2. Real numbers

- ordered sets
- least upper bound property
- fields
- real numbers
- archimedian property
- using supremum and infimum
- absolute value
- triangle inequality
- uncountabality of the real numbers

Ordered sets

Definition 2.1 An **ordered set** is a set S with a relation $<$ called an 'ordering' such that:

1. *Trichotomy.* For all $x, y \in S$, either $x < y$, $x = y$, or $x > y$.
2. *Transitivity.* If $x, y, z \in S$ have $x < y$ and $y < z$, then $x < z$.

---

examples:

- $\mathbf{Z}$ is an ordered set with ordering $m > n \iff m - n \in \mathbf{N}$
- $\mathbf{Q}$ is an ordered set with ordering $p > q \iff p - q = m/n$ for some $m, n \in \mathbf{N}$
- $\mathbf{Q} \times \mathbf{Q}$ is an ordered set with dictionary ordering $(q, r) > (s, t) \iff q > s$, or $q = s$ and $r > t$
- the set $\mathcal{P}(\mathbf{N})$ with ordering defined by $A \prec B$ if $A \subseteq B$ is *not* an ordered set

Least upper bound property

Definition 2.2 Let S be an ordered set and let $E \subseteq S$, then:

- If there exists some $b \in S$ such that $x \leq b$ for all $x \in E$, then E is **bounded above** and b is an **upper bound** of E.

- If there exists some $c \in S$ such that $x \geq c$ for all $x \in E$, then E is **bounded below** and c is a **lower bound** of E.

- If there exists an upper bound b_0 of E such that $b_0 \leq b$ for all upper bounds b of E, then b_0 is the **least upper bound** or the **supremum** of E, written as

$$b_0 = \sup E.$$

- If there exists a lower bound c_0 of E such that $c_0 \geq c$ for all lower bounds c of E, then c_0 is the **greatest lower bound** or the **infimum** of E, written as

$$c_0 = \inf E.$$

---

examples:

- $S = \mathbf{Z}$ and $E = \{-2, -1, 0, 1, 2\}$, then $\inf E = -2$ and $\sup E = 2$

- $S = \mathbf{Q}$ and $E = \{q \in \mathbf{Q} \mid 0 \leq q < 1\}$, then $\inf E = 0$ and $\sup E = 1 \notin E$, *i.e.*, the supremum or infimum need not be in E

- $S = \mathbf{Z}$ and $E = \mathbf{N}$, then $\inf E = 1$ but $\sup E$ does not exist

---

Definition 2.3 *Least upper bound property.* An ordered set S has the least upper bound property if every $E \subseteq S$ which is nonempty and bounded above has a supremum in S.

---

example: $-\mathbf{N} = \{-1, -2, -3, \ldots\}$, to show this (informally), suppose $E \subseteq -\mathbf{N}$ is bounded above, then $-E \subseteq \mathbf{N}$ is bounded below and according to the well ordering principle, $-E$ has a least element $x \in -E$, and thus $-x = \sup E$

Theorem 2.4 If $x \in \mathbf{Q}$ and

$$x = \sup\{q \in \mathbf{Q} \mid q > 0,\ q^2 < 2\},$$

then $x \geq 1$ and $x^2 = 2$.

proof: let $E = \{q \in \mathbf{Q} \mid q > 0,\ q^2 < 2\}$

- $x \geq 1$ since $1 \in E \implies \sup E \geq 1$
- we show $x^2 \geq 2$ by contradiction: suppose $x^2 < 2$, let $h = \min\{\frac{1}{2},\ \frac{2-x^2}{2(2x+1)}\}$
  - since $x \geq 1$ and $x^2 < 2$, we have $0 < h \leq 1/2 < 1$
  - $h < 1 \implies (x+h)^2 = x^2 + 2hx + h^2 < x^2 + 2hx + h$
  - since $h \leq \frac{2-x^2}{2(2x+1)}$, we have

$$(x+h)^2 < x^2 + (2x+1)h \leq x^2 + \frac{1}{2}(2 - x^2) < x^2 + 2 - x^2 = 2 \implies x + h \in E$$

  - $h > 0 \implies x + h > x$, but $x + h \in E \implies x$ is not an upper bound for E, *i.e.*, $x \neq \sup E$, which is a contradiction

- we now show $x^2 \not> 2$ by contradiction: suppose $x^2 > 2$, let $h = \frac{x^2-2}{2x}$
  - since $x^2 > 2$ and $x \geq 1$, we have $h > 0$
  - $h > 0 \implies (x-h)^2 = x^2 - 2hx + h^2 > x^2 - 2hx = x^2 - (x^2 - 2) = 2$
  - let $q \in E$, then $q^2 < 2 < (x-h)^2$, hence

    $$(x-h)^2 - q^2 = ((x-h)+q)((x-h)-q) > 0 \implies (x-h) - q > 0,$$

    $i.e.$, $x - h > q$ for all $q \in E \implies x - h$ is an upper bound for E
  - $h > 0 \implies x > x - h \implies x \neq \sup E$, which is a contradiction
- therefore, $x^2 = 2$

Theorem 2.5 The set $E = \{q \in \mathbf{Q} \mid q > 0,\ q^2 < 2\}$ does not have a supremum in $\mathbf{Q}$.

proof (by contradiction): suppose there exists some $x \in \mathbf{Q}$ such that $x = \sup E$

- by theorem 2.4, we have $x \geq 1$ and $x^2 = 2$
- in particular, $x > 1$ since if $x = 1 \implies x^2 = 1 \neq 2$
- $x \in \mathbf{Q} \implies$ there exist $m, n \in \mathbf{N}$ $(m > n)$ such that $x = m/n$, *i.e.*, $m = nx \in \mathbf{N}$
- let $S = \{k \in \mathbf{N} \mid kx \in \mathbf{N}\} \subseteq \mathbf{N}$, then $S \neq \emptyset$ since $n \in S$
- by the well ordering property, there is a least element $k_0 \in S$
- let $k_1 = k_0(x-1) = k_0 x - k_0 \in \mathbf{Z}$, in particular, $k_1 \in \mathbf{N}$ since $x > 1 \implies k_1 > 0$
- $x^2 = 2 \implies x < 2$ as otherwise $x^2 \geq 4$, hence

$$k_1 = k_0(x-1) < k_0(2-1) = k_0 \implies k_1 \notin S$$

- $k_1 = k_0(x-1) \implies k_1 x = k_0 x^2 - k_0 x$, since $x^2 = 2$, we have

$$k_1 x = 2k_0 - k_0 x = k_0 - k_0(x-1) = k_0 - k_1 \in \mathbf{N} \implies k_1 \in S,$$

  which is a contradiction

Fields

Definition 2.6 A set F is a **field** if it has two operations: addition $(+)$ and multiplication $(\cdot)$ with the following properties.

(A1) If $x, y \in F$ then $x + y \in F$.

(A2) *Commutativity.* For all $x, y \in F$, $x + y = y + x$.

(A3) *Associativity.* For all $x, y, z \in F$, $(x + y) + z = x + (y + z)$.

(A4) There exists an element $0 \in F$ such that $0 + x = x = x + 0$ for all $x \in F$.

(A5) For all $x \in F$, there exists a $y \in F$ such that $x + y = 0$, denoted by $y = -x$.

(M1) If $x, y \in F$ then $x \cdot y \in F$.

(M2) *Commutativity.* For all $x, y \in F$, $x \cdot y = y \cdot x$.

(M3) *Associativity.* For all $x, y, z \in F$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(M4) There exists an element $1 \in F$ such that $1 \cdot x = x = x \cdot 1$ for all $x \in F$.

(M5) For all $x \in F \setminus \{0\}$, there exists an $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$.

(D) *Distributativity.* For all $x, y, z \in F$, $(x + y) \cdot z = x \cdot z + y \cdot z$.

examples:

- $\mathbf{Q}$ is a field
- $\mathbf{Z}$ is not a field since it fails (M5)
- $\mathbf{Z}_2 = \{0, 1\}$ where $1 + 1 = 0$ (mod 2) is a field
- $\mathbf{Z}_3 = \{0, 1, 2\}$ with $c = a + b$ (mod 3), *i.e.*,

$$2 + 1 = 3 = 0 \quad \text{and} \quad 2 \cdot 2 = 4 = 3 + 1 = 1,$$

  is a field

Theorem 2.7 If $x \in F$ where F is a field then $0x = 0$.

---

proof: $xx = (x + 0)x = xx + 0x \implies 0x = 0$

Definition 2.8 A field F is an **ordered field** if F is also an ordered set with ordering $<$ and satisfies:

1. For all $x, y, z \in F$, $x < y \implies x + z < y + z$.
2. If $x > 0$ and $y > 0$ then $xy > 0$.

If $x > 0$ we say x is **positive**, and if $x \geq 0$ we say x is **nonnegative**.

---

examples:

- $\mathbf{Q}$ is an ordered field
- $\mathbf{Z}_2 = \{0, 1\}$ where $1 + 1 = 0$ is not a ordered field
  (if $0 > 1 \implies 0 + 1 > 1 + 1 \implies 1 > 0$; if $1 > 0 \implies 1 + 1 > 1 + 0 \implies 0 > 1$)

Theorem 2.9 Let F be an ordered field and $x, y, z, w \in F$, then:

- If $x > 0$ then $-x < 0$ (and vice versa).
- If $x > 0$ and $y < z$ then $xy < xz$.
- If $x < 0$ and $y < z$ then $xy > xz$.
- If $x \neq 0$ then $x^2 > 0$.
- If $0 < x < y$ then $0 < 1/y < 1/x$.
- If $0 < x < y$ then $x^2 < y^2$.
- If $x \leq y$ and $z \leq w$ then $x + z \leq y + w$.

Theorem 2.10 Let $x, y \in F$ where F is an ordered field. If $x > 0$ and $y < 0$ or $x < 0$ and $y > 0$, then $xy < 0$.

proof:

- $x > 0,\ y < 0 \implies x > 0,\ -y > 0 \implies -xy > 0 \implies xy < 0$
- $x < 0,\ y > 0 \implies -x > 0,\ y > 0 \implies -xy > 0 \implies xy < 0$

Theorem 2.11 *Greatest lower bound.* Let F be an ordered field with the least upper bound property. If $A \subseteq F$ is nonempty and bounded below, then $\inf A$ exists in F.

proof: let $B = \{-x \mid x \in A\}$

- $A \subseteq F$ bounded below $\implies \exists a \in F$, $\forall x \in A$, $a \leq x \implies \exists a \in F$, $\forall x \in A$, $-a \geq -x \implies \exists a \in F$, $\forall x \in B$, $-a \geq x \implies B \subseteq F$ has an upper bound $-a$ (this also shows that if a is a lower bound of A then $-a$ is an upper bound of B)

- F has the least upper bound property $\implies \sup B \in F$

- let $c = \sup B$, then $c \geq x$, $\forall x \in B \implies -c \leq -x$, $\forall x \in B \implies -c \leq x$, $\forall x \in A \implies -c \in F$ is an lower bound of A

- we also have $c \leq -a$ with a being a lower bound of $A \implies -c \geq a \implies -c \in F$ is the greatest lower bound of A, $i.e.$, $-c = \inf A \in F$

Real nubmers

Theorem 2.12 There exists a "unique" ordered field, labeled $\mathbf{R}$, such that $\mathbf{Q} \subseteq \mathbf{R}$ and $\mathbf{R}$ has the least upper bound property.

- one can construct $\mathbf{R}$ using Dedekind cuts or as equivalence classes of Cauchy sequences.

Theorem 2.13 There exists a unique $r \in \mathbf{R}$ such that $r \geq 1$ and $r^2 = 2$, *i.e.*, $\sqrt{2} \in \mathbf{R}$ but $\sqrt{2} \notin \mathbf{Q}$.

proof: let $E = \{x \in \mathbf{R} \mid x > 0,\ x^2 < 2\} \subseteq \mathbf{R}$

- we have $x < 2$ for all $x \in E$ (since if $x \geq 2 \implies x^2 \geq 4$) $\implies$ E is bounded above $\implies$ $\sup E$ exists in $\mathbf{R}$
- let $r = \sup E$, using the same proof for theorem 2.4 we have $r \geq 1$ and $r^2 = 2$
- to show the uniqueness, suppose $\tilde{r} \geq 1$, $\tilde{r}^2 = 2$, then

$$r^2 - \tilde{r}^2 = 0 \implies (r + \tilde{r})(r - \tilde{r}) = 0 \implies r - \tilde{r} = 0 \implies r = \tilde{r}$$

(since $r \geq 1$, $\tilde{r} \geq 1 \implies r + \tilde{r} > 0$)

Theorem 2.14 If $x \in \mathbf{R}$ satisfies $x < \epsilon$ for all $\epsilon \in \mathbf{R}$, $\epsilon > 0$, then $x \leq 0$.

proof by contradiction:

- suppose $x > 0$ satisfies $x \leq \epsilon$ for all $\epsilon > 0$
- $x > 0 \implies 2x > x > 0 \implies x > x/2 > 0$
- take $\epsilon = x/2$ we have $x > \epsilon > 0$, which is a contradiction

Archimedian property

Theorem 2.15 *Archimedian property.* If $x, y \in \mathbf{R}$ and $x > 0$, then there exists an $n \in \mathbf{N}$ such that $nx > y$.

---

proof by contradiction:

- suppose $nx \leq y$ for all $n \in \mathbf{N} \implies \forall n \in \mathbf{N}, n \leq y/x \implies \mathbf{N}$ is bounded above by $y/x \implies$ there exists $\sup \mathbf{N} \in \mathbf{R}$
- let $a = \sup \mathbf{N} \implies a - 1 < a$ is not an upper bound of $\mathbf{N} \implies \exists m \in \mathbf{N}$, $a - 1 < m \implies a < m + 1 \in \mathbf{N} \implies a$ is not an upper bound of $\mathbf{N}$, which is a contradiction

---

Theorem 2.16 *Density of* $\mathbf{Q}$. If $x, y \in \mathbf{R}$ and $x < y$ then there exists some $r \in \mathbf{Q}$ such that $x < r < y$.

---

proof:

- first suppose $0 \leq x < y$, by the Archimedian property, we have

$$n(y - x) > 1 \implies ny > nx + 1$$

for some $n \in \mathbf{N}$

- let $S = \{k \in \mathbf{N} \mid k > nx\} \subseteq \mathbf{N}$, by Archimedian property, there exists some $p \in \mathbf{N}$ such that $p > nx \implies S \neq \emptyset$

- by the well ordering property, there is a least element $m \in S$ such that $m > nx$

- $m \in \mathbf{N} \implies m \geq 1$

- if $m = 1$, then $m - 1 = 0 \implies nx \geq m - 1 = 0$ since $x \geq 0$

- if $m > 1$, then $m - 1 \in \mathbf{N}$ but $m - 1 \notin S$ since $m > m - 1$ is the least element $\implies nx \geq m - 1 \implies m \leq nx + 1 < ny$

- hence, we have

$$nx < m < ny \implies x < m/n < y$$

  for some $m, n \in \mathbf{N}$, $i.e.$, there exists an $r = m/n \in \mathbf{Q}$ such that $x < r < y$

- now suppose $x < 0$, if $x < 0 < y$ then simply take $r = 0$; if $x < y \leq 0$, we have $0 \leq -y < -x$, thus there exists some $\tilde{r} \in \mathbf{Q}$ such that

$$-y < \tilde{r} < -x \implies x < -\tilde{r} < y$$

  (by the first case), $i.e.$, we have $x < r < y$ by taking $r = -\tilde{r}$

Theorem 2.17 Suppose $S \subseteq \mathbf{R}$ is nonempty and bounded above. Then, $x = \sup S$ if and only if:

1. x is an upper bound of S.
2. For all $\epsilon > 0$, there exists some $y \in S$ such that $x - \epsilon < y \leq x$.

proof:

- first suppose $x = \sup S$
  - obviously, x is an upper bound of S
  - for all $\epsilon > 0$, we have $x > x - \epsilon \implies x - \epsilon$ is not an upper bound of S, $i.e.$, there exists some $y \in S$ such that $x - \epsilon < y \leq x$
- now suppose x is an upper bound of S, and satisfies $x - \epsilon < y \leq x$ for all $\epsilon > 0$ and for some $y \in S$, we only need to show that for all z that is an upper bound of S, we have $x \leq z$
  - assume there exists an upper bound z of S smaller than x, $i.e.$, $y \leq z < x$ for all $y \in S$
  - take $\epsilon = x - z > 0$ (since $x > z$) $\implies x \geq y > x - \epsilon = x - x + z = z \implies y > z$ for some $y \in S$, $i.e.$, z is not an upper bound of S, which is a contradiction

Theorem 2.18 Let $S = \{1 - \frac{1}{n} \mid n \in \mathbf{N}\}$, then $\sup S = 1$.

proof:

- if $n \in \mathbf{N}$, then $1 - \frac{1}{n} < 1 \implies 1$ is an upper bound of S

- let $\epsilon > 0$, then by the Archimedian property, for some $n \in \mathbf{N}$, we have

$$n\epsilon > 1 \implies \epsilon > \frac{1}{n} \implies -\epsilon < -\frac{1}{n} \implies 1 - \epsilon < 1 - \frac{1}{n} \leq 1$$

  by theorem 2.17, we have $\sup S = 1$

Remark 2.19 We have similar property as theorem 2.17 for infimum. Suppose $S \subseteq \mathbf{R}$ is nonempty and bounded below, then $x = \inf S$ if and only if:

- x is a lower bound of S.
- For all $\epsilon > 0$, there exists some $y \in S$ such that $x \leq y < x + \epsilon$.

Using supremum and infimum

Definition 2.20 For $x \in \mathbf{R}$ and $A \subseteq \mathbf{R}$, define

$$x + A = \{x + a \mid a \in A\}, \qquad xA = \{xa \mid a \in A\}.$$

Theorem 2.21 Let $A \subseteq \mathbf{R}$ be nonempty, we have:

- If $x \in \mathbf{R}$ and A is bounded above, then $\sup(x + A) = x + \sup A$.
- If $x > 0$ and A is bounded above, then $\sup(xA) = x \sup A$.

proof:

- suppose $x \in \mathbf{R}$ and A is bounded above:
  - for all $a \in A$, we have $a \leq \sup A \implies x + a \leq x + \sup A$, *i.e.*, the set $x + A$ is bounded by $x + \sup A$
  - let $\epsilon > 0$, for some $b \in A$, we have

$$\sup A - \epsilon < b \leq \sup A \implies (x + \sup A) - \epsilon < x + b \leq x + \sup A,$$

  i.e., $\sup(x + A) = x + \sup A$

- suppose $x > 0$ and A is bounded above:
  - for all $a \in A$, $a \le \sup A \implies xa \le x \sup A$, *i.e.*, the set xA is bounded by $x \sup A$
  - let $\epsilon > 0 \implies \epsilon/x > 0$, for some $b \in A$, we have

$$\sup A - \epsilon/x < b \le \sup A \implies x \sup A - \epsilon < xb \le x \sup A,$$

  i.e., $\sup(xA) = x \sup A$

Remark 2.22 Similarly, we can also show that:

- If $x \in \mathbf{R}$ and A is bounded below, then $\inf(x + A) = x + \inf A$.
- If $x > 0$ and A is bounded below, then $\inf(xA) = x \inf A$.
- If $x < 0$ and A is bounded below, then $\sup(xA) = x \inf A$.
- If $x < 0$ and A is bounded above, then $\inf(xA) = x \sup A$.

Theorem 2.23 Let $A, B \subseteq \mathbf{R}$ where $x \le y$ for all $x \in A$, $y \in B$, then $\sup A \le \inf B$.

---

proof: for all $x \in A$, $y \in B$, $x \le y \implies B$ is bounded below by $x \implies x \le \inf B$ $\implies A$ is bounded above by $\inf B \implies \sup A \le \inf B$

Absolute value

Definition 2.24 If $x \in \mathbf{R}$, we define the **absolute value** of x as

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0. \end{cases}$$

Theorem 2.25

- $|x| \geq 0$, and, $|x| = 0$ if and only if $x = 0$.
- $|-x| = |x|$ for all $x \in \mathbf{R}$.
- $|xy| = |x||y|$ for all $x, y \in \mathbf{R}$.
- $|x|^2 = x^2$ for all $x \in \mathbf{R}$.
- $|x| \leq y$ if and only if $-y \leq x \leq y$.
- $-|x| \leq x \leq |x|$ for all $x \in \mathbf{R}$.

Triangle inequality

Theorem 2.26 *Triangle inequality.* For all $x, y \in \mathbf{R}$,

$$|x + y| \leq |x| + |y|.$$

---

proof: let $x, y \in \mathbf{R}$

- $x + y \leq |x| + |y|$
- $-x + -y \leq |-x| + |-y| = |x| + |y| \implies -(|x| + |y|) \leq x + y$
- hence, we have

$$-(|x| + |y|) \leq x + y \leq |x| + |y| \implies |x + y| \leq |x| + |y|$$

Corollary 2.27 *Reverse triangle inequality.* For all $x, y \in \mathbf{R}$,

$$\big||x| - |y|\big| \leq |x - y|.$$

Uncountabality of the real numbers

Definition 2.28 Let $x \in (0, 1]$ and let $d_{-i} \in \{0, 1, \ldots, 9\}$. We say that x is represented by the digits $\{d_{-i} \mid i \in \mathbf{N}\}$, *i.e.*, $x = 0.d_{-1}d_{-2}\cdots$, if

$$x = \sup\{10^{-1}d_{-1} + 10^{-2}d_{-2} + \cdots + 10^{-n}d_{-n} \mid n \in \mathbf{N}\}.$$

---

example: $0.2500\cdots = \sup\{\frac{2}{10},\ \frac{2}{10} + \frac{5}{100},\ \frac{2}{10} + \frac{5}{100} + \frac{0}{1000},\ \ldots\} = \sup\{\frac{1}{5},\ \frac{1}{4}\} = \frac{1}{4}$

Theorem 2.29

- For all set of digits $\{d_{-i} \mid i \in \mathbf{N}\}$, there exists a unique $x \in [0, 1]$ such that $x = 0.d_{-1}d_{-2}\cdots$.
- For all $x \in (0, 1]$, there exists a unique sequence of digits d_{-i} such that $x = 0.d_{-1}d_{-2}\cdots$ and

$$0.d_{-1}d_{-2}\cdots d_{-n} < x \leq 0.d_{-1}d_{-2}\cdots d_{-n} + 10^{-n}, \quad \text{for all } n \in \mathbf{N}. \tag{2.1}$$

- the second part indicates that the digital representation of $1/2$ is $0.4999\cdots$

Theorem 2.30 *Cantor.* The set $(0, 1]$ is uncountable.

proof (by contradiction):

- assume $(0, 1]$ is countable, then there exists a bijection $x\colon \mathbf{N} \to (0, 1]$, let

$$x(n) = 0.d_{-1}^{(n)} d_{-2}^{(n)} \cdots, \quad n \in \mathbf{N},$$

  where $d_{-i}^{(n)}$ denotes the ith decimal of the real number $x(n) \in (0, 1]$, and let

$$e_{-i} = \begin{cases} 1 & d_{-i}^{(i)} \neq 1 \\ 2 & d_{-i}^{(i)} = 1 \end{cases} \tag{2.2}$$

- let $y = 0.e_{-1}e_{-2}\cdots$, since all e_{-i} are nonzero, $e_{-1}, e_{-2}, \ldots$ satisfies (2.1); according to theorem 2.29, we have $0.e_{-1}e_{-2}\cdots$ being the unique decimal representation of y
- again according to theorem 2.29 and all e_{-i} are nonzero, we have $y \in (0, 1] \implies \exists m \in \mathbf{N}$, $y = x(m) = 0.d_{-1}^{(m)} d_{-2}^{(m)} \cdots = 0.e_{-1}e_{-2}\cdots$, however, we have $e_{-m} \neq d_{-m}^{(m)}$ since (2.2), *i.e.*, for all $m \in \mathbf{N}$, $x(m) \neq y$, which is a contradiction

Corollary 2.31 The set of real numbers $\mathbf{R}$ is uncountable.