$.

Demostración. Let $W := \{k \in \mathbb{N} \mid \mathbf{P}(x)\}$. Then W is inductive, thus $\mathbb{N} \subset W$.

Q.E.D.

Definición (Order relation in $\mathbb{N}$)**:** $\forall m, n \in \mathbb{N}$, $m \leq n \longleftrightarrow m \in n \vee m = n$.

Teorema 5.5: $(\mathbb{N}, \leq)$ *is a well ordered set.*

Demostración. Let $l, m, n \in \mathbb{N}$. Clearly $n \leq n$.

If $m \leq n$ and $n \leq m$ then $m \in n \vee m = n$, and $n \in m \vee m = n$. By Theorems 5.1, 5.3 the only possible case is $m = n$.

If $l \leq m$ and $m \leq n$ then $l \in m \vee l = m$, and $m \in n \vee m = n$. If $l = m \wedge m = n$ then $l \leq m$. If $l \in m \wedge m = n$ then $l \leq m$ and similarly for $l = m \wedge m \in n$. Now, if $l \in m \wedge m \in n$, since $\in_n$ is an strict total ordering, $l \leq n$.

Now let, $n \in \mathbb{N}$ and $W = \{k \in \mathbb{N} \mid n \leq k \vee k \leq n\}$. If $n = 0$ then 0 and n are obviously $\leq$-comparable. If $n \neq 0$ then $0 \subset n$ and since $n \in \mathbb{N}$, $0 \in \mathbb{N}$ so 0 and n are $\leq$-comparable. Thus $0 \in W$.

Assume that $k \in W$, then k and n are $\leq$-comparable. Then k^+ is such that $k \in k^+$, so $k \leq k^+$ and either $n \leq k$ or $k \leq n$. If $n \leq k$ then by transitivity $n \leq k^+$. If $k \leq n$ then $k \in n$ or $k = n$, if $k = n$ then $n \in k^+$ so $n \leq k$, and if $k \in n$ then, since $n \in \mathbb{N}$, n is transitive, so $k \subset n$ and $k \in n$ that is $k \cup \{k\} \in n$, so $k^+ \in n$, so $k^+ \in W$. So $\leq$ is a total ordering in $\mathbb{N}$.

Finally, let U be a non-empty set of $\mathbb{N}$ and $l \in U$. Then $l^+ \cap U \neq \varnothing$ and $l^+ \cap U \subset l^+$, so $l^+ \cap U$ has a minimum under $\in_{l^+}$. Define $x := \min l^+ \cap U$. Assume that there is $y \in U$ such that $y \leq x$ and $y \neq x$. Then $y \in x$, that is $y \in l^+$. Therefore $y \in l^+ \cap U$ which contradicts the fact that x is minimum under $\in_{l^+}$. Thus x is the minimum of U under $\leq$.

Q.E.D.

Proposición 5.5: $\forall n \in \mathbb{N} \setminus \{0\}$ *there exists* $r \in \mathbb{N}$ *such that* $r^+ = n$

Demostración. Let $W := \{x \in \mathbb{N} \mid x < n\}$. Obviously $0 \in W$. By Theorem 5.5, we can define $r := \max W$. Then $r^+ \leq n$. Assume that $r^+ < n$, then $r^+ \in W$ and clearly $r < r^+$, a contradiction. Thus $r^+ = n$.

Q.E.D.

§ Peano systems

Algebraic structures and g-induction

For the remaining Peano postulates, we instead define a structure called a Peano system. And in the way, give important definitions that will be used to explore the various structures that we will discover throughout the next sections and chapters.

Definición (n-ary operation)***:*** Let A be a non-empty class, $n \in \mathbb{N} \setminus \{0\}$. Let

$$\begin{array}{rl} F : A^n & \longrightarrow A \\ (a_1, \ldots, a_n) & \mapsto F((a_1, \ldots, a_n)) \end{array}$$

be a function. Then we shall say that F is an n-ary operation. If $B \subset A$ with $A \neq \varnothing$ and $F(B^n) \subset B$ then we say that B is closed under F.

Definición (External left operation)***:*** Let A and B be a non-empty classes. We shall say that $\begin{array}{rl} F_I : B \times A & \longrightarrow A \\ (b, a) & \mapsto F_I((b, a)) \end{array}$ is an external left operation if F_I is a function.

Definición (External right operation)***:*** Let A and B be a non-empty classes. We shall say that $\begin{array}{rl} F_D : A \times B & \longrightarrow A \\ (a, b) & \mapsto F_D((a, b)) \end{array}$ is an external left operation if F_D is a function.

As a short note, a distinguished element is something rather hard to define. It usually denotes an identity for an operation, or a first element, or any important element in the set that is of interest to our study.

Definición (Algebraic structure)***:*** Let $k, l, m, n \in \mathbb{N}$. An element

$$(A, F_1, \ldots, F_k, E_1, \ldots, E_l, R_1, \ldots, R_m, a_1, \ldots, a_n)$$

is said to be an algebraic structure, if

i) A is a non-empty class,

ii) $F_1, \ldots, F_k$ are n_i-ary operations, $n_i \in \mathbb{N} \setminus \{0\}$ and $i \in l^+ \setminus \{0\}$ in A,

iii) $E_1, \ldots, E_l$, are external operations in A,

iv) $R_1, \ldots, R_m$ are relations from A^{n_j} in A which are not functions, $n_j \in \mathbb{N} \setminus \{0, 1\}$ and $j \in m^+ \setminus \{0\}$,

v) $a_1, \ldots, a_n$ are distinguished elements for any of the preceeding elements.

Definición (Algebraic structures of the same kind)***:*** If A and A' are non-empty

classes, we say that

$$(A, F_1, \ldots, F_k, E_1, \ldots, E_l, R_1, \ldots, R_m, a_1, \ldots, a_n)$$

$$(A', F'_1, \ldots, F'_{k'}, E'_1, \ldots, E'_{l'}, R'_1, \ldots, R'_{m'}, a'_1, \ldots, a'_{n'})$$

are algebraic structures of the same kind if

i) $k = k'$, $l = l'$, $m = m'$ and $n = n'$,

ii) F_i and F'_i are n_i-ary operations, $n_i \in \mathbb{N} \setminus \{0\}$ $i \in k^+ \setminus \{0\}$,

iii) E_j and E'_j are external operations (either left or right) over the same class, $j \in l^+ \setminus \{0\}$,

iv) R_q and R'_q are relations from A^{m_q} to A, which are not functions, $m_q \in \mathbb{N} \setminus \{0, 1\}$ and $q \in n^+ \setminus \{0\}$.

Definición (Algebraic structure isomorphism)***:*** If A and A' are non-empty classes,

$$(A, F_1, \ldots, F_k, E_1, \ldots, E_l, R_1, \ldots, R_m, a_1, \ldots, a_n)$$

$$(A', F'_1, \ldots, F'_{k'}, E'_1, \ldots, E'_{l'}, R'_1, \ldots, R'_{m'}, a'_1, \ldots, a'_{n'})$$

are algebraic structures of the same kind, their are said to be isomorphic if

i) There is a bijective function $f : A \longrightarrow A'$ such that:
$a \mapsto f(a)$

1) $f(a_i) = a'_i$ $\forall i \in n^+ \setminus \{0\}$,

2) The functions

$$f^{k_j} : A^{k_j} \longrightarrow (A')^{k_j}$$
$$(\alpha_1, \ldots, \alpha_{k_j}) \mapsto (f(\alpha_1), \ldots, f(\alpha_{k_j}))$$

$\forall j \in k^+ \setminus \{0\}$ are such that

$f \circ F_i(\alpha_1, \ldots, \alpha_{k_j}) = F'_i \circ f^{k_j}(\alpha_1, \ldots, \alpha_{k_j})$, i. e., operations are preserved.

3) The set under which the external operations E_q and E'_q are defined are the same, $\forall q \in l^+ \setminus \{0\}$,

4) $\forall p \in m^+ \setminus \{0\}$,

$((\alpha_1, \ldots, a_{m_p}), \alpha) \in R_p \longrightarrow ((f(\alpha_1), \ldots, f(\alpha_{m_p})), f(\alpha)) \in R'_p$.

When these conditions hold, we denote $A \cong A'$.

We will only work with binary operations, relations on the same sets and external left-operations if not stated otherwise.

Now, an important generalization for the sake of defining a Peano system is the following definition:

Definición (g-inductive with starting element $\boldsymbol{\iota}$)***:*** Let A be a class and $g : A \longrightarrow \mathcal{V}$, $a \mapsto g(a)$
We say that A is inductive over g (or g-inductive) with starting element $\boldsymbol{\iota}$ if

i) $\boldsymbol{\iota} \in A$,

ii) $\forall x \in A$, $g(x) \in A$.

So, the definition of inductive set generalizes to classes. And notice that the previous definition of inductive, defining $\mathrm{S} : \mathbb{N} \longrightarrow \mathbb{N}$ as the succesor function, $n \mapsto n^+$
is a special case where $\mathbb{N}$ is S-inductive with starting element $\varnothing$.

Let us denote the succesor of n by $\mathrm{S}(n)$ from now on.

But still, to generalize the induction principle to g-inductive classes, we define, in a similar way to infinite dimensional hyperspaces on linear algebra,

Definición (Minimally g-inductive classes)***:*** Let A be a g-inductive class with starting element $\boldsymbol{\iota}$. We say that A is minimally g-inductive with starting element $\boldsymbol{\iota}$ if no proper subclass of A is g-inductive with starting element $\boldsymbol{\iota}$.

So now, what Theorem 5.4 can be summed up to is that $\mathbb{N}$ is minimally inductive over $\mathrm{S} : \mathbb{N} \longrightarrow \mathbb{N}$ with starting element $\varnothing$. Now, to generalize:
$n \mapsto S(n)$

Teorema 5.6 (Principle of g-induction)**:** *Let* P(x) *be a property of x and A a minimally g-inductive class with starting element $\boldsymbol{\iota}$. If*

i) $\mathbf{P}(\boldsymbol{\iota})$,

ii) $\forall x \in A$, $\mathbf{P}(x) \implies \mathbf{P}(g(x))$,

then $\mathbf{P}(x)$ $\forall x \in A$.

Demostración. The class $\Omega := \{x \mid \mathbf{P}(x)\}$ is g-inductive with starting element $\boldsymbol{\iota}$. Since A is minimally inductive then $\Omega = A$.
Q.E.D.

Now, we have all the elements to define and in the next subsections prove our main theorem of the section. So we define:

Definición (Peano system)***:*** An algebraic structure (P, Σ, θ) is called a Peano system if it satisfies:

i) $\Sigma : P \longrightarrow P$ is an injective function such that $\theta \notin \Sigma(P)$.
$\rho \mapsto \Sigma(\rho)$

ii) P is minimally Σ-inductive with starting element θ.

Finite recursion theorem (Dedekind's)

For the sake of proving the unicity of a Peano system, and to work our way to the arithmetic of $\mathbb{N}$, we state a theorem that assures the existence and uniqueness of a function for which its definition relies on a base case and a general case that depends on the previous one.

Teorema 5.7 (Dedekind's recursion theorem)**:** *Let A be a non-empty set, $a \in A$ and $f : A \longrightarrow A$ ($a \mapsto f(a)$) a function. Then, there exists a unique function $\phi : \mathbb{N} \longrightarrow A$ ($n \mapsto \phi(n)$) such that*

i) $\phi(0) = a$, and

ii) $\phi(\mathrm{S}(n)) = f(\phi(n))$.

Demostración. First, we prove the existence. Let

$$Rs := \{B \subset \mathbb{N} \times A \mid (0, a) \in B \text{ and } (n, b) \in B \longrightarrow (\mathrm{S}(n), f(b)) \in B\}.$$

$Rs \neq \varnothing$ since $\mathbb{N} \times A \in Rs$. Now, let $\phi = \bigcap_{B \in Rs} B$, then $\phi \neq \varnothing$. Moreover, $\phi \in Rs$ and $\phi \subset B$ for any $B \in Rs$. Therefore $\min Rs = \phi$.

Now, consider the set $W := \{n \in \mathbb{N} \mid !\exists b \in A \text{ such that } (n, b) \in \phi\}$.

We have $(0, a) \in \phi$. Suppose $(0, a') \in \phi$. Then the set $C_0 := \phi \setminus \{(0, a')\}$ is such that $C_0 \in Rs$ and $C_0 \subset \phi$, which contradicts that $\min Rs = \phi$. Therefore $0 \in W$.

Suppose $k \in W$ with $(k, b) \in \phi$, that is (k, b) is unique. Then $(\mathrm{S}(k), f(b)) \in \phi$. Suppose $(\mathrm{S}(k), b') \in \phi$. Then the set $C := \phi \setminus \{(\mathrm{S}(k), b')\}$ is such that $C \in Rs$ and $C \subset \phi$, which contradicts that $\min Rs = \phi$. Therefore $\mathrm{S}(k) \in W$. Applying the induction principle, we have $W = \mathbb{N}$. Thus $\phi : \mathbb{N} \longrightarrow A$ ($n \mapsto \phi(n)$) is a function.

Now, for the uniqueness. Assume there exists $\phi_1 : \mathbb{N} \longrightarrow B$ ($n \mapsto \phi_1(n)$), $\phi_2 : \mathbb{N} \longrightarrow A$ ($n \mapsto \phi_2(n)$) functions satisfying the hypotheses. Let $W_u := \{n \in \mathbb{N} \mid \phi_1(n) = \phi_2(n)\}$. $\phi_1(0) = a = \phi_2(0)$, so $0 \in W_u$. Suppose $k \in W_u$. Then $\phi_1(\mathrm{S}(k)) = f(\phi_1(k)) = f(\phi_2(k)) = \phi_2(\mathrm{S}(k))$. Therefore, applying the induction principle, $W_u = \mathbb{N}$, and so $\phi_1 = \phi_2$. Q.E.D.

Notice that the only property of $\mathbb{N}$ used for the proof is Theorem 5.4. This can be easily replaced by an argument of g-induction, and the proof remains almost the same. So we can state:

Teorema 5.8 (Modified Dedekind's recursion theorem)**:** *Let A be a minimally g-inductive class with starting element $\boldsymbol{\iota}$, B a non-empty class, $b \in B$ and*

$f : B \longrightarrow B$ *a function. Then, there exists a unique function* $\lambda : A \longrightarrow B$
$b \mapsto f(b)$ $x \mapsto \lambda(x)$
such that

i) $\lambda(\iota) = b$, *and*

ii) $\lambda(g(x)) = f(\lambda(x))$.

Demostración. Exercise.

Q.E.D.

Existence and uniqueness of a Peano system

Now, we prove that there's a Peano system and it's isomorphic to any other Peano system. This result lets us start natural numbers in any of its elements, like the usual accepted convention in analysis to use $\mathbb{N}_1 = \mathbb{N} \setminus \{0\}$.

Proposición 5.6: $\mathrm{S} : \mathbb{N} \longrightarrow \mathbb{N}$ *is injective.*
$n \mapsto \mathrm{S}(n)$

Demostración. Suppose that there exists $m, n \in \mathbb{N}$ such that $\mathrm{S}(m) = \mathrm{S}(n)$ but $m \neq n$. Without any loss of generality, suppose $m < n$. We already have $\mathrm{S}(m) \subset \mathrm{S}(n)$. We prove $\mathrm{S}(m) \neq \mathrm{S}(n)$. Consider, since n is transitive, $m \in \mathrm{S}(n)$. By Theorem 5.3 we have $n \notin m$, and by hypothesis $n \neq m$, so $n \notin \mathrm{S}(m)$ that is $\mathrm{S}(m) \neq \mathrm{S}(n)$. It follows that $m = n$.

Q.E.D.

Teorema 5.9 (Existence of a Peano system)**:** $(\mathbb{N}, \mathrm{S}, 0)$ *is a Peano system.*

Demostración. By the preceeding proposition, the succesor function is injective. Now, $n \in \mathrm{S}(n)$ so it has at least one element. Then $\mathrm{S}(n) \neq 0$, $\forall n \in \mathbb{N}$.

Finally, by Theorem 5.4, $\mathbb{N}$ is S-inductive with starting element $\varnothing$.

Q.E.D.

Teorema 5.10 (Uniqueness of Peano systems)**:** *Any two Peano systems are isomorphic.*

Demostración. Assume there are Peano systems (P, Σ, θ) and (P', Σ', θ'). We apply Theorem 5.8. For P, P', θ' and $\Sigma' : P' \longrightarrow P'$, there exists a unique
$\rho' \mapsto \Sigma'(\rho')$
function $\lambda_1 : P \longrightarrow P'$ such that $\lambda(\theta) = \theta'$ and $\lambda_1(\Sigma(\rho)) = \Sigma'(\lambda_1(\rho))$. Using
$\rho \mapsto \lambda_1(\rho)$
Theorem 5.8 again for P', P, θ and $\Sigma : P \longrightarrow P$ we can obtain $\lambda_2 : P' \longrightarrow P$
$\rho \mapsto \Sigma(\rho)$ $\rho' \mapsto \lambda_2(\rho')$
such that $\lambda_2(\theta') = \theta$ and $\lambda_2(\Sigma'(\rho')) = \Sigma(\lambda_2(\rho'))$.

Then $\lambda_2 \circ \lambda_1(\theta) = \lambda_2(\lambda_1(\theta)) = \lambda_2(\theta') = \theta$. Similarly $\lambda_1 \circ \lambda_2(\theta') = \theta'$. Now $\lambda_2 \circ \lambda_1(\Sigma(\rho)) = \lambda_2(\lambda_1(\Sigma(\rho))) = \lambda_2(\Sigma'(\lambda_1(\rho))) = \Sigma(\lambda_2(\lambda_1(\rho)))$.

Also, clearly $\mathrm{Id}_P(\theta) = \theta$ and $\mathrm{Id}_P \circ \Sigma(\rho) = \Sigma \circ \mathrm{Id}_P(\rho)$. So, by Theorem 5,8, that is, the uniqueness of a function $\lambda : P \longrightarrow P$ such that $\lambda(\Sigma(\rho)) = \Sigma(\lambda(\rho))$, implies that $\lambda_2 \circ \lambda_1 = \mathrm{Id}_P$.

Similarly, using an analogous deduction and using the uniqueness of Theorem 5.8, we obtain $\lambda_1 \circ \lambda_2 = \mathrm{Id}_{P'}$. That is $\lambda_1 : P \longrightarrow P'$ is a bijection. Thus $P \cong P'$.

Q.E.D.

Exercises

1) *(Alternate proof for Theorem 5.7)* Let A be a non-empty set and $a \in A$. Define a finite calculation by $f_k : k \longrightarrow A$ such that $f_k(0) = a$ and $f_k(\mathrm{S}(x)) = \mathrm{S}(f_k(x))$ for $k \in \mathbb{N}$. Use this to prove theorem 5.7.

2) Prove Theorem 5.8.

3) *(Double induction principle)* Let A be a minimally g-inductive class with starting element $\boldsymbol{\iota}$ and R a relation that satisfies:

   (i) $(x, \boldsymbol{\iota}) \in R \ \forall x \in A$,

   (ii) $\forall x, y \in A$, if $(x, y) \in R \wedge (y, x) \in R \longrightarrow (x, g(y)) \in R$.

   Then $(x, y) \in R \ \forall x, y \in A$.

4) Let $\mathrm{S}_{\mathcal{Z}} : \mathcal{V} \longrightarrow \mathcal{V}$ and $\mathbb{N}_{\mathcal{Z}}$ be the intersection of all $\mathrm{S}_{\mathcal{Z}}$-inductive classes.

   a) Prove that $(\mathbb{N}_{\mathcal{Z}}, \mathrm{S}_{\mathcal{Z}}, \varnothing)$ is a Peano system.

   b) Find an explicit Peano system isomorphism betweem $(\mathbb{N}, \mathrm{S}, 0)$ and $(\mathbb{N}_{\mathcal{Z}}, \mathrm{S}_{\mathcal{Z}}, \varnothing)$.

5) Prove that if a class A is minimally g-inductive with starting element $\boldsymbol{\iota}$ such that $x \subset g(x) \ \forall x \in A$ then $(A, \subset)$ is a well ordering.

§ Arithmetic on $\mathbb{N}$

Modifications of the recursion theorem

Teorema 5.11 (Generalized recursion theorem)**:** *Let A be a non-empty set, $a \in A$. Suppose $f : \mathbb{N} \times A \longrightarrow A$, $(n,a) \mapsto f((n,a))$ is a function. Then there exists a unique function $\phi : \mathbb{N} \longrightarrow A$, $n \mapsto \phi(n)$ such that*

i) $\phi(0) = a$,

ii) $\forall n \in \mathbb{N}$, $\phi(\mathrm{S}(n)) = f(n, \mathrm{S}(n))$.

Demostración. Same as Theorem 5.7. Q.E.D.

Teorema 5.12 (Modified recursion theorem)**:**
Let $G : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, $(n,m) \mapsto G((n,m))$, $H : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto H(n)$ be functions. Then, there exists a unique function $\phi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, $(n,m) \mapsto \phi((n,m))$ such that

i) $\phi(n,0) = H(n)$, $\forall n \in \mathbb{N}$,

ii) $\phi(x, \mathrm{S}(y)) = G(x, \phi(x,y))$, $\forall x, y \in \mathbb{N}$.

Demostración. Let $n \in \mathbb{N}$. Consider $t_n := H(n)$, $G_n(z) := G(n,z)$ $\forall z \in \mathbb{N}$. Applying Theorem 5.7, there exists a unique function $\phi_n : \mathbb{N} \longrightarrow \mathbb{N}$, $x \mapsto \phi_n(x)$ such that $\phi_n(0) = t_n$ and $\phi_n(\mathrm{S}(y)) = G_n(\phi_n(y))$ $\forall n, y \in \mathbb{N}$.

Define $\phi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, $(n,y) \mapsto \phi_n(y)$. Thus $\phi(n,0) = \phi_n(0) = t_n = H(n)$, and $\phi(n, \mathrm{S}(y)) = \phi_n(\mathrm{S}(y)) = G_n(\phi_n(y)) = G(n, \phi(n,y))$.

Uniqueness follows from the uniqueness of ϕ_n, $\forall n \in \mathbb{N}$. Q.E.D.

Addition

Definición:

By Theorem 5.12, for $\mathrm{Id}_{\mathbb{N}} : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto n$ and $\mathrm{S}(:) \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, $(m,n) \mapsto \mathrm{S}(n)$ there exists a unique function $\phi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, $(m,n) \mapsto \phi((m,n))$ such that $\phi((n,0)) = \mathrm{Id}_{\mathbb{N}}(n) = n$ and $\phi((m, \mathrm{S}(n))) = \mathrm{S}(\phi((m,n)))$.

Let $+ := \phi$, and denote $m + n := +((m, n))$. We call $\begin{array}{l} + : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (m, n) \mapsto m + n \end{array}$ the addition or the sum on $\mathbb{N}$.

Now, we can derive a proposition for a more intuitive notation for $\mathrm{S}(n)$.

Proposición 5.7: $\forall n \in \mathbb{N}$, $\mathrm{S}(n) = n + 1$.

Demostración. Exercise. Q.E.D.

However, we will not use it for now.

Now, we shall show that $\mathbb{N}$ with $\begin{array}{l} + : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (m, n) \mapsto m + n \end{array}$ defines the following structure:

Definición (Monoid)**:** An algebraic structure $(A, *, e)$ is called a monoid if it satisfies

i) $\begin{array}{l} * : A \times A \longrightarrow A \\ a \mapsto f(a) \end{array}$ is an associative binary operation.

ii) $e \in A$ is a distinguished element such that $\forall a \in A$, $a * e = a = e * a$.

iii) If $\forall a, b \in A$, $a * b = b * a$ we say that the structure is a commutative monoid.

Teorema 5.13 (Associative property)**:** $\forall l, m, n \in \mathbb{N}$, $(l + m) + n = l + (m + n)$.

Demostración. Let $l, m \in \mathbb{N}$ and consider $W_{l,m,+,A} := \{n \in \mathbb{N} \mid (l + m) + n = l + (m + n)\}$.

$l+m+0 = l+m = l+(m+0)$, so $0 \in W_{l,m,+,A}$. Now suppose $k \in W_{l,m,+,A}$. Then $(l+m)+\mathrm{S}(k) = \mathrm{S}((l+m)+k) = \mathrm{S}(l+(m+k)) = l+\mathrm{S}(m+k) = l+(m+\mathrm{S}(k))$, therefore $\mathrm{S}(k) \in W_{l,m,+,A}$. Applying the induction principle we have the desired result. Q.E.D.

Teorema 5.14 (Additive identity)**:** $\forall n \in \mathbb{N}$, $n + 0 = n = 0 + n$.

Demostración. By definition, $n+0 = n$ $\forall n \in \mathbb{N}$. Now, let $W_0 := \{n \in \mathbb{N} \mid 0+n = n\}$.

Of course $0 + 0 = 0$ by definition, so $0 \in W_0$. Suppose now that $l \in W_0$, i.e., $0 + l = l$. Therefore $0 + \mathrm{S}(l) = \mathrm{S}(0 + l) = \mathrm{S}(l)$. Applying the induction principle, we have $W_0 = \mathbb{N}$. Q.E.D.

So, by Theorems 5.13 and 5.14, $(\mathbb{N}, +, 0)$ is a monoid. On top of that, we also prove that it is a commutative one.

First, we prove the following useful result:

Proposición 5.8 (Alternative application of the succesor function)**:**
$\forall n, m \in \mathbb{N},\ n + \mathrm{S}(m) = \mathrm{S}(n) + m.$

Demostración. Let $n \in \mathbb{N}$ and consider the set $W_{\mathrm{S}(),n} := \{m \in \mathbb{N} \mid n + \mathrm{S}(m) = \mathrm{S}(n) + m\}$.

We have $n + \mathrm{S}(0) = \mathrm{S}(n + 0) = \mathrm{S}(n) = \mathrm{S}(n) + 0$.

Now suppose that $l \in W_{\mathrm{S}(),n}$, i.e., $n + \mathrm{S}(l) = \mathrm{S}(n) + l$. Now $n + \mathrm{S}(\mathrm{S}(l)) = \mathrm{S}(n + \mathrm{S}(l)) = \mathrm{S}(\mathrm{S}(n) + l) = \mathrm{S}(n) + \mathrm{S}(l)$, that is $\mathrm{S}(l) \in W_{\mathrm{S}(),n}$. Applying the induction principle, we have the desired result.

Q.E.D.

Teorema 5.15 (Commutative property)**:** $\forall n, m \in \mathbb{N},\ n + m = m + n.$

Demostración. Let $n \in \mathbb{N}$ and $W_{n,+,c} := \{m \in \mathbb{N} \mid n+m = m+n\}$. By Theorem 5.14, $0 \in W_{n,+,c}$. Now suppose $l \in W_{n,+,c}$, so now $n+\mathrm{S}(l) = \mathrm{S}(n+l) = \mathrm{S}(l+n) = l + \mathrm{S}(n) = \mathrm{S}(l) + n$ (by Theorem 5.8), that is $\mathrm{S}(l) \in W_{n,+,c}$. So, applying the induction principle we have $W_{n,+,c} = \mathbb{N}$ which brings our desired result.

Q.E.D.

And simple result for operating on, now, the commutative monoid $(\mathbb{N}, +, 0)$.

Teorema 5.16 (Additive cancelation)**:** $\forall l, m, n \in \mathbb{N}$

i) If $l + n = m + n$, then $l = m$, and

ii) if $l + m = l + n$, then $m = n$.

Demostración. i) Let $W_{l,m,+,\not\sigma} := \{n \in \mathbb{N} \mid l + n = m + n \longrightarrow l = m\}$.

Of course $l + 0 = m + 0 \longrightarrow l = m$, so $0 \in W_{l,m,+,\not\sigma}$. Now suppose $k \in W_{l,m,+,\not\sigma}$. Then, if $l+\mathrm{S}(k) = m+\mathrm{S}(k)$, we will have $\mathrm{S}(l+k) = \mathrm{S}(m+k)$, and by Proposition 5.6 $l + k = m + k$. Thus $l = m$, and then $\mathrm{S}(k) \in W_{l,m,+,\not\sigma}$. Applying induction we have the desired result.

ii) follows from applying the commutative property and *i)*.

Q.E.D.

Regarding the order properties of the sum, we prove the following:

Lema 5.2: $\forall n, m \in \mathbb{N},\ m + n \geq n.$

Demostración. Let $U := \{x \in \mathbb{N} \mid m + x \geq x\}$. Clearly $0 \in U$. Now if $l \in W$, then $m + \mathrm{S}(l) = \mathrm{S}(m + l) \geq m + l \geq n$. Applying induction we have $U = \mathbb{N}$.

Q.E.D.

Teorema 5.17: $\forall m, n \in \mathbb{N},\ m \leq n \longleftrightarrow \exists \alpha \in \mathbb{N}$ *such that* $m + \alpha = n.$

Demostración. For $\exists \alpha \in \mathbb{N}$ such that $m + \alpha = n \longrightarrow m \leq n$ is clear.

Let $W := \{x \in \mathbb{N} \mid m + x = n\}$. By Lema 5.2 $W \neq \varnothing$. By Theorem 5,5, W has a minimum. Define $\alpha := \min W$, then $m+\alpha \geq n$. If $m+\alpha > n$, then by Proposition 5.5 there exists $r \in \mathbb{N}$ sucht that $\mathrm{S}(r) = \alpha$. Now $m+\alpha = m+\mathrm{S}(r) = \mathrm{S}(m+r) > n$, thus $m + r \geq n$ and then $r \in W$ and $r < \alpha$, a contradiction. It follows that $m + \alpha = n$.

Q.E.D.

Teorema 5.18: $\forall l, m, n \in \mathbb{N}$, $m \leq n \longleftrightarrow m + l \leq n + l$.

Demostración. If $m = n$ since $\begin{array}{c} + : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (m,n) \mapsto m+n \end{array}$ is a function, we have $m + l = n + l$. Using Theorem 5.16 we get that $m + l = n + l \longrightarrow m = l$ holds.

Assume $m < n$. Then by Theorem 5.17 there exists $\alpha \in \mathbb{N}$ such that $m + \alpha = n$. Now, since $\begin{array}{c} + : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (x,y) \mapsto x+y \end{array}$ is a function, $m + \alpha + l = n + l$. By Lema 5.2 we have that $m + l \leq n + l$.

Now, if $m + l < n + l$, then $\exists \alpha \in \mathbb{N}$ such that $m + l + \alpha = n + l$. That is, by Theorem 5.16 $m + \alpha = n$ and then $m \leq m + \alpha = n$.

Q.E.D.

Finally, to end this subsection:

Teorema 5.19: $m + n = 0 \longleftrightarrow m = 0$ *and* $n = 0$.

Demostración. $m = 0 \wedge n = 0 \longrightarrow m + n = 0$ is immediate. Assume $m + n = 0$. If $m > 0$ or $n > 0$ then, for $m > 0$, $m + n \geq m > 0$, thus $m + n \neq 0$. The same holds for $n > 0$. So $m = 0 \wedge n = 0$.

Q.E.D.

Multiplication

Definición: Now, we proceed in a similar way to the addition.

Consider $\begin{array}{c} f : \mathbb{N} \longrightarrow \mathbb{N} \\ n \mapsto 0 \end{array}$ and $\begin{array}{c} + : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (m,n) \mapsto m+n \end{array}$. Then, by Theorem 5.12 there exists exactly one function $\begin{array}{c} \psi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (m,n) \mapsto \psi((m,n)) \end{array}$ such that $\psi((n, 0)) = f(n) = 0$ and $\psi((m, \mathrm{S}(n))) = +(m, \psi((m, n))) = m + \psi((m, n))$.

Let $\cdot := \psi$. And denote $m \cdot n := \cdot((m, n))$ or simply mn if there's no ambiguity.

We call $\begin{array}{c} \cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \\ (m,n) \mapsto mn \end{array}$ the multiplication or the product on $\mathbb{N}$.

Most of proofs are pretty similar to those of addition. We cover these a bit more faster, most of the times using previous theorems without telling because of laziness.

Teorema 5.20 (Multiplicative indetity)**:** $\forall n \in \mathbb{N},\ 1 \cdot n = n.$

Demostración. Let $W_{1,p} := \{n \in \mathbb{N} \mid 1 \cdot n = n\}$. $0 \in W_{1,p}$, so assume that $k \in W_{1,p}$. Now $1 \cdot \mathrm{S}(k) = 1 \cdot k + 1 = \mathrm{S}(k + 0) = \mathrm{S}(k)$. Hence $W_{1,p} = \mathbb{N}$. Q.E.D.

Teorema 5.21: $\forall n \in \mathbb{N},\ 0 \cdot n = 0 = n \cdot 0.$

Demostración. Let $W_{0,p} := \{n \in \mathbb{N} \mid 0 \cdot n = 0\}$. $0 \in W_{0,p}$, so assume that $k \in W_{0,p}$. Now $0 \cdot \mathrm{S}(k) = 0 \cdot k + 0 = 0$. Hence $W_{0,p} = \mathbb{N}$. Q.E.D.

Teorema 5.22 (Left distribution over sum)**:** $\forall l, m, n \in \mathbb{N},\ l(m + n) = lm + ln$

Demostración. Let $W_{l,d,s} := \{n \in \mathbb{N} \mid l(m+n) = lm+ln\}$. $l(m+0) = lm+l\cdot 0$ so $0 \in W_{l,d,s}$. Assume that $k \in W_{l,d,s}$. Now $l(m+\mathrm{S}(k)) = l\mathrm{S}(m+k) = l(m+k)+l = lm + l\mathrm{S}(k)$. Hence $W_{l,d,s} = \mathbb{N}$. Q.E.D.

Teorema 5.23 (Right distribution over sum)**:** $\forall l, m, n \in \mathbb{N},\ (l+m)n = ln+mn$

Demostración. Let $W_{r,d,s} := \{n \in \mathbb{N} \mid (l+m)n = ln+mn\}$. $(l+m)\cdot 0 = l\cdot 0+m\cdot 0$ so $0 \in W_{r,d,s}$. Assume that $k \in W_{r,d,s}$. Now $(l + m)\mathrm{S}(k) = (l + m)k + (l + m) = (lk + l) + (mk + m) = l\mathrm{S}(k) + m\mathrm{S}(k)$. Hence $W_{r,d,s} = \mathbb{N}$. Q.E.D.

Teorema 5.24 (Associative property)**:** $\forall l, m, n \in \mathbb{N},\ (lm)n = l(mn)$

Demostración. Let $W_{a,p} := \{n \in \mathbb{N} \mid (lm)n = l(mn)\}$. $(lm) \cdot 0 = l(m \cdot 0)$ so $0 \in W_{a,p}$. Assume $k \in W_{a,p}$. Then $(lm)\mathrm{S}(k) = l(mk) + lm = l(mk + m)l\mathrm{S}(k)$. Hence $W_{a,p} = \mathbb{N}$ Q.E.D.

Teorema 5.25 (Commutative property)**:** $\forall m, n \in \mathbb{N},\ mn = nm$

Demostración. Let $W_{c,p} := \{n \in \mathbb{N} \mid mn = nm\}$. By Theorem 5.3.3 $0 \in W_{c,p}$. Assume $l \in W_{c,p}$. Then $m\mathrm{S}(l) = lm + m = (l + 1)m = \mathrm{S}(l)m$. Hence $W_{c,p} = \mathbb{N}$. Q.E.D.

Teorema 5.26 (Multiplicative cancelation)**:** $\forall l, m, n \in \mathbb{N},$

i) If $n \neq 0$ and $ln = mn$ then $l = m$.

ii) If $l \neq 0$ and $ln = lm$ then $n = m$.

Demostración. ii) Assume that $m \neq n$, without loss of generality $m < n$. Then $\exists r \in \mathbb{N}$ such that $m+\mathrm{S}(r) = n$, i.e. $lm+l\mathrm{S}(r) = lm+lr+l = ln$, thus $lr+l = 0$. Then by Theorem 5.16 $l = 0$, a contradiction. Hence $m = n$.

i) Apply the commutative property and then *ii)*. Q.E.D.

Teorema 5.27 (Integral domain property)**:** $\forall m, n \in \mathbb{N},\ mn = 0 \longrightarrow m = 0\ o\ n = 0.$

Demostración. Assume $m \neq 0 \wedge n \neq 0$. Then $\exists r \in \mathbb{N}$ such that $\mathrm{S}(r) = n$. Then $m\mathrm{S}(r) = mr + m = 0$. By Theorem 5.16 $m = 0$, a contradiction. Hence $m = 0 \vee n = 0$.

Q.E.D.

Teorema 5.28: $\forall l, m, n \in \mathbb{N}$, $m < n \longleftrightarrow ml < nl$.

Demostración. $\exists \alpha \in \mathbb{N}$ such that $m + \alpha = n$. Then $(m + \alpha)l = ml + m\alpha = nl$ and by Theorem 5.27 $\alpha l \neq 0$. Hence $ml < nl$.

Now assume that $ml < nl$. It cannot be that $m = l$. If $n < l$ then $\exists \alpha \in \mathbb{N}$ such that $n + \alpha = m$ thus $ml > nl$. Hence $m < n$.

Q.E.D.

Notice that with Theorems 5.20, 5.24 and 5.25 $(\mathbb{N}, \cdot, 1)$ is also a commutative monoid with the additional integral domain property.

Exercises

1) Define exponentiation and prove its common properties.

2) Prove that for any $m, n \in \mathbb{N}$, one and only one statement holds.

   i) $m = n$,

   ii) $m < n$,

   iii) $n < m$,

6
Extension to real numbers

§ **Integers**

§ **Rationals**

§ **Real Numbers**

§ **Complex Numbers**

Equivalence classes modulo n

Bibliografía

[Qui09] Willard Van Orman Quine. *Set Theory and Its Logic*. Revised. Harvard University Press, 2009.