Numbers \((\mathbb{N}, \mathbb{Z}, \mathbb{Q})\)

1 Intro

In this short document we introduce some very basic facts about logic, relations and numbers. We will introduce the formal definitions of the natural numbers, the integers the rationals and the reals. In a calculus course these concepts are taken for granted, but as we shall see there is nothing obvious about their definitions. As a matter of fact, even if the natural numbers have been known to men since the dawn of time, the definition dates back to 1888/1889.

2 Logic

In this section we briefly recall the properties of the symbol \(=\) (equal). We will not deal with anything fancy, we just restate the three principles that were known to the ancient greeks:

\[
\begin{align*}
A &= A \quad (1) \\
A = B &\implies B = A \quad (2) \\
A = B \text{ and } B = C &\implies A = C \quad (3)
\end{align*}
\]

3 Relations

Definition 3.1. Let \(A, B\) be two sets. We define a relation \(\mathcal{R}\) from \(A\) to \(B\) to be a subset of the cartesian product \(A \times B\).

Remark 3.2. We can reread the definition in the following way:

A relation \(\mathcal{R}\) is a set of ordered pairs \((a, b)\) where \(a \in A\) and \(b \in B\) and we say that \(a\) is related to \(b\).

Definition 3.3. A relation \(\mathcal{R}\) from \(A\) to \(B\) is called an equivalence relation if it satisfies the following additional conditions:

1. \(\forall a \in A, \ (a, a) \in \mathcal{R}\)
2. if \((a, b) \in \mathcal{R}\) \(\Rightarrow (b, a) \in \mathcal{R}\)
3. if \((a, b) \in \mathcal{R}\) and \((b, c) \in \mathcal{R}\) \(\Rightarrow (a, c) \in \mathcal{R}\)

Remark 3.4. We can read the previous definition in the following way:

1. every element in \(A\) is related to itself.
2. if \(a\) is related to \(b\), then \(b\) is related to \(a\) (symmetry).
3. if \( a \) is related to \( b \) and \( b \) is related to \( c \), then \( a \) is related to \( c \) (transitivity).

It is very common to denote an equivalence relation with the symbol \( \sim \), and if \( a \) is related to \( b \) we write \( a \sim b \).

**Definition 3.5.** Let \( \sim \) be an equivalence relation from a set \( A \) to the same set \( A \). Let \( a \) be an element in \( A \). We define the equivalence class of \( a \) denoted with \([a]\) as the set of all the elements in \( A \) that are related to \( a \):

\[
[a] = \{ x \in A | a \sim x \}
\]

**Lemma 3.6.** Let \([a]\) and \([b]\) be two equivalence classes for some equivalence relation \( R \) on a set \( A \). The intersection \([a] \cap [b]\) is empty only if \( a \) is not equivalent to \( b \).

The two classes are equal if and only if \( a \) is equivalent to \( b \).

**Proof.** If the intersection is not empty there is an element \( c \) which is in both the two equivalence classes. This implies that \( a \sim c \) and \( b \sim c \). Since the equivalence is symmetric we also have \( c \sim b \) and since it’s transitive we deduce \( a \sim b \) which proves the first statement.

If \( a \) and \( b \) are equivalent and we take any element \( c \in [a] \) we have that \( a \sim c \) and with the same argument we have used above we deduce that \( b \sim c \) which implies that \( c \in [b] \). This proves that \([a] \subset [b]\). We can switch the roles of \( a \) and \( b \) and we obtain that \([b] \subset [a]\) which implies that \([a] = [b]\).

If \([a] = [b]\) we now prove that \( a \sim b \). First we notice that \([a]\) cannot be empty because \( a \sim a \) which implies \( a \in [a] \). Pick any element \( c \in [a] \); since the two classe are equal we have that \( a \sim c \) and \( b \sim c \). Using symmetry and transitivity we deduce that \( a \sim b \).

**Proposition 3.7.** A set \( A \) with an equivalence relation \( \sim \) is a disjoint union of its equivalence classes.

**Proof.** It’s an obvious consequence of the lemma.

Now that we know that a set is a disjoint union of its equivalence classes, it makes sense to define a new set whose elements are the equivalence classes themselves.

**Definition 3.8.** Let \( \sim \) be an equivalence relation from a set \( A \) to the same set \( A \). We define the quotient of \( A \) by the equivalence relation \( \sim \), denoted with \( A/\sim \) as the set of all the equivalence classes of \( A \):

\[
A/\sim = \{ [a] | a \in A \}
\]

**Remark 3.9.** The notion of quotient might seem not very intuitive at the beginning but it turns out to be very natural. Unfortunately at the moment we have not defined any type of number so it’s very hard to make a meaningful example. We postpone examples to the next section.

**Definition 3.10.** Let \( A \) be a set and \( \leq \) a relation of \( A \) with itself. We call \( \leq \) a partial order if the following conditions are satisfied:

1. \( \forall a \in A, \ a \leq a \)
2. if \( a \leq b \) and \( b \leq a \) then \( a = b \)
3. if \( a \leq b \) and \( b \leq c \) then \( a \leq c \)
Remark 3.11. A partial order matches the intuitive notion of something being less than or equal to something else. However there is a subtlety: in our definition we do not assume that any two elements in $A$ can be compared; it might well be that we cannot say about $a$ and $b$ which one is the biggest. If any two elements can be compared we have a total order or just an order relation.

Remark 3.12. A partial order on $A$ is a total order (or an order) if the following additional condition is satisfied:

1. $\forall a, b \in A$, or $a \leq b$ or $b \leq a$

Definition 3.13. Let $A, B$ be two sets and $f$ a relation from $A$ to $B$. We call the triple $(A, B, f)$ a function with domain $A$ and codomain $B$ if the relation $f$ satisfies the following conditions:

1. $\forall a \in A, \exists b \in B \mid (a, b) \in f$
2. $\forall a \in A$ if $(a, b_1) \in f$ and $(a, b_2) \in f \Rightarrow b_1 = b_2$

Remark 3.14. The first condition states that every element in the domain is related to at least one element in the codomain. The second condition states that an element in the domain is related to only one element in the codomain. Since every element $a \in A$ is related to exactly one element $b \in B$ we can denote $b$ with the symbol $f(a)$.

Definition 3.15. The set $f$ of the ordered pairs $(a, f(a)) \in A \times B$ is called the graph of the function $f$. The subset of $B$ of all the elements in $B$ that are related to some element in $A$ is called the image $A$ or the range of $f$ and it’s usually denoted with $f(A)$:

$$f(A) = \{ b \in B \mid \exists a \in A \text{ such that } b = f(a) \}$$

Remark 3.16. According to the definition it is still possible that an element in the codomain is not related to any element in the domain, or to more than one element in the domain. However, functions such that these two phenomena do not occur are very special and they deserve a name:

Definition 3.17. Let $f$ be a function from $A$ to $B$. If for every $b \in B$ there is $a \in A$ satisfying $b = f(a)$ we call the function **surjective**.

If for every $a_1, a_2 \in A$ the condition $f(a_1) = f(a_2)$ implies that $a_1 = a_2$ we call the function **injective**.

If a function is both injective and surjective we call it **bijective** or an **isomorphism** (of sets).

Remark 3.18. The condition of being surjective is equivalent to saying that the range of the function coincides with the codomain.

The condition of being injective means that two distinct elements in the domain cannot be mapped to the same element in the codomain.

4 The natural numbers $\mathbb{N}$

The definition of natural numbers dates back to 1888/1889 and was written independently by Peano and Dedekind.

Definition 4.1. Let $\mathbb{N}$ be a set endowed with a function $S$ from $\mathbb{N}$ to $\mathbb{N}$. We call $\mathbb{N}$ the set of the natural numbers if $\mathbb{N}$ and $S$ satisfy the following conditions:

1. There is an element in $\mathbb{N}$ that we denote with 0.
2. The function \( S \) is injective which means that for all \( n_1, n_2 \in \mathbb{N} \), the condition \( S(n_1) = S(n_2) \) implies that \( n_1 = n_2 \).

3. There is no \( n \in \mathbb{N} \) such that \( S(n) = 0 \).

4. Let \( K \subseteq \mathbb{N} \) such that \( 0 \in K \) and such that \( n \in K \) implies that \( S(n) \in K \), then \( K = \mathbb{N} \).

**Remark 4.2.** We can spell out the definition in the following way.

1. Zero is a natural number.

2. We call \( S(n) \) the successor of \( n \) and to fix the ideas you can think that \( S(n) = n + 1 \) (We haven’t defined + yet). Injectivity of \( S \) means that two natural numbers cannot have the same successor.

3. There is no natural number whose successor is 0.

4. The last axiom is known as **induction**. It says that if a subset of the natural numbers contains 0 and if it contains a natural number \( n \) it contains also its successor, then it must contain every natural number.

   We name the successors of zero in the usual way: \( S(0) = 1, S(1) = 2, \ldots \)

At this moment we have defined the natural numbers as a set but we haven’t defined any operation on them. We can endow the natural numbers with two operations: addition and multiplication:

**Definition 4.3.** We recursively define a function \( + : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) that we call addition in the following way:

\[
\begin{align*}
    n + 0 &= n \\
    n + S(m) &= S(n + m)
\end{align*}
\]

We can try for instance to calculate \( 1 + 2 \). We know that 2 is the successor of 1 so we can use the definition:

\[
    1 + 2 = 1 + S(1) = S(1 + 1) = S(S(0)) = S(S(1)) = S(2) = 3
\]

In the same way we can define a multiplication:

**Definition 4.4.** We recursively define a function \( \cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) that we call multiplication in the following way:

\[
\begin{align*}
    n \cdot 0 &= 0 \\
    n \cdot S(m) &= n \cdot m + n
\end{align*}
\]

We can use the definition and calculate \( 2 \cdot 3 \) in the following way:

\[
\begin{align*}
    2 \cdot 3 &= 2 \cdot S(2) = 2 \cdot 2 + 2 = 2 \cdot S(1) + 2 = 2 \cdot 1 + 2 + 2 = 2 \cdot S(0) + 2 + 2 = 2 \cdot 0 + 2 + 2 + 2 = 2 + 2 + 2 = 6
\end{align*}
\]

As an application of induction we can prove that the addition of natural numbers is associative:

**Proposition 4.5.** For all \( n, m, p \in \mathbb{N} \) the following relation is satisfied:

\[
    n + (m + p) = (n + m) + p
\]
Proof. Choose $n, m \in \mathbb{N}$ once and for all. Denote with $K$ the following set:

$$K = \{p \in \mathbb{N} | n + (m + p) = (n + m) + p\}$$

First we prove the $0 \in K$:

$$(n + m) + 0 = n + m = n + (m + 0)$$

Take any $p \in K$, and prove that also $S(p) \in K$:

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

In the last step we have used that $p \in K$.

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

and this proves that $S(p) \in K$ so by induction $K = \mathbb{N}$. \qed

Exercise 4.6. With this same method we can also prove that:

1. the addition is commutative
2. the product is commutative and associative
3. the number 1 is the neutral element of the product
4. the product is distributive with respect to the addition

Exercise 4.7. You might be led to think that our definition of natural numbers is not stringent, in the sense that there might be different sets of numbers satisfying the properties that we have listed; however this is not the case. Prove that if the set $\mathbb{M}$ and the function $T : \mathbb{M} \to \mathbb{M}$ satisfy all the properties in 4.1 then there is only one isomorphism $\phi$ between $\mathbb{N}$ and $\mathbb{M}$ such that the following diagram is commutative:

$$\begin{array}{ccc}
\mathbb{N} & \xrightarrow{S} & \mathbb{N} \\
\downarrow{\phi} & & \downarrow{\phi} \\
\mathbb{M} & \xrightarrow{T} & \mathbb{M}
\end{array}$$

This is what we usually mean by unique in mathematics.

The natural numbers can be ordered in different ways, but the common way of ordering them is the following:

$$n < S(n)$$

This condition allows us to compare any two natural numbers by recursion. For instance $1 < 3$:

$$1 < S(1) = 2 < S(2) = 3$$

we just need to remember that $<$ is transitive. The natural numbers ordered in this way fulfill a very useful property; every non empty subset of $\mathbb{N}$ has a minimum.

Definition 4.8. If $A$ is an ordered set, we say that $A$ has a minimum if there is $a \in A$ such that $a \leq b$ for all $b \in A$.

Definition 4.9. Let $B$ be an ordered set. If every non empty subset $A \subseteq B$ with the ordering induced by $B$ has a minimum, we say that $B$ is well-ordered.
Proposition 4.10. The natural numbers with the ordered defined above are well-ordered.

Proof. Let \( A \subset \mathbb{N} \) be a non-empty subset. Let \( B \) be the set \( \{ n \in \mathbb{N} \mid n \leq a \ \forall a \in A \} \). The set \( B \) is not empty because it contains at least \( 0 \), since no number has 0 as a successor. There is \( b \in B \) such that \( S(b) \) is not in \( B \). If this were not the case, \( B \) would be \( \mathbb{N} \) by induction and \( A \) would be empty. Since \( S(b) \notin B \) there is \( a_0 \in A \) such that \( S(b) > a_0 \), but \( b \leq a_0 \) so we have:

\[
b \leq a_0 < S(b)
\]

which implies that \( a_0 = b \) so \( a_0 \) is the minimum. \( \square \)

5 The integers \( \mathbb{Z} \)

Now that we have built the natural numbers we are ready to define the integers. Natural numbers do not have inverses with respect to the addition (excluding zero); however we can “manually” add them, the enlarged set that we obtain is known as the set of integers. The method we use to produce the integers might seem a little be involute but at the moment we only have the natural numbers to work with. We need “something” to encode the negative sign of a number and we can do it with an ordered pair of natural numbers \((a, b) \in \mathbb{N} \times \mathbb{N}\). We can interpret the element \((a, 0)\) as \(+a\) and the element \((0, b)\) as \(-b\). In order to have something consistent the pair \((a, b)\) must represent the number \(a - b\). In this way every number has more than one representation; for example \((a, a)\) is always zero and \((a + 1, a)\) is 1. We want every number to be represented by one single object and for this reason we introduce an equivalence relation such that for example all the \((a + 1, a)\) are in the same equivalence class.

Definition 5.1. Let \((a, b)\) and \((c, d)\) be elements in \(\mathbb{N} \times \mathbb{N}\); we define the equivalence relation \(\sim\) in the following way: \((a, b)\) is related to \((c, d)\) if and only if \(a + d = c + b\). We denote with \(\mathbb{Z}\) the quotient \(\mathbb{N} \times \mathbb{N}/\sim\) and we call it the set of integers.

We define an addition on \(\mathbb{Z}\) in the following way. First we introduce an operation on \(\mathbb{N} \times \mathbb{N}\) in the following way:

\[
(a, b) + (c, d) = (a + c, b + d)
\]

We have to make sure that this operation defines an operation on the quotient \(\mathbb{Z}\). An element in \(\mathbb{Z}\) is an equivalence class \([[(a, b)]\] and we can try to define the addition in the following way:

\[
[[a, b]] + [[c, d]] = [[a + c, b + d]]
\]

however if \((a_1, b_1) \in [(a, b)]\) and \((c_1, d_1) \in [(c, d)]\), the equivalence class \([(a_1 + c_1, b_1 + d_1)]\) might not be equal to \([(a + c, b + d)]\); if this were the case the operation wouldn’t be well defined. Since \((a_1, b_1)\) and \((a, b)\) are equivalent they must satisfy \(a_1 + b = b_1 + a\) and for the same reason we have \(c_1 + d = d_1 + c\); this implies that \(a_1 + c_1 + b + d = b_1 + d_1 + a + c\) which means that \((a_1 + c_1, b_1 + d_1)\) is equivalent to \((a + c, b + d)\) which means that:

\[
[(a_1 + c_1, b_1 + d_1)] = [(a + c, b + d)]
\]

which means that the addition is well defined.

We can also define a function from \(\mathbb{Z}\) to \(\mathbb{Z}\) that changes the sign of an element:

\[
[(a, b)] \mapsto -[(a, b)] = [(b, a)]
\]
Remark 5.2. The fact that this function actually changes the sign of an element can be tested with this calculation:

\[ [(a, b)] + [(b, a)] = [(a + b, b + a)] = [(0, 0)] \]

Since the pair \((a, b)\) represents the number \(a - b\), the definition of product is slightly more complicated:

\[ [(a, b)] \cdot [(c, d)] = [(ac + bd, bc + ad)] \]

As we have done with the addition we actually have to prove that this operation is well defined on equivalence classes. The proof is left to the reader.

6 The rationals \(\mathbb{Q}\)

A rational number is just a quotient \(\frac{m}{n}\) where \(m\) is an integer and \(n\) is a natural number which is not 0. In order to represent such an object we can use an ordered pair \((m, n)\) as we have done for the integers. We encounter the same problem though: different pairs can represent the same number, for instance \((3, 2)\) and \((6, 4)\) and \((3a, 2a)\) are all the same number. In order to fix this we need to quotient an equivalence relation. Denote with \(\mathbb{N}^*\) the natural numbers minus 0.

Definition 6.1. On the set \(\mathbb{Z} \times \mathbb{N}^*\) we define the following equivalence relation \(\sim\): the pair \((m, n)\) is equivalent to \((p, q)\) if and only if \(mq = pn\). We denote with \(\mathbb{Q}\) the quotient \(\mathbb{Z} \times \mathbb{N}^* / \sim\) and we call it the set of rational numbers.

Remark 6.2. The construction explained in the definition is a special version of what we call localization of a ring (in this case \(\mathbb{Z}\)).

We can define the addition of two rational numbers in the usual way:

\[ \frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq} \]

on pairs it becomes:

\[ [(m, n)] + [(p, q)] = [(mq + np, nq)] \]

As we have done with the integers we have to check that this definition is compatible with the equivalence relation. If \((m_1, n_1) \in [(m, n)]\) these numbers satisfy the condition \(m_1 n = n_1 m\) and if \((p_1, q_1) \in [(p, q)]\) the condition \(p_1 q = q_1 p\) is satisfied. With a little algebra we have: \((m_1q_1 + n_1p_1)(nq) = m_1nq_1q + n_1p_1qn = n_1mq_1q + n_1q_1pn = (mq + np)n_1q_1\) which implies that \((mq + np, nq)\) is related to \((m_1q_1 + n_1p_1, n_1q_1)\) or equivalently:

\[ [(mq + np, nq)] = [(m_1q_1 + n_1p_1, n_1q_1)] \]

The product of two numbers is just:

\[ [(m, n)] \cdot [(p, q)] = [(mp, nq)] \]

Remark 6.3. Every non zero element in \(\mathbb{Q}\) has an inverse with respect to the product:

\[ [(a, b)] \cdot [(b, a)] = [(ab, ba)] = [(1, 1)] \]