University of Toronto – MAT246H1-S – LEC0201/9201 – Winter 2021

*Concepts in Abstract Mathematics*

# 1 - Natural numbers

Jean-Baptiste Campesato

In this chapter we introduce the set $\mathbb{N}$ of natural numbers. We will start with a minimal axiomatic description of it from which we will derive the main properties of $\mathbb{N}$.

Intuitively, we describe $\mathbb{N}$ starting from $0$ and repeatedly doing the operation $+1$ (we say that we take the successor): $1$ is the successor of $0$, $2$ is the successor of $1$, $3$ is the successor of $2$ and so on...This operation is governed by a few rules in order to make sure that the set we obtain coincides with our intuitive expectation about what should be $\mathbb{N}$.

The method of *proof by induction* is closely related to the nature of $\mathbb{N}$. Hence we will study it at the end of this chapter.

I use the convention that $\mathbb{N}$ is the set of non-negative integers, i.e. $0 \in \mathbb{N}$.

## Contents

## 1 Peano axioms

All the results concerning the natural numbers will derive from the next theorem, that we admit, and which states the existence of $\mathbb{N}$.

**Theorem 1** (Peano axioms)**.** *There exists a set $\mathbb{N}$ together with an element $0 \in \mathbb{N}$ read as* zero *and a function $s : \mathbb{N} \to \mathbb{N}$ read as* successor *such that:*

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

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

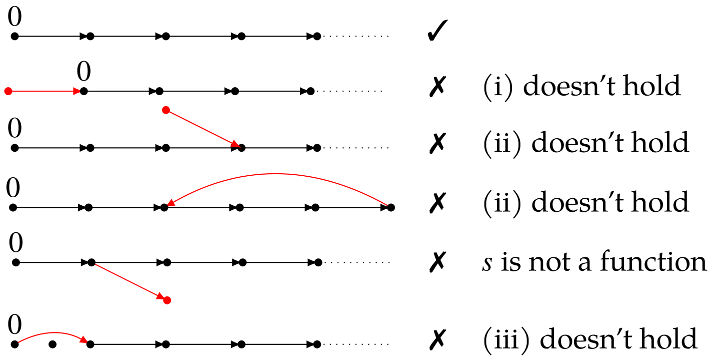
$(ii)$ *If the successor of $n$ equals the successor of $m$ then $n = m$, i.e. $s$ is injective:*

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

$(iii)$ 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 set $\mathbb{N}$ is the set of *natural numbers*. As we will see, all the results of $\mathbb{N}$ will derive from the above basic properties. The last axiom basically means that all the elements of $\mathbb{N}$ can be obtained from 0 by taking the successor iteratively. Intuitively, the successor of $n$ is $s(n) = n + 1$ (actually, it will become formal after we define the addition, see Remark 6).



Below are some basic propositions relying only on Peano axioms.

**Proposition 2.** *Any non-zero natural number is the successor of a natural number, i.e.*

$$\forall n \in \mathbb{N} \setminus \{0\},\ \exists m \in \mathbb{N},\ n = s(m)$$

*Proof.* Set $A = s(\mathbb{N}) \cup \{0\}$. Then

- $A \subset \mathbb{N}$
- $0 \in A$
- $s(A) \subset s(\mathbb{N}) \subset A$

Hence, by the induction principle, $A = \mathbb{N}$.
Let $n \in \mathbb{N} \setminus \{0\}$, then $n \in A$ but $n \neq 0$, therefore $n \in s(\mathbb{N})$. So there exists $m \in \mathbb{N}$ such that $n = s(m)$. ■

**Proposition 3.** *A natural number is never its own successor, i.e.*

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

*Proof.* Set $A = \{n \in \mathbb{N} \ :\ n \neq s(n)\}$. Then

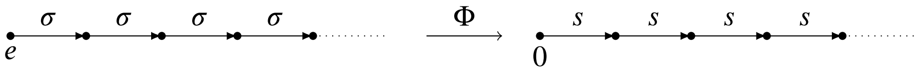
- $A \subset \mathbb{N}$
- $0 \in A$ since $0 \notin s(\mathbb{N})$ (particularly $0 \neq s(0)$)
- $s(A) \subset A$
  Indeed, let $m \in s(A)$. Then $m = s(n)$ for some $n \in A$. So $s(n) \neq n$.
  Since $s$ is injective, we get that $s(s(n)) \neq s(n)$, i.e. $s(m) \neq m$.
  Hence $m \in A$.

So, by the induction principle, $A = \mathbb{N}$. Thus, for every $n \in \mathbb{N}$ we have that $n \neq s(n)$. ■

**Remark 4** (You can skip it)**.** Up to a bijection, $\mathbb{N}$ is uniquely defined by the Peano axioms.
More precisely, if there exists a set $S$, with an element $e \in S$ and a function $\sigma : S \to S$ such that

(i) $e \notin \sigma(S)$
(ii) $\forall x, y \in S,\ \sigma(x) = \sigma(y) \implies x = y$
(iii) $\forall A \subset S,\ \begin{cases} e \in A \\ \sigma(A) \subset A \end{cases} \implies A = S$

then there exists a bijection $\Phi : S \to \mathbb{N}$ such that $\Phi(e) = 0$, $s(\Phi(x)) = \Phi(\sigma(x))$.



# 2 Addition, multiplication and order

## 2.1 Addition

The following proposition defines inductively the function *addition with a*.

**Proposition 5.** *Let $a \in \mathbb{N}$. Then there exists a unique function* $(a+\bullet) : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ b & \mapsto & a+b \end{array}$ *such that*

(*i*) $a+0=a$
(*ii*) $\forall b \in \mathbb{N},\ a+s(b)=s(a+b)$

*Proof.* This function is well defined by the induction principle (i.e. we didn't miss any element of the domain $\mathbb{N}$ using this iterative definition).
Let's check that it is unique. Let $\varphi : \mathbb{N} \to \mathbb{N}$ be such that $\varphi(0)=a$ and $\forall b \in \mathbb{N},\ \varphi(s(b))=s(\varphi(b))$.
Set $A=\{b \in \mathbb{N} \ : \ \varphi(b)=a+b\}$. Then

- $A \subset \mathbb{N}$
- $0 \in A$ since $\varphi(0)=a=a+0$.
- $s(A) \subset A$. Indeed, let $c \in s(A)$. Then $c=s(b)$ for some $b \in A$ and

$$\begin{aligned}\varphi(c) &= \varphi(s(b)) \quad \text{since } c=s(b) \\ &= s(\varphi(b)) \quad \text{by definition of } \varphi \\ &= s(a+b) \quad \text{since } b \in A \\ &= a+s(b) \quad \text{by definition of } a+\bullet \\ &= a+c \quad \text{since } s(b)=c\end{aligned}$$

Hence $c \in A$.

Therefore, by the induction principle, $A=\mathbb{N}$. Thus, for every $b \in \mathbb{N}$ we have that $\varphi(b)=a+b$. ∎

**Remark 6.** We set $1 \coloneqq s(0)$. Then, for $n \in \mathbb{N}$, $n+1=n+s(0)=s(n+0)=s(n)$. As expected...
Hence, from now on, I will use indistinctively $n+1$ or $s(n)$ (depending on which notation seems to be the more convenient).
Similarly, $2 \coloneqq s(1)$, $3 \coloneqq s(2)$, $4 \coloneqq s(3)$ and so on...

**Proposition 7.**

1. $\forall a,b,c \in \mathbb{N},\ a+(b+c)=(a+b)+c$ (the addition is associative)
2. $\forall a,b \in \mathbb{N},\ a+b=b+a$ (the addition is commutative)
3. $\forall a,b,c \in \mathbb{N},\ a+b=a+c \implies b=c$ (cancellation)
4. $\forall a,b \in \mathbb{N},\ a+b=0 \implies a=b=0$

*Proof.*

1. 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

$$\begin{aligned}a+(b+n) &= a+(b+s(c)) \quad \text{since } n=s(c) \\ &= a+s(b+c) \\ &= s(a+(b+c)) \\ &= s((a+b)+c) \quad \text{since } c \in A \\ &= (a+b)+s(c) \\ &= (a+b)+n\end{aligned}$$

   Hence $n \in A$.

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

2. Sketch of proof:
   (a) Prove that $\forall a \in \mathbb{N}$, $0 + a = a + 0$ using the induction principle.
   *Hint:* $0 + s(a) = s(0 + a) = s(a + 0) = s(a) = s(a) + 0$
   (b) Prove that $\forall a \in \mathbb{N}$, $s(a) = 1 + a$ using the induction principle.
   *Hint:* $s(s(a)) = s(1 + a) = (1 + a) + 1 = 1 + (a + 1) = 1 + s(a)$.
   (c) Let $a \in \mathbb{N}$. Prove that $\forall b \in \mathbb{N}$, $a + b = b + a$.
   *Hint:* $a + s(b) = s(a + b) = s(b + a) = b + s(a) = b + (1 + a) = (b + 1) + a = s(b) + a$

3. Set $A = \{a \in \mathbb{N} \,:\, \forall b, c \in \mathbb{N},\ a + b = a + c \implies b = c\}$. Then
   - $A \subset \mathbb{N}$
   - $0 \in A$
   - $s(A) \subset A$
   Indeed, let $n \in s(A)$. Let $b, c \in \mathbb{N}$ such that $n + b = n + c$. We want to prove that $b = c$.
   There exists $a \in A$ such that $n = s(a)$. Then

$$\begin{aligned}
&n + b = n + c\\
\Rightarrow\ & s(a) + b = s(a) + c\\
\Rightarrow\ & b + s(a) = c + s(a) \quad \text{by commutativity}\\
\Rightarrow\ & s(b + a) = s(c + a) \quad \text{by construction of the addition}\\
\Rightarrow\ & b + a = c + a \quad \text{since } s \text{ is injective}\\
\Rightarrow\ & a + b = a + c \quad \text{by commutativity}\\
\Rightarrow\ & b = c \quad \text{since } a \in A
\end{aligned}$$

   Hence $n \in A$.

   Thus, by the induction principle, $A = \mathbb{N}$.

4. Let $a, b \in \mathbb{N}$ be such that $a + b = 0$. Assume by contradiction that $a \neq 0$ or $b \neq 0$.
   Without lost of generality, we may assume that $b \neq 0$ (using commutativity).
   Then, by Proposition 2, $b = s(n)$ for some $n \in \mathbb{N}$. So $0 = a + b = a + s(n) = s(a + n)$.
   Which is a contradiction since $0 \notin s(\mathbb{N})$.

■

## 2.2 Multiplication

The following proposition defines inductively the function *multiplication with a*.

**Proposition 8.** *Let $a \in \mathbb{N}$. Then there exists a unique function* $(a \times \bullet) : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ b & \mapsto & a \times b \end{array}$ *such that*

(*i*) $a \times 0 = 0$
(*ii*) $\forall b \in \mathbb{N}$, $a \times s(b) = (a \times b) + a$

**Proposition 9.**

1. $\forall a, b, c \in \mathbb{N}$, $a \times (b \times c) = (a \times b) \times c$ (the multiplication is associative)
2. $\forall a, b \in \mathbb{N}$, $a \times b = b \times a$ (the multiplication is commutative)
3. $\forall a, b, c \in \mathbb{N}$, $a \times (b + c) = a \times b + a \times c$ *and* $(a + b) \times c = a \times c + b \times c$ ($\times$ is distributive over $+$)
4. $\forall a \in \mathbb{N}$, $a \times 1 = a$
5. $\forall a, b \in \mathbb{N}$, $a \times b = 0 \implies \big(a = 0 \text{ or } b = 0\big)$
6. $\forall a, b, c \in \mathbb{N}$, $\left\{\begin{array}{l} a \times b = a \times c \\ a \neq 0 \end{array}\right. \implies b = c$ (cancellation)

We prove these properties similarly to the ones of the addition.

**Remark 10.** It is common to omit the symbol × when there is no possible confusion (i.e. to simply write $ab$ for $a \times b$).

### 2.3 Order

The following definition is a little bit informal, but it is enough for our purpose.

**Definition 11.** A **binary relation** $\mathcal{R}$ on a set $E$ consists in associating a truth value to every couple $(x, y) \in E^2$ (beware, order matters here).
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 12.**

1. Let $E = \{a, b, c\}$. Since $E$ is finite, we can define a binary relation $\mathcal{R}$ using a truth table as below:

| $x$<br>$y$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | ✓ | ✗ | ✗ |
| $b$ | ✗ | ✗ | ✓ |
| $c$ | ✓ | ✓ | ✗ |

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

2. For $E = \mathbb{R}$, we can define a binary relation as follows:

$$x\mathcal{R}y \Leftrightarrow x^2 - y^2 = x - y$$

The following definition highlights the important properties of the order $\leq$ that you intuitively know.

**Definition 13.** We say that a binary relation $\mathcal{R}$ on a set $E$ is an *order* if
(i) $\forall x \in E,\ x\mathcal{R}x$ (*reflexivity*)
(ii) $\forall x, y \in E,\ \big(x\mathcal{R}y \text{ and } y\mathcal{R}x\big) \implies x = y$ (*antisymmetry*)
(iii) $\forall x, y, z \in E,\ \big(x\mathcal{R}y \text{ and } y\mathcal{R}z\big) \implies x\mathcal{R}z$ (*transitivity*)

**Definition 14.** We say that an order $\mathcal{R}$ on a set $E$ is *total* if

$$\forall x, y \in E,\ x\mathcal{R}y \text{ or } y\mathcal{R}x$$

**Definition 15.** We define the binary relation $\leq$ on $\mathbb{N}$ by

$$\forall a, b \in \mathbb{N},\ \big(a \leq b \Leftrightarrow \exists k \in \mathbb{N},\ b = a + k\big)$$

We read *"a is less than or equal to b"* or *"b is greater than or equal to a"* when $a \leq b$ holds.

**Proposition 16.** *The set of natural numbers* $\mathbb{N}$ *is totally ordered for* $\leq$.

*Proof.*
(i) Reflexivity: let $a \in \mathbb{N}$, then $a = a + 0$ with $0 \in \mathbb{N}$, hence $a \leq a$.
(ii) Antisymmetry: let $a, b \in \mathbb{N}$ be such that $a \leq b$ and $b \leq a$.
Then there exists $k \in \mathbb{N}$ such that $b = a + k$ and there exists $l \in \mathbb{N}$ such that $a = b + l$.
Therefore $a = b + l = a + k + l$. Hence $0 = k + l$ and thus $l = k = 0$ so that $a = b$.
(iii) Transitivity: let $a, b, c \in \mathbb{N}$ be such that $a \leq b$ and $b \leq c$.
Then there exists $k \in \mathbb{N}$ such that $b = a + k$ and there exists $l \in \mathbb{N}$ such that $c = b + l$.
Therefore $c = b + l = a + (k + l)$ with $k + l \in \mathbb{N}$, i.e. $a \leq c$.
(iv) $\leq$ 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 $l \in \mathbb{N}$. The case $l = 0$ is covered by the above case, so we may assume that $l \neq 0$. 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 $b \leq a$.

■

**Definition 17.** Given $a, b \in \mathbb{N}$, we write $a < b$ for $\big(a \leq b$ and $a \neq b\big)$.

**Proposition 18.**

1. *$\forall a, b \in \mathbb{N}$, $a < b \Leftrightarrow a + 1 \leq b$.*
2. *Given $a, b \in \mathbb{N}$, exactly one of the followings occurs: either $a < b$, or $a = b$, or $b < a$.*
   *Particularly, the negation of $a \leq b$ is $b < a$.*

*Proof.*

1. $\Rightarrow$: Let $a, b \in \mathbb{N}$ be such that $a < b$. Then $a \leq b$ so there exists $k \in \mathbb{N}$ such that $b = a + k$.
   Assume by contradiction that $k = 0$ then $a = b$ which is false. Hence $k \neq 0$ and there exists $\tilde{k} \in \mathbb{N}$ such that $k = \tilde{k} + 1$. Then $b = (a + 1) + \tilde{k}$. We proved that $a + 1 \leq b$ as expected.
   $\Leftarrow$: Assume that $a + 1 \leq b$ then there exists $k \in \mathbb{N}$ such that $b = a + 1 + k$.
   - Then $b = a + (1 + k)$ with $1 + k \in \mathbb{N}$ hence $a \leq b$.
   - Assume by contradiction that $a = b$ then $a = a + 1 + k$ hence $0 = 1 + k$ from which we get $0 = 1$, so $0 = s(0)$. We get a contradiction with $0 \notin s(\mathbb{N})$.

2. This property derives from the fact that the order $\leq$ is total.

■

**Proposition 19.**

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 $a + c = a + b + k$. Then $c = b + k$ 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 $0 = s(0)$ but $0 \notin s(\mathbb{N})$).

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 $ac \leq bc$.

■

**Theorem 20** (The well-ordering principle)**.** *The set $\mathbb{N}$ is* well-ordered *for $\leq$.*
*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. ■

We proved that the induction principle implies the well-ordering principle, but they are actually equivalent. In the definition of $\mathbb{N}$, we could have replaced the induction principle by the well-ordering principle.

*Proof that the well-ordering principle implies the induction principle.*
Let $A \subset \mathbb{N}$. Assume that $0 \in A$ and that $s(A) \subset A$. We want to prove that $A = \mathbb{N}$.
Assume by contradiction that $\mathbb{N} \setminus A \neq \varnothing$. Then, by the well-ordering principle, $\mathbb{N} \setminus A$ admits a least element $a \in A$. Obviously, $a \neq 0$ since $0 \in A$.
Since $a \in \mathbb{N} \setminus \{0\}$, there exists $\tilde{a} \in \mathbb{N}$ such that $a = s(\tilde{a})$. Since $s(A) \subset A$, $\tilde{a} \notin A$ (otherwise $a = s(\tilde{a}) \in A$).
But $\tilde{a} < a$. This contradicts the fact that $a$ is the least element of $A$.
Hence $\mathbb{N} \setminus A = \varnothing$ and $A = \mathbb{N}$. ■

**Proposition 21.** $\forall a, b \in \mathbb{N},\ ab = 1 \implies a = b = 1.$

*Proof.* Let $a, b \in \mathbb{N}$ be such that $ab = 1$. Since $a = 0$ or $b = 0$ implies that $ab = 0$, we know that $a \neq 0$ and $b \neq 0$. We have $0 \leq a$ and $a \neq 0$ hence $0 < a$ from which we get $1 \leq a$. Similarly $1 \leq b$.
Then $a = 1 + k$ for some $k \in \mathbb{N}$. Then $1 = ab = b + bk$, i.e. $b \leq 1$. Hence $b = 1$ and $a = a \times 1 = ab = 1$. ■

## 2.4 Summary

The main properties of $(\mathbb{N}, +, \times, \leq, 0, 1)$, where $+, \times$ are two binary laws and $\leq$ is a binary relation, are:

- $+$ is associative: $\forall a, b, c \in \mathbb{N},\ (a + b) + c = a + (b + c)$
- $+$ is commutative: $\forall a, b \in \mathbb{N},\ a + b = b + a$
- 0 is the unit of $+$: $\forall a \in \mathbb{N},\ 0 + a = a + 0 = a$
- Cancellation rule: $\forall a, b, c \in \mathbb{N},\ a + b = a + c \Rightarrow b = c$
- $\forall a, b \in \mathbb{N},\ a + b = 0 \implies a = b = 0.$
- $\times$ is associative: $\forall a, b, c \in \mathbb{N},\ (a \times b) \times c = a \times (b \times c)$
- $\times$ is commutative: $\forall a, b \in \mathbb{N},\ a \times b = b \times a$
- 1 is the unit of $\times$: $\forall a \in \mathbb{N},\ 1 \times a = a \times 1 = a$
- Cancellation rule: for $\forall a, b, c \in \mathbb{N},\ \begin{cases} a \times b = a \times c \\ a \neq 0 \end{cases} \Rightarrow b = c$
- $\times$ is distributive over $+$: $\forall a, b, c \in \mathbb{N},\ a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$
- $\forall a, b \in \mathbb{N},\ a \times b = 0 \implies \big(a = 0 \text{ or } b = 0\big)$
- $\forall a, b \in \mathbb{N},\ ab = 1 \implies a = b = 1$
- $\leq$ is an order on $\mathbb{N}$, i.e.
  - Reflexivity: $\forall a \in \mathbb{N},\ a \leq a$
  - Antisymmetry: $\forall a, b \in \mathbb{N},\ \big(a \leq b \text{ and } b \leq a\big) \Rightarrow a = b$
  - Transitivity: $\forall a, b, c \in \mathbb{N},\ \big(a \leq b \text{ and } b \leq c\big) \Rightarrow a \leq c$

  Besides, this order is total: $\forall a, b \in \mathbb{N},\ a \leq b$ or $b \leq a$
- Well-ordering principle: a nonempty subset $A$ of $\mathbb{N}$ has a least element.
- $\leq$ is compatible with $+$: $\forall a, b, c \in \mathbb{N},\ a \leq b \Rightarrow a + c \leq b + c$
- $\leq$ is compatible with $\times$ : $\forall a, b, c \in \mathbb{N},\ a \leq b \Rightarrow ac \leq bc$
- ⋆ $\forall a, b, c, d \in \mathbb{N},\ \big(a \leq b \text{ and } c \leq d\big) \Rightarrow a + c \leq b + d$
- ⋆ $\forall a, b, c, d \in \mathbb{N},\ \big(a \leq b \text{ and } c \leq d\big) \Rightarrow ac \leq bd$
- $\forall a \in \mathbb{N},\ a \leq 0 \implies a = 0$
- There is no $a \in \mathbb{N}$ such that $0 < a < 1$.
- There is no $a \in \mathbb{N}$ such that $\forall b \in \mathbb{N},\ b \leq a$.
- $\forall a, b \in \mathbb{N},\ a < b \Leftrightarrow a + 1 \leq b$.
- For $a, b \in \mathbb{N}$ we have (exclusively) either $a < b$, or $a = b$, or $b < a$.
  Particularly, the negation of $a \leq b$ is $b < a$.

The properties with a star were not proved in this chapter but will be proved as practice questions.
Except otherwise stated, you can directly use any of the above properties without proving them.

# 3 Proof by induction

In this section we are going to highlight the connection between the *principle of induction* as stated in Theorem 1 and the notion of *proof by induction* that you have already encountered.

## 3.1 Formal statement

*Proof by induction* is closely related to the fact that $\mathbb{N}$ is defined by its initial term 0 and then by taking iteratively its successor. This fact is highlighted in the proof of the following theorem.

**Theorem 22** (Proof by induction)**.** *Let $\mathcal{P}(n)$ be a statement depending on $n \in \mathbb{N}$.*
*If $\mathcal{P}(0)$ is true and if $\mathcal{P}(n) \implies \mathcal{P}(n+1)$ is true for all $n \in \mathbb{N}$, then $\mathcal{P}(n)$ is true for all $n \in \mathbb{N}$. Formally,*

$$\left\{\begin{array}{l}\mathcal{P}(0)\\ \forall n \in \mathbb{N},\ \big(\mathcal{P}(n) \implies \mathcal{P}(n+1)\big)\end{array}\right. \implies \forall n \in \mathbb{N},\ \mathcal{P}(n)$$

The informal idea is that since $\mathcal{P}(0)$ and $\mathcal{P}(0) \implies \mathcal{P}(1)$ are true then $\mathcal{P}(1)$ is true. Then we can repeat the same process: since $\mathcal{P}(1)$ and $\mathcal{P}(1) \implies \mathcal{P}(2)$ are true then $\mathcal{P}(2)$ is true, and so on...
This way $\mathcal{P}(0)$, $\mathcal{P}(1)$, $\mathcal{P}(2)$, $\mathcal{P}(3)$, ... are all true.

*Proof of Theorem 22.*
We define the set $A = \{n \in \mathbb{N} : \mathcal{P}(n) \text{ is true}\}$. Then:

- $A \subset \mathbb{N}$ by definition of $A$.
- $0 \in \mathbb{N}$ since $\mathcal{P}(0)$ is true.
- $s(A) \subset A$
  Indeed, let $n \in s(A)$. Then $n = s(m) = m + 1$ for some $m \in A$. By definition of $A$, $\mathcal{P}(m)$ is true. But by assumption $\mathcal{P}(m) \implies \mathcal{P}(m+1)$ is also true. Hence $\mathcal{P}(m+1)$ is true, meaning that $n = m + 1 \in A$.

Hence, by the *induction principle* of Theorem 1, $A = \mathbb{N}$. Finally, for every $n \in \mathbb{N}$ we have that $\mathcal{P}(n)$ is true. ■

## 3.2 In practice

How to write a *proof by induction*? There are several steps that you should make sure they appear clearly!

- What statement are you proving? What is your $\mathcal{P}(n)$? Particularly, on which parameter are you doing the induction? You should make everything clear for the reader!
- **Base case:** prove that $\mathcal{P}(0)$ is true.
- **Induction step:** prove that if $\mathcal{P}(n)$ is true for some $n \in \mathbb{N}$ then $\mathcal{P}(n+1)$ is also true.
  It is important to clearly write the induction hypothesis and what you want to prove in this step (the reader shouldn't have to guess). Make sure that you used the induction hypothesis somewhere, otherwise there is something suspicious with your proof.

Below are two basic examples:

**Proposition 23.** *For any $n \in \mathbb{N}$, the sum $0 + 1 + 2 + \cdots + n$ is equal to $\frac{n(n+1)}{2}$.*

*Proof.* We are going to prove that $\forall n \in \mathbb{N},\ 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ by induction on $n$.

- **Base case:** Let $n = 0$. Then the sum in the left hand side is equal to 0. And $\frac{n(n+1)}{2} = \frac{0\cdot 1}{2} = 0$. So the equality holds.
- **Induction step:** Assume that $0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for some $n \in \mathbb{N}$ and let's prove that $0 + 1 + 2 + 3 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}$.

$$\begin{aligned}0 + 1 + 2 + 3 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \quad \text{by the induction hypothesis}\\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}\end{aligned}$$

Which proves the induction step. ■

**Proposition 24.** *For any $n \in \mathbb{N}$, the sum of the first $n$ odd numbers is equal to $n^2$.*

*Proof.* We are going to prove that $\forall n \in \mathbb{N},\ 1 + 3 + \cdots + (2n-1) = n^2$ by induction on $n$.

- **Base case:** Let $n = 0$. Then the sum in the left hand side is empty, so it is equal to 0. And $n^2 = 0^2 = 0$. So the equality holds.
- **Induction step:** Assume that the sum of the first $n$ odd numbers is equal to $n^2$ for some $n \in \mathbb{N}$, i.e. $1 + 3 + \cdots + (2n-1) = n^2$.
  Let's prove that $1 + 3 + \cdots + (2n-1) + (2n+1) = (n+1)^2$.
  $$\begin{aligned} 1 + 3 + \cdots + (2n-1) + (2n+1) &= n^2 + 2n + 1 \quad \text{by the induction hypothesis} \\ &= (n+1)^2 \quad \text{by the binomial formula} \end{aligned}$$
  Which proves the induction step.

■

## 3.3 Variants of the induction

### 3.3.1 Strong induction

The strong induction is equivalent to the usual induction (i.e. one may prove that Theorem 22 holds assuming Theorem 25, and that Theorem 25 holds assuming Theorem 22). Nonetheless, in some cases, it may be easier to write a strong induction rather than a usual one.

**Theorem 25** (Strong induction)**.** *Let $\mathcal{P}(n)$ be a statement depending on $n \in \mathbb{N}$.*
*If $\mathcal{P}(0)$ is true and if $\left(P(0), P(1), \dots, \mathcal{P}(n)\right) \implies \mathcal{P}(n+1)$ is true for all $n \in \mathbb{N}$, then $\mathcal{P}(n)$ is true for all $n \in \mathbb{N}$.*
*Formally,*

$$\left\{ \begin{array}{l} \mathcal{P}(0) \\ \forall n \in \mathbb{N},\ \left(\left(\mathcal{P}(0), \mathcal{P}(1), \dots, \mathcal{P}(n)\right) \implies \mathcal{P}(n+1)\right) \end{array} \right. \implies \forall n \in \mathbb{N},\ \mathcal{P}(n)$$

*Proof.* For $n \in \mathbb{N}$, we define $\mathcal{R}(n)$ by

$$\mathcal{R}(n) \text{ is true} \Leftrightarrow \mathcal{P}(0), \mathcal{P}(1), \dots, \mathcal{P}(n) \text{ are true}$$

Assume that $\mathcal{P}(0)$ is true and that $\left(P(0), P(1), \dots, \mathcal{P}(n)\right) \implies \mathcal{P}(n+1)$ is true for all $n \in \mathbb{N}$.
Then $\mathcal{R}(0)$ is true since $\mathcal{P}(0)$ is. And, for all $n \in \mathbb{N}$, $\mathcal{R}(n) \implies \mathcal{R}(n+1)$ is true.
By the usual induction $\mathcal{R}(n)$ is true for any $n \in \mathbb{N}$. Particularly, $\mathcal{P}(n)$ is true for any $n \in \mathbb{N}$ as expected. ■

### 3.3.2 Base case at $n_0$

It may be easier to write a proof by induction starting at a base $n_0 \in \mathbb{N}$ which is not necessarily 0. Below is the corresponding statement for the usual induction, but it is possible to adapt the strong induction similarly.

**Theorem 26.** *Let $n_0 \in \mathbb{N}$. Let $\mathcal{P}(n)$ be a statement depending on a natural number $n \geq n_0$.*
*If $\mathcal{P}(n_0)$ is true and if $\mathcal{P}(n) \implies \mathcal{P}(n+1)$ is true for every natural number $n \geq n_0$, then $\mathcal{P}(n)$ is true for every natural number $n \geq n_0$. Formally,*

$$\left\{ \begin{array}{l} \mathcal{P}(n_0) \\ \forall n \in \mathbb{N}_{\geq n_0},\ \left(\mathcal{P}(n) \implies \mathcal{P}(n+1)\right) \end{array} \right. \implies \forall n \in \mathbb{N}_{\geq n_0},\ \mathcal{P}(n)$$

*Proof.* For $n \in \mathbb{N}$, we define $\mathcal{R}(n)$ by

$$\mathcal{R}(n) \text{ is true} \Leftrightarrow \mathcal{P}(n + n_0) \text{ is true}$$

Then $\mathcal{R}(0)$ is true since $\mathcal{P}(n_0)$ is. And, for all $n \in \mathbb{N}$, $\mathcal{R}(n) \implies \mathcal{R}(n+1)$ is true.
By the usual induction $\mathcal{R}(n)$ is true for any $n \in \mathbb{N}$, i.e. $\mathcal{P}(n)$ is true for any $n \in \mathbb{N}_{\geq n_0}$. ■

Below is an example of induction starting at $n_0 = 5$.

**Proposition 27.** *For any integer $n \geq 5$, $2^n > n^2$.*

*Proof.* We are going to prove that $\forall n \geq 5$, $2^n > n^2$ by induction on $n$.

- **Base case at $n = 5$:** $2^5 = 32 > 25 = 5^2$.
- **Induction step:** Assume that $2^n > n^2$ for some $n \geq 5$ and let's prove that $2^{n+1} > (n+1)^2$.
  Note that $2^{n+1} = 2\times 2^n \geq 2n^2$ by the induction hypothesis. Hence it is enough to prove that $2n^2 > (n+1)^2$ which is equivalent to $n^2 - 2n - 1 > 0$.
  We study the sign of the polynomial $x^2 - 2x - 1$. It is a polynomial of degree 2 with positive leading coefficient and its discriminant is $(-2)^2 - 4 \times (-1) = 8 > 0$. Therefore

| $x$ | $-\infty$ | | $1-\sqrt{2}$ | | $1+\sqrt{2}$ | | $+\infty$ |
|---|---|---|---|---|---|---|---|
| $x^2-2x-1$ | | $+$ | $0$ | $-$ | $0$ | $+$ | |

  Since $5 > 1 + \sqrt{2}$, we know that $n^2 - 2n - 1 > 0$ for $n \geq 5$. Which proves the induction step.

■

**Remark 28.** The above example is interesting because the induction step holds for $n \geq 3$, but $\mathcal{P}(3)$ and $\mathcal{P}(4)$ are false: don't forget the base case! It is crucial!