

Mathematical Analysis 1

Part one: Sets and Numbers

Contents

I	Sets and Numbers	1
1	The Real Numbers	1
1.1	The system of real numbers	1
1.2	Extended Reals	7
1.3	Operations on Sets	8
1.4	Operations with Supremum and Infimum	8
2	Natural Numbers	10
2.1	The Set of Natural Numbers	10
2.2	Principle of Induction	11
2.3	Definitions for Recursion	12
2.4	Well-Ordering of Natural Numbers	13
2.5	Archimedean Property	13
2.6	Bernoulli's Inequality	13
3	The Integers	14
3.1	The Set of Integers	14
4	Rational Numbers	15
4.1	The set of rational numbers	15
4.2	The n -th Root of a Real Number	16
4.3	Logarithms	17
4.4	The Number e	18
4.5	Density of Rationals	19
4.6	Density of Irrationals	19
4.7	Intervals	20

Part I

Sets and Numbers

1 The Real Numbers

1.1 The system of real numbers

The axioms of real numbers can be classified into three groups:

- (a) **Field Axioms**, concerning the operations that can be performed between real numbers;
- (b) **Order Axioms**, related to the ability to compare real numbers to identify the “greater” one;
- (c) **Axiom of Completeness**.

From these axioms, we will deduce all other properties of real numbers.

Field Axioms In the set \mathbb{R} , two operations are defined, addition and multiplication, respectively defined as follows:

$$+ : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \quad (a, b) \mapsto a + b \quad \cdot : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \quad (a, b) \mapsto a \cdot b = ab.$$

such that the following axioms hold:

Axiom 1 (Associativity)

$$\forall a, b, c \in \mathbb{R}, \quad (a + b) + c = a + (b + c) \quad \wedge \quad (ab)c = a(bc);$$

Axiom 2 (Commutativity)

$$\forall a, b \in \mathbb{R}, \quad a + b = b + a \quad \wedge \quad ab = ba;$$

Axiom 3 (Distributivity)

$$\forall a, b, c \in \mathbb{R}, \quad a(b + c) = ab + ac;$$

Axiom 4 (Existence of identity elements)

$$\exists z, v \in \mathbb{R} (z \neq v) : \forall a \in \mathbb{R}, \quad a + 0 = a \quad \wedge \quad a \cdot 1 = a$$

$$\exists z \in \mathbb{R} : \forall a \in \mathbb{R}, \quad a + z = a$$

Axiom 5 (Existence of additive inverses)

$$\forall a \in \mathbb{R}, \exists \bar{a} \in \mathbb{R} : a + \bar{a} = 0$$

Axiom 6 (Existence of multiplicative inverses)

$$\forall a \in \mathbb{R} - \{0\}, \exists \tilde{a} \in \mathbb{R} : a \cdot \tilde{a} = 1$$

with

$$\tilde{a} = a^{-1} = \frac{1}{a}.$$

Uniqueness of the additive identity

Proposition 1.1. *The additive identity z of Axiom 4 is unique and we call it 0.*

Proof. Let $z', z'' \in \mathbb{R}$ such that

$$1. \quad \forall a \in \mathbb{R}, \quad a + z' = a$$

$$2. \quad \forall a \in \mathbb{R}, \quad a + z'' = a$$

From (1), setting $a = z''$, we have that

$$z'' + z' = z''$$

while from (2), setting $a = z'$ we have that

$$z' + z'' = z'.$$

By the commutativity of addition, we have

$$z' = z' + z'' = z'' + z' = z''$$

from which we derive

$$z' = z''.$$

□

Uniqueness of the additive inverse

Proposition 1.2. *For each $a \in \mathbb{R}$, the additive inverse \bar{a} of Axiom 5 is unique and we call it $-a$.*

Proof. Let $\bar{a}, \bar{\bar{a}} \in \mathbb{R}$ such that

$$\forall a \in \mathbb{R}, \quad a + \bar{a} = 0 \quad \wedge \quad a + \bar{\bar{a}} = 0$$

then we have

$$\bar{a} = \bar{a} + 0 = \bar{a} + (a + \bar{\bar{a}}) = (\bar{a} + a) + \bar{\bar{a}} = 0 + \bar{\bar{a}} = \bar{\bar{a}}.$$

□

Annihilation Law of Multiplication

Proposition 1.3.

$$\forall a \in \mathbb{R}, \quad a \cdot 0 = 0.$$

Proof.

$$a \cdot 0 = a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) = (a \cdot 0 + a \cdot 0) + (-a \cdot 0) = a \cdot (0 + 0) + (-a \cdot 0) = a \cdot 0 + (-a \cdot 0) = 0.$$

□

Order Axioms On \mathbb{R} , an order relation is introduced starting from the undefined concept of *positivity*. There exists $\mathbb{R}^+ \subseteq \mathbb{R}$, called the set of *positive* real numbers, which satisfies the following two axioms:

Axiom 7

$$\forall a, b \in \mathbb{R}^+, \quad a + b, ab \in \mathbb{R}^+;$$

Axiom 8

$$\forall a \in \mathbb{R}, \quad a = 0 \vee a \in \mathbb{R}^+ \vee -a \in \mathbb{R}^+;$$

Definition 1.1. We define a relation $<$ in \mathbb{R} by setting

$$\begin{aligned} x < y \vee y > x &\iff \exists \epsilon \in \mathbb{R}^+ : x + \epsilon = y; \\ x \leq y \vee y \geq x &\iff x < y \vee x = y. \end{aligned}$$

We can then define the following sets

$$\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\} \quad \mathbb{R}^- = \{x \in \mathbb{R} : x < 0\}.$$

Theorem 1.4. The relation \leq is a total order relation on \mathbb{R} . In other words, it satisfies the following properties:

a Reflexivity:

$$\forall x \in \mathbb{R}, \quad x \leq x,$$

b Antisymmetry:

$$\forall x, y \in \mathbb{R}, \quad x \leq y \wedge y \leq x \implies x = y,$$

c Transitivity:

$$\forall x, y, z \in \mathbb{R}, \quad x \leq y \wedge y \leq z \implies x \leq z,$$

d Totality:

$$\forall x, y \in \mathbb{R}, \quad x \leq y \vee y \leq x.$$

The relation $<$ satisfies the following properties of compatibility with addition and multiplication:

e Monotonicity with respect to addition:

$$\forall x, y, z \in \mathbb{R}, \quad x < y \implies x + z < y + z,$$

f Monotonicity with respect to multiplication

$$\forall x, y, z \in \mathbb{R}, \quad x < y \wedge z \in \mathbb{R}^+ \implies zx < zy.$$

Proposition 1.5. If $a \cdot b = 0$, then at least one of a or b is 0.

Proposition 1.6.

1. $-b \cdot a = -(b \cdot a)$
2. $-1 \cdot a = -a$

3. The opposite of the opposite of a is a , i.e.,

$$-(-a) = a$$

4. The reciprocal of the reciprocal of a is a , i.e.,

$$\frac{1}{\frac{1}{a}} = a$$

5. If a number is positive, its opposite is negative

6.

$$\forall a, b, c, d \in \mathbb{R}, \quad a < c \quad \wedge \quad b < d \quad \implies \quad a + b < c + d$$

Proof. from $a < c$ and $b < d$ we derive

$$a < c \quad \implies \quad a + b < c + b$$

and

$$b < d \quad \implies \quad c + b < c + d,$$

from which

$$a + b < c + b < c + d \quad \implies \quad a + b < c + d.$$

□

The Continuity Axiom The axioms **1-8** are not exclusive to \mathbb{R} , as they are equally true in the set of rational numbers \mathbb{Q} . What truly characterizes \mathbb{R} is the **continuity property**, which is characterized by the corresponding **continuity axiom**, also known as the **completeness axiom**. Before stating it in one of its numerous equivalent formulations, it is useful to give some definitions.

Upper and Lower Bounds, Maximum and Minimum

Definition 1.2. Let $A \subseteq \mathbb{R}$, and let $m \in \mathbb{R}$. We say that m

- is an **upper bound** for A if

$$\forall x \in A, x \leq m$$

- is a **lower bound** for A if

$$\forall x \in A, x \geq m$$

- is the **maximum** for A if

1. m is an upper bound for A
2. $m \in A$

- is the **minimum** for A if

1. m is a lower bound for A
2. $m \in A$

Uniqueness of the Maximum

Theorem 1.7. The maximum of a set $A \subseteq \mathbb{R}$ (if it exists), is unique.

Proof. Suppose that m' and $m'' \in \mathbb{R}$ both satisfy the definition of maximum for A . By 1) applied to m' and 2) applied to m'' , we have $m'' \leq m'$ and $m' \leq m''$, from which it follows that $m' = m''$. □

Note 1. Let $A = \{\mu\}$ be a singleton of \mathbb{R} and m its upper bound, then there are infinitely many upper bounds. For example, we can take $m + 1$ and more generally $\forall n \in \mathbb{N}, m + n$. Moreover, if A is bounded above and m is an upper bound of A , then every real number $x \geq m$ is still an upper bound of A ; similarly, if A is bounded below and μ is a lower bound of A , then every real number $x \leq \mu$ is still a lower bound of A .

Proposition 1.8. *Let $m \in \mathbb{R}$, then*

- *m is an upper bound for \emptyset , and*
- *m is not an upper bound for $A \subseteq \mathbb{R} \iff \exists x \in A : x > m$.*

Proposition 1.9. *The set \mathbb{R} has neither an upper bound nor a lower bound.*

Proof. We prove by contradiction that \mathbb{R} has an upper bound. If \mathbb{R} has an upper bound, then

$$\exists m \in \mathbb{R} : \forall x \in \mathbb{R}, x \leq m.$$

Let $x = m + 1$, then

$$m + 1 \leq m \implies 1 \leq 0.$$

Which is a contradiction, therefore \mathbb{R} has no upper bound. Similarly, we prove that there is no lower bound.

$$\exists m \in \mathbb{R} : \forall x \in \mathbb{R}, x \geq m$$

Let $x = m - 1$, then

$$m - 1 \geq m \implies -1 \geq 0$$

Which is a contradiction, therefore \mathbb{R} has no lower bound. □

Definition 1.3. Let $A \subseteq \mathbb{R}$, A bounded.

- The maximum of A is denoted by $\max A$.
- The minimum of A is denoted by $\min A$.

Moreover,

- The **set of upper bounds** of A is the set of all real numbers greater than or equal to all elements of A . It is denoted by A^{\leq} .

$$A^{\leq} = \{m \in \mathbb{R} \mid \forall x \in A, x \leq m\}$$

If A has a maximum, we can also regard A^{\leq} as the set of all real numbers greater than or equal to $\max A$,

$$A^{\leq} = \{m \in \mathbb{R} \mid m \geq \max A\} = [\max A; +\infty)$$

- The **set of lower bounds** of A is the set of all real numbers less than or equal to all elements of A . It is denoted by A^{\geq} .

$$A^{\geq} = \{m \in \mathbb{R} \mid \forall x \in A, x \geq m\}$$

If A has a minimum, we can also regard A^{\geq} as the set of all real numbers less than or equal to $\min A$,

$$A^{\geq} = \{m \in \mathbb{R} \mid m \leq \min A\} = (-\infty; \min A]$$

Supremum and Infimum

Definition 1.4.

- We call the **supremum** for A the real number

$$\min A^{\leq}$$

if it exists and is unique, denoted by

$$\sup A$$

- We call the **infimum** for A the real number

$$\max A^{\geq}$$

if it exists and is unique, denoted by

$$\inf A$$

Proposition 1.10. *Let $A \subseteq \mathbb{R}$*

1. *if $m = \max A$ exists, then $m = \sup A$*
2. *if $s = \min A$ exists, then $s = \inf A$*

Characterization of the Supremum

Theorem 1.11. Let $A \subseteq \mathbb{R}$ and $m \in \mathbb{R}$.
The following statements are equivalent:

1. $m = \sup A$
2. The following two properties hold simultaneously:

- (a) $\forall x \in A, x \leq m$
- (b) $\forall \epsilon > 0, \exists x \in A : x > m - \epsilon$

Proof.

a) \implies b) Let $m = \sup A$, then $m = \min A^{\leq} \implies m \in A^{\leq}$, thus m is an upper bound for A (a). Let $\epsilon > 0$, then

$$m - \epsilon < m \implies m - \epsilon \notin A^{\leq}$$

since it is less than the smallest of the upper bounds, thus

$$\exists x \in A : x > m - \epsilon.$$

b) \implies a) $\forall x \in A, x \leq m \implies m \in A^{\leq}$.

Let $t \in A^{\leq} : t < m$, then

$$\exists \epsilon \in \mathbb{R} : t + \epsilon = m.$$

We write $m - \epsilon = t$.

Being an upper bound, we write

$$\forall x \in A, x \leq t$$

which means

$$\forall x \in A, x \leq m - \epsilon$$

which is in contrast with the second hypothesis, thus we obtain $m = \min A^{\leq}$, therefore $m = \sup A$.

□

Bounded and Unbounded Sets, Inferiorly and Superiorly

Definition 1.5. Let $A \subseteq \mathbb{R}$, we say that A is:

- **Bounded above** if $A^{\leq} \neq \emptyset$;
- **Bounded below** if $A^{\geq} \neq \emptyset$;
- **Unbounded above** if $A^{\leq} = \emptyset$;
- **Unbounded below** if $A^{\geq} = \emptyset$;
- **Bounded** if A is bounded both above and below;
- **Unbounded** if A is unbounded both above and below.

Separated Sets

Definition 1.6. Two non-empty subsets $A, B \subset \mathbb{R}$ are called **separated** if

$$\forall a \in A, \forall b \in B, \quad a \leq b.$$

We also observe that:

- if A and B are separated sets, then every element $b \in B$ is an upper bound for A and every element $a \in A$ is a lower bound for B ;
- if A is non-empty and bounded above, and if M is the set of upper bounds of A , then A and M are separated;
- similarly, if A is non-empty and bounded below, and if N is the set of lower bounds of A , then N and A are separated.

The completeness axiom of \mathbb{R} asserts the possibility of interposing a real number between the elements of any pair of separated sets: essentially, it tells us that the real numbers are sufficient in quantity to fill all the "gaps" between pairs of separated sets. The precise statement is as follows:

Axiom 9 (Completeness) For every pair A, B of non-empty and separated subsets of \mathbb{R} , there exists at least one element

$$\exists \xi \in \mathbb{R} : \forall a \in A, \forall b \in B, \quad a \leq \xi \leq b.$$

Note that generally the separating element between two separated sets A and B is not unique: if $A = \{0\}$ and $B = \{1\}$, all points in the interval $[0, 1]$ are separating elements between A and B . However, if A is a non-empty set bounded above and we choose B as the set of upper bounds of A , then there is a unique separating element between A and B . Indeed, every separating element ξ must satisfy the relation

$$\forall a \in A, \forall b \in B, \quad a \leq \xi \leq b;$$

in particular, the first inequality says that ξ is an upper bound for A , meaning $\xi \in B$, and the second tells us that $\xi = \min B$. Since the minimum of B is unique, it follows that the separating element is unique. Similarly, if B is non-empty and bounded below, and we take A as the set of lower bounds of B , then there is a unique separating element between A and B : the maximum of the lower bounds of B .

Supremum Principle

Theorem 1.12. Let $A \subseteq \mathbb{R}, A \neq \emptyset$; a necessary and sufficient condition for the existence of $s \in \mathbb{R}$, with $s = \sup(A)$, is

$$A \neq \emptyset \wedge A^{\leq} \neq \emptyset$$

Proof. Given $A \neq \emptyset$, let $B = A^{\leq}$. We have that

$$\forall a \in A, \forall b \in B, \quad a \leq b.$$

Therefore, by the continuity axiom, there exists $s \in \mathbb{R}$ such that

$$\forall a \in A, \forall b \in B, \quad a \leq s \leq b,$$

so s is the supremum. □

Note 2. Every $A \subseteq \mathbb{R}, A \neq \emptyset$ and bounded above has a supremum. Similarly, every $A \subseteq \mathbb{R}, A \neq \emptyset$ and bounded below has an infimum.

1.2 Extended Reals

Definition 1.7. By the set of **extended reals**, we mean the set

$$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$$

Let $a \in \mathbb{R}$, we have

1.

$$-\infty < a < +\infty$$

2.

$$-\infty + a = -\infty \quad +\infty - a = +\infty$$

3.

$$\forall a > 0, \quad a \cdot (+\infty) = +\infty \quad a \cdot (-\infty) = -\infty$$

4.

$$\forall a < 0, \quad a \cdot (+\infty) = -\infty \quad a \cdot (-\infty) = +\infty$$

5.

$$\frac{a}{+\infty} = \frac{a}{-\infty} = 0$$

1.3 Operations on Sets

Sum of Two Sets

Definition 1.8. Let A and B be two sets, we define the **sum of A and B** and denote it by $A + B$, as the set

$$A + B = \{a + b \mid a \in A \wedge b \in B\}$$

Note 3. If $A = B = \emptyset$, then $A + B = \emptyset$.

Product of Two Sets

Definition 1.9. Let A and B be two sets, we define the **product of A and B** and denote it by $A \cdot B$, as the set

$$A \cdot B = \{a \cdot b \mid a \in A \wedge b \in B\}$$

Note 4. If $A = \emptyset \vee B = \emptyset$, then $A \cdot B = \emptyset$. Moreover, we have:

- $a \cdot B = \{a\} \cdot B = \{a \cdot b \mid b \in B\}$ e.g., $0 \cdot B = 0$
- $-B = -1 \cdot B$, the set of the opposites of the elements of B
- if $0 \notin A$, we can define $A^{-1} = \{a^{-1} \mid a \in A\}$

1.4 Operations with Supremum and Infimum

Let $A, B \subseteq \mathbb{R}$ be non-empty sets. We have the following theorems:

Theorem 1.13.

$$\sup(A \cup B) = \max\{\sup(A), \sup(B)\}$$

Proof. Let

$$s = \sup(A), \quad t = \sup(B), \quad u = \max\{s, t\}.$$

Assume A is unbounded above and let $m \in \mathbb{R}$ be an upper bound of $A \cup B$, then

$$\forall y \in A \cup B, \quad y \leq m.$$

In particular,

$$\forall y \in A, \quad y \leq m,$$

which is impossible because A has no upper bounds. Similarly, we treat the case where B is unbounded above. We are left with the case where A and B are both bounded above, which implies

$$s, t \in \mathbb{R} \implies u \in \mathbb{R},$$

from which it follows that

$$\left. \begin{array}{l} \forall a \in A, \quad a \leq s \\ \forall b \in B, \quad b \leq t \end{array} \right\} \implies a \leq u \wedge b \leq u.$$

Therefore,

$$\forall y \in A \cup B, \quad y \leq u.$$

Now let $\epsilon > 0$ and consider $u - \epsilon$. Then we have:

- $u = s \implies \exists a \in A : a > s - \epsilon;$
- $u = t \implies \exists b \in B : b > t - \epsilon.$

In any case,

$$\exists y \in A \cup B : y > u - \epsilon.$$

□

Theorem 1.14.

$$\sup(A + B) = \sup(A) + \sup(B)$$

Proof. Fix $\alpha \in A$ and $\beta \in B$. Let $m \in (A + B)^\leq$, then

$$\forall a + b \in A + B, \quad a + b \leq m,$$

in particular,

$$\alpha + \beta \leq m,$$

from which we derive

$$m - \alpha \in B^\leq \quad \text{and} \quad m - \beta \in A^\leq.$$

Let $a \in A$ and $b \in B$:

- since $\alpha + b \in (A + B)$, we have $\alpha + b \leq m$, which implies $b \leq m - \alpha$, i.e., $m - \alpha \in B^\leq$;
- since $a + \beta \in (A + B)$, we have $a + \beta \leq m$, which implies $a \leq m - \beta$, i.e., $m - \beta \in A^\leq$.

Therefore, if at least one of A or B is unbounded above, then $A + B$ is also unbounded above, hence the equality holds. Now let A and B be bounded above, we have

$$\sup A = s \in \mathbb{R} \quad \text{and} \quad \sup B = t \in \mathbb{R},$$

which implies that

$$\forall a \in A, a \leq s \quad \wedge \quad \forall b \in B, b \leq t$$

from which, by (1.6.6), we derive

$$a + b \leq s + t,$$

therefore

$$\sup(A + B) = M \leq s + t.$$

As previously noted,

$$\forall \alpha \in A, \quad M - \alpha \in B^\leq,$$

hence $M - \alpha \geq t$, from which $\alpha \leq M - t$. By the arbitrariness of α , we conclude

$$\sup(A) = s \leq M - t,$$

that is, $M \geq s + t$, thus $M = s + t$. □

Theorem 1.15. For every $a \in A$ and for every $b \in B$ with a, b positive, we have

$$\sup(A \cdot B) = \sup(A) \cdot \sup(B).$$

Theorem 1.16. Let $c > 0$, then

$$\sup(c \cdot A) = c \cdot \sup(A).$$

Proof. Let $m \in \mathbb{R}$, we see that

$$m \in A^\leq \quad \Longleftrightarrow \quad c \cdot m \in (c \cdot A)^\leq.$$

Indeed, if

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

then we also have

$$c \cdot a \leq c \cdot m,$$

therefore

$$c \cdot m \in (c \cdot A)^\leq.$$

Conversely, if $c \cdot m \in (c \cdot A)^\leq$, we would have

$$\forall c \cdot a \in (c \cdot A), \quad c \cdot a \leq c \cdot m.$$

and thus, multiplying by $c^{-1} > 0$, we get $a \leq m$, so $m \in A^\leq$. Therefore, if $\sup(A) = +\infty$, then also

$$\sup(c \cdot A) = c \cdot (+\infty) = +\infty.$$

If instead $\sup(A) = s$, then

$$S = \sup(c \cdot A) \leq c \cdot s.$$

Now we must show that

$$c^{-1} \cdot S \in A^{\leq},$$

but this follows from the fact that

$$c(c^{-1} \cdot S) = S \in (c \cdot A)^{\leq}$$

if

$$S \in (c \cdot A)^{\leq}.$$

In conclusion, $s \leq c^{-1} \cdot S$, that is, $c \cdot s \leq S$. Combining the previous conditions, we have

$$S = c \cdot s.$$

□

Theorem 1.17.

$$\sup(-A) = -\inf(A)$$

Proof. Let $m \in \mathbb{R}$. Suppose $m \in (-A)^{\leq}$, which implies

$$\forall -a \in -A, \quad -a \leq m.$$

This is equivalent to saying that

$$\forall a \in A, \quad a \geq -m$$

that is, $-m \in A^{\geq}$. Indeed,

$$\forall a \in A, \quad a \leq m \iff -a \geq -m.$$

Therefore, if

$$\sup(-A) = s \in \mathbb{R},$$

then

$$-s \in A^{\geq},$$

that is,

$$\inf(A) = S \geq -s,$$

but $-(-S) \in A^{\geq}$ implies $-S \in (-A)^{\leq}$, so $-S \geq s$, that is, $S \leq -s$. From this reasoning, we can understand that if $\inf A > 0$, then

$$\sup A^{-1} = \frac{1}{\inf(A)}.$$

□

Theorem 1.18. Let $a > 0$, then

$$\forall a \in A, \quad \inf(A^{-1}) = \frac{1}{\sup(A)}, \quad \inf(A) > 0 \implies \sup A^{-1} = \frac{1}{\inf A}$$

2 Natural Numbers

2.1 The Set of Natural Numbers

Inductive Set

Definition 2.1. A set $I \subseteq \mathbb{R}$ is called **inductive** if:

1. $1 \in I$;
2. $\forall x \in \mathbb{R}, (x \in I \implies x + 1 \in I)$

The collection of inductive sets is denoted by \mathcal{I} .

Set of Natural Numbers

Definition 2.2. The set that contains all inductive sets is called the **set of natural numbers** and is denoted by \mathbb{N} .

$$\mathbb{N} = \bigcap_{I \in \mathcal{J}} I = \{x \in \mathbb{R} \mid \forall I \in \mathcal{J}, x \in I\}.$$

Let us set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; this set satisfies Peano's axioms for natural numbers.

Peano's Axioms Peano defines natural numbers as a system consisting of a set \mathbb{N} in which the operation of "successor" is defined, and an element 1, verifying the following axioms:

1. 1 is a number.
2. The successor of a number is a number.
3. 1 is not the successor of any number.
4. Different numbers have different successors.
5. If $A \subseteq \mathbb{N}$ contains 1 and the successor of each of its elements, then $A = \mathbb{N}$.

The first axiom assures us that \mathbb{N} is not empty, as it contains at least the number 1, which is the first element of \mathbb{N} . The second guarantees that in \mathbb{N} we can count, always taking the successor. The third axiom tells us that counting does not return to 1. The fourth states that we never return to a number already encountered.

We can write the axioms in formal terms, introducing $\sigma(n)$ to indicate the successor of n :

1. $1 \in \mathbb{N}$.
2. $\forall n \in \mathbb{N}, \sigma(n) \in \mathbb{N}$,
3. $\forall n \in \mathbb{N}, \sigma(n) \neq 1$,
4. $\forall n, m \in \mathbb{N}, \sigma(n) = \sigma(m) \implies n = m$,
5. $\forall A \subseteq \mathbb{N}, \{(1 \in A) \wedge (\forall n \in \mathbb{N}, n \in A \implies \sigma(n) \in A)\} \implies A = \mathbb{N}$

Inductiveness of \mathbb{N}

Proposition 2.1. \mathbb{N} is inductive.

Proof. $1 \in \mathbb{N}$, in fact $\forall I \in \mathcal{J}, 1 \in I$. Let $n \in \mathbb{N}$; then $\forall I \in \mathcal{J}, n \in I$, so $n + 1 \in I$. Therefore, $n + 1 \in \mathbb{N}$. □

This implies that every inductive subset of \mathbb{N} coincides with \mathbb{N} , so \mathbb{N} is the smallest possible inductive set.

2.2 Principle of Induction

First Form of the Principle of Induction

Theorem 2.2. If a property $P(n)$ holds for $n = 1$, and if, assuming it true for n , it is shown to be true for $n + 1$, then $P(n)$ is true for every n . This can be formally stated as:

$$P(1) \wedge \{\forall n, P(n) \implies P(n + 1)\} \implies \forall n, P(n).$$

Proof. Consider the set A of natural numbers n for which $P(n)$ is true:

$$A = \{n \in \mathbb{N} \mid P(n)\}.$$

Since by assumption $P(1)$ is true, we have $1 \in A$. Moreover, if $P(n)$ is true (i.e., if $n \in A$), then $P(n + 1)$ is also true, and hence $n + 1 \in A$. By axiom 5, $A = \mathbb{N}$, meaning $P(n)$ is true for every n . □

Second Form of the Principle of Induction

Theorem 2.3. Let $A \subseteq \mathbb{N}$, suppose that:

$$\forall n \in \mathbb{N}, \forall m < n, \quad m \in A \implies n \in A$$

Then $A = \mathbb{N}$.

2.3 Definitions for Recursion

Construction by Recursion

Definition 2.3. To construct E_n for every $n \in \mathbb{N}$, I can proceed as follows:

1. Construct E_1
2. Establish a procedure that gives me E_{n+1} from E_n for every $n \in \mathbb{N}$.

Power with Natural Exponent a^n where $a \in \mathbb{R}$ and $n \in \mathbb{N}$.

1. $a^1 = a$
2. $\forall n \in \mathbb{N}, a^{n+1} = a^n \cdot a$

Summation Let a_1, a_2, \dots, a_n be n real numbers and $i \in \mathbb{N}$. Their sum

$$a_1 + a_2 + \dots + a_n$$

can be compactly expressed using the *summation* symbol:

$$\sum_{i=1}^n a_i$$

which is read as: "summation for i from 1 to n of a_i ". The symbol i is called the *summation index*.

Setting the following,

1.

$$\sum_{i=1}^1 a_i = a_1$$

2.

$$\sum_{i=1}^{n+1} a_i = \sum_{i=1}^n a_i + a_{n+1}$$

Factorial The n factorial, denoted by the symbol $n!$, is the product of the integers from 1 to n , inclusive:

$$n! = 1 \times 2 \times \dots \times (n-2) \times (n-1) \times n.$$

Setting the following:

1.

$$1! = 1$$

2.

$$n! = n(n-1)!$$

2.4 Well-Ordering of Natural Numbers

Well-Ordering of Natural Numbers

Theorem 2.4. *Every non-empty subset of \mathbb{N} has a minimum.*

Proof. Let $T \subseteq \mathbb{N}$ be without a minimum; we will prove that $T = \emptyset$. Consider the complement $A = \mathbb{N} \setminus T$. Using the second principle of induction, we show that

$$\forall n \in \mathbb{N}, \forall m < n, \quad m \in A \implies n \in A.$$

Since A is the complement of T ,

$$\forall m < n, m \notin T$$

implies that also $n \notin T$, thus $T = \emptyset$. □

2.5 Archimedean Property

Archimedean Property

Theorem 2.5. *\mathbb{N} is unbounded above, that is, $\sup(\mathbb{N}) = +\infty$. In symbols:*

$$\forall x \in \mathbb{R}, \exists n \in \mathbb{N} : n > x,$$

hence \mathbb{N} has no upper bounds.

Proof. Suppose that $\sup(\mathbb{N}) = s \in \mathbb{R}$. By theorem (1.11), we have:

$$s = \sup(\mathbb{N}) \implies \forall n \in \mathbb{N}, n \leq s \quad (s \in \mathbb{N}^{\leq}) \quad \wedge \quad \forall \epsilon > 0, \exists n \in \mathbb{N} : n > s - \epsilon.$$

Then

$$s - 1 \notin \mathbb{N}^{\leq}$$

meaning

$$\exists m \in \mathbb{N} : m > s - 1$$

and

$$m + 1 > s,$$

which is impossible. □

2.6 Bernoulli's Inequality

Bernoulli's Inequality

Proposition 2.6.

$$\forall n \in \mathbb{N}, \forall b \geq -1, \quad (1 + b)^n \geq 1 + nb.$$

Proof. We prove by induction on n .

$$\begin{aligned} n = 1 \quad & - (1 + b)^1 = (1 + b) \\ & - 1 + 1 \cdot b = 1 + b \end{aligned}$$

Since $1 + b = 1 + b$, then $p(1)$ is verified.

$$n \rightsquigarrow n + 1$$

$$\begin{aligned} (1 + b)^{n+1} &= (1 + b)^n(1 + b) \implies (1 + nb)(1 + b) \\ (1 + b)^n(1 + b) &\geq (1 + nb)(1 + b) \\ (1 + b)^n(1 + b) &\geq 1 + b + nb + nb^2 \end{aligned}$$

From the fact that

$$1 + b + nb + nb^2 \geq 1 + nb + b = 1 + (n + 1)b$$

it follows that

$$(1 + b)^n(1 + b) \geq 1 + (n + 1)b$$

and thus it is verified for $n + 1$ as well.

□

Proposition 2.7. *If $x > 1$, then*

$$\sup\{x^n \mid n \in \mathbb{N}\} = +\infty$$

Proof. Proceeding by contradiction, suppose that $\sup\{x^n \mid n \in \mathbb{N}\} = s \in \mathbb{N}$, thus the set is bounded above. Let

$$b = \frac{s}{n} > 0 \geq -1,$$

using Bernoulli,

$$\left(1 + \frac{s}{n}\right)^n = (1 + b)^n \geq 1 + nb \geq 1 + s > s$$

Now let n be such that $x \geq 1 + \frac{s}{n}$, i.e.

$$n \geq \frac{s}{x-1} \iff \frac{1}{n} \leq \frac{x-1}{s} \iff \frac{s}{n} \leq x-1 \iff \frac{s}{n} + 1 \leq x.$$

This gives us $x^n > s$, which is impossible, thus the set is unbounded. □

3 The Integers

3.1 The Set of Integers

The Set of Integers

Definition 3.1.

$$\mathbb{Z} = \mathbb{N}_0 \cup (-\mathbb{N}) = \{0, 1, -1, 2, -2, 3, -3, \dots\}$$

Note 5. $n \in \mathbb{Z}$ is odd if $\exists k \in \mathbb{Z} : n = 2k + 1$.

Maximum of a Non-Empty Set of Integers and Upper Boundedness

Proposition 3.1. *Every non-empty set of integers that is upper bounded has a maximum.*

Proof. Let $E \subseteq \mathbb{Z}$ be a non-empty set that is upper bounded. By the Archimedean property

$$\exists n \in \mathbb{N} : \forall k \in E, \quad k < n.$$

Let $T = \{n - k \mid k \in E\}$, we find that $T \subseteq \mathbb{N}$, and

$$T \neq \emptyset \because E \neq \emptyset.$$

Thus, by theorem (2.4),

$$\exists h \in \mathbb{N} : h = \min(T).$$

Setting $m = n - h$, we have

$$m \in E \quad \text{and} \quad \forall j \in E, \quad j \leq m,$$

thus $n - j \geq h$ and

$$j = n - (n - j) \leq n - h = m,$$

therefore $m = \max E$. □

Existence of an integer maximum that does not exceed every real number

Corollary 1. $\forall x \in \mathbb{R}$, there always exists an integer maximum that does not exceed x .

Proof. Let

$$E = \{k \in \mathbb{Z} \mid k \leq x\},$$

then E is non-empty and bounded above. It is non-empty because if $n > -x$ then $-n < x$ and $-n \in \mathbb{Z}$. \square

Integer and fractional parts of a real number

Definition 3.2. The **integer part** of $x \in \mathbb{R}$ is the maximum integer that does not exceed x . We denote it by

$$\text{int } x \quad \text{or} \quad \lfloor x \rfloor.$$

The **fractional part** is denoted by

$$\text{frac } x = x - \text{int } x \quad \text{or} \quad \{x\}.$$

Note 6. We have, obviously, that

$$\forall x \in \mathbb{R}, \quad 0 \leq \text{frac } x < 1.$$

Furthermore, if $n = \text{int } x$, then

•

$$n \leq x < n + 1;$$

•

$$x - 1 < n \leq x;$$

•

$$x = \text{int } x \iff x \in \mathbb{Z}.$$

4 Rational Numbers

4.1 The set of rational numbers

The set of rational numbers

Definition 4.1.

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z} \wedge n \in \mathbb{N} \right\}$$

Existence and irrationality of the square root of 2 Consider the sets

$$A = \{x \in \mathbb{R} \mid x > 0 \wedge x^2 < 2\}, \quad B = \{x \in \mathbb{R} \mid x > 0 \wedge x^2 > 2\}.$$

Observe that $A \neq \emptyset$ (since $1 \in A$) and $B \neq \emptyset$ (since $2 \in B$), from which we derive

$$\left. \begin{array}{l} \forall a \in A, \quad a^2 < 2 \\ \forall b \in B, \quad b^2 > 2 \end{array} \right\} \implies a^2 < 2 < b^2 \wedge a + b > 0.$$

It follows that

$$b - a = \frac{(b-a)(\cancel{b+a})}{\cancel{b+a}} = \frac{b^2 - a^2}{b + a} > 0,$$

i.e., $a < b$. By the axiom of continuity,

$$\exists s \in \mathbb{R} \setminus \mathbb{Q} : \forall a \in A, \forall b \in B, a \leq s \leq b.$$

To show that $s^2 = 2$, we must prove that

$$s^2 \not> 2 \wedge s^2 \not< 2.$$

1. If $s^2 > 2$, let us set

$$z = \frac{s^2 + 2}{2s} = \frac{s + \frac{2}{s}}{2}.$$

We have

$$z - s = \frac{s^2 + 2}{2s} - s = \frac{s^2 + 2 - 2s^2}{2s} = \frac{2 - s^2}{2s} < 0 \implies z < s.$$

Now

$$z^2 = \left(\frac{s^2 + 2}{2s} \right)^2 = \frac{(s^2 + 2)^2}{(2s)^2} = \frac{s^4 + 4s^2 + 4}{4s^2}.$$

Therefore,

$$z^2 - 2 = \frac{s^4 + 4s^2 + 4}{4s^2} - 2 = \frac{s^4 + 4s^2 + 4 - 8s^2}{4s^2} = \frac{s^4 - 4s^2 + 4}{4s^2} = \frac{(s^2 - 2)^2}{4s^2} > 0$$

i.e., $z^2 > 2$. Thus we have some $z \in B$, but $z < s$ is impossible because

$$\forall b \in B, s \leq b.$$

2. If $s^2 < 2$, let us set

$$y = \frac{4s}{s^2 + 2}.$$

We have

$$y - s = \frac{4s}{s^2 + 2} - s = \frac{4s - s^3 - 2s}{s^2 + 2} = \frac{2s - s^3}{s^2 + 2} = \frac{s(2 - s^2)}{s^2 + 2} > 0$$

i.e., $y > s$, but

$$2 - y^2 = 2 - \frac{16s^2}{s^4 + 4s^2 + 4} = \frac{2s^4 + 8s^2 + 8 - 16s^2}{(s^2 + 2)^2} = \frac{2s^4 - 8s^2 + 8}{(s^2 + 2)^2} = \frac{2(s^2 - 2)^2}{(s^2 + 2)^2} > 0$$

i.e., $y^2 < 2$. In conclusion, we have that $y \in A$, but $y > s$ is impossible because

$$\forall a \in A, a \leq s.$$

Suppose that

$$\exists s \in \mathbb{Q} : s^2 = 2 \quad \text{with } (s > 0).$$

Then we would have

$$s^2 = \left(\frac{m}{n} \right)^2 = 2$$

where we can assume that $\frac{m}{n}$ is in lowest terms. We would then have $m^2 = 2n^2$, which means m is even, and we can rewrite $m = 2h$ with $h \in \mathbb{N}$. Thus, $m^2 = 4h^2$, but this implies that $2n^2 = 4h^2$, which leads to $n^2 = 2h^2$, meaning that n^2 is also even, so we can write $n = 2k$. Therefore, we have

$$\frac{m}{n} = \frac{2h}{2k} = \frac{h}{k},$$

which is absurd because we have already assumed that the fraction was in lowest terms. Thus, the number whose square is 2 is real but not rational.

4.2 The n -th Root of a Real Number

Arithmetic n -th Root of a Real Number

Theorem 4.1. Let $n \in \mathbb{N}$ and let $a > 1$, and consider the set

$$E = \{x \in \mathbb{R} \mid x > 0 \wedge x^n < a\}.$$

Since $E \neq \emptyset$ and is bounded above, there exists $s = \sup(E) \in \mathbb{R}$. We will have that s is the unique positive number such that $s^n = a$. This number is called the arithmetic n -th root of a and is denoted by one of the symbols

$$\sqrt[n]{a} \quad \text{or} \quad a^{\frac{1}{n}}.$$

n -th Root of a Real Number

Definition 4.2. Let $n \in \mathbb{N}$ and let $a \geq 0$, we define the **n -th root** of a as follows

$$\sqrt[n]{a} = \begin{cases} 0 & a = 0 \\ 1 & a = 1 \\ 1/s & 0 < a < 1 \\ \text{the number } s \text{ from the previous theorem} & a > 1 \end{cases}$$

In this way, $\sqrt[n]{a}$ is the only real number ≥ 0 whose n -th power is a .

4.3 Logarithms

Logarithm

Definition 4.3. Let $x, b > 0$ and $b \neq 1$. We say that the number $\xi \in \mathbb{R}$ is the **logarithm base b of x** if $b^\xi = x$. This number, if it exists, is unique, and we write:

$$\xi = \log_b x.$$

Note 7. Thus, by definition:

$$b^{\log_b x} = x.$$

Properties of Logarithms The properties of logarithms, which are derived from those of exponentials, taking $x, y, a \in \mathbb{R}^+$, $a \neq 1$, are:

1. $\log_a xy = \log_a x + \log_a y$;
2. $\log_a \frac{x}{y} = \log_a x - \log_a y$;
3. $\log_a x^\alpha = \alpha \log_a x \quad \forall \alpha \in \mathbb{R}$;
4. $\log_a x = \frac{1}{\log_x a} = -\log_{\frac{1}{a}} x \quad (x \neq 1)$;
5. $\log_a a = 1 \quad \log_a 1 = 0$.

Change of Base Formula

Proposition 4.2. Let $a, b > 0$ and $a, b \neq 1$, we have

$$\log_a x = \frac{\log_b x}{\log_b a}$$

Proof. Let

$$\xi = \log_b x \text{ with } x = b^\xi, \quad \alpha = \log_b a \text{ with } a = b^\alpha.$$

We have

$$\alpha \log_a x = \log_a x^\alpha = \log_a (b^\xi)^\alpha = \log_a (b^\alpha)^\xi = \log_a a^\xi = \xi \log_a a = \xi.$$

Thus, we have

$$\alpha \log_a x = \xi,$$

dividing both sides by α , we obtain

$$\log_a x = \frac{\xi}{\alpha} = \frac{\log_b x}{\log_b a}.$$

□

Variation of Bernoulli's Inequality

Proposition 4.3.

$$\forall n \in \mathbb{N}, \forall b \geq 0, \quad (1+b)^n \geq 1 + nb + \frac{n(n-1)}{2}b^2$$

Proof. By induction on n

$$n = 1$$

$$(1+b)^1 = 1+b \geq 1+1 \cdot b + \frac{1 \cdot (1-1)}{2}b^2 = 1+b+0 = 1+b$$

$n \rightsquigarrow n+1$ We have

$$(1+b)^{n+1} = (1+b)^n(1+b),$$

thus

$$\begin{aligned} \left(1 + nb + \frac{n(n-1)}{2}b^2\right)(1+b) &= 1 + nb + \frac{n(n-1)}{2}b^2 + b + nb^2 + \frac{n(n-1)}{2}b^3 \\ &= 1 + nb + b + n\left(\frac{n-1}{2}\right)b^2 + nb^2 + \left(\frac{n(n-1)}{2}\right)b^3 \\ &= 1 + (n+1)b + \left(\frac{n(n-1)}{2} + n\right)b^2 + \left(\frac{n(n-1)}{2}\right)b^3 \\ &= 1 + (n+1)b + \left(\frac{n(n+1)}{2}\right)b^2 + \left(\frac{n(n-1)}{2}\right)b^3 \\ &\geq 1 + (n+1)b + \left(\frac{(n+1)n}{2}\right)b^2 \end{aligned}$$

□

Now let $b = \frac{1}{n}$, we will thus have

$$\begin{aligned} \left(1 + \frac{1}{n}\right)^{n+1} &\geq 1 + (n+1)\frac{1}{n} + \frac{(n+1)n}{n} \frac{1}{n^2} = 1 + 1 + \frac{1}{n} + \frac{n+1}{2n} \\ &= 2 + \frac{1}{2} + \frac{3}{2n} > \frac{5}{2} \implies e \geq \frac{5}{2} \end{aligned}$$

4.4 The Number e

Proposition 4.4. Let

$$e = \inf \left\{ x \in \mathbb{R} \mid \exists n \in \mathbb{N} : x = \left(1 + \frac{1}{n}\right)^{n+1} \right\},$$

then

$$2 \leq e \leq 4.$$

Proof. Let

$$E = \left\{ \left(1 + \frac{1}{n}\right)^{n+1} \mid n \in \mathbb{N} \right\}$$

so that $e = \inf E$. Then we have that

$$\forall x \in E, \exists n \in \mathbb{N} : x = \left(1 + \frac{1}{n}\right)^{n+1}.$$

By Bernoulli's inequality

$$\begin{aligned} (1+b)^n &\geq 1 + nb \implies b = \frac{1}{n} \\ x &\geq 1 + (n+1)\frac{1}{n} = 1 + 1 + \frac{1}{n} = 2 + \frac{1}{n} > 2 \implies e \geq 2 \end{aligned}$$

Moreover,

$$4 \in E \quad \because \quad 4 = \left(1 + \frac{1}{1}\right)^{1+1} \quad \therefore \quad e \leq 4.$$

Thus, we have $2 \leq e \leq 4$. □

4.5 Density of Rationals

Theorem 4.5.

$$\forall a, b \in \mathbb{R} \ (a < b), \exists q \in \mathbb{R} : a < q < b.$$

Proof. Let $n \in \mathbb{N}$ such that $n > \frac{1}{b-a}$. We then have

$$n \cdot (b-a) = nb - na > 1 \quad \implies \quad nb > 1 + na.$$

From the properties of the integer part of a real number, we have:

$$na - 1 < \lfloor na \rfloor \leq na,$$

which leads us to

$$na < \lfloor na \rfloor + 1 \leq na + 1 < nb.$$

Therefore, letting

$$m = 1 + \lfloor na \rfloor \in \mathbb{Z},$$

we get

$$na < m < nb \quad \implies \quad a < \frac{m}{n} < b$$

i.e., $a < q < b$ with $q = \frac{m}{n} \in \mathbb{Q}$. □

4.6 Density of Irrationals

Corollary 2.

$$\forall a, b \in \mathbb{R} \ (a < b), \exists r \in \mathbb{R} \setminus \mathbb{Q} : a < r < b.$$

Proof. Let $q_1, q_2 \in \mathbb{Q}$ such that $a < q_1 < q_2 < b$. We have

$$q_1 = \frac{m_1}{n_1} \wedge q_2 = \frac{m_2}{n_2}$$

so by multiplying everything by n_2 and n_1

$$q_1 = \frac{m_1 n_2}{n_1 n_2} < \frac{n_1 m_2}{n_1 n_2} = q_2$$

thus $m_1 n_2 < n_1 m_2$ from which (since they are integers)

$$1 + m_1 n_2 \leq n_1 m_2.$$

If $s \in \mathbb{R} \setminus \mathbb{Q}$ is positive and $s < 1$

$$m_1 n_2 < m_1 n_2 + s < m_1 n_2 + 1 \leq n_1 m_2$$

Therefore, we divide

$$q_1 = \frac{m_1 n_2}{n_1 n_2} < \frac{m_1 n_2 + s}{n_1 n_2} < \frac{n_1 m_2}{n_1 n_2} = q_2$$

i.e.,

$$q_1 < M < q_2$$

where

$$M = \frac{m_1 n_2 + s}{n_1 n_2} \in \mathbb{R} \setminus \mathbb{Q}.$$

□

4.7 Intervals

Interval

Definition 4.4. Let $I \subseteq \mathbb{R}$. We say that I is an **interval** if, for every pair $a, b \in I$ with $a < b$, and for every $c \in \mathbb{R}$ such that $a < c < b$, then $c \in I$. Every $E \subseteq \mathbb{R}$ with fewer than two elements is an interval, called **degenerate**.

Note 8.

- If I is a non-empty collection of intervals, then the intersection $\bigcap I$ is also an interval.
- The union of two or more intervals is not, in general, an interval.

Open, Closed, and Half-Open Intervals

Proposition 4.6. Let $r \in \mathbb{R}$. The following sets are intervals:

1. $\{x \in \mathbb{R} \mid x \leq r\}$
2. $\{x \in \mathbb{R} \mid x < r\}$
3. $\{x \in \mathbb{R} \mid x \geq r\}$
4. $\{x \in \mathbb{R} \mid x > r\}$

Proof.

1. Let $a, b \in \{x \in \mathbb{R} \mid x \leq r\}$ with $a < b$. If $c \in \mathbb{R}$ such that $a < c < b$, since $b \leq r$, then $c < r$.
2. Let $a, b \in \{x \in \mathbb{R} \mid x < r\}$ with $a < b$. If $c \in \mathbb{R}$ such that $a < c < b$, since $b < r$, then $c < r$.
3. Let $a, b \in \{x \in \mathbb{R} \mid x \geq r\}$ with $a < b$. If $c \in \mathbb{R}$ such that $a < c < b$, since $a \geq r$, then $c > r$.
4. Let $a, b \in \{x \in \mathbb{R} \mid x > r\}$ with $a < b$. If $c \in \mathbb{R}$ such that $a < c < b$, since $a > r$, then $c > r$.

□

To prove point (1), the following sets are all intervals, for $\alpha, \beta \in \mathbb{R}$:

5. $\{x \in \mathbb{R} \mid \alpha < x \wedge x < \beta\} = (\alpha, \beta) =]\alpha, \beta[$
If $\alpha = -\infty$ and $\beta = +\infty$, then $(-\infty, +\infty) = \mathbb{R}$.
6. $\{x \in \mathbb{R} \mid \alpha \leq x \wedge x \leq \beta\} = [\alpha, \beta]$
7. $\{x \in \mathbb{R} \mid \alpha < x \wedge x \leq \beta\} = (\alpha, \beta] =]\alpha, \beta]$
If $\alpha = -\infty$ and β is finite, then $(-\infty, \beta]$.
8. $\{x \in \mathbb{R} \mid \alpha \leq x \wedge x < \beta\} = [\alpha, \beta) = [\alpha, \beta[$
If α is finite and $\beta = +\infty$, then $[\alpha, +\infty)$.

These intervals are non-degenerate if and only if $\alpha < \beta$.