1 The natural numbers

Lecture 1, Monday, August 28th, Last updated: 01/09/23, dmy.
Reading: [3, Ch.2-3]

We assume the notion of *set*, **??**, and take it as a primitive notion to mean a "collection of distinct objects."

Learning Objectives

Next eight lectures:

- To construct the objects:

$$\mathbb{N}, \quad \mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{R}$$

  and define the notion of *sets*, **??**.

- To prove properties and reason with these objects. In the process, you will learn various proof techniques. Most importantly, *proof by induction* and *proof by contradiction*.

This lecture:

- how to define the natural numbers, $\mathbb{N}$, and appreciate the role of *definitions*.

- how to apply induction. In particular, we would see that even proving statements as associativity of natural numbers is nontrivial!

Pedagogy

1. $\mathbb{N}$ is presented differently in distinct foundations, such as ZFC or type theory. Our presentation is to be *agnostic* of the foundation. From a working mathematician point of view, it *does not matter*, how the natural numbers are constructed, as long as they obey the properties of the axioms, 1.1.

2. We take the point of view that in mathematics, there are various type of objects. Among all objects studied, some happened to be *sets*. Some presentation of mathematics[a] will regard all objects as sets.

The various types of mathematics are more or less equivalent in our context.

[a] such as ZFC

Why should we delve into the foundations? Two reasons:

1. Foundational language is how many mathematicians do new mathematics. One defines new axioms and explores the possibilities.

2. How can we even discuss mathematics without having a rigorous understanding of our objects?

Discussion

A *natural (counting) number*[a], as we conceived informally is an element of

$$\mathbb{N} := \{0, 1, 2, \ldots\}$$

What is ambiguous about this?

- What does "$\cdots$" mean? How are we sure that the list does not cycle back?

- How does one perform operations?

- What *exactly* is a natural number? What happens if I say

$$\{0, A, AA, AAA, AAAA, \ldots\}$$

  are the numbers?

We will answer these questions over the course.

[a] It does not matter if we regard 0 as a natural number or not. This is a convention.

Forget about the natural numbers we love and know. If one were to define the *numbers*, one might conclude that the numbers are about a concept.

Axioms 1.1. The *Peano Axioms*: [1] Guiseppe Peano, 1858-1932.

1. 0 is a natural number.
$$0 \in \mathbb{N}$$

2. if n is a natural number then we have a natural number, called the *successor of* n, denoted $S(n)$.
$$\forall n \in \mathbb{N}, S(n) \in \mathbb{N}$$

[1] In 1900, Peano met Russell in the mathematical congress. The methods laid the foundation of *Principa Mathematica*

3. 0 is not the successor of any natural number.

$$\forall n \in \mathbb{N}, S(n) \neq 0$$

4. If $S(n) = S(m)$ then $n = m$.

$$\forall n, m \in \mathbb{N}, S(n) = S(m) \Rightarrow n = m$$

5. Principle of induction. Let $P(n)$ be any *property* on the natural number n. Suppose that

   a. $P(0)$ is true.
   b. When ever $P(n)$ is true, so is $P(S(n))$.

   Then $P(n)$ is true for all n natural numbers.

Discussion

What could be meant by a *property?* The principle of induction is in fact an *axiom schema*, consisting of a collection of axioms.

- "n is a prime".
- "$n^2 + 1 = 3$".

We have not yet shown that any collection of object would satisfy the axioms. This will be a topic of later lectures. So we will assume this for know.

Axiom 1.2. There exists a set $\mathbb{N}$, whose elements are the *natural numbers*, for which 1.1 are satisfied.

There can be many such systems, but they are all equivalent for doing mathematics.

Discussion

With only up to axiom 4: This can be *not* so satisfying. What have we done? We said we have a collection of objects that satisfy some concept F="natural numbers". But how do we know, Julius Ceasar does not belong to this concept?

Definition 1.3. We define the following natural numbers:

$$1 := S(0), 2 := S(1) = S(S(0)), 3 := S(2) = S(S(S(0)))$$

$$4 := S(3), 5 := S(4)$$

Intuitively, we want to continue the above process and say that whatever created iteratively by the above process are the *natural numbers*.

Discussion

- Give a set that satisfies axioms 1 and 2 but not 3.
- Give a set that satisfies axioms 1,2 and 3 but not 4.
- Give a set satisfying axioms 1,2,3 and 4, but not 5.

$$\{n/2 : n \in \mathbb{N}\} = \{0, 0.5, 1, 1.5, 2, 2.5, \cdots\}$$

Proposition 1.4. 1 is not 0.

Proof. Use axiom 3. □

Proposition 1.5. 3 is not equal to 0.

Proof. $3 = S(2)$ by definition, 1.3. If $S(2) = 0$, then we have a contradiction with Axiom 2, 1.1. □

1.1 Addition

Definition 1.6. (Left) Addition. Let $m \in \mathbb{N}$.

$$0 + m := m$$

Suppose, by induction, we have defined $n + m$. Then we define

$$S(n) + m := S(n + m)$$

In the context of 1.13, for each n, our function is $f_n := S : \mathbb{N} \to \mathbb{N}$ is $a_{S(n)} := S(a_n)$ with $a_0 = m$.

Proposition 1.7. For $n \in \mathbb{N}$, $n + 0 = n$.

Proof. Warning: we cannot use the definition 1.6. We will use the principle of induction. What is the *property* here in Axiom 5 of 1.1? The property $P(n)$ is "$0 + n = n$" for each $n \in \mathbb{N}$. We will also have to check the two conditions 5a. and 5b.

a "$P(0)$ *is true.*". People refer to this as the "base case $n = 0$": $0 + 0 = 0$, by 1.6.

b "*If $P(m)$ is true then $P(m+1)$ is true*". The statement "*Suppose $P(m)$ is true*" is often called the "inductive hypothesis". Suppose that $m + 0 = m$. We need to show that $P(S(m))$ *is true*, which is

$$S(m) + 0 = S(m)$$

By def, 1.6,

$$S(m) + 0 = S(m + 0)$$

By hypothesis,

$$S(m + 0) = S(m)$$

By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

Such proof format is the typical example for writing inductions, although in practice we will often leave out the italicized part.

Example

Prove by induction

$$\sum_{i=1}^{n} i^2 := 1^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

We observed that we have successfully shown *right* addition with respect to 0 behaves as expected.

Discussion

What should we expect $n + S(m)$ to be?

- Why can't we use 1.6?
- Where would we use 1.7?

Proof is hw.

Proposition 1.8. Prove that for $n, m \in \mathbb{N}$, $n + S(m) = S(n + m)$.

Proof. We induct on n. Base case: $m = 0$.

5b. Suppose $n + S(m) = S(n + m)$. We now prove the statement for

$$S(n) + S(m) = S(S(n) + m)$$

by definition of 1.6,

$$S(n) + S(m) = S(n + S(m))$$

which equals to the right hand side by hypothesis.

$\square$

Proposition 1.9. Addiction is commutative. Prove that for all $n, m \in \mathbb{N}$,

$$n + m = m + n$$

Proof. We prove by induction on n. With m fixed. We leave the base case away. $\square$

Proposition 1.10. Associativity of addition. For all $a, b, c \in \mathbb{N}$, we have

$$(a + b) + c = a + (b + c)$$

Proof. hw. $\square$

Discussion

Can we define "+" on any collection of things? What are examples of operations which are noncommutative and associative? For example, the collection of words?

$$+ : (\text{Seq. English words}) \times (\text{Seq. English words}) \to (\text{Seq. English words})$$

$$\text{"a"} , \text{"b"} \mapsto \text{"ab"}$$

This can be a meaningless operation. Let us restrict to the collection of *interpreable* outcomes. In the following examples, there is *structural ambiguity.*

1. (Ice) (cream latte)
2. (British) ((Left) (Waffles on the Falkland Islands))
3. (Local HS Dropouts) (Cut) (in Half)
4. (I ride) (the) (elephant in (my pajamas))
5. (We) ((saw) (the) (Eiffel tower flying to Paris.))

2,3 are actuay news title.

What use is there for addition? We can define the notion of *order* on $\mathbb{N}$. We will see later that this is a *relation* on $\mathbb{N}$.

Definition 1.11. Ordering of $\mathbb{N}$. Let $n, m \in \mathbb{N}$. We write $n \geq m$ or $m \leq n$ iff there is $a \in \mathbb{N}$, such that $n = m + a$.

1.2 Multiplication

Now that we have addition, we are ready to define multiplication as 1.6.

Definition 1.12.

$$0 \cdot m := 0$$

$$S(n) \cdot m := (n \cdot m) + m$$

1.3 Recursive definition

What does the induction axiom bring us? Please ignore the following theorem on first read.

Theorem 1.13. Recursion theorem. Suppose we have for each $n \in \mathbb{N}$,

$$f_n : \mathbb{N} \to \mathbb{N}$$

Let $c \in \mathbb{N}$. Then we can assign a natural number a_n for each $n \in \mathbb{N}$ such that

$$a_0 = c \quad a_{S(n)} = f_n(a_n) \forall n \in \mathbb{N}$$

Discussion

The theorem seems intuitively clear, but there can be pitfalls.

- When defining $a_0 = c$, how are we sure this is *not* redefined after some future steps? This is Axiom 3. of 1.1
- When defining $a_{S(n)}$ how are we sure this is not redefined? This uses Axiom 4. of 1.1.
- One rigorous proof is in [1, p48], but requires more set theory.

Proof. The property $P(n)$ of 1.1 is "{ a_n is well-defined}". Start with $a_0 = c$.

- Inductive hypothesis. Suppose we have defined a_n - meaning that there is only one value!
- We can now define $a_{S(n)} := f_n(a_n)$.

□

1.4 References and additional reading

- Nice lecture notes by Robert.
- Russell's book [2, 1,2] for an informal introduction to cardinals.

2 Homework for week 1

[2]

In these exercises: our goal is to get familiar with

- manipulating axioms in a definition.
- the notion of the principle of induction.

Problems:

1. Prove 5 is not equal to 2.
2. (*) Prove 1.8.
3. (*) Prove 1.9, assuming 1.8 if necessary.
4. (*) Prove 1.10 assuming 1.8, 1.9 if necessary.
5. (*) $n \in \mathbb{N}$ is *positive* if and only if $n \neq 0$. Prove that if $a, b \in \mathbb{N}$, *a is positive,* then $a + b$ is positive.
6. (***) Let M be a set with 2023 elements. Let N be a positive integer, $0 \leq N \leq 2^{2023}$. Prove that it is possible to color each subset of S so that
   (a) The union of two white subsets is white.
   (b) The union of two black subsets is black.
   (c) There are exactly N white subsets.
7. (**) Integers 1 to n are written ordered in a line. We have the following algorithm:
   - If the first number is k then reverse order of the first k numbers.

   Prove that 1 appears first in the line after a finite number of steps.
8. (**) We defined $\leq$ of natural numbers in 1.11. A finite sequence $(a_i)_{i=1}^n := \{a_1, \ldots, a_n\}$ of natural numbers is *bounded*, if there exists some other natural number M, such that $a_i \leq M$ for all $1 \leq i \leq n$. Show that every finite sequence of natural numbers, $a_1, \ldots, a_n$, is bounded.

[2] *Due: Week 2, Write the numbering of the three questions to be graded clearly on the top of the page. Each unstarred problem worth 12 points. Each star is an extra 5 points.*

Hints for problems

1: prove using Peano's axioms. First prove 3 is not equal to 0.

6: The number 2023 is irrelevant. Induct on the size of the set M. What happens when $M = 1$? For the inductive argument: suppose the statement is true when M has size n. In the case when M has size $n + 1$, consider when

- $0 \leq N \leq 2^n$. Use the hypothesis on the first n elements.
- $N \geq 2^n$. Use symmetry here that there was nothing special about "white".

7: Let us consider the inductive scenario. If $n + 1$ were in the first position, we are done by induction. Thus, let us suppose $n + 1$ never appears in the first position, *and* it is not in the last position, which is given by number $k \neq n + 1$.

- Would the story be the same if we switch the position of k and $n + 1$?

Discussion

As one observes, both 6 and 7 uses a natural *symmetry* in the problem.

Solutions to Week 1

Featured solutions: Solutions to Q1-6. Q1,5 by Kauí. Q2,3,4, by Granger.

Question 1: Show $5 \neq 2$

We know that $n \neq m \Rightarrow S(n) \neq S(m)$ (4th axiom)

Proof by contradiction:
Let's assume $5 = 2$.
Using contrapositive of 4th axiom: $5 = 2 \Rightarrow 4 = 1$
By the same reason: $4 = 1 \Rightarrow 3 = 0$
By definition, $3 := S(2)$
By the 3rd axiom, 0 cannot be the successor of any number. So, since 3 is the successor of a number (the number 2), then $3 \neq 0$, which contradicts the initial assumption $5 = 2$.
Thus, $5 \neq 2$.

2. Prove that for $n, m \in N$, $n + S(m) = S(n + m)$
(Proof by induction where m is fixed)

Base case $n = 0$
$0 + S(m) = S(0 + m)$
By definition of addition $0 + S(m) := S(m)$ and $0 + m = m$.
Thus, $S(m) = S(m)$, is true.

Inductive hypothesis $n + S(m) = S(n + m)$

We need to show $S(n) + S(m) = S(S(n) + m)$
By definition of addition $S(n) + S(m) := S(n + S(m))$
By the inductive hypothesis $S(n + S(m)) = S(S(n + m))$
Again, by the definition of addition $S(S(n) + m) =S(S(n + m))$
Therefore the left and right hand sides are equivalent, and by induction $\forall n, m \in N$, $n + S(m) = S(n + m)$ is true.

Accessory Proof required for proposition 3. Prove for all-natural number n, $n + 0 = n$.
(Proof by induction)

Base case $n = 0$

By definition of addition, $0 + m = 0$, thus $0 + 0 = 0$ follows as true.

Inductive hypothesis $n + 0 = n$

We need to show $S(n) + 0 = S(n)$
By definition of addition, $S(n) + 0 := S(n + 0)$
By inductive hypothesis, $S(n + 0) = S(n)$
Therefore, by induction, for all natural number n, $n + 0 = n$.

3. Prove that Addition is commutative for all $n, m \in N$, $n + m = m + n$
   (Proof by induction where m is fixed)

   Base case $n = 0$
   $0 + m = m + 0$
   By definition of addition $0 + m = m$.
   By accessory proof of $n + 0 = n$, $m + 0 = m$.
   Therefore $m = m$.

   Inductive hypothesis $n + m = m + n$

   We need to show that $S(n) + m = m + S(n)$.
   By definition of addition, $S(n) + m := S(n + m)$.
   By proof 2, $m + S(n) = S(m + n)$.
   By the inductive hypothesis, $S(m + n) = S(n + m)$.
   Therefore, $S(n + m) = S(n + m)$ is true.
   Therefore, by induction, for all $n, m \in N$, $n + m = m + n$

4. Associativity of addition. For all $a, b, c \in N$, we have $(a + b) + c = a + (b + c)$
   (Proof by induction where b and c are fixed)

   Base case $a = 0$.
   $(0 + b) + c = 0 + (b + c)$.
   By definition of addition $(0 + b) = b$.
   By definition of addition $0 + (b + c) = (b + c)$.
   Therefore, $b + c = b + c$, follows as true.

   Inductive hypothesis $(a + b) + c = a + (b + c)$.

   We need to show that $(S(a) + b) + c = S(a) + (b + c)$.
   By definition of addition, $S(a) + b := S(a + b)$.
   By definition of addition, $S(a + b) + c := S((a + b) + c)$.
   By definition of addition, $S(a) + (b + c) := S(a + (b + c))$.
   Therefore, $S((a + b) + c) = S(a + (b + c))$.

   By the inductive hypothesis, $S((a + b) + c) = S(a + (b + c))$.
   Therefore, $S(a + (b + c)) = S(a + (b + c))$ follows as true.
   Thus, it follows by induction, for all $a, b, c \in N$, we have $(a + b) + c = a + (b + c)$.

Question 5: $n \in N$ is positive if and only if $n \neq 0$. Prove that if $a, b \in N$, a is positive, then $a + b$ is positive.

We know that (I): $n + 0 = 0 + n := n$
We also know that (II): $n + S(m) = S(n) + m := S(n+m)$

Now, let's apply the 5th axiom (induction):

- Base case: $b = 0$
    - Using (I) $a + 0 = a$, which is a positive natural.
- Inductive hypothesis: $a + b$ is a positive natural.
    - We have to show that: $a + S(b)$ is also a positive natural.
    - Using (II): $a + S(b) = S(a + b)$.
    - The 3rd axiom states that 0 is not the successor of any number. Thus, $a + S(b) \neq 0$, since $a + S(b)$ is the successor of $a + b$.
    - Moreover, by the 2nd axiom, $a + S(b)$ is a natural number, since it is the successor of a natural number $(a + b)$.
    - Therefore, $a + S(b)$ is positive, since it is natural and different from 0.
    - Thus, induction follows.

Solution to problem 6:

We will write cs short hand for coloring scheme. We will induct on the size, n, of the set.
What is our property [3]$P(n)$**?:** It is the conjunction of the following two properties:

$R(n)$:

{ $\forall$ set A, $|A| = n$, and $0 \leq N \leq 2^n$, exists cs on the subsets of A so (a) -(c) are true }

$Q(n)$:

{ $\forall$ set A, $|A| = n$, and $0 \leq N \leq 2^n$, exists cs on the subsets of A so (a) -(c') are true }

where (c') is the statement that

"exactly N sets are black".

To be a conjunction means that $P(n)$ is true if and only if $Q(n)$ and $R(n)$ is true. [4]

Base case $P(1)$ **is true:** [5] Let A be any set with $|A| = 1$. In this case, $A = \{a\}$, for some object a. the subsets of $A = \{a\}$ are

$$\emptyset, \{a\}$$

The conditions are easy to check for $0 \leq N \leq 2$, for either the statements $Q(n)$ and $R(n)$. We omit this.

Inductive step: we show that if $P(n)$ **is true (inductive hypothesis) then** $P(n+1)$ **is too.** As $P(n)$ is true, for a choice of $0 \leq N \leq 2^n$, there exists *two* cs on the subsets of any set of size n, so that the union conditions (a)- (c) and (a)-(c') are satisfied, respectively. We will use both cs.

Consider a set A with $n+1$ elements. Let us denote label elements of the set:

$$A = \{a_1, \ldots, a_n, a_{n+1}\}$$

We prove that $R(n+1)$ is true, the same argument holds for $Q(n+1)$. There are two types of subsets, let us call them type I, and type II:

[3] Remember, this is any sentence that we can assign a truth or false value, Ax 5. 1.1.
[4] Although our goal is really to prove that $R(n)$ is true for all n, we will exploit this symmetry during induction.
[5] you can also do $n = 0$. But let us be more fun.

I Those that do not contain a_{n+1}. There are 2^n of them, and these are subsets of $A' := \{a_1, \ldots, a_n\}$.

II Those that contain a_{n+1}. There are $2^{n+1} - 2^n = 2^n$ of them.

We color these sets depending on our choice of N:

1. if $0 \leq N \leq 2^n$. We use the cs of $R(n)$ from the inductive hypothesis and color the subsets of type I (these are subsets of A'). We color all sets of type II (contain a_{n+1}) black. Let us check the conditions: [6]

   (a) If you have two white subsets, they must be type I. Their union is still white, by cs of from hypothesis.

   (b) If the two black subsets are both type I, their union is still type I, and is black by hypothesis. If at least one of them is type II, then their union contains a_{n+1}, hence is of type II, and thus is black by our cs.

2. If $N > 2^n$, this is same as asking a cs on the subsets of A where we color $N' := 2^{n+1} - N \leq 2^n$ subsets black. *Now* we use the cs of $Q(n)$ from the inductive hypothesis on A'. Similar argument from 1.

[6] This is easier to go through yourself and read the explanation.

References

[1] Paul R. Halmos, *Naive set theory*, 1961.

[2] Bertrand Russell, *Introduction to mathematical philosophy* (2022).

[3] Terence Tao, *Analysis I, 4th edition*, 2022.