Lecture 1: Incompleteness of Rational Numbers

Mathematical Analysis

1 Numbers

Definition 1.1 (Natural Numbers)**.** [def:natural-number] Let S denote the *successor*. The *natural numbers* are inductively generated by

$$\mathbb{N} \equiv 0 \mid S(n : \mathbb{N}).$$

Every natural number is obtained from 0 by repeated application of S

LaTeX: \NN

Theorem 1.1 (Natural Number Induction)**.** [thm:natural-number-induction] *Let* $P : \mathbb{N} \to \mathsf{Prop}$*. If*

$$P(0) \quad \textit{and} \quad \forall n : \mathbb{N},\, P(n) \implies P(S(n)),$$

then $P(n)$ *holds for every* $n : \mathbb{N}$

Proof. Let $A = \{n : \mathbb{N} \mid P(n)\}$. The hypotheses say that A contains 0 and is closed under S. Because every natural number is obtained from 0 by repeated application of S, we have $A = \mathbb{N}$ □

Convention 1.1 (Positive Natural Numbers)**.** [conv:positive-natural-numbers] We write

$$\mathbb{N}_1 = \mathbb{N} \setminus \{0\}$$

when zero must be excluded, such as for one-based indices or denominators

LaTeX: \NNOne

Definition 1.2 (Integers)**.** [def:integer] The *integers* are the whole numbers, including the positive integers, the negative integers, and zero:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

LaTeX: \ZZ

Definition 1.3 (Rational Numbers)**.** [def:rational-numbers] A real number is called *rational* if it can be expressed as a quotient of two integers. The set of rational numbers is

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0 \right\}$$

LaTeX: \QQ

Proposition 1.1 (Unique Reduced Form)**.** [prop:unique-reduced-rational-form] *For every* $x \in \mathbb{Q}$*, there exists a unique pair* $p, q \in \mathbb{Z}$ *such that*

$$x = \frac{p}{q}, \qquad q > 0, \qquad \gcd(|p|, q) = 1$$

Remark 1.1. [rem:number-set-inclusions] Under the usual identifications, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$

Definition 1.4 (Floor)**.** [def:floor] The *floor* function $\mathrm{floor} : \mathbb{R} \to \mathbb{Z}$ is characterized, for every $x \in \mathbb{R}$ and $m \in \mathbb{Z}$, by

$$\mathrm{floor}(x) = m \iff m \leq x < m + 1$$

LaTeX: \floorfn (x)

Convention 1.2 (Floor Notation). [conv:floor-notation] For the floor function, write $\lfloor x \rfloor \equiv \text{floor}(x)$

LaTeX: \floor {x}

Definition 1.5 (Ceiling). [def:ceiling] For $x \in \mathbb{R}$, the *ceiling* $\lceil x \rceil$ is the unique $m \in \mathbb{Z}$ satisfying

$$m - 1 < x \leq m$$

LaTeX: \ceil {x}

Theorem 1.2 (Well-Definedness of Floor and Ceiling). [thm:floor-ceiling-well-defined] *For every $x \in \mathbb{R}$:*

- *there exists a unique $m \in \mathbb{Z}$ satisfying $m \leq x < m + 1$, namely $\lfloor x \rfloor$;*
- *there exists a unique $m \in \mathbb{Z}$ satisfying $m - 1 < x \leq m$, namely $\lceil x \rceil$*

Proof. Existence of the floor. Using the Archimedean property, proved later, choose $p, q \in \mathbb{N}$ with $p > -x$ and $q > x + p$. A finite search through $0, 1, \ldots, q$ has a first index k with $x + p < k$: such an index exists because $q > x + p$, and a first one can be selected by natural number induction. Since $x + p > 0$, we have $k \geq 1$, and minimality gives

$$k - 1 \leq x + p < k$$

Thus $m = k - p - 1 \in \mathbb{Z}$ satisfies $m \leq x < m + 1$
Uniqueness of the floor. Suppose $m, r \in \mathbb{Z}$ both satisfy the defining inequalities. If $m < r$, then $m + 1 \leq r \leq x < m + 1$, a contradiction. Interchanging m, r rules out $r < m$, so $m = r$
Existence and uniqueness of the ceiling. Apply the floor result to $-x$. If $m \leq -x < m + 1$, then $c = -m$ satisfies $c - 1 < x \leq c$, so a ceiling exists. Any integer d satisfying $d - 1 < x \leq d$ gives a floor $-d$ of $-x$; uniqueness of that floor yields $-d = m$, hence $d = c$ □

2 Fields

Definition 2.1 (Closed Operation). [def:closed-operation] An operation $*$ is said to be *closed* on a set A if for all $a, b \in A$, we have $a * b \in A$

Definition 2.2 (Field). [def:field] A *field* is a set F equipped with addition and multiplication such that both operations are

- closed operations on F,
- associative, meaning for all $a, b, c \in F$, we have $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- commutative, meaning for all $a, b \in F$, we have $a + b = b + a$ and $a \cdot b = b \cdot a$,
- have distinct identity elements $0, 1 \in F$, meaning $a + 0 = a$, $a \cdot 1 = a$, and $0 \neq 1$,
- each element has an additive inverse, such that for each $a \in F$, there exists $-a \in F$ with $a + (-a) = 0$,
- each non-zero element has a multiplicative inverse, such that for each $a \in F$ with $a \neq 0$, there exists $a^{-1} \in F$ with $a \cdot a^{-1} = 1$, and
- multiplication distributes over addition, meaning $a \cdot (b + c) = a \cdot b + a \cdot c$

Proposition 2.1 ($\mathbb{Q}$ Is a Field). [prop:rationals-are-a-field] *The rational numbers with their usual addition and multiplication form a field*

Remark 2.1 ($\mathbb{N}$ and $\mathbb{Z}$ Are Not Fields). [rem:natural-and-integers-not-fields] The natural numbers and the integers are not fields because they do not have multiplicative inverses for every non-zero element
For a counter example, consider the integer 2. There is no integer x such that $2 \cdot x = 1$

3 Ordered Set

Definition 3.1 (Transitive). [def:transitive] An ordering on a set is *transitive* if

$$\forall x, y, z \in F, \text{ if } x \leq y \text{ and } y \leq z, \text{ then } x \leq z$$

Definition 3.2 (Reflexive). [def:reflexive] An ordering on a set is *reflexive* if

$$\forall x \in F, x \leq x$$

Definition 3.3 (Antisymmetric). [def:antisymmetric] An ordering on a set is *antisymmetric* if

$$\forall x, y \in F, (x \leq y) \land (y \leq x) \implies x = y$$

Definition 3.4 (Partial Order). [def:partial-order] A binary relation $\leq$ on a set F is a *partial order* if it is reflexive, antisymmetric, and transitive

Definition 3.5 (Totality). [def:totality] An ordering on a set F is *total* if every pair of elements is comparable:

$$\forall x, y \in F, \quad x \leq y \lor y \leq x$$

Definition 3.6 (Total Order). [def:total-order] A partial order $\leq$ on F is a *total order* if it also satisfies totality

Convention 3.1 (Order Notation). [conv:order-notation] For $a, b \in F$, define

$$a \geq b \iff b \leq a, \qquad a < b \iff a \leq b \land a \neq b, \qquad a > b \iff b < a$$

Definition 3.7 (Binary Maximum). [def:binary-max] Let X be equipped with a total order $\leq$. The *binary maximum* is the function

$$\max : X \times X \to X \equiv (a, b) \mapsto \begin{cases} a & \text{if } a \geq b, \\ b & \text{otherwise} \end{cases}$$

`LaTeX: \max (a,b)`

Definition 3.8 (Binary Minimum). [def:binary-min] Let X be equipped with a total order $\leq$. The *binary minimum* is the function

$$\min : X \times X \to X \equiv (a, b) \mapsto \begin{cases} a & \text{if } a \leq b, \\ b & \text{otherwise} \end{cases}$$

`LaTeX: \min (a,b)`

Definition 3.9 (Maximum of a Set). [def:set-maximum] Let X be equipped with a total order $\leq$, and let $A \subseteq X$ be nonempty. An element $m \in A$ is a *maximum of* A, written $m = \max(A)$, if

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

`LaTeX: \setmax (A)`

Definition 3.10 (Minimum of a Set). [def:set-minimum] Let X be equipped with a total order $\leq$, and let $A \subseteq X$ be nonempty. An element $m \in A$ is a *minimum of* A, written $m = \min(A)$, if

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

`LaTeX: \setmin (A)`

Proposition 3.1 (Finite Nonempty Families Have a Maximum and Minimum). [prop:finite-max-min-inductive] *Let X be a totally ordered set. For any nonempty finite family $(a_1, \dots, a_n)$ in X, the maximum $\max\{a_1, \dots, a_n\}$ and minimum $\min\{a_1, \dots, a_n\}$ exist. They may be computed inductively:*

$$\max\{a_1\} = a_1, \qquad \max\{a_1, \dots, a_k\} = \max\big(\max\{a_1, \dots, a_{k-1}\},\, a_k\big) \text{ for } k \geq 2,$$

and symmetrically for min

Definition 3.11 (Ordered Field). [def:ordered-field] An *ordered field* is a field F equipped with a total order $\leq$ such that for all $x, y, z \in F$,

- if $x \leq y$, then $x + z \leq y + z$; and
- if $0 \leq x$ and $0 \leq y$, then $0 \leq xy$

Definition 3.12 (Sign Subset Operators). [def:sign-subset-operators] Let F be an ordered field. Define the following subsets of F

$$\begin{aligned} \operatorname{pos}(F) &\equiv \{x : F \mid 0 < x\}, \\ \operatorname{neg}(F) &\equiv \{x : F \mid x < 0\}, \\ \operatorname{nonneg}(F) &\equiv \{x : F \mid 0 \leq x\}, \\ \operatorname{nonpos}(F) &\equiv \{x : F \mid x \leq 0\} \end{aligned}$$

Convention 3.2 (Sign Subsets of an Ordered Field). [conv:sign-subsets] For the sign subset operators, write

$$F_+ \equiv \operatorname{pos}(F), \qquad F_- \equiv \operatorname{neg}(F),$$
$$F_{\geq 0} \equiv \operatorname{nonneg}(F), \quad F_{\leq 0} \equiv \operatorname{nonpos}(F)$$

Thus F_+ and F_- exclude zero

```
LaTeX: \apos {F}, \aneg {F}
LaTeX: \agez {F}, \alez {F}
```

Definition 3.13 (Absolute Value). [def:absolute-value] Let F be an ordered field. The *absolute value* is the function

$$\operatorname{abs} : F \to F \equiv a \mapsto \begin{cases} a, & a \geq 0, \\ -a, & a < 0 \end{cases}$$

Convention 3.3 (Absolute Value Notation). [conv:absolute-value-notation] For readability, we write $|a|$ in place of the function application $\operatorname{abs}(a)$, where abs is defined in definition 3.13. The two forms are interchangeable

```
LaTeX: \abs {a}
```

Lemma 3.1 (Difference Characterization). [lem:difference-characterization] *Let F be an ordered field. For all $a, b \in F$,*

$$a < b \iff 0 < b - a$$

Proof. Since addition preserves order and is cancellative in an ordered field,

$$a < b \iff a - a < b - a \iff 0 < b - a.$$

Here $a - a = 0$ by the additive-inverse axiom in the definition of a field □

Lemma 3.2 (Positive Perturbation). [lem:positive-perturbation] *Let F be an ordered field. For all $s, \varepsilon \in F$,*

$$\varepsilon > 0 \implies s - \varepsilon < s < s + \varepsilon$$

Proof. If $\varepsilon > 0$, then

$$s - (s - \varepsilon) = \varepsilon > 0 \quad \text{and} \quad (s + \varepsilon) - s = \varepsilon > 0.$$

Both inequalities follow from the difference characterization □

4 Indexed Family

Definition 4.1 (Indexed Family). [def:indexed-family] Let I be an index set and let X be a set. An *I-indexed family in X* is a mapping

$$a : I \to X$$

Definition 4.2 (Term). [def:term] Let $a : I \to X$ be an indexed family. For each $i \in I$, the value

$$a(i)$$

is called the *term indexed by i*

Convention 4.1 (Term Notation). [conv:term-notation] For an indexed family $a : I \to X$ and $i \in I$, we write

$$a_i \equiv a(i).$$

This denotes the term indexed by i. The family itself is a

```
LaTeX: \term {a}{i}
```

Definition 4.3 (Sequence). [def:sequence] Let $I = \mathbb{N}$ or $I = \mathbb{N}_1$. An I-indexed family $a : I \to X$ is called a *sequence in X*. Its term $a(n)$, also written a_n, is called the *n-th term*

Example 4.1. The function

$$a : \mathbb{N}_1 \to \mathbb{R} \equiv n \mapsto \frac{1}{n}$$

is a sequence. For example, $a(1) = 1$ and $a_2 = a(2) = \frac{1}{2}$

5 Finite Sums and Products

Definition 5.1 (Finite Summation). [def:finite-summation] Let F be a field. The *finite summation* function is defined recursively by

$$\text{sum} : \mathbb{N}_1 \times \mathbb{N} \times (\mathbb{N}_1 \to F) \to F \equiv (m, n, a) \mapsto \begin{cases} 0 & \text{if } m > n, \\ \text{sum}(m, n-1, a) + a(n) & \text{if } m \leq n. \end{cases}$$

The upper bound may be 0, so the recursion reaches the empty sum $\text{sum}(1, 0, a) = 0$ when $m = n = 1$

```
LaTeX: \finsum (m,n,a)
```

Convention 5.1 (Finite Summation Notation). [conv:finite-summation-notation] For the finite summation function, we write

$$\sum_{m}^{n}(a) \equiv \text{sum}(m, n, a).$$

The bounds m, n are inclusive, and the input a is the whole sequence. For an explicit rule, write, for example,

$$\sum_{1}^{3}(k \mapsto k^2) = (k \mapsto k^2)(1) + (k \mapsto k^2)(2) + (k \mapsto k^2)(3)$$

$$= 1 + 4 + 9 = 14$$

```
LaTeX: \sum _m^n(a)
```

Definition 5.2 (Finite Product). [def:finite-product] Let F be a field. The *finite product* function is defined recursively by

$$\text{prod} : \mathbb{N}_1 \times \mathbb{N} \times (\mathbb{N}_1 \to F) \to F \equiv (m, n, a) \mapsto \begin{cases} 1 & \text{if } m > n, \\ \text{prod}(m, n-1, a) \cdot a(n) & \text{if } m \leq n. \end{cases}$$

The upper bound may be 0, so the recursion reaches the empty product $\text{prod}(1, 0, a) = 1$ when $m = n = 1$

LaTeX: \finprod (m,n,a)

Convention 5.2 (Finite Product Notation). [conv:finite-product-notation] For the finite product function, we write

$$\prod_m^n(a) \equiv \text{prod}(m, n, a).$$

The bounds m, n are inclusive, and the input a is the whole sequence. For example,

$$\begin{aligned} \prod_1^3(k \mapsto k+1) &= (k \mapsto k+1)(1) \cdot (k \mapsto k+1)(2) \cdot (k \mapsto k+1)(3) \\ &= 2 \cdot 3 \cdot 4 = 24 \end{aligned}$$

LaTeX: \prod _m^n(a)

Proposition 5.1 (Linearity of Summation). [prop:summation-linearity] *Let F be a field, $a, b : \mathbb{N}_1 \to F$, $c, d \in F$, and $m, n \in \mathbb{N}_1$. Then*

$$\sum_m^n(k \mapsto c \cdot a(k) + d \cdot b(k)) = c \cdot \sum_m^n(a) + d \cdot \sum_m^n(b)$$

Proposition 5.2 (Index Shift for Summation). [prop:summation-shift] *Let F be a field, $a : \mathbb{N}_1 \to F$, and $m, n, p \in \mathbb{N}_1$ with $m + p, n + p \in \mathbb{N}_1$. Then*

$$\sum_{m+p}^{n+p}(a) = \sum_m^n(k \mapsto a(k+p))$$

Proposition 5.3 (Splitting of Summation). [prop:summation-split] *Let F be a field, $a : \mathbb{N}_1 \to F$, and $m, p, n \in \mathbb{N}_1$ with $m \leq p \leq n$. Then*

$$\sum_m^n(a) = \sum_m^p(a) + \sum_{p+1}^n(a)$$

Proposition 5.4 (Multiplicativity of Product). [prop:product-multiplicativity] *Let F be a field, $a, b : \mathbb{N}_1 \to F$, and $m, n \in \mathbb{N}_1$. Then*

$$\prod_m^n(k \mapsto a(k) \cdot b(k)) = \left(\prod_m^n(a)\right) \cdot \left(\prod_m^n(b)\right)$$

Proposition 5.5 (Index Shift for Product). [prop:product-shift] *Let F be a field, $a : \mathbb{N}_1 \to F$, and $m, n, p \in \mathbb{N}_1$ with $m + p, n + p \in \mathbb{N}_1$. Then*

$$\prod_{m+p}^{n+p}(a) = \prod_m^n(k \mapsto a(k+p))$$

Proposition 5.6 (Splitting of Product). [prop:product-split] *Let F be a field, $a : \mathbb{N}_1 \to F$, and $m, p, n \in \mathbb{N}_1$ with $m \leq p \leq n$. Then*

$$\prod_m^n(a) = \left(\prod_m^p(a)\right) \cdot \left(\prod_{p+1}^n(a)\right)$$

6 Sets

Remark 6.1 (Membership and Classical Logic). [rem:membership-classical-logic] For every set A and every x in the chosen universe, exactly one of $x \in A$ and $x \notin A$ holds

Proof. Let P be the proposition $x \in A$. By the law of excluded middle, $P \vee \neg P$, while the law of non-contradiction gives $\neg(P \wedge \neg P)$. Hence exactly one of $x \in A$ and $x \notin A$ holds □

Definition 6.1 (Intersection). [def:intersection] For sets A and B,

$$x \in A \cap B \iff x \in A \text{ and } x \in B$$

Definition 6.2 (Indexed Intersection). [def:indexed-intersection] Let I be a nonempty index type, and write **Set** for the type of sets. The *indexed intersection* is the function

$$\text{inter} : (I \to \mathbf{Set}) \to \mathbf{Set} \equiv A \mapsto \{x \mid \forall i \in I,\, x \in A(i)\}.$$

Its input A is an indexed family of sets

```
LaTeX: \idxinter (A)
```

Convention 6.1 (Indexed Intersection Notation). [conv:indexed-intersection-notation] For the indexed intersection function, we write

$$\bigcap(A) \equiv \text{inter}(A).$$

The domain of A determines all the indices included. For a sequence $A : \mathbb{N} \to \mathbf{Set}$ and $m, n \in \mathbb{N}$ with $m \leq n$, let $J = \{k \in \mathbb{N} \mid m \leq k \leq n\}$. We also write

$$\bigcap_{m}^{n}(A) \equiv \text{inter}((k : J) \mapsto A(k)).$$

Thus the bounds are inclusive. For example,

$$\bigcap_{1}^{3}(A) = A(1) \cap A(2) \cap A(3).$$

The same bounded notation applies when the sequence starts at 1, provided $m \geq 1$

```
LaTeX: \bigcap (A)
LaTeX: \bigcap _m^n(A)
```

Definition 6.3 (Union). [def:union] For sets A and B,

$$x \in A \cup B \iff x \in A \text{ or } x \in B$$

Definition 6.4 (Indexed Union). [def:indexed-union] Let I be an index type. The *indexed union* is the function

$$\text{union} : (I \to \mathbf{Set}) \to \mathbf{Set} \equiv A \mapsto \{x \mid \exists i \in I,\, x \in A(i)\}.$$

Its input A is an indexed family of sets. If I is empty, then $\text{union}(A) = \emptyset$

```
LaTeX: \idxunion (A)
```

Convention 6.2 (Indexed Union Notation). [conv:indexed-union-notation] For the indexed union function, we write

$$\bigcup(A) \equiv \text{union}(A).$$

The domain of A determines all the indices included. For a sequence $A : \mathbb{N} \to \mathbf{Set}$ and $m, n \in \mathbb{N}$ with $m \leq n$, let $J = \{k \in \mathbb{N} \mid m \leq k \leq n\}$. We also write

$$\bigcup_{m}^{n}(A) \equiv \text{union}((k : J) \mapsto A(k)).$$

Thus the bounds are inclusive. For example,

$$\bigcup_{1}^{3}(A) = A(1) \cup A(2) \cup A(3).$$

The same bounded notation applies when the sequence starts at 1, provided $m \geq 1$

```
LaTeX: \bigcup (A)
LaTeX: \bigcup _m^n(A)
```

Definition 6.5 (Complement)**.** [def:complement] Given a universal set U and $A \subseteq U$, the complement of A is $A^c = U \setminus A$; equivalently,

$$x \in A^c \iff x \notin A$$

Definition 6.6 (Set Difference)**.** [def:set-difference] For sets A and B,

$$x \in A \setminus B \iff x \in A \text{ and } x \notin B$$

Definition 6.7 (Subset)**.** [def:subset] For sets A and B,

$$A \subseteq B \iff \text{for every } x, \quad x \in A \implies x \in B$$

Definition 6.8 (Set Equality)**.** [def:set-equality] For sets A and B,

$$A = B \iff A \subseteq B \text{ and } B \subseteq A$$

Theorem 6.1 (De Morgan's Laws)**.** [thm:de-morgan-laws] *For sets A and B in a universal set U,*

$$(A \cap B)^c = A^c \cup B^c \quad \textit{and} \quad (A \cup B)^c = A^c \cap B^c.$$

For an indexed family $A : I \to \mathbf{Set}$ with I nonempty and $A(i) \subseteq U$ for every $i \in I$, also

$$\Big(\bigcap(A)\Big)^c = \bigcup(i \mapsto A(i)^c), \qquad \Big(\bigcup(A)\Big)^c = \bigcap(i \mapsto A(i)^c)$$

Example 6.1 (Nested Sequence)**.** [eg:nested-sequence] Let

$$A : \mathbb{N}_1 \to \mathbf{Set} \equiv n \mapsto \{k \in \mathbb{N}_1 \mid n \leq k\}.$$

For example, $A_1 = \{1, 2, 3, \ldots\}$ and $A_5 = \{5, 6, 7, \ldots\}$. Since $A(1) \supset A(2) \supset \cdots$, this is a nested sequence of sets. Moreover,

$$\bigcup(A) = A(1) = \mathbb{N}_1, \qquad \bigcap(A) = \emptyset.$$

The union equals $A(1)$ because every $A(n)$ is contained in $A(1)$. The intersection is empty because each $p \in \mathbb{N}_1$ is excluded by $A(p + 1)$

7 Mapping

Definition 7.1 (Mapping)**.** [def:mapping] A mapping $f : A \to B$ is a set of rule st.:

$$\forall x \in A, \exists! y = f(x) \in B \leftrightarrow \forall x \in A, \exists! y \in B \text{ st. } (x, y) \in f$$

Definition 7.2 (Domain)**.** [def:domain] The *domain* of a mapping $f : A \to B$ is the set A

Definition 7.3 (Codomain)**.** [def:codomain] The *codomain* of a mapping $f : A \to B$ is the set B

Definition 7.4 (Range)**.** [def:range] The *range* of a mapping $f : A \to B$ is a set C such that:

$$C = \{y : \exists x \in A, \text{ st. } y = f(x)\}$$

Remark 7.1 (Range and codomains are different). [rem:range-and-codomains-are-different] The range is a subset of codomain. Notice that some of the values in the codomain is not reachable
For example,

$$f = x^2 : \mathbb{R} \to \mathbb{R}$$

The codomain is $\mathbb{R}$ but the range is $\mathbb{R}_{\geq 0}$
Let $\mathbb{B} \equiv \{\text{tt}, \text{ff}\}$ denote the set of Boolean values

Definition 7.5 (Injective Mapping/One to One Mapping)**.** [def:injective-mapping] A mapping $f : A \to B$ is called *injective* or *one to one* if

$$f(x_1) = f(x_2) \implies x_1 = x_2$$

equivalently,

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

Example 7.1. The following is an injective mapping:

$$f : \mathbb{B} \to \mathbb{Z}, \qquad \text{tt} \mapsto 0, \quad \text{ff} \mapsto 1$$

Definition 7.6 (Surjective Mapping/onto Mapping)**.** [def:surjective-mapping] A mapping $f : A \to B$ is called *surjective* or *onto* if

$$\forall y \in B, \exists x \in A, \text{ st. } f(x) = y$$

equivalently,

$$\text{Range}(f) = B$$

Example 7.2. The following is a surjective mapping:

$$g : \mathbb{Z} \to \mathbb{B}, \qquad g(n) = \begin{cases} \text{tt}, & n = 0, \\ \text{ff}, & n \neq 0 \end{cases}$$

Definition 7.7 (Bijective Mapping)**.** [def:bijective-mapping] A mapping $f : A \to B$ is called *bijective* if it is both injective and surjective

Example 7.3. The following is a bijective mapping, so it is also injective and surjective:

$$h : \{0, 1\} \to \mathbb{B}, \qquad 0 \mapsto \text{tt}, \quad 1 \mapsto \text{ff}$$

8 Distance

Redirect (Distance) [def:distance]
Moved to definition distance.

9 Bounds

Definition 9.1 (Bounded Above)**.** [def:bounded-above] A set A is *bounded above* in the universe U if

$$\exists b \in U, \forall a \in A, a \leq b$$

Such b is called an *upper bound* of A

Definition 9.2 (Bounded Below)**.** [def:bounded-below] A set A is *bounded below* in the universe U if

$$\exists b \in U, \forall a \in A, a \geq b$$

Such b is called a *lower bound* of A

Definition 9.3 (Least Upper Bound/Supremum)**.** [def:supremum] s is the *least upper bound* or *supremum* of a set A if

1. s is an upper bound of A
2. $\forall b$ is an upper bound of A, $s \leq b$

`LaTeX: \sup (A)`

Proposition 9.1 (ε-Criterion for the Supremum)**.** [prop:epsilon-supremum] *Let F be an ordered field, let $A \subseteq F$ be nonempty, and let $s \in F$. Then $s = \sup A$ if and only if*

1. s is an upper bound of A; and

2. for every $\varepsilon \in F_+$, $s - \varepsilon$ is not an upper bound of A

Equivalently,

$$s = \sup A \iff \begin{cases} \forall x \in A, & x \leq s, \\ \forall \varepsilon \in F_+, & \exists x \in A \text{ s.t. } s - \varepsilon < x \end{cases}$$

Proof. In order to proof ε-Characterization of the Supremum, we need to proof both directions are true

(a):

$$s = \sup A \implies \begin{cases} \forall x \in A, & x \leq s, \\ \forall \varepsilon \in F_+, & \exists x \in A \text{ s.t. } s - \varepsilon < x \end{cases}$$

According to the definition of supremum, we know that s is an upper bound of A, ie, $\forall x \in A, x \leq s$
Take arbitrary $\varepsilon \in F$ with $\varepsilon > 0$. By lemma 3.2, $s' \equiv s - \varepsilon$, $s' < s$
Again, according to the definition of supremum, we know $\forall b$ is an upper bound of $A, s \leq b$. Since $s' < s$, we have that s' is not an upper bound of A
Therefore, $s' = s - \varepsilon$ is not an upper bound of A. According to the definition of upper bound, $\exists x \in A$, $x > s' \implies \exists x > s - \varepsilon$
So, (a) part is proven

(b):

$$\begin{cases} \forall x \in A, & x \leq s, \\ \forall \varepsilon \in F_+, & \exists x \in A \text{ s.t. } s - \varepsilon < x \end{cases} \implies s = \sup A$$

Assume $\forall x \in A, \quad x \leq s$ and $\forall \varepsilon \in F_+, \quad \exists x \in A$ s.t. $s - \varepsilon < x$, and suppose for contradiction that $s \neq \sup A$
From $\forall x \in A, \quad x \leq s$, it follows that s is an upper bound of A
If $s \neq \sup A$, then there exists an upper bound b of A such that $b < s$. Let $\varepsilon \equiv s - b > 0$. By the assumption, there exists $x \in A$ such that $s - \varepsilon < x$. However, $s - \varepsilon = s - (s - b) = b$, so $b < x$, contradicting that b is an upper bound of A
So (b) is proven □

Definition 9.4 (Greatest Lower Bound/Infimum)**.** [def:infimum] i is the *greatest lower bound* or *infimum* of a set A if

1. i is a lower bound of A
2. $\forall b$ is a lower bound of A, $i \geq b$

`LaTeX: \inf (A)`

Proposition 9.2 (ε-Criterion for the Infimum). [prop:epsilon-infimum] *Let F be an ordered field, let $A \subseteq F$ be nonempty, and let $i \in F$. Then $i = \inf A$ if and only if*

1. *i is a lower bound of A; and*
2. *for every $\varepsilon \in F_+$, $i + \varepsilon$ is not a lower bound of A*

Equivalently,

$$i = \inf A \iff \begin{cases} \forall x \in A, & i \leq x, \\ \forall \varepsilon \in F_+, & \exists x \in A \text{ s.t. } x < i + \varepsilon \end{cases}$$

Convention 9.1. We use the notation $\sup A$ to denote the supremum of a set A and $\inf A$ to denote the infimum of a set A

Remark 9.1 (Supremums and Infimums are unique). [rem:supremum-infimum-uniqueness] If a set A has a supremum, then it is unique. If a set A has an infimum, then it is unique

Pf. Supremums are unique. Assume there are 2 supremums for set A, s_1, s_2. Where $s_1 \neq s_2$
Since $\forall s$ is an upper bound of A, $s_1 \leq s$, also $s_2 \leq s$
Notice that s_1 is an upper bound of A, and s_2 is a least upper bound, so $s_2 \leq s_1$
Also, s_2 is an upper bound of A, and s_1 is a least upper bound, so $s_1 \leq s_2$
Trivially, $s_1 = s_2$. Contradicts with $s_1 \neq s_2$
So there are no multiple supremum. Supremums are unique for each set □

Proposition 9.3 (Extrema Agree with Infimum and Supremum). [prop:extrema-and-bounds] *Let X be a totally ordered set, and let $S \subseteq X$ be nonempty*

1. *If S has a minimum, then its infimum exists and*

$$\min(S) = \inf(S)$$

2. *If S has a maximum, then its supremum exists and*

$$\max(S) = \sup(S)$$

Proof. **TODO** □

Definition 9.5 (Bounded Set). [def:bounded-set] A set A is *bounded* in the universe U if it is both bounded above and bounded below

10 Axiom of Completeness

Definition 10.1 (Complete Ordered Field). [def:complete-ordered-field] A *complete ordered field* is an ordered field F such that every nonempty set $A \subseteq F$ that is bounded above has a least upper bound in F

Remark 10.1 (Hierarchy of Order Structures). [rem:order-structure-hierarchy] Just now discussed the four ordered structures, each strictly extends the previous one and unlocks one new capability. When stating a theorem, use the weakest tier that suffices

- Partial order: comparison via $\leq$ (reflexive, antisymmetric, transitive). Minimal and maximal elements make sense when they exist
- Total order: adds totality, so any two elements are comparable. This is the minimum needed to define intervals

- Ordered field: adds the field operations $+, -, \cdot$ compatible with $\leq$. Enables absolute value, distance, and ε-arguments
- Complete ordered field: adds the Axiom of Completeness. Suprema and infima of bounded sets exist, and limit-existence results (e.g. NIP) require this tier

Axiom 10.1 (Axiom of Completeness)**.** [axm:aoc] *Every nonempty set $A \subseteq \mathbb{R}$ that is bounded above has a least upper bound in $\mathbb{R}$*

Remark 10.2 (Identification with the Reals). [rem:complete-field-identification] Every complete ordered field F is *structurally equivalent* to $\mathbb{R}$: there is a unique bijection $F \to \mathbb{R}$ preserving addition, multiplication, and order. Whenever F is complete, we identify it with $\mathbb{R}$ through this correspondence

Lemma 10.1 (Supremum–Infimum Equivalence)**.** [lem:supremum-infimum-equivalence] *Let F be an ordered field. The following statements are equivalent:*

1. *Every nonempty set $A \subseteq F$ that is bounded above in F has a supremum in F*
2. *Every nonempty set $A \subseteq F$ that is bounded below in F has an infimum in F*

Consequently, the definition of a complete ordered field may equivalently use the infimum property. In particular, the Axiom of Completeness is equivalent to the assertion that every nonempty subset of $\mathbb{R}$ bounded below has an infimum in $\mathbb{R}$

Proof. First assume the supremum property, and let $A \subseteq F$ be nonempty and bounded below. Define

$$-A = \{-a : a \in A\}.$$

Then $-A$ is nonempty and bounded above, so let $s = \sup(-A)$. For every $a \in A$, we have $-a \leq s$, and hence $-s \leq a$. Thus $-s$ is a lower bound of A. If ℓ is any lower bound of A, then $-\ell$ is an upper bound of $-A$. Therefore $s \leq -\ell$, so $\ell \leq -s$. Hence $-s = \inf A$
Conversely, assume the infimum property, and let $A \subseteq F$ be nonempty and bounded above. Then $-A$ is nonempty and bounded below, so let $i = \inf(-A)$. For every $a \in A$, we have $i \leq -a$, and hence $a \leq -i$. Thus $-i$ is an upper bound of A. If u is any upper bound of A, then $-u$ is a lower bound of $-A$. Therefore $-u \leq i$, so $-i \leq u$. Hence $-i = \sup A$ □

Remark 10.3 (Integers and Natural Numbers). [rem:integers-naturals-not-fields] Neither $\mathbb{Z}$ nor $\mathbb{N}$ is a field, so neither can be called a complete ordered field. As ordered sets, however, their nonempty subsets that are bounded above have greatest elements

Example 10.1. If $A = \frac{1}{n} : n \in \mathbb{N}_1$, then $\sup A = 1$ and $\inf A = 0$. Although it has a infimum, it does not have a minimum since $0 \notin A$

Corollary 10.1 (Supremum and Infimum Existence in $\mathbb{R}$)**.** [cor:supremum-infimum-existence] *Every nonempty set $A \subseteq \mathbb{R}$ that is bounded above has a least upper bound in $\mathbb{R}$ and every nonempty set $A \subseteq \mathbb{R}$ that is bounded below has a greatest lower bound in $\mathbb{R}$*

Proof. The supremum statement is the Axiom of Completeness, and the infimum statement follows from lemma 10.1 □

Remark 10.4 (Intuition for Completeness). [rem:intuition-for-completeness] We can have a set, let's say,

$$S = \{r \in \mathbb{Q} : r^2 < 3\}, \text{where } r \subset \mathbb{Q} \subset \mathbb{R}$$

Although the set S is bounded above in $\mathbb{Q}$, it does not have a supremum in $\mathbb{Q}$. According to the AoC, we know that $\exists s \in \mathbb{R}, s = \sup S$. This means we can find a number that can be described as the least upper bound a subset of rational numbers which is not in the rational numbers

11 Irrational Numbers

Lemma 11.1 (Parity of a Square). [lem:square-parity] *For every $n \in \mathbb{Z}$,*

$$n^2 \text{ is even} \iff n \text{ is even},$$

and equivalently,

$$n^2 \text{ is odd} \iff n \text{ is odd}$$

Proposition 11.1 (No Rational Square Root of 2). [prop:no-rational-square-root-of-two] *There is no $q \in \mathbb{Q}$ such that $q^2 = 2$*

Proof. Suppose, for contradiction, that some $q \in \mathbb{Q}$ satisfies $q^2 = 2$
According to the proposition 1.1, and $q \in \mathbb{Q}$

$$\exists p, r \in \mathbb{Z}, q = \frac{p}{r}, r > 0, \gcd(|p|, r) = 1$$

Then we have

$$\left(\frac{p}{r}\right)^2 = 2 \implies p^2 = 2r^2$$

Since p^2 is even, the square-parity lemma implies that p is even. Therefore,

$$\exists k \in \mathbb{Z}, \quad p = 2k$$

So,

$$(2k)^2 = 2r^2 \implies 2k^2 = r^2$$

By the same argument, r is also even. Meaning that both p and r are even, which contradicts the assumption that $\gcd(|p|, r) = 1$
So, it contradicts the assumption that $q \in \mathbb{Q}$ satisfies $q^2 = 2$. Therefore, there is no $q \in \mathbb{Q}$ such that $q^2 = 2$ □

Remark 11.1 (Larger Number System). [rem:sqrt-two-larger-number-system] Within $\mathbb{Q}$, the proposition only says that the equation $q^2 = 2$ has no solution $q \in \mathbb{Q}$. Writing $\sqrt{2} \notin \mathbb{Q}$ presupposes a larger number system in which $\sqrt{2}$ exists

Remark 11.2 (Completeness). [rem:rational-incompleteness] The existence, in a larger number system, of some $x \notin \mathbb{Q}$ satisfying $x^2 = 2$ does not by itself prove that $\mathbb{Q}$ is incomplete. Incompleteness must be demonstrated internally by finding a nonempty subset of $\mathbb{Q}$ that is bounded above in $\mathbb{Q}$ but has no supremum in $\mathbb{Q}$, as in Proposition 11.3

Convention 11.1 (Irrational Numbers). [conv:irrational-numbers] We use $\mathbb{I}$ to denote the set of *irrational numbers*

`LaTeX: \II`

Remark 11.3 (Number Sets). [rem:number-sets-inclusions-real] The set of real numbers $\mathbb{R}$ is the union of the set of rational numbers $\mathbb{Q}$ and the set of irrational numbers $\mathbb{I}$:

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$$

Also, in normal conventions, we have:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

`LaTeX: \RR`

Proposition 11.2 (Integer–Irrational Root Dichotomy). [prop:nth-root-dichotomy] *For $x, n \in \mathbb{N}$ with $n > 1$, $\sqrt[n]{x} \in \mathbb{Z}$ if x is a perfect n-th power, and otherwise $\sqrt[n]{x} \in \mathbb{I}$*

Remark 11.4 (Sources of Irrational). [rem:sources-of-irrational]

- By proposition 11.2, $\sqrt[n]{x}$ is irrational whenever $x \in \mathbb{N}$, $n > 1$, and x is not a perfect n-th power
- Taking logarithms
- Constants defined by taking limits, such as π and e

Remark 11.5 (Irrational Numbers Are Not Closed). [rem:irrational-not-closed] The irrational numbers are not closed under addition, multiplication, or exponentiation. For example,

$$\sqrt{2} + (-\sqrt{2}) = 0, \qquad \sqrt{2} \cdot \sqrt{2} = 2, \qquad (\sqrt{3})^{\log_3 4} = 2,$$

where all the inputs are irrational. Although $\pi, e \in \mathbb{I}$, it is not known whether either $\pi + e$ or πe is irrational; both are expected to be transcendental. By contrast, e^{π} has been proved transcendental, and is therefore irrational

Proposition 11.3 (The Rational Numbers Are Not Complete). [prop:rationals-not-complete] *$\mathbb{Q}$ is not a complete ordered field. In fact, the set*

$$A = \{q \in \mathbb{Q} : q^2 < 2\}$$

is nonempty and bounded above in $\mathbb{Q}$, but it has no supremum in $\mathbb{Q}$

Proof. The set A is nonempty because $1 \in A$. It is bounded above in $\mathbb{Q}$ by 2: if some $q \in A$ satisfied $q > 2$, then $q^2 > 4 > 2$, contradicting $q^2 < 2$
Suppose, for contradiction, that A has a supremum $s \in \mathbb{Q}$. Since $1 \in A$, we have $s \geq 1$
First suppose $s^2 < 2$, and define

$$h = \frac{2 - s^2}{2s + 2} \in \mathbb{Q}.$$

Then $h > 0$; moreover, $s \geq 1$ implies $h < 2$. Hence

$$\begin{aligned}(s + h)^2 &= s^2 + h(2s + h) \\ &< s^2 + h(2s + 2) \\ &= 2.\end{aligned}$$

Thus $s + h \in A$, but $s + h > s$, contradicting that s is an upper bound of A. Therefore $s^2 \not< 2$
Now suppose $s^2 > 2$, and define

$$h = \frac{s^2 - 2}{2s} \in \mathbb{Q}, \qquad t = s - h.$$

Then $h > 0$, so $t < s$, and

$$t = \frac{s^2 + 2}{2s} > 0, \qquad t^2 = (s - h)^2 = 2 + h^2 > 2.$$

If some $q \in A$ satisfied $q > t$, then $q > t > 0$ and

$$q^2 - t^2 = (q - t)(q + t) > 0,$$

so $q^2 > t^2 > 2$, contradicting $q \in A$. Consequently every $q \in A$ satisfies $q \leq t$, making t an upper bound of A. This contradicts the minimality of s, because $t < s$. Therefore $s^2 \not> 2$
By totality, $s^2 = 2$. This contradicts the fact that no rational number has square 2. Hence A has no supremum in $\mathbb{Q}$, so $\mathbb{Q}$ is not complete □