Course: Set Theory(Natural Numbers)

Sebastián Caballero

January 4, 2023

A simple notes template. Inspired by Tufte-LaTeXclass and beautiful notes by

`https://github.com/abrandenberger/course-notes`

1 *Motivation*

We've so far developed an interesting axiom system for the basics structures in set theory. With that, we can generalize many areas like algebra, analysis and more using sets, like a theory of everything. But what about numbers? They are a very strong concept in mathematics and its role is crucial. We can define what are numbers in term of sets? Yes! There are many possible constructions for them, but we are going to take the standard one that makes the most sense.

2 *Peano's axioms*

In our way to describe and construct numbers, we first need to think on what properties our construction needs. For example, when we constructed functions, they behave like the intuitive idea of pairing an element of the domain with exactly one element in the codomain. So, what properties must natural numbers obey? First, we need to think on the special element 0, which is a key part in thinking on further constructions. We also need to generate all the other numbers and we need induction on the set. These are called Peano Axioms for natural numbers. Summarizing:

Axiom 2.1 (Peano Axioms)**.** *A set which obey the Peano Axioms is a set N with a special element 0_N and a function $S : N \to N$ such that:*

- $0_N \in N$
- *For all $x, y \in N$ if $S(x) = S(y)$ then $x = y$*
- $0_N \neq S(x)$ *for all $x \in N$*
- *If $A \subseteq N$ such that $0_N \in A$, and if $x \in A$ then $S(x) \in A$, then $A = N$*

Ok, with these simple axioms we can develop a lot of theory on what we are looking to construct natural numbers. The most natural

feature in natural numbers is induction and with Peano Axioms, we can use it freely. Let's state a theorem for seeing how to use it:

Theorem 2.1. *Suppose N satisfies Peano Axioms. Then for all $x \in N$ other than 0_N, $x = S(y)$ for some $y \in N$.*

Proof. We will do it by induction. So, first define a set A as:

$$A := \{x \in N : x = 0_N \vee \exists y(y \in N \wedge x = S(y))\}$$

So, by definition, $0_N \in A$. Suppose that $x \in A$ and automatically, $S(x) \in A$. So, we have that $A = N$ and this property holds for all elements in N. □

Ok, it was so easy. So, let's prove a theorem a bit more complicated.

Theorem 2.2. *Suppose N satisfies Peano Axioms. Then for all $x \in N$, $S(x) \neq x$*

Proof. Again, define A as a subset of N and use induction to prove that it is N.

$$A := \{x \in N : x \neq S(x)\}$$

First, $0_N \in A$ because $0 \neq S(x)$ for all $x \in N$. Suppose that $x \in A$, so $x \neq S(x)$, and we are going to prove by contradiction that $S(x) \in A$. Suppose that $S(x) = S(S(x))$, but since S is injective, then $x = S(x)$ and it contradicts the fact that $x \in A$, so $S(x) \neq S(S(x))$ and $S(x) \in A$. We conclude that it is a valid property for all elements in N. □

This show us that every natural number has a successor and it is not itself. For example, we start we 0, and then by 1 and the successor of 1 is 2 which is different from 1 and so on. Another property needed is the functions that are defined by recursion, like the factorial. Remember that:

$$0! = 1$$
$$n! = n(n-1)!$$

So for calculate 4 factorial we do $4(3!)$ and we calculate 3! and so on until we get it is 24. For get sure we can do it, we have a theorem for that but it is a bit more complicated than it seems. So, our task is to construct a system that obeys Peano Axioms, call it $\mathbb{N}$ and prove that this system is in unique in essence.

3 Construction of $\mathbb{N}$

So far, we have just two sets that we know exist in our theory, the inductive set(Axiom 7) and the empty set(Axiom 2). Notice that the inductive set is likewise we want in the natural numbers, but we don't know if there is something more in the set(For example, $\mathcal{P}(\mathcal{P}(\emptyset))$) so our task is take any set that is just inductive. How we do that? Easy, with the intersection. If we call the set given by axiom 7 as $\mathcal{I}$ then we define the set of natural numbers as follows:

Definition 3.1 (Natural numbers)**.** *We define the set of natural numbers and noted by* $\mathbb{N}$ *as:*

$$\mathbb{N} := \bigcap \{x \in \mathcal{P}(\mathcal{I}) : \emptyset \in x \wedge \forall y(y \in x \to y \cup \{y\} \in x)\}$$

and any element of $\mathbb{N}$ *is called a natural number.*

So, let us think this a while. The first element we are given in the set is $\emptyset$ and later $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$ and so on. The first question that arises is whenever $\mathbb{N}$ is inductive.

Theorem 3.1. $\mathbb{N}$ *is inductive*

Proof. First, notice that $\emptyset \in \mathbb{N}$ since $\emptyset \in x$ for all $x \in \mathcal{P}(\mathcal{I})$. Suppose that $y \in \mathbb{N}$, then $y \in x$ for all $x \in \mathcal{P}(\mathcal{I})$ that are inductive, so $y \cup \{y\}$ is in all those sets and $y \cup \{y\} \in \mathbb{N}$. □

Good! So, we know that $\mathbb{N}$ is inductive. And we have an infinite list of elements in this set. So, how we choose 0 and $S : \mathbb{N} \to \mathbb{N}$? The answer is easy, since $\emptyset$ is the most basic set we know, it will be 0 and S will be defined as the successor in the inductive definition.

Definition 3.2. *For the set* $\mathbb{N}$ *we define that* $0 := \emptyset$ *and we define the function* $S : \mathbb{N} \to \mathbb{N}$ *as* $S(n) = n \cup \{n\}$ *for all* $n \in \mathbb{N}$*. We call it the successor of* n *and it is denoted as* n^+*.*

Ok, with that, we are just ready for prove what is needed for us in order to give $\mathbb{N}$ a structure. We are going to prove that indeed $\mathbb{N}$ holds Peano Axioms.

Theorem 3.2. $\mathbb{N}$ *with* 0 *and* S *holds Peano Axioms*

Proof. We need to show that all properties holds:

- First, if $x, y \in \mathbb{N}$ such that $S(x) = S(y)$ then $x \cup \{x\} = y \cup \{y\}$. So, we know that $y \in x^+$ so $y \in x$ or $y \in \{x\}$, but also $x \in y^+$ so $x \in y$

or $x \in \{y\}$. we have four possibilities:

1. If $x \in y$ and $y \in x$, we contradict axiom of foundation
2. If $x \in y$ and $y \in \{x\}$, we contradict axiom of foundation because $x = y$ but $x \in y$ so $x \in x$
3. If $x \in \{y\}$ and $y \in x$, we contradict axiom of foundation by the same reason
4. If $x \in \{y\}$ and $y \in \{x\}$ then $x = y$

We conclude that always $x = y$.

- Since $0 = \emptyset$ and $x \in x^+$ for all $x \in \mathbb{N}$, it is not possible that $x \in 0$ for some x, so $0 \neq x^+$ for all $x \in \mathbb{N}$
- Suppose that $A \subseteq \mathbb{N}$ is such that $0 \in A$ and for $x \in A$, $x^+ \in A$. By definition, A is inductive, so $A \in \mathcal{P}(\mathcal{I})$ and therefore $\mathbb{N} \subseteq A$, so we conclude that $A = \mathbb{N}$.

□

We have proved that $\mathbb{N}$ is a set with all the requirements we wanted! But is this set unique in its behave? Well, we can define an isomorphism between a set that holds Peano Axioms and $\mathbb{N}$, but for that, we need a tool that is powerful.

When we define $n!$, we define $0! = 1$ and later $n! = n(n-1)!$, and this is called a definition by recursion. Can we do it with natural numbers? Yes! That is what state the next theorem.

Theorem 3.3 (Recursion principle). *Let X be a set with a special element 0_X, and let $h : \mathbb{N} \times X \to X$ be a function. There exists a unique function $f : \mathbb{N} \to X$ such that:*

$$f(0) = 0_X$$
$$f(n^+) = h(n, f(n))$$

Proof. So, since $\mathbb{N}$ and X are nonempty we can create the function as:

$$\bigcap \{S \subseteq \mathbb{N} \times X : (0, 0_X) \in S \wedge \forall n \forall x((n, x) \in S \to (n^+, h(n, x)) \in S)\}$$

call it f. We can prove by induction that f is functional, so:

- Suppose that $(0, x)$ and $(0, y)$ are in f. We can assure that $x = 0_X$ or $y = 0_X$, but suppose that $x \neq 0_X$. Then define $S = f \setminus \{(0, x)\}$ and notice that $S \subseteq f$, but also $(0, 0_X) \in S$ and if $(n, a) \in S$ then $(n^+, h(n, a)) \in S$ by properties of f, so $f \subseteq S$ and therefore $f = S$, but this is a contradiction because $f \neq f \setminus \{(0, x)\}$, so $x = y$.

- Suppose that n have exactly one image and suppose that $(n^+, x)$and (n^+, y) in f and that $x \neq y$. One of them must be $h(n, f(n))$ so suppose it is not x. Define $S = f \setminus \{(n^+, x)\}$ and it is obvious that $S \subseteq f$. It is easy again to prove that $f \subseteq S$(It uses the fact that $f(n)$ is well defined) and we could have the contradiction of the base case. So, $x = y$.

And it is easy to see that it is whole since $(0, 0_X) \in f$ and by induction all $n \in \mathbb{N}$ has a image. □

Now, this will let us define operations and more in $\mathbb{N}$ but first, we want to show that every system that also satisfies Peano Axiom is in essence the same as $\mathbb{N}$.

Theorem 3.4. *For any set X that satisfies Peano Axioms, there is a function $f : \mathbb{N} \to X$ such that:*

1. *f is a bijection*
2. *$f(0) = 0_X$*
3. *$f(S(n)) = S_X(f(n))$, for all $n \in \mathbb{N}$*

Proof. The same statement let us define $h : \mathbb{N} \times X \to X$ such that $h(n, x) = S_X(x)$. Then by the other theorem we can define $f : X \to Y$

$$\begin{aligned} f(0) &= 0_X \\ f(n^+) &= S_X(f(n)) \end{aligned}$$

By definition, we satisfies 2 and 3. We just need to show that f is bijective.

- **Injective:** Let $A := \{n \in \mathbb{N} : \forall n' \in \mathbb{N}(f(n) = f(n') \to n = n')\}$, and let's prove that $A = N$. First, suppose that $n = 0$ and take x such that $x \neq n$, so $y^+ = x$ for some $y \in \mathbb{N}$, so $f(x) = f(y^+) = S_X(f(y))$ and since X satisfies Peano Axioms, then $0_X \neq S_X(a)$ for all $a \in X$, the $f(x) \neq f(n)$.
  Now, suppose this holds for n in general, and let's prove it for n^+. Suppose that $n^+ \neq x$. If $x = 0$, we are done but if it is not, then $x = a^+$ for some $a \in \mathbb{N} \setminus \{n\}$, and therefore:

$$\begin{aligned} f(x) &= f(a^+) \\ &= S_X(f(a)) \end{aligned}$$

  And also:

$$f(n^+) = S_X(f(n))$$

And by hypothesis, since $n \neq a$ then $f(a) \neq f(n)$, and $S_X(f(a)) = S_X(f(n))$. So, we have proved that $A = \mathbb{N}$ and f is injective.

- **Surjective:** Let $B := \{x \in X : \exists n \in \mathbb{N}(f(n) = x)\}$. We are going to prove that $B = X$. First, $0_X = f(0)$, so $0_X \in B$. Suppose that in general for $x \in X$, exists $n \in \mathbb{N}$ such that $f(n) = x$. Now, for n^+ we will have:

$$\begin{aligned} f(n^+) &= S_X(f(n)) \\ &= S_X(x) \end{aligned}$$

So $S_X(x) \in B$ and therefore $B = X$.

□

Corollary 3.1. *Any two structures that satisfies the Peano Axioms are isomorphic*

Proof. Suppose N_1, N_2 with $0_1, 0_2$ and S_1, S_2 are structures that satisfies Peano Axioms. Then, there are functions $f : \mathbb{N} \to N_1$ and $g : \mathbb{N} \to N_2$. Since f is bijective, it has an inverse which is also an isomorphism and if you compose $g \circ f$ that function will be the isomorphism needed. □

4 Order in $\mathbb{N}$

So far, our work has been focused on give a basic and unique structure to natural numbers. Now, our work is to create order in this set that acts just like the common order. How can we do that? Well, remember that $0 = \emptyset$ and $1 = \{\emptyset\}$, and then $2 = \{\emptyset, \{\emptyset\}\}$, but in general, it means that $n = \{0, 1, \ldots, n-1\}$, so we can define order in terms of whenever a set is inside other.

Definition 4.1 (Order in $\mathbb{N}$). *We shall say that if $n, m \in \mathbb{N}$, then $n < m$ if and only if $n \in m$. We say that $n \leq m$ if and only if $n < m$ or $n = m$*

Simple? Yes, but we are going to prove now that this generates a linear order in n.

Theorem 4.1. *The order given above holds the properties:*

- *Reflexive*
- *Antisymmetric*
- *Transitive*

Proof. The reflexive and Antisymmetric properties are consequences of the axiom of foundation and the definition for the weaker order. To prove that the order is Transitive, for fixed m, n we create the set:

$$A := \{p \in \mathbb{N} : m \in n \wedge n \in p \to m \in p\}$$

So, for $p = 0$, since $0 = \emptyset$ then $n \in \emptyset$ is false and the statement is true since $F \to F$ is true. Suppose that $p \in A$, we want to prove that $p^+ \in A$. So, since $n \in p^+$ then there are two options:

- $n \in p$: This implies that $m \in p$, and since $p \subseteq p^+$, then $m \in p^+$
- $n = p$: So, basically $m \in p$, and again $m \in p^+$

So $A = \mathbb{N}$ and therefore this property holds for any m, n, p. To □

So, with that we have that $\mathbb{N}$ has a partial order. In our way to prove that this order is total, we need to prove some little propositions.

Lemma 4.1. *If $m \in n$ then $m^+ \in n^+$*

Proof. For a fixed m, we will create the set:

$$A := \{n \in \mathbb{N} : m \in n \to m^+ \in n^+\}$$

So, $0 \in A$ since the antecedent is false. Now, suppose that $n \in A$. Assume that $m \in n^+$, and we are going to prove that $m^+ \in n^{++}$. So, if $m \in n^+$ there are two options. $m \in n$ or $m = n$. If $m \in n$, then $m^+ \in n^+$ and since $n^+ \subseteq n^{++}$ then $m^+ \in n^{++}$. If $m = n$, then $m^+ = n^+$ and $m^+ \in n^{++}$. □

Lemma 4.2. *For all $n \in \mathbb{N}$, if $n \neq 0$, then $0 \in n$.*

Proof. So, we can create the set:

$$A := \{n \in \mathbb{N} : 0 \in n \vee 0 = n\}$$

It is obvious that $0 \in A$. Suppose that $n \in A$, and $n \neq 0$. Then by definition, $0 \in n$. Now, since $n \subseteq n^+$, $0 \in n^+$ and therefore $A = \mathbb{N}$. □

Theorem 4.2. $\mathbb{N}$ *is linearly ordered by* $\in$

Proof. For a fixed $m \in \mathbb{N}$, define

$$A := \{n \in \mathbb{N} : n \in m \vee m \in n \vee n = m\}$$

So, if $m = 0$, it is obvious that $n = 0$ is in A. If $m \neq 0$, by the Lemma 4.2, $n = 0 \in m$. Suppose now that $n \in A$. So, we have three options:

- $n = m$, then $m \in m^+ = n^+$
- $m \in n$, and since $n \subseteq n^+$, we have that $m \in n^+$
- $n \in m$, so since m is not empty, there is $x \in \mathbb{N}$ such that $x^+ = m$. So $n \in x \cup \{x\}$, if $n = x$, then $n^+ = x^+ = m$. Else, since $n \in x$, $n^+ \in x^+ = m$.

Note that if $n \neq m$ and $m \in n$, by the axiom of foundation, $m \notin n$ and viceversa. And if $n = m$, then $n \notin m$ and $m \notin n$. □

Along with the induction, the rockstar property of $\mathbb{N}$ is the well ordering principle. We will end this section by proving it.

Lemma 4.3. *For all $n, m \in \mathbb{N}$, $m < n^+$ if and only if $m \leq n$*

Proof. $\Leftarrow$) Suppose $m < n^+$. Then $m \in n^+ = n \cup \{n\}$, so $m = n$ in which case, $m \leq n$ or $m \in n$, which again implies that $m \leq n$.

$\Rightarrow$) Suppose $m \leq n$. Then $m = n$ in which case since $n \in n^+$ then $m = n < n^+$ or $m \in n$, and since $n \subseteq n^+$ then $m \in n^+$ which implies that $m < n^+$.

□

Theorem 4.3 (Well ordering principle)**.** *Let X be a nonempty subset of $\mathbb{N}$. It holds that:*

$$(\exists x)(x \in X \wedge \forall y(y \in x \to x \leq y))$$

Proof. Suppose that this is false. So, for the set X we would have that:

$$(\forall x)(x \in X \to (\exists y)(y \in X \wedge y < x))$$

And so, we could create the next set:

$$A := \{n \in \mathbb{N} : (\forall m)(m \in \mathbb{N} \wedge m \leq n \to m \notin X)\}$$

And then, we would have that $0 \in A$, since the only element that is less or equal to 0 is itself and it cannot be in X since it would imply that X has a least element. Suppose that $n \in A$, and we are going to prove by contradiction that $n^+ \in A$. Suppose $n^+ \in X$, and then for all $m \in \mathbb{N}$, the fact that $m < n^+$ implies that $m \leq n$ and by induction hypothesis, $m \notin X$, so there is not element in X such that $y < n^+$, and it cannot be then in X.

We conclude that $A = \mathbb{N}$, and so, for all $n \in \mathbb{N}$, it is true that any element less or equal than n is not in X, in particular, since $n \leq n$ then $n \notin X$ for all X and X would be empty, contradicting the hypothesis. □

5 *Arithmetic for natural numbers*

The last thing we need to describe about natural numbers is how we can operate them. This should let us define three operations $+$, $\cdot$ and exponentiation, that behaves in the way we have learnt from school. For example, we will prove that $n+1=n^+$ and so on.

Remember the definition by recursion? That is the trick. Because we need that $m+0=0$ and if we think in addition in terms of the successor of n, we can define $m+n^+=m+(n+1)=(m+n)+1$, so we will use this to define the addition over natural numbers.

Definition 5.1 (Addition in $\mathbb{N}$). *Let m be a fixed natural number, we define for all $n\in\mathbb{N}$ as:*

$$\begin{aligned} m+n &= m & n &= 0\\ m+n^+ &= (m+n)^+ & n &\in \mathbb{N}\end{aligned}$$

We define this thinking in the theorem as follows:

Since m is fixed, we will define $f_m:\mathbb{N}\to\mathbb{N}$ but we need $h:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$, so we define $h(x,y)=y^+$ and this way, we will get:

$$\begin{aligned} f_m(0) &= m\\ f_m(n^+) &= h(n,f_m(n))=(f_m(n))^+\end{aligned}$$

But we denote $f_m(n)$ as $m+n$.

This gets with our intuition on natural numbers and also about the theorems we have proved so far. So, let's prove the important properties that come with the definition for addition:

Theorem 5.1 (Properties of $+$). *Let n,m,p be natural numbers.*

- $m+(n+p)=(m+n)+p$
- $0+n=n$
- $n+1=n^+$
- $m+n^+=m^++n$
- $m+n=n+m$

Proof. Suppose that n,m,p are natural numbers. The trick is to use induction for the most right variable since the definition is for a fixed value to the left and variable to the right.

- For $p=0$, the left side will be $m+(n+0)=m+n$ and the right

side will be $(m+n)+0 = m+n$. Suppose it is true for p, and:

$$\begin{aligned} m+(n+p^+) &= m+(n+p)^+ \\ &= (m+(n+p))^+ \\ &= ((m+n)+p)^+ \\ &= (m+n)+p^+ \end{aligned}$$

- For $n = 0$, then $0+0 = 0$ by definition, so it is true. Suppose it is true for n, so:

$$\begin{aligned} 0+n^+ &= (0+n)^+ \\ &= n^+ \end{aligned}$$

- By definition, we have:

$$\begin{aligned} n+1 &= n+0^+ \\ &= (n+0)^+ \\ &= n^+ \end{aligned}$$

- For $n = 0$, $m+0^+ = m+1 = m^+$, and $m^+ + 0 = m^+$. Suppose it is true for n and then:

$$\begin{aligned} m+n^{++} &= (m+n^+)^+ \\ &= (m^+ + n)^+ \\ &= m^+ + n^+ \end{aligned}$$

- For $n = 0$, $m+0 = m$ by definition and $0+m = m$. Suppose it is true for n, so:

$$\begin{aligned} m+n^+ &= (m+n)^+ \\ &= (n+m)^+ \\ &= n+m^+ \\ &= n^+ + m \end{aligned}$$

□

Ok! addition works just like we wanted! So time to define in a similar way what is multiplication. Think in the value of $m \cdot 0 = 0$, and we want that since $n^+ = n+1$, $m \cdot (n+1) = m \cdot n + m$.

Definition 5.2 (Multiplication of $\mathbb{N}$). *Let m a fixed natural num-*

ber and a variable natural number n, we define:

$$\begin{aligned} m \cdot n &= 0 & n &= 0 \\ m \cdot n^+ &= (m \cdot n) + m & n &\in \mathbb{N} \end{aligned}$$

Again, the justification for this definition is given by recursion on Peano systems.

We take $\mathbb{N}$ with the element 0. For a fixed $m \in \mathbb{N}$ we use the function $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that $h(x, y) = y + m$. So, we define the function $f_m : \mathbb{N} \to \mathbb{N}$ as:

$$\begin{aligned} f_m(0) &= 0 \\ f_m(n^+) &= h(n, f_m(n)) = f_m(n) + m \end{aligned}$$

Although we write $f_m(n)$ as $m \cdot n$.

Now, we are going to associate the properties of multiplication and addition in the next theorem.

Theorem 5.2 (Property of multiplication)**.** *Let m, n, p be natural numbers.*

- $m \cdot (n + p) = (m \cdot n) + (m \cdot p)$
- $m \cdot (n \cdot p) = (m \cdot n) \cdot p$
- $0 \cdot n = 0$
- $n \cdot 1 = n$
- $1 \cdot n = n$
- $(m + n) \cdot p = m \cdot p + n \cdot p$
- $m \cdot n = n \cdot m$

Proof. Suppose that n, m, p are natural numbers. The trick is to use induction for the most right variable since the definition is for a fixed value to the left and variable to the right.

- $p = 0$ the left side is $m \cdot (n + 0) = m \cdot n$, and the right side is $(m \cdot n) + (m \cdot 0) = (m \cdot n) + 0 = m \cdot n$. Suppose it is true for p.

$$\begin{aligned} m \cdot (n + p^+) &= m \cdot (n + p)^+ \\ &= (m \cdot (n + p)) + m \\ &= (m \cdot n + m \cdot p) + m \\ &= m \cdot n + (m \cdot p + m) \\ &= m \cdot n + m \cdot p^+ \end{aligned}$$

- For $p = 0$ the left side $m \cdot (n \cdot 0) = m \cdot 0 = 0$, and the right side will be $(m \cdot n) \cdot 0 = 0$, so it is true. Suppose that is true for p, so:

$$\begin{aligned} m \cdot (n \cdot p^+) &= m \cdot ((n \cdot p) + n) \\ &= m \cdot (n \cdot p) + m \cdot n \\ &= (m \cdot n) \cdot p + m \cdot n \\ &= (m \cdot n) \cdot p^+ \end{aligned}$$

- For $n = 0$ we will have that $0 \cdot 0 = 0$ by definition. Suppose it is true for n, then:

$$\begin{aligned} 0 \cdot n^+ &= 0 \cdot (n + 1) \\ &= 0 \cdot n + 0 \cdot 1 \\ &= 0 + 0 \cdot 0^+ \\ &= (0 \cdot 0) + 0 \\ &= 0 \end{aligned}$$

- By definition $n \cdot 1 = n \cdot 0^+ = (n \cdot 0) + n = 0 + n = n$.
- For $n = 0$, by the previous property $0 \cdot 1 = 0$. Suppose it is true for n, then:

$$\begin{aligned} 1 \cdot n^+ &= 1 \cdot (n + 1) \\ &= 1 \cdot n + 1 \cdot 1 \\ &= n + 1 \cdot 0^+ \\ &= n + (1 \cdot 0) + 1 \\ &= n + 0 + 1 \\ &= n + 1 \\ &= n^+ \end{aligned}$$

- For $p = 0$, the left side $(m + n) \cdot 0 = 0$, and the right side $m \cdot 0 + n \cdot 0 = 0 + 0 = 0$. Since it is true for $p = 0$ suppose it is true for p in general. Then:

$$\begin{aligned} (m + n) \cdot p^+ &= ((m + n) \cdot p) + (m + n) \\ &= m \cdot p + n \cdot p + m + n \\ &= m \cdot p + m + n \cdot p + n \\ &= m \cdot p^+ + n \cdot p^+ \end{aligned}$$

- For $n = 0$ we have that $m \cdot 0 = 0$ and $0 \cdot m = 0$, so it is true for

$n = 0$. Suppose it is true for n, we will have:

$$\begin{aligned} m \cdot n^+ &= (m \cdot n) + m \\ &= (n \cdot m) + m \\ &= n \cdot m + 1 \cdot m \\ &= (n+1) \cdot m \\ &= n^+ \cdot m \end{aligned}$$

□

Good! We need just a last operation given by multiplication: exponentiation. Similar to what we did, we use what we defined.

Definition 5.3 (Exponentiation on $\mathbb{N}$). *Let m be a fixed natural number with $m \neq 0$, and let n be a variable natural number:*

$$\begin{aligned} m^n &= 1 && n = 0 \\ m^{n^+} &= m^n \cdot m && n \in \mathbb{N} \end{aligned}$$

And for 0 we define $0^n = 0$ for $n > 1$.

Again, what we did was in terms of the recursive theorem as follows:

We take for a fixed $m \neq 0$ the function $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, such that $h(x, y) = y \cdot m$. We can define the function $f_m : \mathbb{N} \to \mathbb{N}$ as:

$$\begin{aligned} f_m(0) &= 1 \\ f_m(n^+) &= h(n, f_m(n)) = f_m(n) \cdot m \end{aligned}$$

And we usually write $f_m(n)$ as m^n.

So we can concrete the properties of operations within $\mathbb{N}$.

Theorem 5.3 (Properties of exponentiation). *Let m, n, p be natural numbers:*

- $1^n = 1$
- $n^1 = n$
- $m^{n+p} = m^n \cdot m^p$
- $(m^n)^p = m^{n \cdot p}$
- $(m \cdot n)^p = m^p \cdot n^p$

Proof. Suppose that n, m, p are natural numbers. The trick is to use induction for the most right variable since the definition is for a fixed value to the left and variable to the right.

- $1^0 = 1$ by definition for it is true for $n = 0$. Suppose it is true for n, so:

$$\begin{aligned} 1^{n^+} &= 1^n \cdot 1 \\ &= 1 \cdot 1 \\ &= 1 \end{aligned}$$

- n^1 is n^{0^+} and by definition it is $n^0 \cdot n = 1 \cdot n = n$.
- For $p = 0$ the left side is $m^{n+0} = m^n$ and the right side is $m^n \cdot m^0 = m^n \cdot 1 = m^n$. So it is true for $p = 0$, and we can suppose it is true for n in general. So,

$$\begin{aligned} m^{n+p^+} &= m^{(n+p)^+} \\ &= m^{n+p} \cdot m \\ &= m^n \cdot m^p \cdot m \\ &= m^n \cdot m^{p^+} \end{aligned}$$

- When $p = 0$ the left side is $(m^n)^0 = 1$ by definition and the right side is $m^{n \cdot 0} = m^0 = 1$. We can assume that it is true for p in general, and therefore:

$$\begin{aligned} (m^n)^{p^+} &= (m^n)^p \cdot (m^n) \\ &= m^{n \cdot p} \cdot m^n \\ &= m^{n \cdot p + n} \\ &= m^{n \cdot (p+1)} \\ &= m^{n \cdot p^+} \end{aligned}$$

- When $p = 0$ the left side is $(m \cdot n)^0 = 1$ by definition and $m^0 \cdot p^0 = 1 \cdot 1 = 1$. Assume it is true for n in general:

$$\begin{aligned} (m \cdot n)^{p^+} &= (m \cdot n)^p \cdot (m \cdot n) \\ &= m^p \cdot n^p \cdot m \cdot n \\ &= m^p \cdot m \cdot n^p \cdot n \\ &= m^{p^+} \cdot n^{p^+} \end{aligned}$$

□

And we are almost done! We just need to prove that we have the monotony in these operations. That means, that the operations must obey the order over which we defined the structure for $\mathbb{N}$.

Theorem 5.4. *For all $a, m, n \in \mathbb{N}$:*

- *If $m < n$ then $a + m < a + n$*
- *If $a > 0$ and $m < n$ then $a \cdot m < a \cdot n$*
- *If $a > 1$ and $m < n$ then $a^m < a^n$*

Proof. For all $a, m \in \mathbb{N}$ we are going to prove it by induction over n.

- For $n = 0$ it is obvious. The general case is when we take $n = m^+$, so we take that $(m + a) < (m + a)^+$ but it implies that $(m + a) < m^+ + a$ and therefore $m + a < n + a$. Suppose that it is true in general for n, and we are going to prove it for n^+. We can assume that $m < n < n^+$ since if $n \leq m$ it is what we have just proved. So, we have:

$$\begin{aligned} a + n^+ &= (a + n)^+ \\ &> a + n \\ &> a + m \end{aligned}$$

- For all cases when $n < m$ it is obvious. So, if we take $n = m^+$ we would take:

$$\begin{aligned} a \cdot m^+ &= a \cdot m + m \\ &> a \cdot m + 0 \\ &= a \cdot m \end{aligned}$$

  So we can assume it is true for n in general and that $m < n < n^+$ and we would have:

$$\begin{aligned} a \cdot n^+ &= a \cdot n + a \\ &> a \cdot n + 0 \\ &= a \cdot n \\ &> a \cdot m \end{aligned}$$

- The cases when $n < m$ are trivial. If we take $n = m^+$ then we would have that:

$$\begin{aligned} a^{m^+} &= a^m \cdot a \\ &> a^m \cdot 1 \\ &= a^m \end{aligned}$$

  So it is true for m^+. Suppose that it is true for n and that $m < n <$

n^+ so we would have:

$$\begin{aligned} a^{n^+} &= a^n \cdot a \\ &> a^n \cdot 1 \\ &= a^n \\ &> a^m \end{aligned}$$

□

And with this, we are done with the construction over natural numbers. Now, our interest is to explain with them what is a finite set.

6 *Finite sets*

When a set is finite? Our intuition says us that we can say that a set is finite if we can count its elements. For example, the set $\{3, 4, 5\}$ is finite because it only has 3 elements, and we know that $\mathbb{N}$ is infinite because we can't count all its elements. This concepts works very well, but how do we count when a set has n elements? Remember that for any natural number $n = \{0, 1, \ldots, n-1\}$ so every natural number has its very number of elements. So, we can say that there is a way to associate each element of n with each element of the other set if it is finite.

Definition 6.1 (Finite and infinite sets)**.** *Let X be a set, we say that X is finite if there is $n \in \mathbb{N}$ such that there is a bijection $f : X \to n$. If such number does not exists, then it is infinite.*

This idea is useful in the sense that we can associate sizes of sets with sets themselves. And it follows our intuition, so we need some results that let us derive intuitive but important results. For example, we need to show that $\mathbb{N}$ is infinite and we need to show that if $m < n$ then there cannot be such bijection.

Theorem 6.1 (Pigeon-hole principle)**.** *Suppose $f : n \to n$ is an injective function for $n \in \mathbb{N}$, then f must be Surjective.*

Proof. This is ridiculous true for $n = 0$, since there is not function from $\emptyset$ to itself that is injective but no Surjective. For $n = 1$ the unique function is $f(0) = 0$ that is injective and surjective. So, suppose it is true for n in general.

Let $f : n^+ \to n^+$ be an injective function, we need to pay attention to the restriction over n. There are two cases:

- $Ran(f|_n) \subseteq n$: in that case, the function $f|_n$ is injective and for all elements in n there is an element m such that $f|_n = (m)$, so since $f = f|_n \cup \{(n, n)\}$ we can see that the theorem is true.
- $Ran(f|_n) \not\subseteq n$: We would have that for some $x \in n$, $f(x) = n$ and also there must be $y \in n$ such that $f(n) = y$. We have then represented as a permutation the next situation:

$$\begin{pmatrix} 0 & 1 & \dots & x & \dots & n \\ f(0) & f(1) & \dots & n & \dots & y \end{pmatrix}$$

So we need to create a function with domain n, and what we are going to do is make it a function from n to n that is injective. It will look like:

$$\left(\begin{array}{ccccccc|c} 0 & 1 & \dots & x & \dots & n-1 & & n \\ f(0) & f(1) & \dots & y & \dots & f(n-1) & & n \end{array}\right)$$

So formally we have the function $g : n \to n$ such that:

$$g(i) = \begin{cases} y & i = x \\ f(i) & i \neq x \end{cases}$$

And note that this function is injective(This is thanks to the injective property of f) and therefore it is surjective. With this in mind, take $b \in n^+$, so we could have:

- $b = n$, in that case $f(x) = n$
- $b \neq y$, so we can be sure that $b \in n$ and therefore there is $a \in n$ such that $g(a) = b$. If $b = y$ then $g(x) = f(n) = y$. If it is not the case, then $g(a) = f(a) = b$

So we have just proved that f must be surjective.

□

This can be reformulated as *If we have a function $f : n \to n$ that is not surjective, it cannot be injective*. But if it is not surjective, $Ran(f) \subset n$ so what we are saying is that if we try to pair n with a proper subset, at least two different elements must map to the same image.

Corollary 6.1. *If A is a finite subset, and if $B \subset A$ there is not surjective any function $f : A \to B$ such that f is injective.*

And this incredibly let us prove that $\mathbb{N}$ is an infinite set. The proof is as elegant as one could think and this will derive some useful facts about the nature of infinity.

Theorem 6.2. *The set $\mathbb{N}$ is infinite*

Proof. Suppose there is a $n \in \mathbb{N}$ such that exists a bijection $f : \mathbb{N} \to n$, so we can create the restriction $f|_n : n \to n$, such that $f|_n(i) = f(i)$ for $i \in n$. Now, this means that the function $f|_n$ is injective since f is injective, so by the Pigeon-hole principle $f|_n$ is surjective. So $Ran(f|_n) = Ran(f) = n$. This means that $f(n) \in n$ although $n \notin n$, and also that there is an element $x \in n$ such that $f(x) = f(n)$, but since f is a bijection, $x = n$ and so $n \in n$ which is a contradiction! So $\mathbb{N}$ must be infinite. □

So far even when the axiom of infinite and more tools have talked us about the existence of infinite sets, this is the first time we can prove that a set is infinite. Now, there are sets that although are infinite they have the same size as $\mathbb{N}$, so we will make a definition for that.

Definition 6.2 (Countable sets). *Let X be a set. If there is a bijection $f : X \to \mathbb{N}$ we say that X is infinite countable. We say that a set is countable if it is finite or infinite countable and is no countable in other case.*

7 Exercises

The exercises are taken from Classic Set Theory: For Guided Independent Study By Derek Goldrei

Problem 1. *Show that for all $n, m \in \mathbb{N}$, $m < n$ if and only if $m \subset n$*

Proof. $\Rightarrow$) Suppose that $m < n$, so $m \in n$, and now suppose that $p \in m$. We have seen that in $\mathbb{N}$ the relation $\in$ is transitive, so $p \in n$, but this implies that $m \subset n$.

$\Leftarrow$) Suppose that $m \subset n$, it is impossible that $m = n$ because $(\exists x)(x \in n \wedge x \notin m)$ and if $n < m$ then $n \subset m$ but this would mean that $m \subset m$ which is absurd. So, we must conclude by the trichotomy that $m < n$.

□

Problem 2. *Show that for all $n \in \mathbb{N}$, if $x \in n$, then $x \in \mathbb{N}$.*

Proof. For $n = 0$, it is absurdly true. If $n = 1$, then $n = \{0\}$ and $0 \in \mathbb{N}$. Suppose this is true in general for n, and suppose that $x \in n^+$. Then, $x \in n$ or $x = n$. If $x \in n$, by the hypothesis $x \in \mathbb{N}$ and if $x = n$ it is obvious that $x \in \mathbb{N}$. □

Problem 3. *Show that for all $m, n \in \mathbb{N}$, $\min\{n, m\} = n \cap m$.*

Proof. Without loss of generality, we can suppose that $n \leq m$ and so $\min\{n, m\} = n$. This would implies that $n \subseteq m$ and therefore $n \cap m = n$, so $\min\{n, m\} = n \cap m$. □

Problem 4. *Show that for all $m, n, a \in \mathbb{N}$:*

- *If $a + m = a + n$ then $m = n$*
- *If $a > 0$ and $a \cdot m = a \cdot n$ then $m = n$*
- *If $a > 1$ and $a^m = a^n$ then $m = n$*

Proof. Suppose that $m \neq n$, then $m < n$ or $n < m$. Suppose with no loss of generality that $m < n$, so by the monotony laws we have:

- $a + m < a + n$
- If $a > 0$, $a \cdot m < a \cdot n$
- If $a > 1$, $a^m < a^n$

And since the relation $<$ is irreflexive(In other words, that $n \not< n$) then it is not possible that they are equal. So:

- $a + m \neq a + n$
- If $a > 0$, $a \cdot m \neq a \cdot n$
- If $a > 1$, $a^m \neq a^n$

□

Problem 5. *Let $n, m \in \mathbb{N}$:*

- *Show that $m + n = 0$ if and only if $m = n = 0$*
- *Show that $m \cdot n$ if and only if $m = 0$ or $n = 0$*

Proof. It is obvious the left side of both propositions. Now, for prove the other sides:

- Suppose $n \neq 0$ and m could be or not 0. Since $n \neq 0$ then $(\exists x)(x \in \mathbb{N} \wedge x^+ = n)$. This implies that:

$$\begin{aligned} m + n &= m + x^+ \\ &= (m + x)^+ \end{aligned}$$

  And since $a^+ \neq 0$ for any $a \in \mathbb{N}$, we have that $m + n \neq 0$.

- Suppose $m \cdot n = 0$ and that $n \neq 0$. Then, we can assure that $(\exists x)(x \in \mathbb{N} \wedge x^+ = n)$ and therefore:

$$\begin{aligned} m \cdot n &= m \cdot x^+ \\ &= (m \cdot x) + m = 0 \end{aligned}$$

  So by the previous proposition we can conclude that $m \cdot x = 0$, and especially $m = 0$.

□

Problem 6. *Prove that for all $n, m \in \mathbb{N}$, $m \leq n$ if and only if exists $k \in \mathbb{N}$ such that $m + k = n$.*

Proof. $\Rightarrow$) For $n = 0$ this is true easily true. Suppose it is true for n and suppose that $m \leq n^+$. If $m = n^+$ it is obvious so if $m < n^+$ then $m < n$ or $m = n$. For the first case, there is k such that $m + k = n$ and then $m + (k + 1) = n^+$. If $m = n$ then $m + 1 = n^+$.

$\Leftarrow$) The case for when $n = 0$ is trivial. Suppose this is true n, so that for n^+ if there is k such that $m + k = n^+$ there are two possibilities. If $k = 0$ then $m = n^+$. Else, $\exists x \in \mathbb{N}$ such that $x^+ = k$ and therefore:

$$\begin{aligned} m + k &= n^+ \\ m + x^+ &= n^+ \\ (m + x)^+ &= n^+ \\ m + x &= n \end{aligned}$$

And by the induction hypothesis, we have that $m \leq n$ and since $n < n^+$ then $m \leq n^+$.

□

Problem 7. *Prove that for all $a, b \in \mathbb{N}$, if $b > 0$ then there exists unique q, r such that $r < b$ and $a = bq + r$*

Proof. For a fixed $b > 0$, it is easy to see that the proposition is true for $a = 0$, since $0 = b \cdot 0 + 0$. Suppose $a = b \cdot q + r$ for $q, r \in \mathbb{N}$ and $r < b$. There are two cases, if $r^+ = b$ then:

$$\begin{aligned} a &= b \cdot q + r \\ a^+ &= b \cdot q + r^+ \\ a^+ &= b \cdot q + b \\ a^+ &= b \cdot (q + 1) + 0 \end{aligned}$$

But if $r^+ < b$ then

$$\begin{aligned} a &= b \cdot q + r \\ a^+ &= b \cdot q + r^+ \end{aligned}$$

And in any case, the proposition is true. So, it is true for all a. To prove that this is unique, then take $a = b \cdot q + r$ and $a = b \cdot p + s$ such that $p, q, r, s \in \mathbb{N}$ and $r, s < b$. Assume that $r \leq s$ so we would have that

$$\begin{aligned} b \cdot p + s &= b \cdot q + r \\ &\leq b \cdot q + s \end{aligned}$$

And we conclude that $p \leq q$. In the other hand, we have:

$$\begin{aligned} b \cdot q &\leq b \cdot q + r \\ &= b \cdot p + s \\ &< b \cdot p + b \\ &= b \cdot (p + 1) \end{aligned}$$

So $b \cdot q < b \cdot (p + 1)$ and we would have that $q < p + 1$, so we have in summary that $p \leq q < p + 1$ which is only possible if $p = q$. And now, it follows easily that $r = s$. □