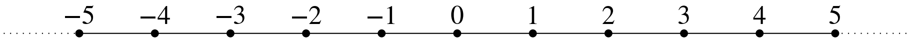
Integers

January 21st, 2021

Introduction – 1

You already used to negative integers. But they are missing in the set $\mathbb{N}$ from Chapter 1.



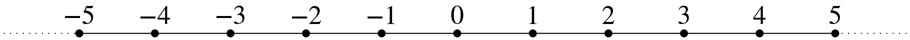
We are going to construct $\mathbb{Z}$, the set of integers, by adding negative integers to $\mathbb{N}$.

There are several ways to do so.

Usually: $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$ for $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$.
Intuitively (a, b) stands for $a - b$, but, since such an expression is not unique (e.g. $7 - 5 = 10 - 8$), we need to "identify" some couples giving the same integer (e.g. $(7, 5) = (10, 8)$).
Note that we use $a + d = b + c$ and not $a - b = c - d$ because "–" is not defined yet!

Introduction – 1

You already used to negative integers. But they are missing in the set $\mathbb{N}$ from Chapter 1.



We are going to construct $\mathbb{Z}$, the set of integers, by adding negative integers to $\mathbb{N}$.

There are several ways to do so.

Usually: $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$ for $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$.
Intuitively (a, b) stands for $a - b$, but, since such an expression is not unique (e.g. $7 - 5 = 10 - 8$), we need to "identify" some couples giving the same integer (e.g. $(7, 5) = (10, 8)$).
Note that we use $a + d = b + c$ and not $a - b = c - d$ because "–" is not defined yet!

Today, I will use a more naive approach. The counterpart is that the definitions of $+$ and $\times$ are going to be more tedious.

Introduction – 2

It took centuries for negative integers to be widely accepted and used: during the 18th century, most mathematicians were still reluctant about using them.

« Il faut avouer qu'il n'est pas facile de fixer l'idée des quantités négatives, & que quelques habiles gens ont même contribué à l'embrouiller par les notions peu exactes qu'ils en ont données. Dire que la quantité négative est au-dessous du rien, c'est avancer une chose qui ne se peut pas concevoir. Ceux qui prétendent que 1 n'est pas comparable à −1, & que le rapport entre 1 & −1 est différent du rapport entre −1 & 1, sont dans une double erreur […] Il n'y a donc point réellement & absolument de quantité négative isolée : −3 pris abstraitement ne présente à l'esprit aucune idée. »

Jean Le Rond d'Alembert, 1751.

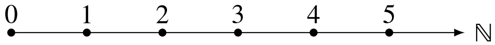
« [Negative numbers] darken the very whole doctrines of the equations and make dark of the things which are in their nature excessively obvious and simple. »

Francis Maseres, 1758.

Negative integers

Notations

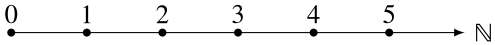
- Given $n \in \mathbb{N} \setminus \{0\}$, we introduce the symbol $-n$ read as *minus* n.



Negative integers

Notations

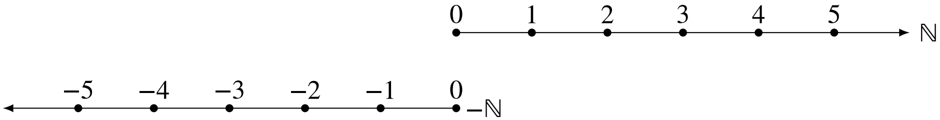
- Given $n \in \mathbb{N} \setminus \{0\}$, we introduce the symbol $-n$ read as *minus* n.
- We fix the convention that $-0 = 0$.



Negative integers

Notations

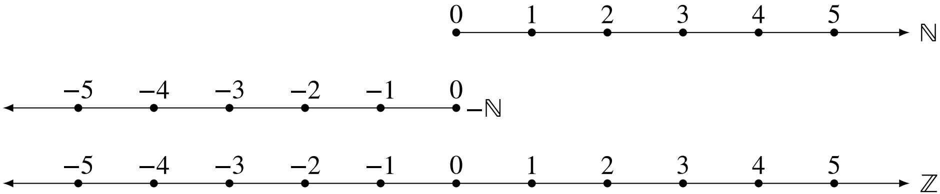
- Given $n \in \mathbb{N} \setminus \{0\}$, we introduce the symbol $-n$ read as *minus* n.
- We fix the convention that $-0 = 0$.
- We define the set $-\mathbb{N} := \{-n \ : \ n \in \mathbb{N}\}$.



Negative integers

Notations

- Given $n \in \mathbb{N} \setminus \{0\}$, we introduce the symbol $-n$ read as *minus* n.
- We fix the convention that $-0 = 0$.
- We define the set $-\mathbb{N} \coloneqq \{-n \ : \ n \in \mathbb{N}\}$.
- Then the *set of integers* is $\mathbb{Z} \coloneqq (-\mathbb{N}) \cup \mathbb{N}$.



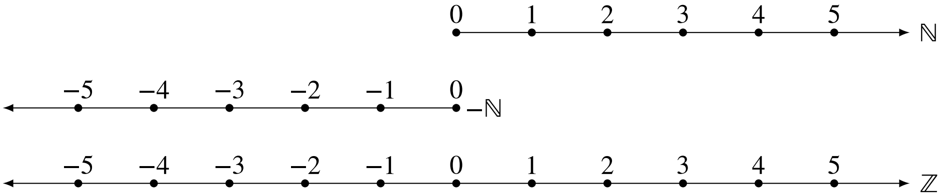
Negative integers

Notations

- Given $n \in \mathbb{N} \setminus \{0\}$, we introduce the symbol $-n$ read as *minus* n.
- We fix the convention that $-0 = 0$.
- We define the set $-\mathbb{N} := \{-n \ : \ n \in \mathbb{N}\}$.
- Then the *set of integers* is $\mathbb{Z} := (-\mathbb{N}) \cup \mathbb{N}$.

Remarks

- $(-\mathbb{N}) \cap \mathbb{N} = \{0\}$
- $\mathbb{N} \subset \mathbb{Z}$



Addition

Definition: addition

For $m, n \in \mathbb{N}$, we set:

- $m + n$ for the usual addition in $\mathbb{N}$
- $(-m) + (-n) = -(m + n)$
- $m + (-n) = \begin{cases} k \text{ where } k \text{ is the unique natural integer such that } m = n + k \text{ if } n \leq m \\ -k \text{ where } k \text{ is the unique natural integer such that } n = m + k \text{ if } m \leq n \end{cases}$
- $(-m) + n = n + (-m)$ where $n + (-m)$ is defined above

We've just defined $+ : \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (a, b) & \mapsto & a + b \end{array}$.

Addition

Definition: addition

For $m, n \in \mathbb{N}$, we set:

- $m + n$ for the usual addition in $\mathbb{N}$
- $(-m) + (-n) = -(m + n)$
- $m + (-n) = \begin{cases} k \text{ where } k \text{ is the unique natural integer such that } m = n + k \text{ if } n \leq m \\ -k \text{ where } k \text{ is the unique natural integer such that } n = m + k \text{ if } m \leq n \end{cases}$
- $(-m) + n = n + (-m)$ where $n + (-m)$ is defined above

We've just defined $+ : \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (a, b) & \mapsto & a + b \end{array}$.

Remark

There is no contradiction for the overlapping cases $m = 0$ or $n = 0$.

Multiplication

Definition: multiplication

For $m, n \in \mathbb{N}$, we set:

- $m \times n$ for the usual product in $\mathbb{N}$
- $(-m) \times (-n) = m \times n$
- $m \times (-n) = -(m \times n)$
- $(-m) \times n = -(m \times n)$

We've just defined $\times : \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ (a, b) & \mapsto & a \times b \end{array}$.

Remark

We may simply write ab for $a \times b$ when there is no possible confusion.

Notation

For $n \in \mathbb{N}$, we set $-(-n) = n$. Then $-a$ is well-defined for any $a \in \mathbb{Z}$.

Properties

- $+$ is associative: $\forall a, b, c \in \mathbb{Z},\ (a+b)+c = a+(b+c)$
- 0 is the unit of $+$: $\forall a \in \mathbb{Z},\ a+0 = 0+a = a$
- $-a$ is the additive inverse of a: $\forall a \in \mathbb{Z},\ a+(-a) = (-a)+a = 0$
- $+$ is commutative: $\forall a, b \in \mathbb{Z},\ a+b = b+a$
- $\times$ is associative: $\forall a, b, c \in \mathbb{Z},\ (ab)c = a(bc)$
- $\times$ is distributive with respect to $+$: $\forall a, b, c \in \mathbb{Z},\ a \times (b+c) = ab+ac$ et $(a+b)c = ac+bc$
- 1 is the unit of $\times$: $\forall a \in \mathbb{Z},\ 1 \times a = a \times 1 = a$
- $\times$ is commutative: $\forall a, b \in \mathbb{Z},\ ab = ba$
- $\forall a, b \in \mathbb{Z},\ ab = 0 \Rightarrow \left(a = 0 \text{ or } b = 0\right)$

Notation

From now on, we may simply write $a-b$ for $a+(-b)$ and $-a+b$ for $(-a)+b$.

Order

Definition

We extend the binary relation $\leq$ from $\mathbb{N}$ to $\mathbb{Z}$ with $\forall a, b \in \mathbb{Z},\ a \leq b \Leftrightarrow b - a \in \mathbb{N}$.

Proposition

$\leq$ defines a total order on $\mathbb{Z}$.

Order

Definition

We extend the binary relation $\leq$ from $\mathbb{N}$ to $\mathbb{Z}$ with $\forall a, b \in \mathbb{Z},\ a \leq b \Leftrightarrow b - a \in \mathbb{N}$.

Proposition

$\leq$ defines a total order on $\mathbb{Z}$.

Proof.

- *Reflexivity.* Let $a \in \mathbb{Z}$, then $a - a = 0 \in \mathbb{N}$ so $a \leq a$.
- *Antisymmetry.* Let $a, b \in \mathbb{Z}$. Assume that $a \leq b$ and that $b \leq a$. Then $b - a \in \mathbb{N}$ and $a - b \in \mathbb{N}$. So $a - b = -(b - a) \in (-\mathbb{N})$. Hence $a - b \in (-\mathbb{N}) \cap \mathbb{N} = \{0\}$ and thus $a = b$.
- *Transitivity.* Let $a, b, c \in \mathbb{Z}$. Assume that $a \leq b$ and that $b \leq c$. Then $b - a \in \mathbb{N}$ and $c - b \in \mathbb{N}$. Thus $c - a = (c - b) + (b - a) \in \mathbb{N}$, i.e. $a \leq c$.
- Let $a, b \in \mathbb{Z}$. Then $b - a \in \mathbb{Z} = (-\mathbb{N}) \cup (\mathbb{N})$.
  First case: $b - a \in \mathbb{N}$ then $a \leq b$.
  Second case: $b - a \in (-\mathbb{N})$, then $a - b = -(b - a) \in \mathbb{N}$ and $b \leq a$.
  Hence the order is total. ∎

Properties of the order

Proposition

1. $\mathbb{N} = \{a \in \mathbb{Z},\ 0 \leq a\}$
2. $\forall a, b, c \in \mathbb{Z},\ a \leq b \Leftrightarrow a + c \leq b + c$
3. $\forall a, b, c, d \in \mathbb{Z},\ \left(a \leq b \text{ and } c \leq d\right) \Rightarrow a + c \leq b + d$
4. $\forall a, b \in \mathbb{Z},\ \forall c \in \mathbb{N} \setminus \{0\},\ a \leq b \Leftrightarrow ac \leq bc$
5. $\forall a, b \in \mathbb{Z},\ \forall c \in (-\mathbb{N}) \setminus \{0\},\ a \leq b \Leftrightarrow bc \leq ac$

Properties of the order

Proposition

1. $\mathbb{N} = \{a \in \mathbb{Z},\ 0 \leq a\}$
2. $\forall a, b, c \in \mathbb{Z},\ a \leq b \Leftrightarrow a + c \leq b + c$
3. $\forall a, b, c, d \in \mathbb{Z},\ \left(a \leq b \text{ and } c \leq d\right) \Rightarrow a + c \leq b + d$
4. $\forall a, b \in \mathbb{Z},\ \forall c \in \mathbb{N} \setminus \{0\},\ a \leq b \Leftrightarrow ac \leq bc$
5. $\forall a, b \in \mathbb{Z},\ \forall c \in (-\mathbb{N}) \setminus \{0\},\ a \leq b \Leftrightarrow bc \leq ac$

Proof.

1. Let $a \in \mathbb{Z}$. Then $0 \leq a \Leftrightarrow a = a - 0 \in \mathbb{N}$.
2. Let $a, b, c \in \mathbb{Z}$. Then $a \leq b \Leftrightarrow b - a \in \mathbb{N} \Leftrightarrow (b + c) - (a + c) \in \mathbb{N} \Leftrightarrow a + c \leq b + c$.
3. Let $a, b, c, d \in \mathbb{Z}$. Assume that $a \leq b$ and that $c \leq d$. Then $b - a \in \mathbb{N}$ and $d - c \in \mathbb{N}$. Hence $(b + d) - (a + c) = (b - a) + (d - c) \in \mathbb{N}$, i.e. $a + c \leq b + d$.
4. Let $a, b \in \mathbb{Z}$ and $c \in \mathbb{N}$.
   $\Rightarrow$: Assume that $a \leq b$. Then $b - a \in \mathbb{N}$, thus $bc - ac = (b - a)c \in \mathbb{N}$. Therefore $ac \leq bc$.
   $\Leftarrow$: Assume that $c \neq 0$ and that $ac \leq bc$. Then $bc - ac = (b - a)c \in \mathbb{N}$. Assume by contradiction that $(b - a) \in (-\mathbb{N}) \setminus \{0\}$ then, by definition of the multiplication, $(b - a)c \in (-\mathbb{N}) \setminus \{0\}$, which is a contradiction. Hence $b - a \in \mathbb{N}$, i.e. $a \leq b$. ∎

Consequences of the well-ordering principle

Theorem

1. A non-empty subset A of $\mathbb{Z}$ which is bounded from below has a least element, i.e.

$$\exists m \in A, \forall a \in A, m \leq a$$

2. A non-empty subset A of $\mathbb{Z}$ which is bounded from above has a greatest element, i.e.

$$\exists m \in A, \forall a \in A, a \leq m$$

Consequences of the well-ordering principle

Theorem

1. A non-empty subset A of $\mathbb{Z}$ which is bounded from below has a least element, i.e.
$$\exists m \in A, \forall a \in A, m \leq a$$
2. A non-empty subset A of $\mathbb{Z}$ which is bounded from above has a greatest element, i.e.
$$\exists m \in A, \forall a \in A, a \leq m$$

Proof.

1. Assume that A is a non-empty subset of $\mathbb{Z}$ which is bounded from below.
Then there exists $k \in \mathbb{Z}$ such that $\forall a \in A, k \leq a$. Define $S = \{a - k \ : \ a \in A\}$.
Then S is a non-empty subset of $\mathbb{N}$ (indeed, $\forall a \in A, 0 \leq a - k$).
By the well-ordering principle, there exists $\tilde{m} \in S$ such that $\forall a \in A, \tilde{m} \leq a - k$.
Then $m = \tilde{m} + k$ is the least element of A (note that $\tilde{m} \in S$ so $m = \tilde{m} + k \in A$). ∎