

Concepts in Abstract Mathematics

NATURAL NUMBERS – 2



UNIVERSITY OF
TORONTO

January 14th, 2021

From last Tuesday: Peano's axioms

Theorem: Peano axioms

There exists a set $\mathbb{N}$ together with an element $0 \in \mathbb{N}$ "zero" and a function $s : \mathbb{N} \rightarrow \mathbb{N}$ "successor" such that:

- 1 0 is not the successor of any element of $\mathbb{N}$, i.e. 0 is not in the image of s :

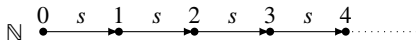
$$0 \notin s(\mathbb{N})$$

- 2 If the successor of n equals the successor of m then $n = m$, i.e. s is injective:

$$\forall n, m \in \mathbb{N}, s(n) = s(m) \implies n = m$$

- 3 *The induction principle.* If a subset of $\mathbb{N}$ contains 0 and is closed under s then it is $\mathbb{N}$:

$$\forall A \subset \mathbb{N}, \left\{ \begin{array}{l} 0 \in A \\ s(A) \subset A \end{array} \right. \implies A = \mathbb{N}$$



The addition – 1

We are going to define $\mathbb{N} \rightarrow \mathbb{N}$
 $b \mapsto a + b$ for a given $a \in \mathbb{N}$.

The addition – 1

We are going to define $\mathbb{N} \rightarrow \mathbb{N}$
 $b \mapsto a + b$ for a given $a \in \mathbb{N}$.

How to do so? What would be a good definition to obtain what you intuitively know about $+$?

The addition – 1

We are going to define $\mathbb{N} \rightarrow \mathbb{N}$
 $b \mapsto a + b$ for a given $a \in \mathbb{N}$.

How to do so? What would be a good definition to obtain what you intuitively know about $+$?

The idea is to define it inductively using the following properties we would like to have:

- $a + 0 = a$
- For $b \in \mathbb{N}$, $a + (b + 1) = (a + b) + 1$

The addition – 1

We are going to define $\mathbb{N} \rightarrow \mathbb{N}$
 $b \mapsto a + b$ for a given $a \in \mathbb{N}$.

How to do so? What would be a good definition to obtain what you intuitively know about $+$?

The idea is to define it inductively using the following properties we would like to have:

- $a + 0 = a$
- For $b \in \mathbb{N}$, $a + (b + 1) = (a + b) + 1$
So if $a + b$ is already defined, then we can define $a + (b + 1)$.
Remember that intuitively $+1$ is "taking the successor".

The addition – 1

We are going to define $\begin{matrix} \mathbb{N} & \rightarrow & \mathbb{N} \\ b & \mapsto & a + b \end{matrix}$ for a given $a \in \mathbb{N}$.

How to do so? What would be a good definition to obtain what you intuitively know about $+$?

The idea is to define it inductively using the following properties we would like to have:

- $a + 0 = a$
- For $b \in \mathbb{N}$, $a + (b + 1) = (a + b) + 1$
So if $a + b$ is already defined, then we can define $a + (b + 1)$.
Remember that intuitively $+1$ is "taking the successor".

Formally, we prove:

Proposition

Let $a \in \mathbb{N}$. Then there exists a unique function $(a + \bullet) : \begin{matrix} \mathbb{N} & \rightarrow & \mathbb{N} \\ b & \mapsto & a + b \end{matrix}$ such that

- 1 $a + 0 = a$ 2 $\forall b \in \mathbb{N}, a + s(b) = s(a + b)$

The above result is a consequence of the induction principle.

Remark

Set $1 := s(0)$. Then, as expected, for $n \in \mathbb{N}$, we have

$$n + 1 = n + s(0) = s(n + 0) = s(n)$$

Hence, from now on, I will use indistinctively $n + 1$ or $s(n)$.

The addition – 2

Remark

Set $1 := s(0)$. Then, as expected, for $n \in \mathbb{N}$, we have

$$n + 1 = n + s(0) = s(n + 0) = s(n)$$

Hence, from now on, I will use indistinctively $n + 1$ or $s(n)$.

We can prove the following properties.

Proposition

- $\forall a, b, c \in \mathbb{N}, a + (b + c) = (a + b) + c$ (*the addition is associative*)
- $\forall a, b \in \mathbb{N}, a + b = b + a$ (*the addition is commutative*)
- $\forall a, b, c \in \mathbb{N}, a + b = a + c \implies b = c$ (*cancellation*)
- $\forall a, b \in \mathbb{N}, a + b = 0 \implies a = b = 0$

The addition – 3

Proof that $\forall a, b, c \in \mathbb{N}, a + (b + c) = (a + b) + c$.

The addition – 3

Proof that $\forall a, b, c \in \mathbb{N}, a + (b + c) = (a + b) + c$.

Let $a, b \in \mathbb{N}$. Set $A = \{c \in \mathbb{N} : a + (b + c) = (a + b) + c\}$. Then

- $A \subset \mathbb{N}$
- $0 \in A$. Indeed, $a + (b + 0) = a + b = (a + b) + 0$.
- $s(A) \subset A$. Indeed, let $n \in s(A)$ then $n = s(c)$ for some $c \in A$. Therefore
$$a + (b + n) = a + (b + s(c)) = a + s(b + c) = s(a + (b + c)) = s((a + b) + c) = (a + b) + s(c) = (a + b) + n.$$
Hence $n \in A$.

Thus, by the induction principle, $A = \mathbb{N}$ and for any $c \in \mathbb{N}$, $a + (b + c) = (a + b) + c$. ■

The addition – 3

Proof that $\forall a, b, c \in \mathbb{N}, a + (b + c) = (a + b) + c$.

Let $a, b \in \mathbb{N}$. Set $A = \{c \in \mathbb{N} : a + (b + c) = (a + b) + c\}$. Then

- $A \subset \mathbb{N}$
- $0 \in A$. Indeed, $a + (b + 0) = a + b = (a + b) + 0$.
- $s(A) \subset A$. Indeed, let $n \in s(A)$ then $n = s(c)$ for some $c \in A$. Therefore
$$a + (b + n) = a + (b + s(c)) = a + s(b + c) = s(a + (b + c)) = s((a + b) + c) = (a + b) + s(c) = (a + b) + n.$$
Hence $n \in A$.

Thus, by the induction principle, $A = \mathbb{N}$ and for any $c \in \mathbb{N}$, $a + (b + c) = (a + b) + c$. ■

Proof that $\forall a, b \in \mathbb{N}, a + b = 0 \implies a = b = 0$.

The addition – 3

Proof that $\forall a, b, c \in \mathbb{N}, a + (b + c) = (a + b) + c$.

Let $a, b \in \mathbb{N}$. Set $A = \{c \in \mathbb{N} : a + (b + c) = (a + b) + c\}$. Then

- $A \subset \mathbb{N}$
- $0 \in A$. Indeed, $a + (b + 0) = a + b = (a + b) + 0$.
- $s(A) \subset A$. Indeed, let $n \in s(A)$ then $n = s(c)$ for some $c \in A$. Therefore
$$a + (b + n) = a + (b + s(c)) = a + s(b + c) = s(a + (b + c)) = s((a + b) + c) = (a + b) + s(c) = (a + b) + n.$$
Hence $n \in A$.

Thus, by the induction principle, $A = \mathbb{N}$ and for any $c \in \mathbb{N}$, $a + (b + c) = (a + b) + c$. ■

Proof that $\forall a, b \in \mathbb{N}, a + b = 0 \implies a = b = 0$.

Let $a, b \in \mathbb{N}$ be such that $a + b = 0$. Assume by contradiction that $a \neq 0$ or $b \neq 0$.

Without loss of generality, we may assume that $b \neq 0$ (using commutativity).

Then $b = s(n)$ for some $n \in \mathbb{N}$.

So $0 = a + b = a + s(n) = s(a + n)$.

Which is a contradiction since $0 \notin s(\mathbb{N})$. ■

The multiplication – 1

We define inductively $\begin{array}{ccc} \mathbb{N} & \rightarrow & \mathbb{N} \\ b & \mapsto & a \times b \end{array}$ for a given $a \in \mathbb{N}$ using the following desired properties:

- $a \times 0 = 0$
- For $b \in \mathbb{N}$, $a \times (b + 1) = (a \times b) + a$
So if $a \times b$ is already defined, then we can define $a \times (b + 1)$.

The multiplication – 1

We define inductively $\begin{array}{ccc} \mathbb{N} & \rightarrow & \mathbb{N} \\ b & \mapsto & a \times b \end{array}$ for a given $a \in \mathbb{N}$ using the following desired properties:

- $a \times 0 = 0$
- For $b \in \mathbb{N}$, $a \times (b + 1) = (a \times b) + a$
So if $a \times b$ is already defined, then we can define $a \times (b + 1)$.

Formally, we prove:

Proposition

Let $a \in \mathbb{N}$. Then there exists a unique function $(a \times \bullet) : \begin{array}{ccc} \mathbb{N} & \rightarrow & \mathbb{N} \\ b & \mapsto & a \times b \end{array}$ such that

- ① $a \times 0 = 0$ ② $\forall b \in \mathbb{N}, a \times s(b) = (a \times b) + a$

The multiplication – 1

We define inductively $\begin{array}{c} \mathbb{N} \\ b \end{array} \mapsto \begin{array}{c} \mathbb{N} \\ a \times b \end{array}$ for a given $a \in \mathbb{N}$ using the following desired properties:

- $a \times 0 = 0$
- For $b \in \mathbb{N}$, $a \times (b + 1) = (a \times b) + a$
So if $a \times b$ is already defined, then we can define $a \times (b + 1)$.

Formally, we prove:

Proposition

Let $a \in \mathbb{N}$. Then there exists a unique function $(a \times \bullet) : \begin{array}{c} \mathbb{N} \\ b \end{array} \mapsto \begin{array}{c} \mathbb{N} \\ a \times b \end{array}$ such that

- ① $a \times 0 = 0$ ② $\forall b \in \mathbb{N}, a \times s(b) = (a \times b) + a$

Remark

It is common to simply write ab for $a \times b$ when there is no possible confusion.

Proposition

- $\forall a, b, c \in \mathbb{N}, a \times (b \times c) = (a \times b) \times c$ (*the multiplication is associative*)
- $\forall a, b \in \mathbb{N}, a \times b = b \times a$ (*the multiplication is commutative*)
- $\forall a, b, c \in \mathbb{N}, a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$ ($\times$ *is distributive over* $+$)
- $\forall a \in \mathbb{N}, a \times 1 = a$
- $\forall a, b \in \mathbb{N}, a \times b = 0 \implies (a = 0 \text{ or } b = 0)$
- $\forall a, b, c \in \mathbb{N}, \begin{cases} a \times b = a \times c \\ a \neq 0 \end{cases} \implies b = c$ (*cancellation*)

Definition: binary relation

A **binary relation** $\mathcal{R}$ on a set E consists in associating a truth value to every couple $(x, y) \in E^2$. We say that x is related to y by $\mathcal{R}$, denoted $x\mathcal{R}y$, if the value *true* is assigned to (x, y) .

Examples

- ❶ Let $E = \{a, b, c\}$. We can define a binary relation $\mathcal{R}$ using a truth table as below:

$\begin{array}{c} x \\ \diagdown \\ y \end{array}$	a	b	c
a	✓	✗	✗
b	✗	✗	✓
c	✓	✓	✗

Here $a\mathcal{R}a$, $a\mathcal{R}c$, $b\mathcal{R}c$ and $c\mathcal{R}b$.

- ❷ For $E = \mathbb{R}$, we can define a binary relation as follows: $\forall (x, y) \in \mathbb{R}^2, x\mathcal{R}y \Leftrightarrow x^2 - y^2 = x - y$.

Definition: order

We say that a binary relation $\mathcal{R}$ on a set E is an *order* if

- 1 $\forall x \in E, x\mathcal{R}x$ (*reflexivity*)
- 2 $\forall x, y \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}x) \implies x = y$ (*antisymmetry*)
- 3 $\forall x, y, z \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}z) \implies x\mathcal{R}z$ (*transitivity*)

We say that the order $\mathcal{R}$ is *total* if additionally $\forall x, y \in E, x\mathcal{R}y$ or $y\mathcal{R}x$.

Definition: order

We say that a binary relation $\mathcal{R}$ on a set E is an *order* if

- 1 $\forall x \in E, x\mathcal{R}x$ (*reflexivity*)
- 2 $\forall x, y \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}x) \implies x = y$ (*antisymmetry*)
- 3 $\forall x, y, z \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}z) \implies x\mathcal{R}z$ (*transitivity*)

We say that the order $\mathcal{R}$ is *total* if additionally $\forall x, y \in E, x\mathcal{R}y$ or $y\mathcal{R}x$.

Definition: the usual order $\leq$ on $\mathbb{N}$

We define the binary relation $\leq$ on $\mathbb{N}$ by $\forall a, b \in \mathbb{N}, (a \leq b \Leftrightarrow \exists k \in \mathbb{N}, b = a + k)$.

The intuition behind this definition is that $a \leq b$ if we need to add some k to a in order to reach b .

Definition: order

We say that a binary relation $\mathcal{R}$ on a set E is an *order* if

- 1 $\forall x \in E, x\mathcal{R}x$ (*reflexivity*)
- 2 $\forall x, y \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}x) \implies x = y$ (*antisymmetry*)
- 3 $\forall x, y, z \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}z) \implies x\mathcal{R}z$ (*transitivity*)

We say that the order $\mathcal{R}$ is *total* if additionally $\forall x, y \in E, x\mathcal{R}y$ or $y\mathcal{R}x$.

Definition: the usual order $\leq$ on $\mathbb{N}$

We define the binary relation $\leq$ on $\mathbb{N}$ by $\forall a, b \in \mathbb{N}, (a \leq b \Leftrightarrow \exists k \in \mathbb{N}, b = a + k)$.

The intuition behind this definition is that $a \leq b$ if we need to add some k to a in order to reach b .

Notation

We write $a < b$ for $(a \leq b \text{ and } a \neq b)$.

Theorem

The set of natural numbers $\mathbb{N}$ is totally ordered for $\leq$.

Theorem

The set of natural numbers $\mathbb{N}$ is totally ordered for $\leq$.

Proof.

① *Reflexivity.* Let $a \in \mathbb{N}$, then $a = a + 0$ with $0 \in \mathbb{N}$, hence $a \leq a$.

② *Antisymmetry.* Let $a, b \in \mathbb{N}$ be such that $a \leq b$ and $b \leq a$.

Then there exists $k, l \in \mathbb{N}$ such that $b = a + k$ and $a = b + l$.

Therefore $a = b + l = a + k + l$. Hence $0 = k + l$ and thus $l = k = 0$ so that $a = b$.

③ *Transitivity.* Let $a, b, c \in \mathbb{N}$ be such that $a \leq b$ and $b \leq c$.

Then there exists $k, l \in \mathbb{N}$ such that $b = a + k$ and $c = b + l$.

Therefore $c = b + l = a + (k + l)$ with $k + l \in \mathbb{N}$, i.e. $a \leq c$.

④ *$\leq$ is total.* Let $a \in \mathbb{N}$. Set $A = \{b \in \mathbb{N} : a \leq b \text{ or } b \leq a\}$. Then

- $A \subset \mathbb{N}$
- $0 \in A$, indeed $a = 0 + a$ so that $0 \leq a$.
- $s(A) \subset A$

Indeed, let $n \in s(A)$. Then $n = s(b)$ for some $b \in A$, i.e. $a \leq b$ or $b \leq a$.

- If $a \leq b$ then $b = a + k$ for some $k \in \mathbb{N}$, $n = s(b) = b + 1 = a + k + 1$ with $k + 1 \in \mathbb{N}$, so that $a \leq n$.

- If $b \leq a$ then $a = b + l$ for some $l \in \mathbb{N}$. We may assume that $l \neq 0$ (since $a = b$ was in the above case).

Then $l = \tilde{l} + 1$ for some $\tilde{l} \in \mathbb{N}$. Hence $a = b + l = b + \tilde{l} + 1 = b + 1 + \tilde{l} = n + \tilde{l}$, i.e. $n \leq a$.

In both cases $n \in A$.

Therefore, by the induction principle, $A = \mathbb{N}$. So, for all $b \in \mathbb{N}$, either $a \leq b$ or $b \leq a$.

Proposition

- 1 $\forall a \in \mathbb{N}, a \leq 0 \implies a = 0$
- 2 $\forall a, b, c \in \mathbb{N}, a + b \leq a + c \implies b \leq c$
- 3 There is no $a \in \mathbb{N}$ such that $0 < a < 1$.
- 4 There is no $a \in \mathbb{N}$ such that $\forall b \in \mathbb{N}, b \leq a$.
- 5 $\forall a, b, c \in \mathbb{N}, a \leq b \implies ac \leq bc$

Proposition

- 1 $\forall a \in \mathbb{N}, a \leq 0 \implies a = 0$
- 2 $\forall a, b, c \in \mathbb{N}, a + b \leq a + c \implies b \leq c$
- 3 There is no $a \in \mathbb{N}$ such that $0 < a < 1$.
- 4 There is no $a \in \mathbb{N}$ such that $\forall b \in \mathbb{N}, b \leq a$.
- 5 $\forall a, b, c \in \mathbb{N}, a \leq b \implies ac \leq bc$

Proof.

- 1 Let $a \in \mathbb{N}$ be such that $a \leq 0$. Then there exists $k \in \mathbb{N}$ such that $0 = a + k$. Hence $a = k = 0$.
- 2 Let $a, b, c \in \mathbb{N}$. Assume that $a + b \leq a + c$. Then there exists $k \in \mathbb{N}$ such that $a + c = a + b + k$. Thus $c = b + k$ so that $b \leq c$ as expected.
- 3 Let $a \in \mathbb{N}$. Assume that $a < 1$, then there exists $l \in \mathbb{N} \setminus \{0\}$ such that $1 = a + l$. Since $l \neq 0$, $l = k + 1$ for some $k \in \mathbb{N}$, and $1 = a + k + 1$ so that $0 = a + k$. Therefore $a = 0$.
- 4 Assume by contradiction that there exists $a \in \mathbb{N}$ such that $\forall b \in \mathbb{N}, b \leq a$. Then $a + 1 \leq a$ hence $1 \leq 0$, i.e. $0 = 1 + k$ for some $k \in \mathbb{N}$. Therefore $1 = 0$ which is a contradiction (otherwise $0 = s(0)$).
- 5 Let $a, b, c \in \mathbb{N}$. Assume that $a \leq b$. Then $b = a + k$ for some $k \in \mathbb{N}$. Thus $bc = (a + k)c = ac + kc$ with $kc \in \mathbb{N}$. Therefore $ac \leq bc$.

The well-ordering principle

Theorem: the well-ordering principle

A nonempty subset A of $\mathbb{N}$ has a least element, i.e. there exists $n \in A$ such that $\forall a \in A, n \leq a$.

The well-ordering principle

Theorem: the well-ordering principle

A nonempty subset A of $\mathbb{N}$ has a least element, i.e. there exists $n \in A$ such that $\forall a \in A, n \leq a$.

Proof.

Let's prove the contrapositive, i.e. if a subset $A \subset \mathbb{N}$ doesn't have a least element then it is empty.

The well-ordering principle

Theorem: the well-ordering principle

A nonempty subset A of $\mathbb{N}$ has a least element, i.e. there exists $n \in A$ such that $\forall a \in A, n \leq a$.

Proof.

Let's prove the contrapositive, i.e. if a subset $A \subset \mathbb{N}$ doesn't have a least element then it is empty.

Let $B = \{a \in \mathbb{N} : \forall i \leq a, i \notin A\}$.

The well-ordering principle

Theorem: the well-ordering principle

A nonempty subset A of $\mathbb{N}$ has a least element, i.e. there exists $n \in A$ such that $\forall a \in A, n \leq a$.

Proof.

Let's prove the contrapositive, i.e. if a subset $A \subset \mathbb{N}$ doesn't have a least element then it is empty.

Let $B = \{a \in \mathbb{N} : \forall i \leq a, i \notin A\}$.

- $B \subset \mathbb{N}$

The well-ordering principle

Theorem: the well-ordering principle

A nonempty subset A of $\mathbb{N}$ has a least element, i.e. there exists $n \in A$ such that $\forall a \in A, n \leq a$.

Proof.

Let's prove the contrapositive, i.e. if a subset $A \subset \mathbb{N}$ doesn't have a least element then it is empty.

Let $B = \{a \in \mathbb{N} : \forall i \leq a, i \notin A\}$.

- $B \subset \mathbb{N}$
- $0 \in B$ (otherwise 0 would be the least element of A).

The well-ordering principle

Theorem: the well-ordering principle

A nonempty subset A of $\mathbb{N}$ has a least element, i.e. there exists $n \in A$ such that $\forall a \in A, n \leq a$.

Proof.

Let's prove the contrapositive, i.e. if a subset $A \subset \mathbb{N}$ doesn't have a least element then it is empty.

Let $B = \{a \in \mathbb{N} : \forall i \leq a, i \notin A\}$.

- $B \subset \mathbb{N}$
- $0 \in B$ (otherwise 0 would be the least element of A).
- $s(B) \subset B$

Indeed, if $n \in s(B)$, then $n = s(a)$ for $a \in B$, i.e. $\forall i \leq a, i \notin A$.

Note that $n = a + 1 \notin A$ otherwise it would be the least element of A .

Therefore $\forall i \leq n, i \notin A$, i.e. $n \in B$.

The well-ordering principle

Theorem: the well-ordering principle

A nonempty subset A of $\mathbb{N}$ has a least element, i.e. there exists $n \in A$ such that $\forall a \in A, n \leq a$.

Proof.

Let's prove the contrapositive, i.e. if a subset $A \subset \mathbb{N}$ doesn't have a least element then it is empty.

Let $B = \{a \in \mathbb{N} : \forall i \leq a, i \notin A\}$.

- $B \subset \mathbb{N}$
- $0 \in B$ (otherwise 0 would be the least element of A).
- $s(B) \subset B$

Indeed, if $n \in s(B)$, then $n = s(a)$ for $a \in B$, i.e. $\forall i \leq a, i \notin A$.

Note that $n = a + 1 \notin A$ otherwise it would be the least element of A .

Therefore $\forall i \leq n, i \notin A$, i.e. $n \in B$.

Thus, by the induction principle, $B = \mathbb{N}$ so A is empty. 