Adiel González

Introduction

Contents

1
First order logic

1.1 The language of FOL

A completely formal study on formal languages and its full capabilities won't be explored here. What we do instead is try to give enough intuiton to not turn this into mathematical logic notes but still contemplate some definitions necessary to not leave important notions like "property" as a vague term.

A formal language consists of various symbols. These symbols can form expressions by concatenating them in various ways. A **chain** is the yuxtaposition of various symbols. When a chain makes sense we say that we have an **formula** of our language. We define what it means for a chain of first order logic symbols to be a formula.

Definition: The formal language of first order logic, denoted by $\mathcal{L}_1$, consists of

i) propositional variables $x_1, x_2, \ldots, x_n, \ldots$,

ii) logical connectives $\neg$, $\longrightarrow$,

iii) the universal quantifier $\forall$,

iv) parenthesis (,), [,]

Definition: A chain γ of $\mathcal{L}_1$ is an $\mathcal{L}_1$**-formula** if and only if

i) γ is a propositional variable.

ii) γ is the chain $(\neg\alpha)$ where α is a formula.

iii) γ is the chain $(\alpha \longrightarrow \beta)$ where α and β are formulas.

iv) γ is the chain $(\forall x \alpha)$ where x is a variable and α a formula.

v) There's no other way to create a formula.

A criteria to verify if a certain chain is a formula is to try to find a finite succession of formulas where the final term is the chain and any other term are subchains of our chain that are formulas and are obtained using previous formulas. This can be interpreted as decomposing every part of our chain and veryfing that they are formulas.

Example 1.1: *The chain* $((\neg(x_1 \longrightarrow x_2)) \longrightarrow ((\neg x_1) \longrightarrow (\neg x_2)))$ *is a formula. We can construct the sequence:*

1. x_1
2. x_2
3. $(x_1 \longrightarrow x_2)$
4. $(\neg x_1)$
5. $(\neg x_2)$
6. $((\neg x_1) \longrightarrow (\neg x_2))$
7. $((\neg(x_1 \longrightarrow x_2)) \longrightarrow ((\neg x_1) \longrightarrow (\neg x_2)))$.

Any formula of our language has a sequence for its construction, so we call it construction sequence. The collection of all formulas of $\mathcal{L}_1$ will be denoted by $\mathrm{Frm}(\mathcal{L}_1)$.

From the logical connectives we can derive the next definitions

Definition: Given two formulas α and β,

i) introducing the symbol $\wedge$, $(\alpha \wedge \beta)$ is defined as $(\neg(\alpha \longrightarrow (\neg\beta)))$.

ii) introducing the symbol $\vee$, $(\alpha \vee \beta)$ is defined as $((\neg\alpha) \longrightarrow \beta)$.

iii) introducing the symbol $\longleftrightarrow$, $\alpha \longleftrightarrow \beta$ is defined as $((\alpha \longrightarrow \beta) \wedge (\beta \longrightarrow \alpha))$

We need to assign truth values for our language of logic, which is, a bivalent logic. A propositional variable can have any two values true or false that are represented by T and F, respectively. We need a way to assign values to our formulas, that is, something like a function, at least, a function only in intuition.

Definition: Given a function v to assign T or F for any variable of $\mathcal{L}_1$, the evaluation for any formula in $\mathrm{Frm}(\mathcal{L}_1)$ is given by the function $\bar{v}$ as:

$$\begin{aligned} \bar{v}(x_n) &= v(x_n), \\ \bar{v}(\neg\alpha) &= \begin{cases} F & \text{if } \bar{v}(\alpha) = T \\ T & \text{if } \bar{v}(\alpha) = F \end{cases} \\ \bar{v}(\alpha \longrightarrow \beta) &= \begin{cases} F & \text{if } \bar{v}(\alpha) = T \text{ and } \bar{v}(\beta) = F \\ T & \text{otherwise} \end{cases} \end{aligned}$$

In the usual first course on logic fashion, we represent the possible valuations for any variable and its respective evaluation by a table called **truth table**, here, assuming the evaluation on formulas α and β:

α	β	$(\alpha \longrightarrow \beta)$
T	T	T
F	T	T
T	F	F
F	F	T

α	β	$(\alpha \wedge \beta)$
T	T	T
F	T	F
T	F	F
F	F	F

α	β	$(\alpha \vee \beta)$
T	T	T
F	T	T
T	F	T
F	F	F

α	β	$(\alpha \longleftrightarrow \beta)$
T	T	T
F	T	F
T	F	F
F	F	T

α	$(\neg\alpha)$
T	F
F	T

Example 1.2: *Let us evaluate the formula (verify it)* $(((\neg x_1) \wedge x_1) \longrightarrow (x_2 \longrightarrow x_3))$ *for the evaluation* v *where* $v(x_1) = F, v(x_2) = T, v(x_3) = T$. *For this, we evaluate* $((\neg x_1) \wedge x_1)$, *therefore* $(\neg((\neg x_1) \longrightarrow (\neg x_1)))$, *succesively,* $((\neg x_1) \longrightarrow (\neg x_1))$, $(\neg x_1)$, *and* $v(x_1) = F$. *Therefore* $\bar{v}((\neg x_1)) = T$ *and then* $\bar{v}(((\neg x_1) \longrightarrow (\neg x_1))) = T$ *so then* $\bar{v}((\neg((\neg x_1) \longrightarrow (\neg x_1)))) = F$. *Now* $\bar{v}((x_2 \longrightarrow x_3)) = T$ *and then* $\bar{v}((((\neg x_1) \wedge x_1) \longrightarrow (x_2 \longrightarrow x_3))) = T$. *In general, no matter the valuation on* x_1 *and the formula in the place of* $(x_1 \longrightarrow x_3)$, *the whole formula evaluates in* T. *The reader can verify this using truth tables.*

This example is no more than a mere torture that I imagined would be useful to show that the definition works.

Now, to define what it means to satisfy and to correctly infere, we define:

Definition: We say that a truth assignment v satisfies a formula α if and only if $\bar{v}(\alpha) = T$.

Definition: For a formula α:

i α is a **tautology** if v satisfies α for every valuation v.

ii α is an indetermination if there is a valuation v that satisfies α but not every valuation satisfies α.

iii α is a contradiction if no valuation satisfies α.

1.2 Propositional logic

1.3 First order predicate logic

2
Elements of set theory

2.1 Zermelo-Fraenkel

2.2 Set algebra

2.3 Classes of sets

3
Relations and functions

3.1 Relations

3.2 Functions

3.3 Equivalence relations and partitions

3.4 Orders

4
Natural numbers

We begin the construction of our usual known number systems by defining the natural numbers. The intuitive idea of them being used to count kind of relates to their formal construction. The problem of defining every natural number can be reduced to defining the first natural number. For our construction, the first natural number is 0, so then we can define the succesor of a natural number, find out if it also satisfies the definition of one and have every natural number determined. Given all basic definitions we want to bring the class of all natural numbers $\boldsymbol{\omega}$ into set theory so we can apply everything we know about sets to show and construct all of its properties, obtaining what is called a Zermelo's Universe, to then finally construct the rest of our number systems how we want them to behave. Of course, this can be achieved in ZF set theory or another set theory via different methods. The one treated in these notes is given by Von Neuamnn. Other constructions can be found in [Qui09].

4.1 Notions and construction

When thinking about a natural number, the first thing that comes to mind may be a group of n things. That is, we already use the natural number n to define it. A circular definition like this cannot be given to formalize the natural numbers. But we can still preserve the idea, establishing the idea of having x elements without recurring to the object x. Therefore, we define:

Definition (Equipotence)***:*** Let A, B be sets. We define the class relation on $\mathcal{V}$ by

$$A \sim B \longleftrightarrow \text{ there exists a bijection } f : A \longrightarrow B$$

.

This class relation is a class equivalence relation. Thus, it can form a partition for $\mathcal{V}$. This way we can choose a convenient representative for the sets that have n elements and we avoid the circular definition. In essence, every natural number should contain any previous natural number, that's the core idea behind Von Neumann's construction.

Now, since we want an order for natural numbers, consider $\in$ as a total ordering on a set n. The question of it being strict or not may require to talk about well founded sets, but we can avoid it for now. Since we want our natural numbers to be contained in greater natural numbers we will have that $n \in m$ only if m is greater than n, but this definition also implies that $n \subset m$. This specific property is called transitivity. Formally:

Definition: A set x is said to be transitive if $y \in x \implies y \subset x$.

Definition (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 $\boldsymbol{\omega}$ 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.

Definition (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

Proposition 4.1: *If $n \in \boldsymbol{\omega}$ and $y \in n$ then $y \in \boldsymbol{\omega}$.*

Proof. 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.

Lemma 4.1: *$\forall n \in \boldsymbol{\omega}$, n is ordinary, in other words, $n \notin n$.*

Proof. 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.

Proposition 4.2: *$\forall n, m \in \boldsymbol{\omega}$, it cannot be that both $n \in m$ and $m \in n$.*

Proof. If $n \in m$ and $m \in n$ then by transitivity $m \subset n$, therefore $n \in n$ which contradicts the preceeding Lema 4.1 Q.E.D.

Proposition 4.3: *If $n \in \boldsymbol{\omega}$ then $n^+ \in \boldsymbol{\omega}$.*

Proof. Let $x \in n^+$ and $y \in x$. Then $x \in n$ or $x \in \{n\}$. If $x \in n$ then $x \in \boldsymbol{\omega}$, 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 4.1, 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.

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

Definition (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.

Theorem 4.1: *There is an inductive set.*

Proof. 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.

Theorem 4.2: *If $n \in \boldsymbol{\omega}$, n is in every inductive set.*

Proof. Let A be an inductive set. Assume that there is $n \in \boldsymbol{\omega}$ such that $n \notin A$. Then, $n \in n^+ \setminus A$, and $n^+ \in \boldsymbol{\omega}$ so we can define $x := \min n^+ \setminus A$ under $\in_{n^+}$. Now $x \in \boldsymbol{\omega}$ 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):

Theorem 4.3 (Theorem of infinity)**:** $\boldsymbol{\omega} \in \mathcal{V}$.

Proof. Let A be an inductive set. Then by Theorem 4.2 and Axiom **??**

$$\boldsymbol{\omega} = \{n \in A \mid n \text{ is a natural number}\} \subset A$$

so $\boldsymbol{\omega} \in \mathcal{V}$.
Q.E.D.

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

From Theorem 4.3 follows the known principle of induction.

Theorem 4.4 (Induction Principle)**:** *Let* P(x) *be a property of x. If*

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

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

then $\mathbf{P}(n)$ $\forall n \in \boldsymbol{\omega}$.

Proof. Let $W := \{k \in \boldsymbol{\omega} \mid \mathbf{P}(x)\}$. Then W is inductive, thus $\boldsymbol{\omega} \subset W$.

Q.E.D.

Definition (Order relation in $\boldsymbol{\omega}$)***:*** $\forall m, n \in \boldsymbol{\omega}$, $m \leq n \longleftrightarrow m \in n \vee m = n$.

Theorem 4.5: $(\boldsymbol{\omega}, \leq)$ *is a well ordered set.*

Proof. Let $l, m, n \in \boldsymbol{\omega}$. 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 4.1, 4.2 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, $n \in \boldsymbol{\omega}$ and $W = \{k \in \boldsymbol{\omega} \mid n \leq k \vee k \leq n\}$. If $n = 0$ then 0 and n are obviously $\leq$-comparable. If $n \neq 0$ then $0 \subset n$ and since $n \in \boldsymbol{\omega}$, $0 \in \boldsymbol{\omega}$ 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 $n \in \boldsymbol{\omega}$, 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 $\boldsymbol{\omega}$.

Finally, let U be a non-empty set of $\boldsymbol{\omega}$ 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.

Proposition 4.4: $\forall n \in \boldsymbol{\omega} \setminus \{0\}$ *there exists* $r \in \boldsymbol{\omega}$ *such that* $r^+ = n$

Proof. Let $W := \{x \in \boldsymbol{\omega} \mid x < n\}$. Obviously $0 \in W$. By Theorem 4.5, 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.

4.2 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.

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

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

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.

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

Definition (External right operation)***:*** Let A and B be a non-empty classes. We shall say that $\begin{aligned} F_D : A \times B &\longrightarrow A \\ (a, b) &\mapsto F_D((a, b)) \end{aligned}$ 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.

Definition (Algebraic structure)***:*** Let $k, l, m, n \in \boldsymbol{\omega}$. 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, $n_i \in \boldsymbol{\omega} \setminus \{0\}$ 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,
$n_j \in \boldsymbol{\omega} \setminus \{0, 1\}$ and $j \in m^+ \setminus \{0\}$,

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

Definition (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, $n_i \in \boldsymbol{\omega} \setminus \{0\}$ $i \in k^+ \setminus \{0\}$,

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, $m_q \in \boldsymbol{\omega} \setminus \{0, 1\}$ and $q \in n^+ \setminus \{0\}$.

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

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

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

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

i) There is a bijective function $\begin{array}{c} f : A \longrightarrow A' \\ {\scriptstyle a \mapsto f(a)} \end{array}$ such that:

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

2) The functions

$$\begin{array}{c} f^{k_j} : A^{k_j} \longrightarrow (A')^{k_j} \\ {\scriptstyle (\alpha_1, \dots, \alpha_{k_j}) \mapsto (f(\alpha_1), \dots, f(\alpha_{k_j}))} \end{array}$$

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

$f \circ F_i(\alpha_1, \dots, \alpha_{k_j}) = F'_i \circ f^{k_j}(\alpha_1, \dots, \alpha_{k_j})$, 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) $\forall p \in m^+ \setminus \{0\}$,

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

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:

Definition (g-inductive with starting element $\boldsymbol{\iota}$)***:*** Let A be a class and $\begin{array}{c} g : A \longrightarrow \mathcal{V} \\ {\scriptstyle a \mapsto g(a)} \end{array}$. 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 $\begin{array}{c} \mathrm{S} : \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega} \\ {\scriptstyle n \mapsto n^+} \end{array}$ as the succesor function, is a special case where $\boldsymbol{\omega}$ 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,

Definition (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 4.4 can be summed up to is that $\boldsymbol{\omega}$ is minimally inductive over $\underset{n \mapsto S(n)}{\mathrm{S} : \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ with starting element $\varnothing$. Now, to generalize:

Theorem 4.6 (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 $\mathbf{P}(x)\ \forall x \in A$.

Proof. 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:

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

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

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 $\boldsymbol{\omega}$, 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.

Theorem 4.7 (Dedekind's recursion theorem)**:** *Let A be a non-empty set, $a \in A$ and* $\underset{a \mapsto f(a)}{f : A \longrightarrow A}$ *a function. Then, there exists a unique function* $\underset{n \mapsto \phi(n)}{\phi : \boldsymbol{\omega} \longrightarrow A}$ *such that*

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

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

Proof. First, we prove the existence. Let

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

$Rs \neq \varnothing$ since $\boldsymbol{\omega} \times A \in Rs$. 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 $W := \{n \in \boldsymbol{\omega} \mid !\exists b \in A \text{ such that } (n, b) \in \phi\}$.

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 $W = \boldsymbol{\omega}$. Thus $\begin{array}{c}\phi : \boldsymbol{\omega} \longrightarrow A \\ n \mapsto \phi(n)\end{array}$ is a function.

Now, for the uniqueness. Assume there exists $\begin{array}{c}\phi_1 : \boldsymbol{\omega} \longrightarrow B \\ n \mapsto \phi_1(n)\end{array}$, $\begin{array}{c}\phi_2 : \boldsymbol{\omega} \longrightarrow A \\ n \mapsto \phi_2(n)\end{array}$ functions satisfying the hypotheses. Let $W_u := \{n \in \boldsymbol{\omega} \mid \phi_1(n) = \phi_2(n)\}$. $\phi_1(0) = a = \phi_2(0)$, 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, $W_u = \boldsymbol{\omega}$, and so $\phi_1 = \phi_2$.

Q.E.D.

Notice that the only property of $\boldsymbol{\omega}$ used for the proof is Theorem 4.4. This can be easily replaced by an argument of g-induction, and the proof remains almost the same. So we can state:

Theorem 4.8 (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 $\begin{array}{c}f : B \longrightarrow B \\ b \mapsto f(b)\end{array}$ a function. Then, there exists a unique function $\begin{array}{c}\lambda : A \longrightarrow B \\ x \mapsto \lambda(x)\end{array}$ such that*

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

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

Proof. 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 $\boldsymbol{\omega}_1 = \boldsymbol{\omega} \setminus \{0\}$.

Proposition 4.5: $\begin{array}{c}\mathrm{S} : \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega} \\ n \mapsto \mathrm{S}(n)\end{array}$ *is injective.*

Proof. Suppose that there exists $m, n \in \boldsymbol{\omega}$ 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 4.2 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.

Theorem 4.9 (Existence of a Peano system)**:** $(\boldsymbol{\omega}, \mathrm{S}, 0)$ *is a Peano system.*

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

Finally, by Theorem 4.4, $\boldsymbol{\omega}$ is S-inductive with starting element $\varnothing$.

Q.E.D.

Theorem 4.10 (Uniqueness of Peano systems)**:** *Any two Peano systems are isomorphic.*

Proof. Assume there are Peano systems (P, Σ, θ) and (P', Σ', θ'). We apply Theorem 4.8. For P, P', θ' and $\begin{array}{l}\Sigma' : P' \longrightarrow P' \\ \quad \rho' \mapsto \Sigma'(\rho')\end{array}$, there exists a unique function $\begin{array}{l}\lambda_1 : P \longrightarrow P' \\ \quad \rho \mapsto \lambda_1(\rho)\end{array}$ such that $\lambda(\theta) = \theta'$ and $\lambda_1(\Sigma(\rho)) = \Sigma'(\lambda_1(\rho))$. Using Theorem 4.8 again for P', P, θ and $\begin{array}{l}\Sigma : P \longrightarrow P \\ \quad \rho \mapsto \Sigma(\rho)\end{array}$ we can obtain $\begin{array}{l}\lambda_2 : P' \longrightarrow P \\ \quad \rho' \mapsto \lambda_2(\rho')\end{array}$ 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 4.8, that is, the uniqueness of a function $\begin{array}{l}\lambda : P \longrightarrow P \\ \quad \rho \mapsto \lambda(\rho)\end{array}$ 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 4.8, we obtain $\lambda_1 \circ \lambda_2 = \mathrm{id}_{P'}$. That is $\begin{array}{l}\lambda_1 : P \longrightarrow P' \\ \quad \rho \mapsto \lambda_1(\rho)\end{array}$ is a bijection. Thus $P \cong P'$.

Q.E.D.

Exercises

1) *(Alternate proof for Theorem 4.7)* Let A be a non-empty set and $a \in A$. Define a finite calculation by $\begin{array}{l}f_k : k \longrightarrow A \\ \quad x \mapsto f(x)\end{array}$ such that $f_k(0) = a$ and $f_k(\mathrm{S}(x)) = \mathrm{S}(f_k(x))$ for $k \in \boldsymbol{\omega}$. Use this to prove theorem 4.7.

2) Prove Theorem 4.8.

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 $\begin{array}{l}\mathrm{S}_{\mathcal{Z}} : \mathcal{V} \longrightarrow \mathcal{V} \\ \quad x \mapsto \{x\}\end{array}$ and $\boldsymbol{\omega}_{\mathcal{Z}}$ be the intersection of all $\mathrm{S}_{\mathcal{Z}}$-inductive classes.

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

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

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.

4.3 Arithmetic on $\boldsymbol{\omega}$

Modifications of the recursion theorem

Theorem 4.11 (Generalized recursion theorem)**:** *Let A be a non-empty set, $a \in A$. Suppose* $\underset{(n,a) \mapsto f((n,a))}{f : \boldsymbol{\omega} \times A \longrightarrow A}$ *is a function. Then there exists a unique function* $\underset{n \mapsto \phi(n)}{\phi : \boldsymbol{\omega} \longrightarrow A}$ *such that*

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

ii) $\forall n \in \boldsymbol{\omega}$*,* $\phi(\mathrm{S}(n)) = f(n, \mathrm{S}(n))$*.*

Proof. Same as Theorem 4.7. Q.E.D.

Theorem 4.12 (Modified recursion theorem)**:**
Let $\underset{(n,m) \mapsto G((n,m))}{G : \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ *,* $\underset{n \mapsto H(n)}{H : \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ *be functions. Then, there exists a unique function* $\underset{(n,m) \mapsto \phi((n,m))}{\phi : \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ *such that*

i) $\phi(n, 0) = H(n)$*,* $\forall n \in \boldsymbol{\omega}$*,*

ii) $\phi(x, \mathrm{S}(y)) = G(x, \phi(x, y))$*,* $\forall x, y \in \boldsymbol{\omega}$*.*

Proof. Let $n \in \boldsymbol{\omega}$. Consider $t_n := H(n)$, $G_n(z) := G(n, z)$ $\forall z \in \boldsymbol{\omega}$. Applying Theorem 4.7, there exists a unique function $\underset{x \mapsto \phi_n(x)}{\phi_n : \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ such that $\phi_n(0) = t_n$ and $\phi_n(\mathrm{S}(y)) = G_n(\phi_n(y))$ $\forall n, y \in \boldsymbol{\omega}$.

Define $\underset{(n,y) \mapsto \phi_n(y)}{\phi : \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$. 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, $\forall n \in \boldsymbol{\omega}$. Q.E.D.

Addition

Definition:

By Theorem 4.12, for $\underset{n \mapsto n}{\mathrm{id}_{\boldsymbol{\omega}} : \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ and $\underset{(m,n) \mapsto \mathrm{S}(n)}{\mathrm{S}(:)\, \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ there exists a unique function $\underset{(m,n) \mapsto \phi((m,n))}{\phi : \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ such that $\phi((n, 0)) = \mathrm{id}_{\boldsymbol{\omega}}(n) = n$ and $\phi((m, \mathrm{S}(n))) = \mathrm{S}(\phi((m, n)))$.

Let $+ := \phi$, and denote $m + n := +((m, n))$. We call $\underset{(m,n) \mapsto m+n}{+ : \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega}}$ the addition or the sum on $\boldsymbol{\omega}$.

Now, we can derive a proposition for a more intuitive notation for $\mathrm{S}(n)$.
Proposition 4.6: $\forall n \in \boldsymbol{\omega}$, $\mathrm{S}(n) = n + 1$.

Proof. Exercise. Q.E.D.

However, we will not use it for now.

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

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

i) $\begin{array}{c} * : A \times A \longrightarrow A \\ a \mapsto f(a) \end{array}$ 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.

Theorem 4.13 (Associative property)**:** $\forall l, m, n \in \boldsymbol{\omega},\ (l+m)+n = l+(m+n)$.

Proof. Let $l, m \in \boldsymbol{\omega}$ and consider $W_{l,m,+,A} := \{n \in \boldsymbol{\omega} \mid (l+m)+n = l+(m+n)\}$.

$l + m + 0 = l + m = l + (m + 0)$, 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.

Theorem 4.14 (Additive identity)**:** $\forall n \in \boldsymbol{\omega},\ n+0 = n = 0+n$.

Proof. By definition, $n + 0 = n\ \forall n \in \boldsymbol{\omega}$. Now, let $W_0 := \{n \in \boldsymbol{\omega} \mid 0+n = n\}$.

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 $W_0 = \boldsymbol{\omega}$. Q.E.D.

So, by Theorems 4.13 and 4.14, $(\boldsymbol{\omega}, +, 0)$ is a monoid. On top of that, we also prove that it is a commutative one.

First, we prove the following useful result:

Proposition 4.7 (Alternative application of the succesor function)**:**
$\forall n, m \in \boldsymbol{\omega},\ n+\mathrm{S}(m) = \mathrm{S}(n)+m$.

Proof. Let $n \in \boldsymbol{\omega}$ and consider the set $W_{\mathrm{S}(),n} := \{m \in \boldsymbol{\omega} \mid n+\mathrm{S}(m) = \mathrm{S}(n)+m\}$.

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.

Theorem 4.15 (Commutative property)**:** $\forall n, m \in \boldsymbol{\omega},\ n+m = m+n$.

Proof. Let $n \in \boldsymbol{\omega}$ and $W_{n,+,c} := \{m \in \boldsymbol{\omega} \mid n+m = m+n\}$. By Theorem 4.14, $0 \in W_{n,+,c}$. 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 4.7), that is $\mathrm{S}(l) \in W_{n,+,c}$. So, applying the induction principle we have $W_{n,+,c} = \boldsymbol{\omega}$ which brings our desired result. Q.E.D.

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

Theorem 4.16 (Additive cancelation)**:** $\forall l, m, n \in \boldsymbol{\omega}$

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

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

Proof. *i*) Let $W_{l,m,+,\not{c}} := \{n \in \boldsymbol{\omega} \mid l+n=m+n \longrightarrow l=m\}$.

Of course $l+0=m+0 \longrightarrow l=m$, so $0 \in W_{l,m,+,\not{c}}$. Now suppose $k \in W_{l,m,+,\not{c}}$. Then, if $l+\mathrm{S}(k)=m+\mathrm{S}(k)$, we will have $\mathrm{S}(l+k)=\mathrm{S}(m+k)$, and by Proposition 4.5 $l+k=m+k$. Thus $l=m$, and then $\mathrm{S}(k) \in W_{l,m,+,\not{c}}$. 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:

Lemma 4.2: $\forall n, m \in \boldsymbol{\omega},\ m+n \geq n$.

Proof. Let $U := \{x \in \boldsymbol{\omega} \mid m+x \geq x\}$. 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 $U=\boldsymbol{\omega}$.

Q.E.D.

Theorem 4.17: $\forall m, n \in \boldsymbol{\omega},\ m \leq n \longleftrightarrow \exists \alpha \in \boldsymbol{\omega}$ *such that* $m+\alpha=n$.

Proof. For $\exists \alpha \in \boldsymbol{\omega}$ such that $m+\alpha=n \longrightarrow m \leq n$ is clear.

Let $W := \{x \in \boldsymbol{\omega} \mid m+x=n\}$. By Lema 4.2 $W \neq \varnothing$. By Theorem 4.5, W has a minimum. Define $\alpha := \min W$, then $m+\alpha \geq n$. If $m+\alpha > n$, then by Proposition 4.4 there exists $r \in \boldsymbol{\omega}$ 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.

Theorem 4.18: $\forall l, m, n \in \boldsymbol{\omega},\ m \leq n \longleftrightarrow m+l \leq n+l$.

Proof. If $m=n$ since $\begin{array}{c} +: \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega} \\ (m,n) \mapsto m+n \end{array}$ is a function, we have $m+l=n+l$. Using Theorem 4.16 we get that $m+l=n+l \longrightarrow m=l$ holds.

Assume $m<n$. Then by Theorem 4.17 there exists $\alpha \in \boldsymbol{\omega}$ such that $m+\alpha=n$. Now, since $\begin{array}{c} +: \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega} \\ (x,y) \mapsto x+y \end{array}$ is a function, $m+\alpha+l=n+l$. By Lema 4.2 we have that $m+l \leq n+l$.

Now, if $m+l<n+l$, then $\exists \alpha \in \boldsymbol{\omega}$ such that $m+l+\alpha=n+l$. That is, by Theorem 4.16 $m+\alpha=n$ and then $m \leq m+\alpha=n$.

Q.E.D.

Finally, to end this subsection:

Theorem 4.19: $m+n=0 \longleftrightarrow m=0$ *and* $n=0$.

Proof. $m=0 \wedge n=0 \longrightarrow m+n=0$ 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

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

Consider $\begin{array}{l} f : \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega} \\ \quad n \mapsto 0 \end{array}$ and $\begin{array}{l} + : \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega} \\ \quad (m,n) \mapsto m+n \end{array}$. Then, by Theorem 4.12 there exists exactly one function $\begin{array}{l} \psi : \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega} \\ \quad (m,n) \mapsto \psi((m,n)) \end{array}$ 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 $\begin{array}{l} \cdot : \boldsymbol{\omega} \times \boldsymbol{\omega} \longrightarrow \boldsymbol{\omega} \\ \quad (m,n) \mapsto mn \end{array}$ the multiplication or the product on $\boldsymbol{\omega}$.

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.

Theorem 4.20 (Multiplicative indetity)**:** *$\forall n \in \boldsymbol{\omega}$, $1 \cdot n = n$.*

Proof. Let $W_{1,p} := \{n \in \boldsymbol{\omega} \mid 1 \cdot n = n\}$. $0 \in W_{1,p}$, 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 $W_{1,p} = \boldsymbol{\omega}$.
Q.E.D.

Theorem 4.21: *$\forall n \in \boldsymbol{\omega}$, $0 \cdot n = 0 = n \cdot 0$.*

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

Theorem 4.22 (Left distribution over sum)**:** *$\forall l, m, n \in \boldsymbol{\omega}$, $l(m+n) = lm + ln$*

Proof. Let $W_{l,d,s} := \{n \in \boldsymbol{\omega} \mid l(m+n) = lm + ln\}$. $l(m+0) = lm + l \cdot 0$ 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 $W_{l,d,s} = \boldsymbol{\omega}$.
Q.E.D.

Theorem 4.23 (Right distribution over sum)**:** *$\forall l, m, n \in \boldsymbol{\omega}$, $(l+m)n = ln + mn$*

Proof. Let $W_{r,d,s} := \{n \in \boldsymbol{\omega} \mid (l+m)n = ln + mn\}$. $(l+m) \cdot 0 = l \cdot 0 + m \cdot 0$ 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 $W_{r,d,s} = \boldsymbol{\omega}$.
Q.E.D.

Theorem 4.24 (Associative property)**:** *$\forall l, m, n \in \boldsymbol{\omega}$, $(lm)n = l(mn)$*

Proof. Let $W_{a,p} := \{n \in \boldsymbol{\omega} \mid (lm)n = l(mn)\}$. $(lm) \cdot 0 = l(m \cdot 0)$ 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 $W_{a,p} = \boldsymbol{\omega}$
Q.E.D.

Theorem 4.25 (Commutative property)**:** *$\forall m, n \in \boldsymbol{\omega}$, $mn = nm$*

Proof. Let $W_{c,p} := \{n \in \boldsymbol{\omega} \mid mn = nm\}$. By Theorem 4.3.3 $0 \in W_{c,p}$. Assume $l \in W_{c,p}$. Then $m\mathrm{S}(l) = lm + m = (l+1)m = \mathrm{S}(l)m$. Hence $W_{c,p} = \boldsymbol{\omega}$.
Q.E.D.

Theorem 4.26 (Multiplicative cancelation)**:** *$\forall l, m, n \in \boldsymbol{\omega}$,*

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

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

Proof. *ii*) Assume that $m \neq n$, without loss of generality $m < n$. Then $\exists r \in \boldsymbol{\omega}$ 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 4.16 $l = 0$, a contradiction. Hence $m = n$.

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

Theorem 4.27 (Integral domain property)**:** $\forall m, n \in \boldsymbol{\omega},\ mn = 0 \longrightarrow\ m = 0\ o\ n = 0.$

Proof. Assume $m \neq 0 \wedge n \neq 0$. Then $\exists r \in \boldsymbol{\omega}$ such that $\mathrm{S}(r) = n$. Then $m\mathrm{S}(r) = mr + m = 0$. By Theorem 4.16 $m = 0$, a contradiction. Hence $m = 0 \vee n = 0$. Q.E.D.

Theorem 4.28: $\forall l, m, n \in \boldsymbol{\omega},\ m < n \longleftrightarrow ml < nl.$

Proof. $\exists \alpha \in \boldsymbol{\omega}$ such that $m + \alpha = n$. Then $(m + \alpha)l = ml + m\alpha = nl$ and by Theorem 4.27 $\alpha l \neq 0$. Hence $ml < nl$.

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

Notice that with Theorems 4.20, 4.24 and 4.25 $(\boldsymbol{\omega}, \cdot, 1)$ 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 $m, n \in \boldsymbol{\omega}$, one and only one statement holds.
    i) $m = n$,
    ii) $m < n$,
    iii) $n < m$,

5
Extension to real numbers

5.1 Integers and rationals

5.2 Real numbers

5.3 Beyond reals

6
About infinity

6.1 Ordinals

6.2 Cardinality

6.3 The Axiom of Choice

A
Equivalence classes modulo n

B
Categories

B.1 Elements of categories

B.2 Formalization of categories

C
Mathematical logic

C.1 Metamathematics

C.2 Formalization

C.3 Beyond FOL

Bibliography

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