1

Set of real numbers

The set of rational numbers, denoted as $\mathbb{Q}$, is defined as

$$\mathbb{Q} = \left\{ \frac{p}{q} : \quad p \in \mathbb{Z}, \quad q \in \mathbb{Z}^* \right\}.$$

Let $m \in \mathbb{N}$, the number $\sqrt{m}$ is defined as a solution of $x^2 = m$. We consider the case where m is primeand we suppose that $\sqrt{m} \in \mathbb{Q}$; thus, there exists $a \in \mathbb{N}$ and $b \in \mathbb{N}^*$ such that a, b are coprime and $\sqrt{m} = a/b$. Therefore

$$a^2 = mb^2. \tag{1.1}$$

Since m is primeand divide mb^2 then m divides a. Hence, $a = m\alpha$ for some $\alpha \in \mathbb{N}$. This transforms (1.1) to $m\alpha^2 = b^2$. Again, m is prime and divides $m\alpha^2 = b^2$; thus, m divides b. This is a contradiction since a and b are coprime. Therefore, $x = \sqrt{m}$ is not rational.

Proposition 1.1. *Let $m \in \mathbb{N}$ be a prime number. Then, $\sqrt{m}$ is irrational.*

We define the set $\mathbb{R}$ as the set formed by all rational and irrational numbers.

$$\begin{array}{lll} \mathbb{R}^* = \{x \in \mathbb{R} : \quad x \neq 0\}, & \mathbb{R}_+ = \{x \in \mathbb{R} : \quad x \geq 0\}, & \mathbb{R}_- = \{x \in \mathbb{R} : \quad x \leq 0\}, \\ \mathbb{N}^* = \{x \in \mathbb{N} : \quad n \neq 0\}, & \mathbb{N}_n^* = \{x \in \mathbb{N} : \quad 1 \leq x \leq n\}, & \mathbb{N}_n = \{x \in \mathbb{R} : \quad 0 \leq n \leq 0\}. \end{array}$$

1.1. Algebraic structure of the set of real numbers.

The set $\mathbb{R}$ equipped with the binary operations "$+$" and "$\cdot$" is a field since it satisfies the following properties :

- Commutativity : $x + y = y + x$ and $x \cdot y = y \cdot x$ for any $x, y \in \mathbb{R}$.
- Associativity : $(x + y) + z = x + (y + z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for any $x, y, z \in \mathbb{R}$.
- Identity element for "$+$" : There exists an element denoted 0 such that $x + 0 = 0 + x = x$ for any $x \in \mathbb{R}$.
- Additive inverse : For any x in $\mathbb{R}$, there exists an element $-x$ such that $x + (-x) = 0$.
- Identity element for "$\cdot$" : There exists an element denoted 1, such as $x \cdot 1 = 1 \cdot x = x$ for any $x \in \mathbb{R}$.
- Multiplicative inverse : For any $x \in \mathbb{R}^*$, there exists an element denoted x^{-1} (or $1/x$) such that $x \cdot x^{-1} = 1$.
- Distributivity : $x \cdot (y + z) = x \cdot y + x \cdot z$ for any $\forall x, y, z \in \mathbb{R}$.

The set $\mathbb{R}$ is totally ordered with respect to the natural order "$\leq$". In other words; for any $x, y \in \mathbb{R}$ we have $x \leq y$ or $y \leq x$. The total order relation satisfies the following properties :

- *Reflexivity* : $x \leq x$ for any $x \in \mathbb{R}$.
- *Antisymmetry* : for $x, y \in \mathbb{R}$, if $x \leq y$ and $y \leq x$ then $x = y$.
- *Transitivity* : for $x, y, z \in \mathbb{R}$, if $x \leq y$ and $y \leq z$ then $x \leq z$.
- *Compatibility of "$\leq$" and "$+$"* : for $x, y, z, w \in \mathbb{R}$, if $x \leq y$ and $z \leq w$ then $x + z \leq y + w$.
- *Compatibility of "$\leq$" and "$\cdot$"* : for $x, y \in \mathbb{R}$ and $z \in \mathbb{R}_+$, if $x \leq y$ then $z \cdot x \leq z \cdot y$.

Definition 1.1 (Absolute Value). *The set $\mathbb{R}$ is valuable in the sense that it can be equipped with the absolute value function defined as follows :*

$$\begin{aligned} |\cdot| : \mathbb{R} &\longrightarrow \mathbb{R}_+ \\ x &\longmapsto |x| = \begin{cases} x & si \quad x \geq 0 \\ -x & si \quad x \leq 0 \end{cases} \end{aligned} \tag{1.2}$$

Proposition 1.2. *The absolute value function is said to be non-negative (meaning that $|x| \geq 0$ for any $x \in \mathbb{R}$) and $|x| = 0$ if and only if $x = 0$. Moreover, for any $x, y \in \mathbb{R}$ we have*

$$|x \cdot y| = |x| \cdot |y|, \quad |x+y| \leq |x| + |y|, \quad |x| - |y| \leq |x+y|, \quad \big||x| - |y|\big| \leq |x-y|.$$

Proof.

- Let $x \in \mathbb{R}$ such that $|x| = 0$, bu using the definition of the absolute value given by (1.2) we get $x = 0$.
- A discussion based on the sign of x and y combined with (1.2) yields $|x \cdot y| = |x| \cdot |y|$.
- Let $z \in \mathbb{R}$, we have $|z| = z$ if $z \geq 0$, and $|z| = -z \geq z$ if $z \leq 0$; thus, $z \leq |z|$ for any $z \in \mathbb{R}$. Let $x, y \in \mathbb{R}$
  - In the case where $x + y \geq 0$, we get $|x + y| = x + y \leq |x| + |y|$.
  - In the case where $x + y < 0$, we get $|x + y| = -x - y \leq |-x| + |-y] = |x| + |y|$.

  In conclusion : $|x + y| \leq |x| + |y|$ for any $x, y \in \mathbb{R}$.
- We have already shown that $|V + W| \leq |V| + |W|$ for any $V, W \in \mathbb{R}$, hence

$$|V + W| - |W| \leq |V|. \tag{1.3}$$

Let's consider the specific case where $V = x + y$ and $W = -y$, this yields :

$$|x| - |y| \leq |x + y|. \tag{1.4}$$

Hence, the third assertion of the proposition. Let now $V = x + y$ and $W = -x$, the condition (1.3) gives :

$$|y| - |x| \leq |x + y|. \tag{1.5}$$

The conditions (1.4)-(1.5) provide the fourth assertion.

□

Theorem 1.1 (Newton's binomial formula). *Let $a, b \in \mathbb{R}$ and $n \in \mathbb{N}^* \setminus \{1\}$. Then*

$$\left(a + b\right)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k. \tag{1.6}$$

such that $C_n^k = \dfrac{n!}{k!(n-k)!}$ for any $(n, k) \in \mathbb{N} \times \mathbb{N}$ with $k \leq n$.

Proof. by induction on the integer n :

- For $n = 2$: we have $\left(a + b\right)^2 = a^2 + 2ab + b^2$, since $C_2^0 = C_2^2 = 1$ and $C_2^1 = 2$ we obtain

$$\left(a + b\right)^2 = C_2^0 a^2 + C_2^1 ab + C_2^2 b^2 = \sum_{k=0}^{2} C_2^k a^{2-k} b^k.$$

- Assume that for some $n \in \mathbb{N}^* \setminus \{1\}$ we have (1.6). Using the fact that $\left(a + b\right)^{n+1} = (a + b)\left(a + b\right)^n$ and the induction hypothesis (1.6) we get

$$(a + b)^{n+1} = \left(\sum_{k=0}^{n} C_n^k a^{n-k+1} b^k\right) + \left(\sum_{k=0}^{n} C_n^k a^{n-k} b^{k+1}\right).$$

Using the change of index $l = k+1$ at the level of the second sum of the previous equation, we get

$$\begin{aligned}(a+b)^{n+1} &= \left(\sum_{k=0}^{n} C_n^k a^{n-k+1} b^k\right) + \left(\sum_{l=1}^{n+1} C_n^{l-1} a^{n-l+1} b^l\right) \\ &= C_n^0 a^{n+1} b^0 + \left(\sum_{k=1}^{n} \left(C_n^k + C_n^{k+1}\right) a^{n-k+1} b^k\right) + C_n^n a^0 b^{n+1}. \qquad (1.7)\end{aligned}$$

Since $C_n^0 = C_{n+1}^0$, $C_n^k + C_n^{k+1} = C_{n+1}^k$ and $C_n^n = C_{n+1}^{n+1}$; the expression (1.7) becomes as

$$(a+b)^{n+1} = C_{n+1}^0 a^{n+1} b^0 + \left(\sum_{k=1}^{n} C_{n+1}^k a^{n-k+1} b^k\right) + C_{n+1}^{n+1} a^0 b^{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k a^{n-k+1} b^k.$$

– In conclusion : we have (1.6) for any $k \in \mathbb{N}^* \setminus \{1\}$.

□

Example 1.1. The calculus yields

$$\sum_{k=1}^{n} (k+1)^3 = \left(\sum_{k=1}^{n} k^3\right) + 3\left(\sum_{k=1}^{n} k^2\right) + 3\left(\sum_{k=1}^{n} k\right) + \left(\sum_{k=1}^{n} 1\right),$$

using the index change $m = k+1$ at the left of the previous equation, we get

$$\sum_{m=2}^{n+1} m^3 = \left(\sum_{k=1}^{n} k^3\right) + 3\left(\sum_{k=1}^{n} k^2\right) + 3\frac{n(n+1)}{2} + n,$$

therefore

$$(n+1)^3 + \sum_{m=2}^{n} m^3 = 1 + \left(\sum_{k=2}^{n} k^3\right) + 3\left(\sum_{k=1}^{n} k^2\right) + 3\frac{n(n+1)}{2} + n,$$

finally

$$\sum_{k=1}^{n} k^2 = \frac{1}{3}\left[(n+1)^3 - 1 - 3\frac{n(n+1)}{2} - n\right] = \frac{(2n+1)(n+1)n}{6}.$$

△

1.2. Maximum, minimum and integer part.

The upper and lower bounds of a given subset of $\mathbb{R}$ is an essential notion in analysis and calculus, not only for describing the structure of the set of real numbers but also for studying numerical sequences and functions.

Definition 1.2. *Let $\mathbb{E} \subset \mathbb{R}$ be non-empty set, and let $\alpha \in \mathbb{R}$.*

- *We say that α is an upper bound of $\mathbb{E}$ (or that $\mathbb{E}$ is upper bounded* by α) if $x \leq \alpha$ for every $x \in \mathbb{E}$.*
- *We say that α is lower bound of $\mathbb{E}$ (or that $\mathbb{E}$ is lower bounded* by α) if $\alpha \leq x$ for every $x \in \mathbb{E}$.*
- *We call the supremum of $\mathbb{E}$, denoted* $\mathrm{Sup}(\mathbb{E})$*, the smallest upper bound of the set $\mathbb{E}$.*
- *We call the infimum of $\mathbb{E}$, denoted* $\mathrm{Inf}(\mathbb{E})$*, the largest lower bound of the set $\mathbb{E}$.*
- *We say that $\mathbb{E}$ is bounded if it is upper and lower bounded.*

* In some books, the terminology "upper bounded" (respectively "lower bounded") is replaced by "bounded above" (respectively "bounded below")

Example 1.2. For instance, the set $A = [0, 2[$ has $[2, +\infty[$ as the set of upper bounds, $]-\infty, 0]$ as the set of lower bounds, the supremum of A is 2, and the infimum is 0 (see Figure 1.1).

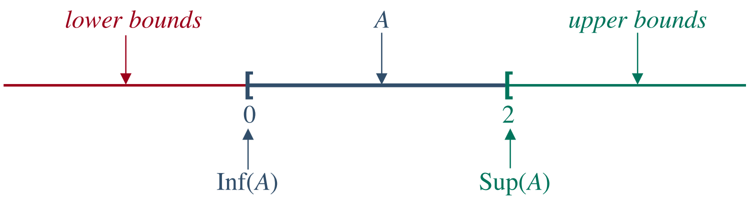

FIGURE 1.1

△

Proposition 1.3. *Let $\mathbb{E} \subset \mathbb{R}$ non-empty set. Then*

- *M is the supremum of $\mathbb{E}$ if and only if for any $\varepsilon > 0$ there exists $x \in \mathbb{E}$ such as $M - \varepsilon \leq x$.*
- *m is the infimum of $\mathbb{E}$ if and only if for any $\varepsilon > 0$ there exists $x \in \mathbb{E}$ such as $m + \varepsilon \geq x$.*

Proof. Both statements can be proved using proof by contradiction :

- *Proof of the first statement* : Assume that for some $\varepsilon > 0$ and for any $x \in \mathbb{E}$ we have $M - \varepsilon > x$; hence, $M - \varepsilon$ is an upper bound of $\mathbb{E}$. Therefore, $M = \operatorname{Sup}\mathbb{E} < M - \varepsilon$, which is absurd.
- *Proof of the second statement* : Assume that for some $\varepsilon > 0$ and for any $x \in \mathbb{E}$ we have $m + \varepsilon < x$; hence, $m + \varepsilon$ is a lower bound of $\mathbb{E}$. Therefore, $m = \operatorname{Inf}\mathbb{E} > m + \varepsilon$, which is absurd. □

Proposition 1.4. *Let $\mathbb{E} \subset \mathbb{R}$ non-empty. Then,* $\operatorname{Sup}(\mathbb{E})$ *and* $\operatorname{Inf}(\mathbb{E})$ *(when exist) are unique.*

Axiom 1.1 (completeness axiom). *Any upper-bounded (respectively lower-bounded) non-empty subset of $\mathbb{R}$ has a supremum (respectively an infimum).*

Definition 1.3. *Let $\mathbb{E} \subset \mathbb{R}$ non-empty, in the case where* $\operatorname{Sup}(\mathbb{E}) \in \mathbb{E}$ *(respectively* $\operatorname{Inf}(\mathbb{E}) \in \mathbb{E}$*) we call* $\operatorname{Sup}(\mathbb{E})$ *the maximum (respectively the minimum) of $\mathbb{E}$, and we denote it* $\operatorname{Max}(\mathbb{E})$ *(respectively* $\operatorname{Min}(\mathbb{E})$*).*

Example 1.3. Let $\mathcal{A}$ be the set defined as

$$\mathcal{A} = \left\{ x_n = (-1)^n + \frac{1}{n}; \quad n \in \mathbb{N}^* \right\}.$$

We have two situations, n even or n odd, hence

$$\mathcal{A} = \underbrace{\left\{ x_{2p} = 1 + \frac{1}{2p}; \quad p \in \mathbb{N}^* \right\}}_{\mathscr{C}_1} \bigcup \underbrace{\left\{ x_{2p+1} = -1 + \frac{1}{2p+1}; \quad p \in \mathbb{N} \right\}}_{\mathscr{C}_2},$$

- The case of the set $\mathscr{C}_1$: the function $1 + 1/(2p)$ is decreasing, so

$$\operatorname{Sup}\mathscr{C}_1 = 1 + \frac{1}{2p}\bigg|_{p=1} = \frac{3}{2}, \quad \operatorname{Inf}\mathscr{C}_1 = \lim_{n\to+\infty} 1 + \frac{1}{2p} = 1.$$

  Thus $\operatorname{Min}\mathscr{C}_1$ does not exists and $\operatorname{Max}\mathscr{C}_2 = 3/2$.
- The case of the set $\mathscr{C}_2$: the function $1 - 1/(2p+1)$ is increasing, therefore

$$\operatorname{Inf}\mathscr{C}_2 = 1 - \frac{1}{2p+1}\bigg|_{p=0} = 0, \quad \operatorname{Sup}\mathscr{C}_2 = \lim_{n\to+\infty} 1 - \frac{1}{2p+1} = 1.$$

  this gives $\operatorname{Min}\mathscr{C}_2 = 0$ and $\operatorname{Max}\mathscr{C}_2 = \nexists$.

In conclusion, we have the following table :

	Inf	Sup	Min	Max
$\mathscr{C}_1$	1	3/2	$\nexists$	3/2
$\mathscr{C}_2$	0	1	0	$\nexists$
$\mathcal{A}$	0	3/2	0	3/2

△

Proposition 1.5 (Archimede's axiom). *Let $\mathbb{N}$ be the set of the natural integer. Then*

$$\forall x \in \mathbb{R}_+, \quad \exists m \in \mathbb{N} : \quad m \geq x.$$

Proof. By contradiction, assume that

$$\exists x \in \mathbb{R}_+, \quad \forall m \in \mathbb{N} : \quad m < x,$$

hence $\mathbb{N}$ is upper bounded by x ; thus, $\mathbb{N}$ has a supremum (see Axiom 1.1). Proposition 1.3 ensures the existence of $n \in \mathbb{N}$ such that $\mathrm{Sup}(\mathbb{N}) - 1 < n$; Tterefore, $\mathrm{Sup}(\mathbb{N}) < n + 1$. Or $n + 1 \in \mathbb{N}$, hence the contradiction. □

Proposition 1.6. *Let $x \in \mathbb{R}$, then there exists a unique integer $n \in \mathbb{Z}$ such that $n \leq x < n + 1$.*

Definition 1.4 (The integer part*). *The integer part of $x \in \mathbb{R}$ is the integer* $\mathrm{floor}(x) \in \mathbb{Z}$ *satisfies*

$$\mathrm{floor}(x) \leq x < \mathrm{floor}(x) + 1.$$

* The integer part of x (or floor function) can be denoted as $[x]$ as well as $\lfloor x \rfloor$. The function $\mathrm{ceil}(x) = \mathrm{floor}(x) + 1$, denoted as well $\lceil x \rceil$, is called the ceiling function.

Example 1.4. Let $x = 1 + 2/m$ with $m \in \mathbb{N}^*$, we have $1 \leq 1 + 2/m < 2$ for any $m \geq 3$. Then, for $m \in \mathbb{N}^*$ with $m \geq 3$ we have $\mathrm{floor}(1 + 2/m) = 1$. In the case where $m = 1$ we obtain $x = 3$, thus $\mathrm{floor}(x) = 3$. The case where $m = 2$ leads to $x = 2$, so $\mathrm{floor}(x) = 2$.

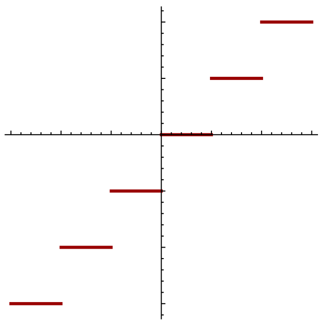

FIGURE 1.2 : $\mathrm{floor}(\cdot)$ over $[-3, +3]$

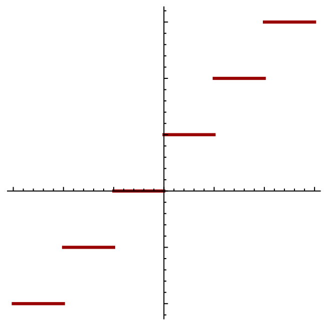

FIGURE 1.3 : $\mathrm{ceil}(\cdot) = \mathrm{floor}(\cdot) + 1$ over $[-3, +3]$ △

Proposition 1.7. *For any $x \in \mathbb{R}$ we have*
- $\mathrm{floor}(x) \leq x < \mathrm{floor}(x + 1)$.
- $\mathrm{floor}(x + 1) = \mathrm{floor}(x) + 1$.
- $\mathrm{floor}(x) + \mathrm{floor}(y) \leq \mathrm{floor}(x + y) \leq \mathrm{floor}(x) + \mathrm{floor}(y) + 1$.
- $x - 1 < \mathrm{floor}(x) \leq x$.

Proof.

− Let $x \in \mathbb{R}$, the definition of the integer part of $x + 1$ leads to

$$\mathrm{floor}(x + 1) \leq x + 1 < \mathrm{floor}(x + 1) + 1. \tag{1.8}$$

hence $x < \mathrm{floor}(x + 1)$. Combining this with the definition of the integer part of x, we obtain the first assertion of the proposition.

− For any $x \in \mathbb{R}$ we have $\mathrm{floor}(x) \leq x < \mathrm{floor}(x) + 1$, thus

$$\mathrm{floor}(x) + 1 \leq x + 1 < (\mathrm{floor}(x) + 1) + 1, \tag{1.9}$$

Since there is no integer in $\left]\mathrm{floor}(z), z\right[$ and in $\left]z, \mathrm{floor}(z)\right[$, the constraints (1.8)–(1.9) give

$$\mathrm{floor}(x) + 1 \leq \mathrm{floor}(x + 1), \quad \mathrm{floor}(x + 1) + 1 \leq (\mathrm{floor}(x) + 1) + 1.$$

This ensures the second assertion of the proposition.

- For any $x, y \in \mathbb{R}$, we have $\operatorname{floor}(x) \leq x < \operatorname{floor}(x) + 1$, $\operatorname{floor}(y) \leq y < \operatorname{floor}(y) + 1$; hence

$$\operatorname{floor}(x+y) \leq x + y < \operatorname{floor}(x+y) + 2, \tag{1.10}$$

moreover thus

$$\operatorname{floor}(x+y) \leq x + y < \operatorname{floor}(x+y) + 1 \tag{1.11}$$

Since there is no integer in $\left]\operatorname{floor}(z), z\right[$ and in $\left]z, \operatorname{floor}(z)\right[$, the conditions (1.10)-(1.11) provide

$$\operatorname{floor}(x) + \operatorname{floor}(y) \leq \operatorname{floor}(x+y), \quad \operatorname{floor}(x) + \operatorname{floor}(y) + 1 \geq \operatorname{floor}(x+y) + 1.$$

Hence, the third assertion of the proposition.

- For $x \in \mathbb{R}$ we have $\operatorname{floor}(x) \leq x < \operatorname{floor}(x) + 1$, thus $\operatorname{floor}(x) \leq x$ and $x - 1 \leq \operatorname{floor}(x)$. Hence the fourth assertion of the proposition. □

Proposition 1.8. *The set of rational numbers $\mathbb{Q}$ is dense in $\mathbb{R}$, which means*

$$\forall x, y \in \mathbb{R} : \quad x < y, \quad \exists r \in \mathbb{Q} : \quad x < r < y.$$

Proof. Let $x, y \in \mathbb{R}$ such that $x < y$. Achimede's axiome (Proposition 1.5) gives the existence of $\eta \in \mathbb{N}$ such as $\eta > 1/(y-x) > 0$, this leads to $y > x + 1/\eta$. Since $\eta x - 1 < \rho \leq \eta x$ with $\rho = \operatorname{floor}(\eta x)$, we get

$$\begin{cases} \rho \leq \eta x \\ \eta x - 1 < \rho \end{cases} \Longrightarrow \begin{cases} \dfrac{\rho+1}{\eta} \leq x + \dfrac{1}{\eta} \\ x < \dfrac{\rho+1}{\eta} \end{cases} \Longrightarrow \begin{cases} \dfrac{\rho+1}{\eta} < y \\ x < \dfrac{\rho+1}{\eta}. \end{cases}$$

Therefore, $x < r < y$ with $r = (\rho+1)/\eta \in \mathbb{Q}$. This finishes the proof. □