UMA204: Introduction to Basic Analysis

Naman Mishra

January 2024

Contents

Lecture **01:** Mon 01 Jan '24

The course

Instructor: Prof. Purvi Gupta
Office: L-25
Office hours: Wed 17:00–18:00
Lecture hours: MW 12:00–12:50, Thu 9:00–9:50
Tutorial hours: Fri 12:00–12:50

We assume the following.

- Basics of set theory
- Existence of $\mathbb{N} = \{0, 1, 2, \ldots\}$ with the usual operations $+$ and $\cdot$

For a recap, refer lectures 1 to 3 of UMA101.

Chapter 1

Number Systems

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

1.1 The Naturals

(Recall from UM101) $\mathbb{N}$ is the unique minimal inductive set granted by the ZFC axioms. Addition and multiplication are defined by the recursion principle and we showed that they

- are associative and commutative,
- admit identity elements 0 and 1 respectively,
- satisfy the distributive law,
- satisfy cancellation laws,
- but do not admit inverses.

1.2 Relations

(Recall) A relation on a set A is a subset $R \subseteq A \times A$. We write $a\ R\ b$ to denote $(a, b) \in R$.

Definition 1.1 (Partial order)**.** A relation R on A is called a *partial order* if it is

- reflexive – $a\ R\ a$ for all $a \in A$;
- antisymmetric – if $a\ R\ b$ and $b\ R\ a$ then $a = b$ for all $a, b \in A$;
- transitive – if $a\ R\ b$ and $b\ R\ c$ then $a\ R\ c$ for all $a, b, c \in A$.

Additionally, if for all $x, y \in A$, $x\ R\ y$ or $y\ R\ x$, then R is called a *total order.*

A set A equipped with a partial order $\leq$ is called a *partially ordered set* (or *poset*).
A set A equipped with a total order $\leq$ is called a *totally ordered set* or simply an *ordered set.*

Examples.

- $(\mathbb{N}, \leq)$ where we say that $a \leq b$ if $\exists\, c \in \mathbb{N}$ such that $a + c = b$.
- $(\mathbb{N}, |)$ where we say that $a \mid b$ if $\exists\, c \in \mathbb{N}$ such that $a \cdot c = b$.

In UMA101, we defined order slightly differently, where we said that either $a < b$ or $b < a$ but never both. This is a "strict order". We will denote a weak partial order by $\leq$ and a strict partial order by $<$. (the notation is suggestive of how to every order there is a corresponding strict order and vice versa).

Definition 1.2 (Equivalence)**.** An *equivalence relation* on a set A is a relation R satisfying

- reflexivity;
- symmetry – if $a\ R\ b$ then $b\ R\ a$ for all $a, b \in A$;
- transitivity.

Notation. We write $[x]_R$ to denote the set $\{y \in A \mid x\ R\ y\}$.

Proposition 1.3. The collection $\mathscr{A} = \{[x]_R \mid x \in A\}$ partitions A under any equivalence relation R on A.

Proof. For every $x \in A$, $x \in [x]_R$ and so $\bigcup \mathscr{A} = A$.

Let $[x]_R \cap [y]_R \neq \varnothing$, where $x, y \in A$. Then there exists $z \in A$ such that

$x \; R \; z$ and $y \; R \; z$, from which it follows that $x \; R \; y$ and $[x]_R = [y]_R$. $\square$

1.3 The Integers

We cannot solve $3 + x = 2$ in $\mathbb{N}$. We introduce $\mathbb{Z}$ to solve this problem.

Consider the relation R on $\mathbb{N} \times \mathbb{N}$ given by

$$(a, b) \; R \; (c, d) \iff a + d = b + c.$$

(check that this is an equivalence relation trivial).

Definition 1.4. We define $\mathbb{Z}$ to be the set of equivalence classes of R, notated $\mathbb{N} \times \mathbb{N}/R$.

Further, define

- $[(a, b)] +_{\mathbb{Z}} [(c, d)] := [(a + c, b + d)]$;
- $[(a, b)] \cdot_{\mathbb{Z}} [(c, d)] := [(ac + bd, ad + bc)]$.
- $z_1 \leq_{\mathbb{Z}} z_2$ iff there exists $n \in \mathbb{N}$ such that $z_1 +_{\mathbb{Z}} [(n, 0)] = z_2$ (alternatively, $[(a, b)] \leq_{\mathbb{Z}} [(c, d)]$ iff $a + d \leq b + c$).

We need to check that these are well-defined. What does this mean? Consider

$$\begin{aligned} [(1, 2)] +_{\mathbb{Z}} [(3, 4)] &= [(4, 6)] \\ [(3, 4)] +_{\mathbb{Z}} [(3, 4)] &= [(6, 8)] \end{aligned}$$

Our definition must ensure that $[(4, 6)] = [(6, 8)]$.
In general, the definitions are well-defined if they are independent of the choice of representatives. Throughout this section, we will omit the parentheses in $[(a, b)]$ and write it as $[a, b]$.

Lecture 02: Tue 02 Jan '24

Proposition 1.5. The operations $+_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$ and the relation $\leq_{\mathbb{Z}}$ are well-defined.

Proof. Suppose $x = [a, b] = [a', b']$ and $y = [c, d] = [c', d']$. Then

$$\begin{aligned} a + b' &= a' + b \\ c + d' &= c' + d \\ (a + c) + (b' + d') &= (a' + c') + (b + d) \\ (a + c, b + d) &\ R\ (a' + c', b' + d') \\ [a + c, b + d] &= [a' + c', b' + d'] \end{aligned}$$

Since $\leq_{\mathbb{Z}}$ is defined in terms of $+_{\mathbb{Z}}$, it is also well-defined. For multiplication,

$$\begin{aligned} (a + b')c + (a' + b)d &= (a' + b)c + (a + b')d \\ (ac + bd) + (a'd + b'c) &= (a'c + b'd) + (ad + bc) \\ [ac + bd, ad + bc] &= [a'c + b'd, a'd + b'c] \end{aligned}$$

and symmetrically

$$[a'c + b'd, a'd + b'c] = [a'c' + b'd', a'c' + b'd']$$

so by transitivity

$$[ac + bd, ad + bc] = [a'c' + b'd', a'c' + b'd'] \qquad \square$$

Proposition 1.6. The relation $\leq_{\mathbb{Z}}$ is a total order on $\mathbb{Z}$.

Proof. Let $x = [a, b], y = [c, d] \in \mathbb{Z}$. Since $x +_{\mathbb{Z}} [0, 0] = [a + 0, b + 0] = x$, $x \leq_{\mathbb{Z}} x$.

Suppose $x \leq_{\mathbb{Z}} y$ and $y \leq_{\mathbb{Z}} x$. Then there exist $m, n \in \mathbb{N}$ such that $x + [m, 0] = y$ and $y +_{\mathbb{Z}} [n, 0] = x$. Thus $x +_{\mathbb{Z}} [m, 0] +_{\mathbb{Z}} [n, 0] = [a + m + n, b] = [a, b]$. This gives $a + m + n + b = a + b$ and so $m + n = 0$. This can only be when $m = n = 0$ and so $x = y$.

Now suppose $x \leq_{\mathbb{Z}} y$ and $y \leq_{\mathbb{Z}} z$. Then there exist $m, n \in \mathbb{N}$ such that $x + [m, 0] = y$ and $y +_{\mathbb{Z}} [n, 0] = z$. This immediately gives $x + [m + n, 0] = z$ and so $x \leq_{\mathbb{Z}} z$.

For trichotomy, note that either $a + d \leq b + c$ or $b + c \leq a + d$ by trichotomy of $(\mathbb{N}, \leq)$. In the first case, $a + d + n = b + c$ for some $n \in \mathbb{N}$, so $[a, b] +_{\mathbb{Z}} [n, 0] = [c, d]$. Thus $x \leq_{\mathbb{Z}} y$. Similarly, in the second case, $y \leq x$. $\square$

Definition 1.7 (Ring)**.** A *ring* is a set S with two binary operations $+$ and $\cdot$ such that for all $a, b, c \in S$,

(R1) addition is associative,

(R2) addition is commutative,

(R3) there exists an additive identity 0,

(R4) there exists an additive inverse $-a$,

(R5) multiplication is associative,

(R6) there exists a multiplicative identity 1,

(R7) multiplication is distributive over addition (on both sides).

For a *commutative ring*, we require additionally that

(CR1) multiplication is commutative.

Note that inverses are unique, since if $a + b = 0$ and $a + b' = 0$, then $b = (b' + a) + b = b' + (a + b) = b'$.

Definition 1.8 (Ordered Ring)**.** An *ordered ring* is a ring S with a total order $\leq$ such that for all $a, b, c \in S$,

(OR1) $a \leq b$ implies $a + c \leq b + c$,

(OR2) $0 \leq a$ and $0 \leq b$ implies $0 \leq ab$.

Theorem 1.9.

- $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, \leq_{\mathbb{Z}})$ is an ordered (commutative) ring.
- The map $f = n \mapsto [n, 0]$ from $\mathbb{N}$ to $\mathbb{Z}$ is an injective map that respects $+$, $\cdot$ and $\leq$. That is, for all $n, m \in \mathbb{N}$,

  (i) $f(n + m) = f(n) +_{\mathbb{Z}} f(m)$,

  (ii) $f(nm) = f(n) \cdot_{\mathbb{Z}} f(m)$,

  (iii) $n \leq m \iff f(n) \leq_{\mathbb{Z}} f(m)$.

  In other words, f is an isomorphism onto a subset of $\mathbb{Z}$.

Proof. For the first part of the theorem, we check all commutative ring axioms. We omit the subscripts on $+$ and $\cdot$ for brevity.

(R1) Addition is associative:

$$\begin{aligned}\big([a,b]+[c,d]\big)+[e,f] &= [a+c,b+d]+[e,f]\\ &= [a+c+e,b+d+f]\\ &= [a,b]+[c+e,d+f]\\ &= [a,b]+\big([c,d]+[e,f]\big)\end{aligned}$$

(R2) Addition is commutative: immediate from commutativity of $+$ on $\mathbb{N}$.

(R3) Additive identity: $[a,b]+[0,0]=[a+0,b+0]=[a,b]$.

(R4) Additive inverse: $[a,b]+[b,a]=[a+b,b+a]=[0,0]$ since $a+b+0=b+a+0$.

(R5) Multiplication is associative:

$$\begin{aligned}\big([a,b]\cdot[c,d]\big)\cdot[e,f] &= [ac+bd,ad+bc]\cdot[e,f]\\ &= [ace+bde+adf+bcf,ade+bce+acf+bdf]\\ &= [a(ce+df)+b(cf+de),a(cf+de)+b(ce+df]\\ &= [a,b]\cdot[ce+df,cf+de]\\ &= [a,b]\cdot\big([c,d]\cdot[e,f]\big)\end{aligned}$$

(R6) Multiplicative identity: $[a,b]\cdot[1,0]=[a,b]$.

(R7) Multiplication distributes over addition:

$$\begin{aligned}[a,b]\cdot\big([c,d]+[e,f]\big) &= [a,b]\cdot[c+e,d+f]\\ &= [ac+ae+bd+bf,ad+af+bc+be]\\ &= [ac+bd,ad+bc]+[ae+bf,af+be]\\ &= [a,b]\cdot[c,d]+[a,b]\cdot[e,f]\end{aligned}$$

Distributivity on the other side follows from commutativity proved below.

For commutativity of multiplication,

$$\begin{aligned}[a,b]\cdot[c,d] &= [ac+bd,ad+bc]\\ &= [ca+db,cb+da]\\ &= [c,d]\cdot[a,b]\end{aligned}$$

?? follows immediately from the definition. For **??**, suppose $0\le x,y\in\mathbb{Z}$. Then $x=[n,0]$ and $y=[m,0]$ for some $n,m\in\mathbb{N}$. Thus $xy=[nm,0]$ and so $0\le xy$.

The second part is again yawningly brute force.

(i) $f(n+m) = [n+m, 0] = [n, 0] + [m, 0] = f(n) +_{\mathbb{Z}} f(m)$.

(ii) $f(nm) = [nm, 0] = [n, 0] \cdot [m, 0] = f(n) \cdot_{\mathbb{Z}} f(m)$.

(iii) $n \leq m \iff \exists\, k \in \mathbb{N}(n+k=m) \iff \exists\, k \in \mathbb{N}\big([n,0]+[k,0] = [m,0]\big) \iff f(n) \leq_{\mathbb{Z}} f(m)$. □

Thus, we may view $(\mathbb{N}, +, \cdot, \leq)$ as a subset of $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, \leq_{\mathbb{Z}})$, denote $[n, 0]$ as n and drop $\mathbb{Z}$ in the subscript. We further define $-[a,b] \coloneqq [b,a]$ and $z_1 - z_2 \coloneqq z_1 + (-z_2)$.

Moreover, we have the following properties.

Proposition 1.10.

- There are no zero divisors in $\mathbb{Z}$. That is, for all $x, y \in \mathbb{Z}$, $xy = 0$ implies $x = 0$ or $y = 0$.
- The cancellation laws hold: for all $x, y, z \in \mathbb{Z}$, $x + y = x + z$ implies $y = z$, and $xy = xz$ implies $x = 0$ or $y = z$.
- (trichotomy) For all $z \in \mathbb{Z}$, $z = n$ or $z = -n$ for some $n \in \mathbb{N}$.

Proof.
- From trichotomy proven below, we have $x = n$ or $x = -n$ and $y = m$ or $y = -m$ for some $n, m \in \mathbb{N}$. In any case $xy = nm$ or $xy = -nm$. Since there are no zero divisors in $\mathbb{N}$, $xy = 0$ implies $n = 0$ or $m = 0$, which in turn implies $x = 0$ or $y = 0$.
- The first cancellation law follows from the fact that additive inverses exist. For the second, note that $xy = xz \iff x(y-z) = 0$ and invoke the fact that there are no zero divisors.

  Here we have also used that $-xz = x(-z)$, since $-\tilde{z} = -1 \cdot \tilde{z}$ for all $\tilde{z} \in \mathbb{Z}$, and multiplication is associative and commutative.
- Let $z = [a, b]$. From trichotomy of $\leq$ on $\mathbb{N}$ we know that either $a + n = b$ or $a = b + n$ for some $n \in \mathbb{N}$. (which $\mathbb{N}$?) That is, either $z = [0, n] = -n$, or $z = [n, 0] = n$.

□

1.4 The Rationals

We cannot solve $3x = 2$ in $\mathbb{Z}$.

Proof. Suppose $3x = 2$ for some $x = [a, b] \in \mathbb{Z}$. Then

$$\begin{aligned} 3x &= 2 \\ [3, 0] \cdot [a, b] &= [2, 0] \\ [3a, 3b] &= [2, 0] \\ 3a &= 3b + 2 \end{aligned}$$

What now? $\square$

We define $\mathbb{Z}^*$ to be $\mathbb{Z} \setminus \{0\}$ and define the relation R on $\mathbb{Z} \times \mathbb{Z}^*$ by $(a, b)R(c, d)$ if $ad = bc$. Then R is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^*$.

Definition 1.11. We define $\mathbb{Q}$ to be the set of equivalence classes of R, notated $\mathbb{Z} \times \mathbb{Z}^*/R$.

We define operations $+_\mathbb{Q}$ and $\cdot_\mathbb{Q}$ on $\mathbb{Q}$ by

$$\begin{aligned} [(a, b)] +_\mathbb{Q} [(c, d)] &:= [(ad + bc, bd)] \\ [(a, b)] \cdot_\mathbb{Q} [(c, d)] &:= [(ac, bd)] \end{aligned}$$

Since there are no zero divisors in $\mathbb{Z}$, $bd \neq 0$.

We define an order $\leq_\mathbb{Q}$ on $\mathbb{Q}$ by

$$[(a, b)] \leq_\mathbb{Q} [(c, d)] \iff (ad - bc)bd \leq 0.$$

We will again omit the parentheses in this section.

Proposition 1.12. The operations $+_\mathbb{Q}$, $\cdot_\mathbb{Q}$ and the relation $\leq_\mathbb{Q}$ are well-defined.

Proof. Suppose $[a, b] = [a', b']$ and $[c, d] = [c', d']$. Then

$$\begin{aligned} ab' &= a'b \\ cd' &= c'd \\ (ad + bc)(b'd') &= (a'd' + b'c')(bd) \\ [ad + bc, bd] &= [a'd' + b'c', b'd'] \end{aligned}$$

For multiplication,

$$
\begin{aligned}
(ac)(b'd') &= (a'c')(bd) \\
[ac, bd] &= [a'c', b'd']
\end{aligned}
$$

For order,

$$
\begin{aligned}
& (ad - bc)bd \leq 0 \\
\iff & (b'd')(ad - bc)bd(b'd') \leq 0 \\
\iff & (ab'dd' - bb'cd')bdb'd' \leq 0 \\
\iff & (a'bdd' - bb'c'd)bdb'd' \leq 0 \\
\iff & (bd)^2(a'd' - b'c')b'd' \leq 0 \\
\iff & (a'd' - b'c')b'd' \leq 0
\end{aligned}
$$

since $bd \neq 0 \neq b'd'$. Thus $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$ and $\leq_{\mathbb{Q}}$ are well-defined. □

Proposition 1.13. The relation $\leq_{\mathbb{Q}}$ is a total order on $\mathbb{Q}$.

Proof. **Transitivity:** Suppose $(ad - bc)bd \leq 0$ and $(cf - de)df \leq 0$. Then $(adf - bcf)bdf \leq 0$ and $(bcf - bde)bdf \leq 0$. Adding these gives $(adf - bde)bdf \leq 0$ and so $(af - be)bf \leq 0$.

Antisymmetry: Suppose $(ad - bc)bd \leq 0$ and $(cb - da)db \leq 0$. Then $(ad - bc)bd = 0$ which gives $ad = bc$ so $x = y$. □

Theorem 1.14.

- $(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, \leq_{\mathbb{Q}})$ is an ordered field.
- The map $f = z \mapsto [z, 1]$ from $\mathbb{Z}$ to $\mathbb{Q}$ is an injective map that respects $+$, $\cdot$ and $\leq$. That is, for all $z_1, z_2 \in \mathbb{Z}$,
  (i) $f(z_1 + z_2) = f(z_1) +_{\mathbb{Q}} f(z_2)$,
  (ii) $f(z_1 z_2) = f(z_1) \cdot_{\mathbb{Q}} f(z_2)$,
  (iii) $z_1 \leq z_2 \iff f(z_1) \leq_{\mathbb{Q}} f(z_2)$.

  In other words, f is a commutative ring isomorphism into $\mathbb{Q}$.

Proof. For the first part, we check all ordered field axioms. We again omit the subscripts on $+$ and $\cdot$ for brevity. Numbering is from UMA101.

(F1) $+$ and $\cdot$ are commutative: immediate from commutativity of $+$ and $\cdot$ on $\mathbb{Z}$.

(F2) $+$ and $\cdot$ are associative:

$$\begin{aligned}\big([a,b]+[c,d]\big)+[e,f] &= [ad+bc,bd]+[e,f]\\ &= [(ad+bc)f+bde,bdf]\\ &= [adf+b(cf+de),bdf]\\ &= [a,b]+[cf+de,df]\\ &= [a,b]+\big([c,d]+[e,f]\big)\end{aligned}$$

Associativity of $\cdot$ is immediate from associativity on $\mathbb{Z}$.

(F3) Distributivity:

$$\begin{aligned}[a,b]\cdot\big([c,d]+[e,f]\big) &= [a,b]\cdot[cf+de,df]\\ &= [acf+ade,bdf]\\ &= [abcf+abde,b^2df] && (b \text{ is nonzero})\\ &= [(ac)(bf)+(bd)(ae),(bd)(bf)]\\ &= [ac,bd]+[ae,bf]\end{aligned}$$

(F4) Identities: $[0,1]\neq[1,1]$, $[a,b]+[0,1]=[a,b]$ and $[a,b]\cdot[1,1]=[a,b]$.

(F5) Additive inverse: $[a,b]+[-a,b]=[0,1]$.

(F6) Multiplicative inverse: $[a,b]\cdot[b,a]=[1,1]$ for $a\neq 0 \iff [a,b]\neq[0,1]$.

For the second part,

(i) $f(z_1+z_2)=[z_1+z_2,1]=[z_1,1]+[z_2,1]$.

(ii) $f(z_1z_2)=[z_1z_2,1]=[z_1,1]\cdot[z_2,1]$.

(iii) $f(z_1)\leq f(z_2) \iff (z_1-z_2)\leq 0 \iff z_1\leq z_2$. $\square$

We now introduce the division operation $/ : \mathbb{Q}\times\mathbb{Q}^*\to\mathbb{Q}$ by $a/b=\frac{a}{b}=ab^{-1}$.

Notation. Note that every rational number $x=[a,b]$ can be written as $x=a/b$. We thus largely drop the notation $[a,b]$ and write a/b instead.

We will now accept basic algebraic manipulations of rational numbers without justification.

Lecture 03: Wed 03 Jan '24

Definition 1.15 (Exponentiation)**.** The recursion principle guarantees the existence of $\text{pow} : \mathbb{Z} \times \mathbb{N} \to \mathbb{N}$ such that for all $n, m \in \mathbb{N}$,

$$\begin{aligned} \text{pow}(m, 0) &= 1 \\ \text{pow}(m, n+1) &= m \cdot \text{pow}(m, n) \end{aligned}$$

We extend this to $\text{pow} : \mathbb{Q}^* \times \mathbb{Z} \to \mathbb{Q}$ as follows.

$$\text{pow}\left(\frac{a}{b}, m\right) := \begin{cases} a^m/b^m & \text{if } m \in \mathbb{N} \\ b^m/a^m & \text{if } -m \in \mathbb{N} \end{cases}$$

We write z^n to denote $\text{pow}(z, n)$.

Remark. Note that we have defined 0^0 to be 1, but we don't really care.

Proposition 1.16. Expoentiation is well-defined.

Proof. Let $a/b = \tilde{a}/\tilde{b} \in \mathbb{Q}$. That is, $a\tilde{b} = b\tilde{a} \in \mathbb{Z}$. For $m \in \mathbb{N}$, thus $a^m\tilde{b}^m = b^m\tilde{a}^m$ (easily proved by induction).

Similarly if $-m \in \mathbb{N}$. □

Theorem 1.17. There exists no $x \in \mathbb{Q}$ such that $x^2 = 2$.

We first make note of the following lemma.

Lemma 1.18. Let $x \in \mathbb{Q}$. Then there exists $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ such that $x = p/q$.

In particular, if $x > 0$, then $x = p/q$ for some $p \in \mathbb{N}$, $q \in \mathbb{N}^*$.

Proof. Let $x = a/b$. If $b \in \mathbb{N}$, we are done. Otherwise, $x = -a/-b$ and $-b \in \mathbb{N}$. □

We will make use of the well-ordered property of $(\mathbb{N}, \leq)$ proved below in **??**.

Proof of **??**. Suppose there exists such an x. By the field properties, $(-x)^2 = x^2$. Thus we may assume $x \geq 0$. Let $x = p/q$ for some $q \in \mathbb{N}^*$. Since $x \geq 0$, we have $p \geq 0 \iff p \in \mathbb{N}$.

Let $A = \{q \in \mathbb{N}^* \mid x = p/q \text{ for some } p \in \mathbb{N}\}$. A is non-empty.

By the well-ordering principle, A has a least element q_0. Let $p_0 \in \mathbb{N}$ such that $x = p_0/q_0$.

We know that $1 < x < 2$ [why? because $(\cdot)^2$ is an increasing function on positive rationals (why? difference of squares)] and so $0 < p_0 - q_0 < q_0$. Now

$$\begin{aligned} \frac{2q_0 - p_0}{p_0 - q_0} &= \frac{2 - x}{x - 1} \\ &= \frac{(2 - x)(x + 1)}{x^2 - 1} \\ &= 2x + 2 - x^2 - x \\ &= x, \end{aligned}$$

in contradiction to the minimality of q_0. $\square$

Theorem 1.19 (Well-ordering principle)**.** Every non-empty subset of $\mathbb{N}$ has a least element.

Proof. Let $S \subseteq \mathbb{N}$ be non-empty. We define $P(n)$ to be "if $n \in S$, then S has a least element". Clearly $P(0)$ holds.

Suppose $P(k)$ holds for all $k \leq n \in \mathbb{N}$.
If $n + 1 \notin S$, $P(n + 1)$ holds vacuously.
If $\exists\, m \in S(m < n + 1)$, then $P(n + 1)$ holds by virtue of $P(m)$.
Otherwise $n + 1 \in S$ and $\forall\, m \in S(n + 1 \leq m)$, so that $n + 1$ is the least element of S.

In any case, $P(n + 1)$ holds. $\square$

Theorem 1.20. Let

$$\begin{aligned} A &= \left\{x \in \mathbb{Q} \mid x^2 < 2\right\} \\ B &= \left\{x \in \mathbb{Q} \mid x^2 > 2, x > 0\right\} \end{aligned}$$

Then A has no largest element and B has no smallest element.

Proof. Let $a \in A$. $a > -2$ since otherwise $a^2 \geq 4$. Let $c = a + \frac{2-a^2}{2+a}$. Clearly

$c > a$. Now

$$\begin{aligned} c &= \frac{2a+2}{2+a} \\ c^2 &= \frac{4a^2+8a+4}{4+4a+a^2} \\ c^2 - 2 &= \frac{2a^2-4}{(2+a)^2} < 0 \end{aligned}$$

Thus $c \in A$.

For B, let $c = b + \frac{2-b^2}{2+b} = \frac{2b+2}{2+b}$. Clearly $0 < c < b$ and $c^2 - 2 = \frac{2b^2-4}{(2+b)^2} > 0$. Thus $c \in B$. □

Corollary 1.21. $(\mathbb{Q}, \leq)$ does not have the least upper bound property.

Proof. Let b be an upper bound of A. Clearly $b > 0$. b cannot be in A since A has no largest element. b cannot have square 2 by **??**. Thus $b \in B$. But since B has no smallest element, there is a $b' \in B$ which is less than b.

For any $a \in A$, if $a < 0$ then $a < b'$. Otherwise, $0 < (b')^2 - a^2 = (b'-a)(b'+a)$ and so $a < b'$. Thus b' is an upper bound of A which is less than b.

Since b was arbitrary, A cannot have a least upper bound. □

1.5 Ordered Fields with LUB

(Recall from UMA101 Lecture 6) Given an ordered set $(X, \leq)$, a subset $S \subseteq X$ is said to be *bounded above* (resp. below) if there exists $x \in X$ such that for all $s \in S$, $s \leq x$ (resp. $x \leq s$), and any such x is called an *upper* (resp. lower) *bound* of S.

A (The) *supremum* or least upper bound of S is an element $x \in X$ such that x is an upper bound of S and for all upper bounds y of S, $x \leq y$. Similarly, infimum or greatest lower bound.

$(X, \leq)$ is said to have the least upper bound property if every non-empty bounded above subset of X admits a supremum.

Proposition 1.22. $(\mathbb{Q}, \leq)$ does not have the least upper bound property.

Proof. From **??**, we know that A has no largest element and B has no smallest element.

Let s be a supremum of A. Since there is no largest element in A, $s \notin A$. From **??**, we know that $s^2 \neq 2$. Thus by trichotomy, $s^2 > 2$ and so $s \in B$. But then there is an $s' \in B$ which is less than s but also an upper bound of A. This is a contradiction. $\square$

Theorem 1.23. Every ordered field F "contains" $\mathbb{Q}$, *i.e.*, there exists an injective map $f : \mathbb{Q} \to F$ that respects $+$, $\cdot$ and $\leq$.

We will notate this statement as $\mathbb{Q} \subseteq F$.

Proof. Let $f : \mathbb{Z} \to F$ be defined as

$$f(n) = \begin{cases} 0_F & \text{if } n = 0 \\ \underbrace{1_F + \cdots + 1_F}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{(-1_F) + \cdots + (-1_F)}_{m \text{ times}} & \text{if } n = -m, m > 0 \end{cases}$$

Note that $f(-n) = -f(n)$ for all $n \in \mathbb{N}$. Let us show that $f(n+m) = f(n) + f(m)$ for all $n, m \in \mathbb{Z}$.

Case 1: $n = 0$ or $m = 0$. Immediate.

Case 2: $n > 0$ and $m > 0$. Then

$$\begin{aligned} f(n+m) &= \underbrace{1_F + \cdots + 1_F}_{n+m \text{ times}} \\ &= \underbrace{1_F + \cdots + 1_F}_{n \text{ times}} + \underbrace{1_F + \cdots + 1_F}_{m \text{ times}} \\ &= f(n) + f(m) \end{aligned}$$

Case 3: $n < 0$ and $m < 0$. Then $f(n+m) = -f((-n) + (-m)) = -(f(-n) + f(-m)) = f(n) + f(m)$.

Case 4: $nm < 0$. WLOG, let $m < 0 < n$. Suppose $0 < n + m$. Then $f(n+m) + f(-m) = f(n+m-m) = f(n)$ from case 2. Now suppose $n + m < 0$. Then $f(n) + f(-n-m) = f(n-n-m) = -f(m)$ from case 3. In either case, $f(n+m) = f(n) + f(m)$.

Now consider $f(nm)$. If $nm = 0$, then $f(nm) = 0_F = f(n)f(m)$. If

$0 < n, m$, then

$$\begin{aligned} f(nm) &= \overbrace{1_F + \cdots + 1_F}^{nm \text{ times}} \\ &= \underbrace{\overbrace{(1_F + \cdots + 1_F)}^{n \text{ times}} + \cdots + \overbrace{(1_F + \cdots + 1_F)}^{n \text{ times}}}_{m \text{ times}} \\ &= \underbrace{(1_F + \cdots + 1_F)}_{n \text{ times}} \cdot \underbrace{(1_F + \cdots + 1_F)}_{m \text{ times}} \\ &= f(n)f(m) \end{aligned}$$

If either of n, m is negative, then we take the negative sign out and use the above case.

Thus f respects $+$ and $\cdot$.

Suppose that $m < n$. Then $f(n) - f(m) = f(n) + f(-m) = f(n-m) = (n-m)1_F$ (where $z1_F$ is notation for 1_F added z times). $n - m$ is positive, but 1_F added to itself a positive number of times must be positive. This is because $0_F < 1_F$ (UMA101) and so $k1_F < (k+1)1_F$ for all $k \in \mathbb{N}^+$. Induction gives $0_F < k1_F$ for all $k \in \mathbb{N}^+$. Thus $f(m) < f(n)$ and so f respects $<$ (and hence $\leq$).

Finally, injectivity of f follows from order preservation.

We extend f to $\mathbb{Q}$ by defining $f(a/b) = f(a)f(b)^{-1}$. This continues to be an isomorphism. □

Lecture 04: Wed 10 Jan '24

Definition 1.24 (Archimedean property)**.** An ordered field F is said to have the *Archimedean property* if for every $x, y > 0$, there exists an $n \in \mathbb{N} \subseteq F$ such that $nx > y$.

Theorem 1.25. $\mathbb{Q}$ has the Archimedean property.

Proof. Let $x, y > 0$ be rationals. If $x > y$, $n = 1$ works. Suppose $x \leq y$. It suffices to show that $\exists\, n \in \mathbb{N}(nr > 1)$, where $r = x/y$. Since r is positive, we have $p, q \in \mathbb{N}^*$ such that $r = p/q$. Let $n = 2q$. This gives $nr > 1$. □

Remark. Not all ordered fields have the Archimedean property.

Theorem 1.26. Let F be an ordered field with the LUB property. Then F has the Archimedean property.

Proof. Let $x, y > 0$. Suppose $\forall n \in \mathbb{N}(nx \leq y)$. Let $A = \{nx \mid n \in \mathbb{N}\}$. Clearly A is non-empty and bounded above. Then $\sup A$ exists and so there exists an $m \in \mathbb{N}$ such that $\sup A - x < mx$. Thus $\sup A < (m+1)x \in A$, a contradiction. $\square$

Theorem 1.27. Let F be an ordered field with the LUB property. Then $\mathbb{Q}$ is dense in F, *i.e.*, given $x < y \in F$, there exists a rational $r \in \mathbb{Q}$ such that $x < r < y$.

Proof. Follows from **??** and problem 4 on assignment 1. $\square$

1.6 The Reals

Theorem 1.28 (Dedekind/Cauchy)**.** There exists a unique (up to isomorphism) ordered field with the LUB property.

We first recover some properties of supremums.

Lemma 1.29. Let F be an ordered field with the LUB property. Let A and B be non-empty bounded above subsets of F. Then $\sup A + \sup B = \sup(A+B)$. Further, if all elements of A and B are non-negative, then $\sup A \sup B = \sup(AB)$.

Here $A + B \coloneqq \{a + b \mid a \in A, b \in B\}$ and $AB \coloneqq \{ab \mid a \in A, b \in B\}$.

Proof. Let $\alpha = \sup A$ and $\beta = \sup B$. For all $a \in A$ and $b \in B$, $a+b \leq \alpha+\beta$. Thus $\alpha + \beta$ is an upper bound of $A + B$.

Let $c < \alpha + \beta$. Since $c - \beta < \alpha$, there exists an $a \in A$ larger than $c - \beta$. Then $c - a < \beta$ and so there exists a $b \in B$ larger than $c - a$. Thus $c < a + b \in A + B$ and so $\alpha + \beta = \sup(A + B)$.

Now suppose all elements of A and B are non-negative. If $\alpha = 0$ or $\beta = 0$, then $\alpha\beta = 0$ and so $\alpha\beta = \sup(AB)$.

For all $a \in A$ and $b \in B$, $ab \leq \alpha\beta$. Let $c < \alpha\beta$. Since $c/\beta < \alpha$, there exists an $a \in A$ larger than c/β. Then $c/a < \beta$ and so there exists a $b \in B$ larger than c/a. Thus $c < ab \in AB$ and so $\alpha\beta = \sup(AB)$. $\square$

Proof of uniqueness. Let F and G be OFWLUB. Let h be identity on

$\mathbb{Q} \subseteq F, G$. For $z \in F$ let

$$A_z = \{w \in \mathbb{Q} \mid w <_F z\}.$$

Claim: A_z is non-empty and bounded above when viewed as a subset of G, and therefore has a supremum in G.

First, A_z is non-empty by density applied to $(z - 1_F, z)$ or Archimedean applied to $-z$. Secondly, by Archimedean (or density) there exists a *rational* upper bound q of A_z in F. This q is also an upper bound of A_z in G.
By LUB, A_z has a supremum in G.

We define $h(z) := \sup_G A_z$. For this we need to show that $h(r) = r$ for all $r \in \mathbb{Q}$, so that the definitions coincide. Let $r \in \mathbb{Q}$ so that $A_r = \{w \in \mathbb{Q} \mid w <_F r\}$. Clearly r is an upper bound of A_r in G. For any $g \in G$, there is some $q \in \mathbb{Q}$ such that $g <_G q <_G r$ (by density of $\mathbb{Q}$ in G). Thus g cannot be an upper bound of $A_r \subseteq G$. Thus $r = \sup_G A_r = h(r)$.

Claim: h preserves order.

Let $z < w \in F$. By density of $\mathbb{Q}$ in F, there exist rationals r, s, t such that $z < r < s < t < w$. Then $A_z \subsetneq A_w$ as subsets of F and hence of G. Thus

$$h(z) = \sup_G A_z \leq_G r < s < t \leq_G \sup_G A_w = h(w).$$

Claim: h preserves addition.

It is sufficient to show that $A_{x+y} = A_x + A_y$, where set addition is defined pairwise. If a rational $q \in A_x + A_y$, then clearly $q <_F x + y$ and so $q \in A_{x+y}$. Let $q \in A_{x+y} \iff q <_F x + y$. Then $q - x \in A_y$. Since A_y has no largest element (by density), there exists an $r \in A_y$ with $q - x < r < y$. Then $q - r < x$ and so $q - r \in A_x$. Thus $q = (q - r) + r \in A_x + A_y$ which gives equality of the sets.
From the previous lemma, $\sup A_x + \sup A_y = \sup(A_x + A_y) = \sup A_{x+y}$ and so h preserves addition.

Claim: h preserves multiplication.

Let $0 < x, y \in F$. Let $A_z^+ = \{w \in \mathbb{Q} \mid 0 < w <_F z\}$. We will show that $A_{xy}^+ = A_x^+ A_y^+$, where set product is defined pairwise. If a rational $q \in A_x^+ A_y^+$, then clearly $0 < q <_F xy$ and so $q \in A_{xy}^+$. Let $q \in A_{xy}^+ \iff 0 < q <_F xy$. Then $q/x \in A_y^+$. Since A_y^+ has no largest element, there exists an $r \in A_y^+$ with $q/x < r < y$. Then $q/r < x$ and so $q/r \in A_x^+$. Thus $q = (q/r) \cdot r \in A_x^+ A_y^+$ which gives equality of the sets.
From the previous lemma, $\sup A_x^+ \sup A_y^+ = \sup(A_x^+ A_y^+) = \sup A_{xy}^+$ and so h preserves multiplication of positive elements.
Since h preserves addition, h preserves additive inverses. So h preserves multiplication of all elements. □

1.6.1 Dedekind's Construction

Definition 1.30 (Dedekind cut)**.** A *Dedekind cut* is a non-empty proper subset $A \subsetneq \mathbb{Q}$ such that

(i) if $a \in A$, then $b \in A$ for all $b \in \mathbb{Q}$ with $b < a$.

(ii) if $a \in A$, then there exists a $c \in A$ such that $a < c$.

Definition 1.31 ($\mathbb{R}$)**.** We define

$$\mathbb{R} := \left\{A \in 2^{\mathbb{Q}} \mid A \text{ is a Dedekind cut}\right\}.$$

Further,

(i) $A \leq B \iff A \subseteq B$;

(ii) $A + B = \{a + b \mid a \in A, b \in B\}$.

(iii) for $A, B > 0$,

$$A \cdot B = \{q \in \mathbb{Q} \mid q \leq rs \text{ for some } r \in A, s \in B\}.$$

If $A < 0$ but $B > 0$, then $A \cdot B = -((-A) \cdot B)$. If $B < 0$ but $A > 0$, then $A \cdot B = -(A \cdot (-B))$. If $A < 0$ and $B < 0$, then $A \cdot B = (-A) \cdot (-B)$.

Proposition 1.32. *$O = \{z \in \mathbb{Q} \mid z < 0\}$ is the additive identity of $\mathbb{R}$. For any $A \in \mathbb{R}$,*

$$B = \{x \in \mathbb{Q} \mid \exists\, r \in O(r - x \notin A)\}$$

is an additive inverse of A.

Proof. Let $A \in \mathbb{R}$. For all $a \in A$, there exists $a' \in A$ larger than a. So

$a - a' \in O$ and thus $a' + (a - a') = a \in A + O$.

For all $a \in A + O$, there exists $a' \in A$ and $o \in O$ such that $a = a' + o$. But then $a' > a$, so $a \in A$. Thus $A + O = A$.

Let B be as defined. Let $a + b \in A + B$ where $a \in A$ and $b \in B$. Then there exists $r \in O$ such that $r - b \notin A$. So $r - b > a$ and thus $a + b < r < 0$.

Now let $o \in O$. Since O has no largest element, there exists an $o' \in O$ such that $o' > o$. Let $a \in A$. Consider the set $\alpha = \{n \in \mathbb{Z} \mid a + n(o' - o) \in A\}$. By archimedean property of $\mathbb{Q}$, α is bounded. It is obviously non-empty fucker. Thus it has a supremum n. Let $a' = a + n(o' - o)$. $a' + (o' - o) = o' - (o - a') \notin A$ because n was supremum. This gives $o - a' \in B$. Thus $o \in A + B$. $\square$

Lecture 05: Thu 11 Jan '24

Theorem 1.33. $\mathbb{R}$ has the least upper bound property.

Proof. Let α be a non-empty subset of $\mathbb{R}$ that is bounded above. We claim that $S = \bigcup_{A \in \alpha} A$ is the supremum of α.

s **is a cut:** Since S is a union of a non-empty set of non-empty sets, it is non-empty. Since S is bounded above, say by some cut C, we have $S \subseteq C \subsetneq \mathbb{Q}$ and so $S \neq \mathbb{Q}$. If $a \in S$, then $a \in A$ for some $A \in \alpha$. Since A is a cut, every rational smaller than a is contained in A and thereby in S. Moreover, there exists an $a' \in A$ which is larger than a. Thus $a' \in S$ is larger than a.

upper bound: $A \subseteq S$ for all $A \in \alpha$.

least upper bound: For any $D \subsetneq S$, let $b \in S \setminus D$. But since $b \in A$ for some $A \in \alpha$, D is not an upper bound of α. $\square$

Dedekind's construction is an "order completion". Thus all the order properties (LUB, density) are nice, but arithmetic is ugly.

1.6.2 Cauchy's Construction

There seem to be sequences in $\mathbb{Q}$ that "should" have a limit (*e.g.*, a monotone and bounded sequence) but do not (within $\mathbb{Q}$). We construct equivalence classes of sequences which "converge" to the same number, and define reals by those classes.

Definition 1.34 (Sequence)**.** A sequence of rational numbers is a $f\colon \mathbb{N} \to \mathbb{Q}$. We usually denote $f(k)$ by a_k and call it the k-th term of the sequence. The function f is usually written as $(a_k)_{k\in\mathbb{N}}$.

Definition 1.35. A sequence $(a_k)_{k\in\mathbb{N}} \subseteq \mathbb{Q}$ is said to be

(i) $\mathbb{Q}$-bounded if there exists an $M \in \mathbb{Q}$ such that $|a_k| \leq M$ for all $k \in \mathbb{N}$.

(ii) $\mathbb{Q}$-Cauchy if for every rational $\epsilon > 0$, there exists an $N \in \mathbb{N}$ such that $|a_m - a_n| < \epsilon$ for all $m, n \geq N$.

(iii) convergent in $\mathbb{Q}$ if there exists an $L \in \mathbb{Q}$ such that for all (rational) $\varepsilon > 0$, there exists an $N \in \mathbb{N}$ such that $|a_n - L| < \varepsilon$ for all $n \geq N$.

Exercise 1.36. Show that if a sequence is convergent in $\mathbb{Q}$, then it is $\mathbb{Q}$-Cauchy, and if it is $\mathbb{Q}$-Cauchy, then it is $\mathbb{Q}$-bounded.

Remark. From UMA101, we know that if a sequence is convergent in $\mathbb{Q}$, the limit is unique. We also know arithmetic laws of limits (which we proved over $\mathbb{R}$, but they hold over $\mathbb{Q}$as well).

Definition 1.37. Two sequences $a = (a_n)_{n\in\mathbb{N}}$ and $b = (b_n)_{n\in\mathbb{N}}$ are said to be *equivalent* if their difference converges to 0.

Proposition 1.38. Let $\mathcal{C}$ denote the space of $\mathbb{Q}$-cauchy sequences. Then $\sim$ given by $a \sim b$ if a and b are equivalent (as per the previous definition) is an equivalence relation.

Proof. Reflixivity and symmetry are immediate. Transitivity follows from the triangle inequality. $\square$

Definition 1.39 ($\mathbb{R}$)**.** We define

$$\mathbb{R} \coloneqq \mathcal{C}/\sim.$$

Further,

(i) $[a] +_{\mathbb{R}} [b] \coloneqq [a+b]$.

(ii) The additive identity $0 = [(0)_{n\in\mathbb{N}}]$.

(iii) $[a] \cdot_{\mathbb{R}} [b] \coloneqq [a \cdot b]$.

(iv) $[a] >_{\mathbb{R}} 0$ if there exists a rational $c > 0$ and an $N \in \mathbb{N}$ such that $a_n > c$ for all $n \geq N$. From positivity, we can define order as $[a] >_{\mathbb{R}} [b]$ iff there is some $[d] > 0$ such that $[a] + [d] = [b]$.

Proposition 1.40. The operations $+\mathbb{R}$ and $\cdot_{\mathbb{R}}$ and the relationn $>_{\mathbb{R}}$ are well-defined.

Proof. Let $a \sim a'$ and $b \sim b'$. Then $a+b-(a'+b') = (a-a')+(b-b') \to 0$. □

Lecture 06: Mon 15 Jan '24

We define an isomorphism from $\mathbb{Q}$ into $\mathbb{R}$ as

$$r \in \mathbb{Q} \mapsto [(r, r, \dots)] \in \mathbb{R}.$$

Theorem 1.41. $(\mathbb{R}, +, \cdot, \leq)$ satisfies the Archimedean property.

Proof. Let $[a], [b] > 0$ be in $\mathbb{R}$. Since $[b]$ is $\mathbb{Q}$-Cauchy, there exists a positive $M \in \mathbb{Q}$ such that $b_n < M$ for all $n \in \mathbb{N}$.

Since $[a] > 0$, let $c \in \mathbb{Q}^+$ and $N \in \mathbb{N}$ be such that $a_n > c$ for all $n \geq N$. By the Archimedean property of $\mathbb{Q}$, there exists an $m \in \mathbb{N}$ such that $mc > M$. Thus $b_n < M < mc < ma_n$ for all $n \geq N$. Thus $(m+1)a_n - b_n > ma_n - b_n + c > c$ for all $n \geq N$ and so $[m+1][a] > [b]$. □

Theorem 1.42. $(\mathbb{R}, +, \cdot, \leq)$ satisfies the LUB property.

Proof. Let $A \subseteq \mathbb{R}$ be a non-empty bounded above set.

For $n \in \mathbb{N}^*$, let $U_n = \left\{m \in \mathbb{Z} : \frac{m}{n} \text{ is an upper bound of } A\right\}$. From the Archimedean property of $\mathbb{R}$, U_n is non-empty and bounded below. By well-ordering, U_n has a minimum $m(n)$. Let $a_n = \frac{m(n)}{n}$ for each $n \in \mathbb{N}^*$.

Claim: $(a_n)_{n\in\mathbb{N}^*}$ is $\mathbb{Q}$-Cauchy.
Let ε be a positive rational number. By Archimedean, there $\frac{1}{n} < \varepsilon$ for all n above some N in $\mathbb{N}$. Note that for any $n \in \mathbb{N}^*$, a_n is an upper bound of A, and $a_n - \frac{1}{n}$ is not an upper bound of A.

Thus for any $n, n' \geq N^*$, we have

$$\frac{m(n)}{n} > \frac{m(n')}{n'} - \frac{1}{n'} \qquad \frac{m(n')}{n'} > \frac{m(n)}{n} - \frac{1}{n}$$
$$a_n - a_{n'} > -\frac{1}{n'} \qquad a_n - a_{n'} < \frac{1}{n}$$

and so $|a_n - a_{n'}| < \max\{\frac{1}{n}, \frac{1}{n'}\} < \varepsilon$.

Claim: $[(a_n)]$ is an upper bound of A.
Suppose there exists some $[x] > [a]$. That is, there is some positive rational c such that $c < x_n - a_n$ for all n larger than some $N_1 \in \mathbb{N}^*$. Since (x_n) is $\mathbb{Q}$-Cauchy, $-c/2 < x_n - x_m < c/2$ for all n, m larger than some $N_2 \in \mathbb{N}^*$. □

Lecture 07: Wed 17 Jan '24

1.7 The Complex Numbers

Definition 1.43. A *complex number* is an ordered pair of real numbers. We define operations on the set $\mathbb{C}$ of complex numbers as follows.

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$
$$|(a, b)| = \sqrt{a^2 + b^2}$$

We further define i to be $(0, 1)$.

Remark. These operations make $\mathbb{C}$ a *normed field*.

Theorem 1.44. The map $f : \mathbb{R} \to \mathbb{C}$ given by $f(x) = (x, 0)$ is an isomorphism into $\mathbb{C}$.

This allows us to identify $x \in \mathbb{R}$ with $(x, 0) \in \mathbb{C}$.

Remark. $(a, b) = a + ib$ for any $a, b \in \mathbb{R}$. $i^2 = -1$.

0 is the additive identity and $(-a) + i(-b)$ is the additive inverse of $a + ib$.

1 is the multiplicative identity and for $a+ib\neq 0$, $\frac{a}{a^2+b^2}+i\frac{-b}{a^2+b^2}$ is the multiplicative inverse of (a,b).

Theorem 1.45 (Cauchy-Schwarz inequality)**.** Let $a_1,a_2,\ldots,a_n$ and $b_1,b_2,\ldots,b_n$ be real numbers. Then

$$\Big|\sum_{j=1}^n a_j\overline{b_j}\Big|^2 \le \Big(\sum_{j=1}^n |a_j|^2\Big)\Big(\sum_{j=1}^n |b_j|^2\Big).$$

Proof. Let $\lambda = u+iv\in\mathbb{C}$.

$$\begin{aligned}0 &\le \sum_{j=1}^n (a_j+\lambda b_j)\overline{(a_j+\lambda b_j)}\\ &= \sum_{j=1}^n (a_j\overline{a_j}+\overline{\lambda}a_j\overline{b_j}+\lambda b_j\overline{a_j}+|\lambda|^2 b_j\overline{b_j})\\ &= \sum_{j=1}^n |a_j|^2 + 2[u\Re(A)+v\Im(A)]+(u^2+v^2)B\end{aligned}$$

where $A=\sum_{j=1}^n a_j\overline{b_j}$ and $B=\sum_{j=1}^n |b_j|^2$.

Let the right hand expression be $F(u,v)$. Then $F_u(u,v)=2\Re(A)+2uB$ and $F_v(u,v)=2\Im(A)+2vB$. Setting both to be 0 gives $u=-\frac{\Re(A)}{B}$ and $v=-\frac{\Im(A)}{B}$. These values of u and v give $\lambda=-A/B$. Thus

$$F(u,v)=\sum_{j=1}^n |a_j|^2 - \frac{2|A|^2}{B}+\frac{|A|^2}{B}$$

and so

$$|A|^2\le \sum_{j=1}^n |a_j|^2\sum_{j=1}^n |b_j|^2. \qquad \square$$

Chapter 2

Metric Spaces

2.1 Definitions & examples

Definition 2.1. A *metric space* is a pair (X, d) consisting of a set X and a "distance function" $d\colon X \times X \to [0, \infty)$ such that

(M1) $d(x, y) = 0$ iff $x = y$,

(M2) $d(x, y) = d(y, x)$,

(M3) $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

Examples.

- $X = \mathbb{R}$, $d(x, y) = |x - y|$.
- (Real Euclidean space) $X = \mathbb{R}^n$. The inner product $\langle x,\, y\rangle = \sum_{j=1}^n x_j y_j$ gives the *Euclidean* distance $d(x, y) = \sqrt{\langle x - y,\, x - y\rangle}$.
- (Discrete metric) Let X be any set. Then $[x \neq y]$ is a distance function on X.
- $X = \mathbb{R}^n$, $p \in [1, \infty]$. For $p \neq \infty$,

  $$d_p(x, y) = \left(\sum_{j=1}^n |x_j - y_j|^p\right)^{1/p}$$

  and

  $$d_\infty(x, y) = \max_{1 \leq j \leq n} |x_j - y_j|.$$

  If $p \neq 2$, then d_p is not induced by an inner product.

- For any metric space (X, d) and a subset $Y \subseteq X$, the restriction of d to $Y \times Y$ is a distance on Y.

Proposition 2.2. Given $a, b \in \mathbb{R}^n$,

$$\big|\|a\| - \|b\|\big| \leq \|a + b\| \leq \|a\| + \|b\|.$$

Proof. From Cauchy-Schwarz,

$$\begin{aligned}
\|a + b\|^2 &= \langle a + b,\, a + b\rangle \\
&= \|a\|^2 + 2\langle a,\, b\rangle + \|b\|^2 \\
&\leq \|a\|^2 + 2\|a\|\|b\| + \|b\|^2 \\
&= (\|a\| + \|b\|)^2.
\end{aligned}$$

□

Lecture 08: Thu 18 Jan '24

2.2 Metric Topology

Definition 2.3. Let (X, d) be a metric space.

(i) The *open ball* centered at p or radius $\varepsilon > 0$ is the set

$$B_d(p; \varepsilon) := \{x \in X : d(p, x) < \varepsilon\}$$

This set is also called the ε-neighborhood of p. Similarly, the *closed ball* centered at p or radius $\varepsilon > 0$ is the set

$$\{x \in X : d(p, x) \leq \varepsilon\}$$

(ii) Given a set $E \subseteq X$ and $p \in X$, p is an *interior point* of E if there exists some $\varepsilon > 0$ such that the ε-neighborhood $B(p; e)$ is contained in E. The collection of all interior points of E, denoted E°, is called the *interior* of E.

(iii) A set $E \subseteq X$ is said to be *open* if it is equal to its interior.

(iv) The collection of all open sets of (X, d) is called the d-topology on X.

Remark. The empty set is always open.

Examples.

- The open ball on $\mathbb{R}$ is an interval $(p - \varepsilon, p + \varepsilon)$.
-

- For the discrete metric,

$$B_d(p;\varepsilon) = \begin{cases} \{p\} & \varepsilon < 1 \\ X & \varepsilon \geq 1 \end{cases}$$

  Every set is open, by taking any $\varepsilon = 1$.

Proposition 2.4. Every open ball is an open set.

Proof. Let (X, d) be the metric. Let $p \in X$, $\varepsilon > 0$, and $q \in B(p;\varepsilon)$. Choose $\delta = \varepsilon - d(p,q) > 0$ works. We show that $B(q;\delta) \subseteq B(p;\varepsilon)$. Let $r \in B(q;\delta)$. Then from the triangle inequality,

$$\begin{aligned} d(p,r) &\leq d(p,q) + d(q,r) \\ &< d(p,q) + \delta \\ &= \varepsilon \end{aligned}$$

□

Proposition 2.5. The union of any collection of open sets is open, and the intersection of any finite collection of open sets is open.

Proof. Let $\mathscr{U}$ be a collection of open sets. Let $E = \bigcup_{U \in \mathscr{U}} U$. For any $p \in E$, p is contained in some $U \in \mathscr{U}$. Then there exists some $\varepsilon > 0$ such that $B(p;\varepsilon) \subseteq U \subseteq E$.

Let $U_1, \ldots, U_n$ be open sets and let $E = \bigcap_{i=1}^n U_i$. For any $p \in E$, $p \in U_i$ for all i. Then there exist $\varepsilon_1, \ldots, \varepsilon_n > 0$ such that $B(p;\varepsilon_i) \subseteq U_i$ for all i. Letting ε be the minimum of the ε_i's, we have $B(p;\varepsilon) \subseteq U_i$ for all i. So $B(p;\varepsilon) \subseteq E$. □

Definition 2.6. Let (X, d) be a metric space and $E \subseteq X$.

(i) Given $p \in X$, we say that p is an *accumulation point* of E if for every $\varepsilon > 0$, $B(p;\varepsilon)$ contains a point $q \in E$ such that $q \neq p$.

(ii) A point $p \in E$ is said to be *isolated* in E if it is not an accumulation point of E.

Examples.

- In the discrete metric, every point is isolated in every subset.
- Finite subsets have no accumulation points.

Remarks.

- p need not lie in E to be an accumulation point.
- If p is an accumulation point of E, then every neighborhood of p contains infinitely many points of E.

Lecture 09: Mon 21 Jan '24

2.3 Compactness

Lecture 10: Wed 24 Jan '24

> **Definition 2.7.** A subset $E \subseteq (X, d)$ is said to be bounded if there exists a $p \in X$ and $M > 0$ such that $E \subseteq B(p; M)$.

Consider $E = \{p \in \mathbb{Q} : 2 < p^2 < 3\}$. Then E is both closed and bounded in $(\mathbb{Q}, |\cdot|)$. However, continuous functions on E are neither uniformly continuous nor bounded.

> **Definition 2.8.** Let $E \subseteq (X, d)$. An open cover $\{\mathcal{U}_\alpha\}_{\alpha \in \Lambda}$ of E in X is a collection of open sets $\mathcal{U}_\alpha$ such that $E \subseteq \bigcup_{\alpha \in \Lambda} \mathcal{U}_\alpha$.

> **Definition 2.9.** A subset $E \subseteq (X, d)$ is said to be compact if any open cover $\mathcal{U} = \{\mathcal{U}_\alpha\}_{\alpha \in \Lambda}$ of E in X admits a finite subcover of E, *i.e.*, there exist $\alpha_1, \dots, \alpha_k \in \Lambda$ such that $E \subseteq \bigcup_{i=1}^k \mathcal{U}_{\alpha_i}$.

Examples.

- $E \subseteq (X, d)$ is finite. Let $\mathcal{U}$ be an open cover of $E = \{p_1, \dots, p_n\}$. Then for each $p_j \in E$, there exists $\alpha_j \in \Lambda$ such that $p_j \in \mathcal{U}_{\alpha_j}$. Then $E \subseteq \bigcup_{j=1}^n \mathcal{U}_{\alpha_j}$.
- $E = (0, 1)$ is not compact in $(\mathbb{R}, |\cdot|)$.

  Proof. Let $\mathcal{U}_n = (\frac{1}{n+2}, \frac{1}{n})$ for $n \in \mathbb{N}^*$. Then $\mathcal{U} = \{\mathcal{U}_n\}_{n \in \mathbb{N}^*}$ is an open cover of E. However, $\mathcal{U}$ does not admit a finite subcover of E. For any finite $\{\mathcal{U}_{n_1}, \dots, \mathcal{U}_{n_k}\}$, let $n_0 = \max\{n_j : 1 \leq j \leq k\}$. Then $\bigcup \mathcal{U}_{n_j} \subseteq (\frac{1}{n_0+2}, 1)$ and thus is not a cover of E. □
- $E = [0, 1]$ is compact in $(\mathbb{R}, |\cdot|)$. In fact, all rectangles (sets of the form $[a_1, b_1] \times \cdots \times [a_n, b_n]$) are compact in $(\mathbb{R}^n, \|\cdot\|)$.

Theorem 2.10. Let $E \subseteq (\mathbb{R}^n, \|\cdot\|)$. Then the following are equivalent:

(1) E is compact.

(2) E is closed and bounded.

(3) Every infinite subset of E admits a limit point in E.

Proof. We show (1) $\implies$ (2) in a general metric space (X, d). Let $E \subseteq X$ be compact. Let $z \in E^c$. For any $y \in E$, let $\delta_y = d(y, z)/2$. Note that $B(z, \delta_y) \cap B(y, \delta_y) = \varnothing$.

Then $\mathcal{U} = \{B(y; \delta_y) : y \in E\}$ is an open cover of E. Since E is compact, $\mathcal{U}$ admits a finite subcover of E. That is, there exist $y_1, \ldots, y_k \in E$ such that $E \subseteq \bigcup_{i=1}^k B(y_i; \delta_{y_i})$. Let $\delta = \min\{\delta_{y_i}\}$. Then $B(z; \delta) \cap \bigcup_{i=1}^k B(y_i; \delta_{y_i}) = \varnothing$, so $B(z; \delta) \subseteq E^c$.

For boundedness, take the largest ball in the finite subcover of $\bigcup_{R>0} B(p; R)$ for some $p \in E$.

We show (2) $\implies$ (1) in $(\mathbb{R}^n, \|\cdot\|)$. We first show that for any $R \in \mathbb{R}$, the set $[-R, R]^n$ is compact. WLOG let $R = 1$. □

Lecture 11: Thu 25 Jan '24

Theorem 2.11. Let $\{K_\alpha\}_{\alpha \in \Lambda}$ be a collection of compact sets in (X, d) such that any non-empty finite subcollection has non-empty intersection. Then $\bigcap_{\alpha \in \Lambda} K_\alpha \neq \varnothing$.

Proof. Suppose $\bigcap_{\alpha \in \Lambda} K_\alpha = \varnothing$. No element in K_1 is in every other K_α. Let $\mathcal{U}_\alpha = K_\alpha^c$ for each α. Any point in K_1 is in at least one $\mathcal{U}_\alpha$. Then $\mathcal{U}_\alpha$ is an open cover of K_1. But since K_1 is compact, there is a finite subcover $\mathcal{U}_{\alpha_1}, \ldots, \mathcal{U}_{\alpha_n}$. But then $K_1 \subseteq (K_{\alpha_1} \cap \cdots \cap K_{\alpha_n})^c$, so $K_{\alpha_1} \cap \cdots \cap K_{\alpha_n} = \varnothing$. Contradiction. □

Theorem 2.12. Every closed subset of a compact set is compact.

Proof. Let $E \subseteq Y \subseteq (X, d)$ where Y is compact and E is closed. Let $\mathcal{U}$ be an open cover of E in X. Then $\mathcal{U} + E^c$ is an open cover of Y. Let $\mathcal{V}$ be a finite subcover of $\mathcal{U} + E^c$. Then $\mathcal{V} - E^c$ is a finite subcover of $\mathcal{U}$. This is because for any $x \in E$, $x \in \mathcal{V}$ (because $x \in Y$) but $x \notin E^c$, so $x \in \mathcal{V} - E^c$. □

Theorem 2.13. Every infinite subset of a compact set has a limit point in the compact set.

Proof. Suppose $E \subseteq (X, d)$ is compact and $F \subseteq E$ is infinite. Suppose F has no limit point in E. Then for every $z \in E$, let $B(z, \varepsilon_z)$ be a neighbourhood of z that contains no point of F (except possibly z). Then $\{B(z, \varepsilon_z)\}_{z \in E}$ is an open cover of E. However, since E is compact, there is a finite subcover. Since each $B(z, \varepsilon_z)$ contains at most one point of F, there are only finitely many points of F. Contradiction. $\square$

Proof that (3) $\implies$ (2). Suppose (3) holds on some $E \subseteq (\mathbb{R}^n, \|\cdot\|)$ but E is not bounded. Let $x_0 \in E$. We can produce a sequence $(x_n)_{n \in \mathbb{N}} \subseteq E$ such that

$$\|x_{n+1}\| > \|x_n\| + 1 \text{ for all } n \in \mathbb{N}.$$

Now suppose (3) holds on E but E is not closed. Then there exists a $z \in E^c$ such that z is a limit point of E. Then there exists a sequence $(x_n)_{n \in \mathbb{N}} \subseteq E$ such that $\|x_j - z\| < \frac{1}{j}$ for all $j \in \mathbb{N}$. The set $F = \{x_n\}_{n \in \mathbb{N}}$ is infinite (otherwise, the minimum distance is the infimum, which is zero, but $z \notin E$). Then F must have a limit point in E.

For any $y \in \mathbb{R}^n$,

$$\begin{aligned} \|x_j - y\| &\geq \|z - y\| - \|x_j - z\| \\ &\geq \|z - y\| - \frac{1}{j}. \end{aligned}$$

If $\|z - y\|$ is positive, then there are only finitely many x_j within a distance $\|z - y\|$ of y. Hence y can be a limit point of F only if $y = z$. $\square$

Theorem 2.14. Let $E \subseteq Y \subseteq (X, d)$ where Y is compact in X. Then E is compact in Y if and only if it is compact in X.

Lecture 12: Mon 29 Jan '24

2.4 Connected Sets

Definition 2.15.

(a) Let (X, d) be a metric space. A pair of sets $A, B \subseteq X$ are said to be *separated* in X if $\overline{A} \cap B = A \cap \overline{B} = \varnothing$.

(b) A set $E \subseteq X$ is said to be *disconnected* if it is the union of two separated sets in X.

(c) E is *connected* if it is not disconnected.

Examples.

- Sets $A = (-1, 0)$ and $B = (0, 1)$ are separated in $\mathbb{R}$. Note that sgn is continuous on $A \cup B$ but does not satisfy the intermediate value property.

  However, if $A = (-1, 0]$ instead, then all continuous functions on $A \cup B$ satisfy the intermediate value property.

- The empty set is connected.
- $\mathbb{Q}$ is disconnected in $\mathbb{R}$. The partition $\{\mathbb{Q} \cap (-\infty, \sqrt{2}), \mathbb{Q} \cap (\sqrt{2}, \infty)\}$ separates $\mathbb{Q}$.
- $\mathbb{Q}$ is disconnected even in $\mathbb{Q}$.

Exercise 2.16. Let $E \subseteq Y \subseteq (X, d)$. Then E is connected relative to Y iff E is cpnnected in X.

Theorem 2.17. Let $E \subseteq \mathbb{R}$. Then E is connected iff E is convex, *i.e.*, for all $x < y \in E$, $[x, y] \subseteq E$.

Proof. Suppose E is connected, but not convex, *i.e.*, there exist $x < y \in E$ and some $r \in (x, y)$ that is not in E. Then $A = (-\infty, r] \cap E$ and $B = [r, \infty) \cap E$ separate E.

Conversely, suppose E is convex but not connected. Then there exist $A, B \subseteq E$ that separate E. Let $x \in A$ and $y \in B$ and suppose WLOG that $x < y$. Note that $A \cap [x, y]$ is non-empty and bounded. Let $r = \sup(A \cap [x, y])$.

By the lemma below, $r \in \overline{A \cap [x, y]} \subseteq \overline{A} \cap [x, y]$ so $r \in \overline{A}$. Disconnectedness forces that $r \notin B \iff r \in A$ so $x \leq r < y$.

But since r is the supremum of $A \cap [x, y]$, $(r, y) \subseteq B$. This gives $r \in \overline{B}$, violating the separation of A and B. $\square$

2.5 The Cantor Set

Definition 2.18 (Perfect set)**.** A set $E \subseteq (X, d)$ is said to be *perfect* if every point of E is a limit point of E.

Note that $E = [0, 1]$ is perfect in $\mathbb{R}$. Can we produce a "sparse" perfect set? Throwing away isolated points makes the set open. Throwing away a finite number of open sets preserves perfectness, but there are still *intervals of positive length*.

Can we produce a perfect set such that

(i) it contains no intervals of positive length?

(ii) E is *nowhere dense*, *i.e.*, $(\overline{E})^\circ = \varnothing$?

Note that the second condition implies the first.

Lecture 13: Wed 31 Jan '24

Definition 2.19 (Ternary expansion)**.** Let $x \in [0, 1]$. A *ternary expansion* of x is a sequence $(d_1, d_2, \dots) \subseteq \{0, 1, 2\}$ such that

$$x = \sup\left\{ D_k = \sum_{j=1}^{k-1} \frac{d_j}{3^j} : k \geq 1 \right\}$$

which is equivalent to

$$\sum_{j=1}^{\infty} \frac{d_j}{3^j} = x$$

We write $x = 0.d_1 d_2 d_3 \dots$ to denote this.

Example. For $x = \frac{1}{3}$, we have both $x = 0.1000\dots$ and $x = 0.0222\dots$, so ternary expansions are not unique.

Let $I_0 = [0, \frac{1}{3}]$, $I_1 = [\frac{1}{3}, \frac{2}{3}]$ and $I_2 = [\frac{2}{3}, 1]$. Let $x \in [0, 1]$. Choose $d_1 = j$ such that $x \in I_j$ (in ambiguous cases, pick any one). Then

$$\begin{aligned} x &\in \left[\frac{d_1}{3}, \frac{d_1 + 1}{3}\right] \\ \implies 0 &\leq x - \frac{d_1}{3} \leq \frac{1}{3} \\ \implies D_1 &\leq x \leq D_1 + \frac{1}{3} \end{aligned}$$

	0	1	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{4}{9}$	$\frac{1}{2}$
A	$0.000\ldots$		$0.100\ldots$	$0.200\ldots$	$0.1100\ldots$	$0.111\ldots$
B		$0.222\ldots$	$0.022\ldots$	$0.122\ldots$	$0.1022\ldots$	$0.111\ldots$

Table 2.1: Scheme A vs Scheme B

Let I_{j0}, I_{j1}, I_{j2} be the subdivisions of I_j. Choose $d_2 = l$, where $x \in I_{jl}$ iff

$$\begin{aligned} x &\in \left[\frac{d_1}{3} + \frac{d_2}{9}, \frac{d_1}{3} + \frac{d_2+1}{9}\right] \\ &\implies D_2 \leq x \leq D_2 + \frac{1}{9} \end{aligned}$$

How do we break ties?

Scheme A If at the k^{th} state, $x \in [0,1)$ is an endpoint of 2 intervals, pick the right interval. This gives a unique expansion. That is, pick d_k such that $D_k \leq x < D_k + \frac{1}{3}$.

Scheme B For $x \in (0,1]$, always pick the left interval. That is, pick d_k such that $D_k < x \leq D_k + \frac{1}{3}$.

We make the following observations:

- Ambiguity only occurs at endpoints of "middle thirds".
- Say x is an endpoint of a middle third. Let k be the first stage where ambiguity occurs. Then if x is the left endpoint, scheme A gives $x = 0.d_1d_2\ldots d_{k-1}1000\ldots$ and scheme B gives $x = 0.d_1d_2\ldots d_{k-1}0222\ldots$. If x is the right endpoint, scheme A gives $x = 0.d_1d_2\ldots d_{k-1}2000\ldots$ and scheme B gives $x = 0.d_1d_2\ldots d_{k-1}1222\ldots$.

  Note that this ambiguity can be resolved by a scheme C, which picks the expansion which has no 1 starting from the point of ambiguity.

Theorem 2.20. There exists a non-empty $E \subseteq [0,1]$ such that

(i) E is compact.

(ii) $E = \{\text{limit points of } E\}$.

(iii) $E^\circ = \overline{E}^\circ = \emptyset$.

(iv) E is uncountable.

Proof.

$$E = \{x \in [0,1] : x \text{ admits at least one ternary expansion with only 0's and 2's}\}$$

We can construct this set by removing the middle thirds.

$$\begin{aligned}
E_0 &= [0,1] \\
E_1 &= E_0 \setminus \left(\frac{1}{3}, \frac{2}{3}\right) \\
&= \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right] \\
E_2 &= E_1 \setminus \left[\left(\frac{1}{9}, \frac{2}{9}\right) \cup \left(\frac{4}{9}, \frac{5}{9}\right) \cup \left(\frac{7}{9}, \frac{8}{9}\right)\right] \\
E_m &= E_{m-1} \setminus \bigcup_{k=0}^{3^{m-1}-1} \left(\frac{3k+1}{3^m}, \frac{3k+2}{3^m}\right)
\end{aligned}$$

We claim that $E = \bigcap_{m=1}^{\infty} E_m$ satisfies the conditions of the theorem. We have that E is non-empty.

Since E is the intersection of closed sets, E is closed. Since E is bounded, E is compact.

We have that $E^\circ = \varnothing$ since E does not contain any open intervals. *Formally*, we will show that for any interval (a,b), there exist k and m such that $\left(\frac{3k+1}{3^m}, \frac{3k+2}{3^m}\right)$ is contained in (a,b).

Heuristically, we see that the length of the removed intervals is $\frac{1}{3} + \frac{1}{9} + \cdots = 1$, so that the remaining set cannot contain any interval of positive length.

Uncountability is by a diagonal argument. □

Lecture 14: Thu 01 Feb '24

Chapter 3

Sequences & Series

3.1 Sequences & Subsequences

Definition 3.1. Let (X, d) be a metric space. A squence in X is a function $f\colon \mathbb{N} \to X$, more commonly written as $(f(k))_{k\in\mathbb{N}} \subseteq X$.

We say that a sequence $(x_n)_{n\in\mathbb{N}}$ *converges* in X if there exists an $x \in X$ such that for every $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that for all $n \geq N$, $d(x_n, x) < \varepsilon$. In this case, we call x a limit of $(x_n)_{n\in\mathbb{N}}$ and write

$$\lim_{k\to\infty} x_k = x \quad \text{or} \quad x_k \to x \text{ as } k \to \infty.$$

If $(x_n)_{n\in\mathbb{N}}$ does not converge, we say that it *diverges*.

Examples.

- When $(X, d) = (\mathbb{R}, |\cdot|)$, this definition reduces to the definition in UMA101.
- Let $x_n = (\frac{1}{n}, \frac{2}{n^2}) \in (\mathbb{R}^2, \|\cdot\|)$ for each $n \geq 1$.
  We claim that $\lim_{n\to\infty} x_n = (0, 0)$.

  Proof. Let $\varepsilon > 0$. Choose an $N > \frac{\sqrt{5}}{\varepsilon}$. Then for all $n \geq N$,

$$\begin{aligned}\left\|\left(\frac{1}{n}, \frac{2}{n^2}\right)\right\|^2 &= \frac{1}{n^2} + \frac{4}{n^4} \\ &\leq \frac{5}{n^2} \\ &< \varepsilon.\end{aligned}$$

□

- Let $x = \left(\frac{1}{n}, (-1)^n\right)_{n\in\mathbb{N}^*}$ with standard norm. Then $(x_n)_{n\in\mathbb{N}^*}$ diverges.

Theorem 3.2. Let (X, d) be a metric space.

(i) Let $(x_n)_{n\in\mathbb{N}} \subseteq X$. Then, $\lim_{n\to\infty} x_n = x$ iff every ε-ball centred at x contains all but finitely many terms of (x_n).

(ii) Suppose $\lim_{n\to\infty} x_n = x$ and $\lim_{n\to\infty} x_n = y$. Then $x = y$.

(iii) If $(x_n)_{n\in\mathbb{N}} \subseteq X$ converges, then $\{x_n : n \in \mathbb{N}\}$ is a bounded set in (X, d).

(iv) Let $E \subseteq X$. Then $x \in \overline{E}$ iff there exists a sequence $(x_n) \subseteq E$ such that $\lim_{n\to\infty} x_n = x$.

Proof.

(i) Let (x_n) be convergent to x. Then all terms except the first N lie inside the ε- neighborhood of x. The converse is similarly true.

(ii) Let x and y be distinct limits of (x_n). Choose $\varepsilon = \frac{d(x,y)}{2} > 0$. Then for large enough n,

$$\begin{aligned} d(x, y) &\leq d(x, x_n) + d(x_n, y) \\ &< \varepsilon + \varepsilon \\ &= d(x, y). \end{aligned}$$ □

(iii) Let (x_n) be convergent to x. Let N be such that for all $n \geq N$, $d(x_n, x) < 1$. Then $\rho = \sum_{k=0}^{N} d(x_k, x) + 1$ works as a radius for $B(x, \rho) \supseteq \{x_n : n \in \mathbb{N}\}$.

(iv) Let $x \in \overline{E}$. Then every ε-neighborhood of x intersects E. By the axiom of choice, we can choose a sequence $(x_n) \subseteq E$ such that $d(x_n, x) < \frac{1}{n}$. This converges to x.

Conversely if there exists a sequence $(x_n) \to x$ within E, then every ε-neighborhood of x intersects E.

Definition 3.3. Let $(x_n)_{n\in\mathbb{N}} \subseteq X$. Let $(n_k)_{k\in\mathbb{N}}$ be a strictly incresing sequence in $\mathbb{N}$. Then $(x_{n_k})_{k\in\mathbb{N}}$ is called a *subsequence* of (x_n).

Any limit of a subsequence of (x_n) is called a *subsequential limit* of (x_n).