Chapter One Sets, Relations and Orders

Part of this chapter is a review of some topics covered in the Mathematical Foundation course.

<u>Part 1</u>.

A, B, C, X, Y, Z, etc. — denote sets.

$\emptyset$ — denotes the empty set.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – denote the sets of positive integers, integers, rational numbers, real numbers, and complex numbers, respectively.

<u>Comparing Sets</u>. Let A, B be sets.

$A \subseteq B$: $\forall x,\ x \in A \Rightarrow x \in B$.

$A = B$: $(A \subseteq B) \wedge (B \subseteq A)$ (i.e., $\forall x,\ x \in A \Leftrightarrow x \in B$).

$A \subset B$ (or $A \subsetneqq B$): $(A \subseteq B) \wedge (B \not\subseteq A)$ (i.e., $(\forall x,\ x \in A \Rightarrow x \in B) \wedge (\exists y,\ y \in B \wedge y \notin A)$).

<u>Set Operations</u>. Let A, B be sets.

$A \cup B \ = \ \{x : x \in A \ \vee \ x \in B\}$

$A \cap B \ = \ \{x : x \in A \ \wedge \ x \in B\}$

$A - B \ = \ \{x : x \in A \ \wedge \ x \notin B\}$

$A \times B \ = \ \{(x, y) : x \in A \ \wedge \ y \in B\}$

$\mathcal{P}(A) \ = \ \{X : X \subseteq A\}$ — denotes the power of A.

For a family $\{A_i\}_{i \in I}$ of sets, we can also define $\displaystyle\bigcup_{i \in I} A_i$, $\displaystyle\bigcap_{i \in I} A_i$ and $\displaystyle\prod_{i \in I} A_i$.

<u>DeMorgan's Laws</u>. $\displaystyle A - \bigcup_{i \in I} A_i \ = \ \bigcap_{i \in I} (A - A_i), \qquad A - \bigcap_{i \in I} A_i \ = \ \bigcup_{i \in I} (A - A_i)$

<u>Relations</u>. Let A, B be sets.

Any subset of $A \times B$ is called a <u>relation</u> from A to B.

E.g., $\emptyset$, $A \times B$ are relations from A to B.

- If $R \subseteq A \times B$, then $R^{-1} \ = \ \{(b, a) \in B \times A : (a, b) \in R\}$.

- If $R \subseteq A \times B$ and $S \subseteq B \times C$, then $S \circ R \ = \ \{(a, c) \in A \times C : \exists b \in B, (a, b) \in R \wedge (b, c) \in S\}$.

Functions. Let A, B be sets.

A relation f from A to B is called a function from A to B if

(i) $\forall a \in A, \exists b \in B, (a, b) \in f$;

(ii) $(a, b) \in f \land (a, c) \in f \Rightarrow b = c$ (the vertical line test).

In this case, we write $f : A \to B$, $a \mapsto b$ or $b = f(a)$.

(So, we actually identify a function with its usual graph.)

The set A is called the domain of f.

The range of f is defined by $\text{range}(f) = \{b \in B : \exists a \in A, b = f(a)\}$.

(In fact, for any relation from A to B, we can define its domain and range.)

- If $f : A \to B$, then $f^{-1} \subseteq B \times A$ may not be a function from B to A.
- If $f : A \to B$ and $g : B \to C$, then $g \circ f : A \to C$.
- $f : A \to B$ is called onto (or surjective) if $\text{range}(f) = B$.
- $f : A \to B$ is called one-to-one (or injective) if $(a_1, b) \in f \land (a_2, b) \in f \implies a_1 = a_2$ (the horizontal line test). That is, $f(a_1) = f(a_2) \implies a_1 = a_2$ (the cancellation law), or equivalently, $a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$.
- $f : A \to B$ is called bijective if f is both surjective and injective.

Relations on A. Let $R \subseteq A \times A$. E.g., $\emptyset$, $A \times A$.

$id_A = \{(a, a) : a \in A\}$ is called the identity function of A (written as $id_A : A \to A$, $a \mapsto a$).

- We write aRb if $(a, b) \in R$, and $a \not R b$ if $(a, b) \notin R$.

Some Properties of Relations on A. Let $R \subseteq A \times A$.

(i) R is reflexive: $\forall a \in A, aRa$ (i.e., $id_A \subseteq R$).

(ii) R is symmetric: $\forall a, b \in A, aRb \Longrightarrow bRa$ (i.e., $R^{-1} = R$).

(iii) R is antisymmetric: $\forall a, b \in A, aRb \land bRa \Longrightarrow a = b$ (i.e., $R \cap R^{-1} \subseteq id_A$).

(iv) R is transitive: $\forall a, b, c \in A, aRb \land bRc \Longrightarrow aRc$ (i.e., $R \circ R \subseteq R$).

Equivalence Relations on A. If $R \subseteq A \times A$ is reflexive, symmetric and transitive, then R is called an equivalence relation on A. In this case, we write $a \sim b$ if aRb.

For $a \in A$, $[a] = \{b \in A : a \sim b\}$, called the equivalence class of a.

$A/_\sim = \{\, [a] : a \in A\}$, called the quotient of the equivalence relation.

The function $q : A \to A/_\sim$, $a \mapsto [a]$ is called the quotient map.

Examples. (Check)

1) $A \times A$ is the largest equivalence relation on A, and now $\forall a \in A$, $[a] = A$.

id_A is the smallest equivalence relation on A, and now $\forall a \in A$, $[a] = \{a\}$.

2) Let A be the set of all students in the class. For a, $b \in A$, we define $a \sim b$ if the last digits in their student IDs are the same. Then $\sim$ is an equivalence relation.

Question. How large can the quotient $A/_\sim$ be now?

3) Let $f : A \to B$. For a_1, $a_2 \in A$, define $a_1 \sim a_2$ if $f(a_1) = f(a_2)$. Then $\sim$ is an equivalence relation on A. We can prove that there exists a bijection $h : A/_\sim \to \mathrm{range}(f)$ such that $h \circ q = f$, where $q : A \to A/_\sim$ is the quotient map.

Orders on A. If $R \subseteq A \times A$ is reflexive, antisymmetric and transitive, then R is called a partial order on A. In this case, we write $a \preceq b$ if aRb, and $a \prec b$ if $a \preceq b$ but $a \neq b$.

Examples. (Check)

i) id_A is the smallest partial order on A.

Question. Is there the largest partial order on A?

ii) Let $A = \{0, 1\}$. We can prove that A has totally three partial orders and has no largest partial order.

iii) If R is both an equivalence relation and a partial order, then $R = id_A$.

iv) On the power $\mathcal{P}(A)$ of A, define $X \preceq Y$ if $X \subseteq Y$. Then $\preceq$ is a partial order on $\mathcal{P}(A)$.

A partial order $\preceq$ on A is called a linear order or total order (which is simply called order in the book) if $\forall a, b \in A$, $(a \prec b) \vee (b \prec a) \vee (a = b)$. In this case, $R \cup R^{-1} = A \times A$.

Examples. (Check)

a) id_A is not a linear order on A.

b) The usual order $\leq$ on $\mathbb{R}$ (or on $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$) is a linear order.

c) For $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, define $(x_1, y_1) \preceq (x_2, y_2)$ if $x_1 \leq x_2$ and $y_1 \leq y_2$. Then $\preceq$ is a partial order but not a linear order on $\mathbb{R}^2$.

Chapter One Sets, Relations and Orders

<u>Part 2</u>.

<u>**Smallest/Largest Elements, Minimal/Maximal Elements, Lower/Upper Bounds**</u>.

Let $(A, \preceq)$ be a partially ordered set and $a_0 \in A$.

a_0 is called the <u>smallest element</u> of A if $\forall a \in A$, $a_0 \preceq a$;

a_0 is called the <u>largest element</u> of A if $\forall a \in A$, $a \preceq a_0$.

- If the smallest/largest element exists, it must be unique. (Why?)

a_0 is called a <u>minimal element</u> of A if $\forall a \in A$, $a \preceq a_0 \implies a = a_0$;

a_0 is called a <u>maximal element</u> of A if $\forall a \in A$, $a_0 \preceq a \implies a = a_0$.

- $\exists$ smallest element $\implies \exists!$ minimal element;

  $\exists$ largest element $\implies \exists!$ maximal element.

- There may exist more than one minimal/maximal element.

Let $B \subseteq A$. $a \in A$ is called an <u>upper bound</u> of B if $\forall b \in B$, $b \preceq a$. In this case, we say that B is <u>bounded above</u> (by a). The <u>least upper bound</u> (or the <u>supremum</u>) of B is defined by

$$\text{lub}(B) = \sup(B) = \text{the smallest upper bound of } B.$$

Similarly, we can define a <u>lower bound</u> of B, and define the <u>greatest lower bound</u> (or the <u>infimum</u>) of B by $\text{glb}(B) = \inf(B) = \text{the largest lower bound of } B.$.

- $\sup(B)$ and $\inf(B)$ may not exist, and may not be in B even if they exist.

Well-ordered Sets.

A linearly ordered set A is called well-ordered if every non-empty subset of A has a smallest element.

Examples.

(i) Any finite linearly ordered set is well-ordered.

(ii) $\mathbb{Z}$ (with the usual order) is not well-ordered.

Well-Ordering Principle (WOP). $\mathbb{N}$ (with the usual order) is well-ordered.

- WOP $\iff$ PMI (Principle of Mathematical Induction).

Least-Upper-Bound Property.

A linearly ordered set A is said to have the least-upper-bound property if

$$\forall \emptyset \neq E \subseteq A,\ E \text{ is bounded above } \implies \sup(E) \text{ exists in } A.$$

Similarly, A is said to have the greatest-lower-bound property if

$$\forall \emptyset \neq E \subseteq A,\ E \text{ is bounded below } \implies \inf(E) \text{ exists in } A.$$

E.g., $\mathbb{Z}$ has the least-upper-bound property;

$\mathbb{Q}$ does not have this property (consider $\{r \in \mathbb{Q} : r^2 < 2\}$).

Theorem A. Let A be a linearly ordered set. Then

A has the least-upper-bound property $\iff$ A has the greatest-lower-bound property.

Proof. "$\Longrightarrow$". Let $\emptyset \neq E \subseteq A$ such that E is bounded below. We show that $\inf(E)$ exists.

Let L be the set of all lower bounds of E. Then $L \neq \emptyset$, and L is bounded above since $y \preceq a$ for all $y \in L$ and $a \in E$. By the assumption, $a_0 = \sup(L)$ exists in A.

Claim: $a_0 = \inf(E)$ (the greatest lower bound of E).

Since each $a \in E$ is an upper bound of L and $a_0 = \sup(L)$, $a_0 \preceq a$ for all $a \in E$. So, a_0 is a lower bond of E.

If $a_0 \prec b$, then $b \notin L$ since a_0 is an upper bound of L. Therefore, a_0 is the greatest lower bound of E; that is, $a_0 = \inf(E)$.

"$\Longleftarrow$". It can be proved similarly. ■

Completeness Axiom.

A linearly ordered set A is said to satisfy the Completeness Axiom if whenever S, T are non-empty subsets of A such that $a \preceq b$ for all $a \in S$ and $b \in T$, there exists $x \in A$ such that $a \preceq x \preceq b$ for all $a \in S$ and $b \in T$.

Theorem B. Let A be a linearly ordered set. Then

A has the least-upper-bound property $\iff$ A satisfies the Completeness Axiom.

Proof. "$\Longrightarrow$". It is easy to prove this. (Check)

"$\Longleftarrow$". See the proof of Theorem 12.1(a) in Traynor's Notes, page 35. ■

Chapter One Sets, Relations and Orders

Part 3.

Ordered Fields.

A field is a set $\mathbb{F}$ with two operations, called addition and multiplication and denoted by $(x, y) \mapsto x + y$ and $(x, y) \mapsto xy$, which satisfy the following field axioms (A), (M) and (D):

(A1) $\forall x, y \in \mathbb{F}$, $x + y \in \mathbb{F}$.

(A2) $\forall x, y \in \mathbb{F}$, $x + y = y + x$.

(A3) $\forall x, y, z \in \mathbb{F}$, $(x + y) + z = x + (y + z)$.

(A4) $\exists 0 \in \mathbb{F}$, $\forall x \in \mathbb{F}$, $0 + x = x + 0 = x$.

(A5) $\forall x \in \mathbb{F}$, $\exists (-x) \in \mathbb{F}$, $x + (-x) = (-x) + x = 0$.

(M1) $\forall x, y \in \mathbb{F}$, $xy \in \mathbb{F}$.

(M2) $\forall x, y \in \mathbb{F}$, $xy = yx$.

(M3) $\forall x, y, z \in \mathbb{F}$, $(xy)z = x(yz)$.

(M4) $\exists 1 \in \mathbb{F}$ with $1 \neq 0$, $\forall x \in \mathbb{F}$, $1x = x1 = x$.

(M5) $\forall x \in \mathbb{F}$ with $x \neq 0$, $\exists \frac{1}{x} \in \mathbb{F}$, $x\frac{1}{x} = \frac{1}{x}x = 1$.

(D) $\forall x, y, z \in \mathbb{F}$, $x(y + z) = xy + xz$.

(A2), (M2) — commutativity

(A3), (M3) — associativity

(A4), (M4) — identity

(A5), (M5) — invertible elements

(D) — distributivity

- In a field, we often use $x - y$ to denote $x + (-y)$, and use $\frac{y}{x}$ to denote $y\frac{1}{x}$.

A field $\mathbb{F}$ is called an ordered field if $\mathbb{F}$ is also a linearly ordered set such that

(i) $\forall x, y, z \in \mathbb{F}$, $y \prec z \implies x + y \prec x + z$;

(ii) $\forall x, y \in \mathbb{F}$, $(x \succ 0) \wedge (y \succ 0) \implies xy \succ 0$.

- (i) is equivalent to "$y \prec z \implies y - x \prec z - x$";

  (ii) is equivalent to "$(x \succ 0) \wedge (y \succ z) \implies xy \succ xz$".

The Ordered Fields $\mathbb{Q}$ and $\mathbb{R}$.

It is easy to see that $\mathbb{Q}$ is an ordered field.

As we know, $\mathbb{Q}$ does not have the least-upper-bound property. The theorem below shows that $\mathbb{Q}$ can be "extended" to an ordered field $\mathbb{R}$ such that $\mathbb{R}$ has the least-upper-bound property.

Theorem C. There exists an ordered field $\mathbb{R}$, called the real field, which has the least-upper-bound property and contains $\mathbb{Q}$ as a subfield.

That is, $\mathbb{Q} \subseteq \mathbb{R}$ and the inclusion map $i : \mathbb{Q} \to \mathbb{R}$, $r \mapsto r$ preserves the field operations and order, called an ordered field homomorphism.

Proof. See Appendix on pages 17 - 21 in the book. ■

- Using WOP and the fact that $\mathbb{R}$ has the least-upper-bound property, we can prove that $\mathbb{Q}$ is dense in $\mathbb{R}$ (see Traynor's Notes, page 37).

Some Properties on Supremum and Infimum in Linearly Ordered Sets.

Let S be a linearly ordered set. In the following, A and B are non-empty subsets of S, and we assume that all sup and inf exist.

Recall: $c = \sup(A)$ if and only if $(\forall a \in A, a \preceq c)$ and $[\forall u \in S, (\forall a \in A, a \preceq u) \implies c \preceq u]$.

$d = \inf(A)$ if and only if $(\forall a \in A, d \preceq a)$ and $[\forall \ell \in S, (\forall a \in A, \ell \preceq a) \implies \ell \preceq d]$.

- In $\mathbb{R}$, $c = \sup(A)$ if and only if $\underline{(\forall a \in A, a \leq c) \text{ and } (\forall \varepsilon > 0, \exists\, a_0 \in A, c - \varepsilon < a_0)}$.

  $d = \inf(A)$ if and only if $\underline{(\forall a \in A, d \leq a) \text{ and } (\forall \varepsilon > 0, \exists\, a_0 \in A, a_0 < d + \varepsilon)}$.

- **(i)** $\inf(A) \preceq \sup(A)$.

  (ii) If $A \subseteq B$, then $\sup(A) \preceq \sup(B)$ and $\inf(B) \preceq \inf(A)$.

  (iii) $\sup(A \cup B) = \max\{\sup(A), \sup(B)\}$ and $\inf(A \cup B) = \min\{\inf(A), \inf(B)\}$.

Chapter One Sets, Relations and Orders

Part 4.

Supremum and Infimum operations on $\mathbb{R}$.

For A, $B \subseteq \mathbb{R}$ and $c \in \mathbb{R}$, $A+B \subseteq \mathbb{R}$ and $cA \subseteq \mathbb{R}$ are defined by

$$A+B = \{a+b : a \in A, b \in B\} \quad \text{and} \quad cA = \{ca : a \in A\}.$$

Fact. If $a, b \in \mathbb{R}$ and $\forall \varepsilon > 0$, $a \leq b + \varepsilon$, then $a \leq b$.

Property 1. $\sup(A+B) = \sup(A) + \sup(B)$, $\quad \inf(A+B) = \inf(A) + \inf(B)$.

Proof. $\forall a \in A$ and $b \in B$, $a \leq \sup(A)$ and $b \leq \sup(B)$, and thus $a + b \leq \sup(A) + \sup(B)$. So, $\sup(A)+\sup(B)$ is an upper bound of $A+B$. Therefore, $\underline{\sup(A+B) \leq \sup(A) + \sup(B)}$.

Conversely, $\forall \varepsilon > 0$, $\exists a_0 \in A$ and $b_0 \in B$ such that

$$\sup(A) - \varepsilon < a_0 \ \text{ and } \ \sup(B) - \varepsilon < b_0.$$

Thus $\sup(A) + \sup(B) - 2\varepsilon < a_0 + b_0 \leq \sup(A+B)$. Hence,

$$\forall \varepsilon > 0, \sup(A) + \sup(B) < \sup(A+B) + 2\varepsilon.$$

Since $\varepsilon > 0$ is arbitrary, by the Fact, we have $\underline{\sup(A) + \sup(B) \leq \sup(A+B)}$.

Therefore, we have $\sup(A+B) = \sup(A) + \sup(B)$.

Similarly, we can prove that $\inf(A+B) = \inf(A) + \inf(B)$. ∎

Property 2. If $c > 0$, then $\sup(cA) = c\sup(A)$ and $\inf(cA) = c\inf(A)$.

Proof. $\forall a \in A$, $a \leq \sup(A)$ and hence $ca \leq c\sup(A)$ (since $c > 0$). Thus $c\sup(A)$ is an upper bound of cA. So, $\underline{\sup(cA) \leq c\sup(A)}$. Replacing A by cA and c by $\frac{1}{c}$, we have

$$\sup(A) = \sup\left(\tfrac{1}{c}(cA)\right) \leq \tfrac{1}{c}\sup(cA);$$

that is, $\underline{c\sup(A) \leq \sup(cA)}$. Therefore, we have $\sup(cA) = c\sup(A)$.

Similarly, we can prove that $\inf(cA) = c\inf(A)$. ∎

Property 3. $\sup(-A) = -\inf(A)$ and $\inf(-A) = -\sup(A)$.

Proof. $\forall a \in A$, $a \geq \inf(A)$, i.e., $-a \leq -\inf(A)$. Thus $-\inf(A)$ is an upper bound of $-A$, and hence $\underline{\sup(-A) \leq -\inf(A)}$.

Conversely, $\forall a \in A$, $-a \leq \sup(-A)$, i.e., $a \geq -\sup(-A)$. Thus $-\sup(-A)$ is a lower bound of A, and hence $-\sup(-A) \leq \inf(A)$, or $\underline{\sup(-A) \geq -\inf(A)}$.

Therefore, we have $\sup(-A) = -\inf(A)$.

Replacing A by $-A$, we also get $\inf(-A) = -\sup(A)$. ∎

Property 4. If $c < 0$, then $\sup(cA) = c\inf(A)$ and $\inf(cA) = c\sup(A)$.

Proof. Let $d = -c$. Then $d > 0$ and $c = -d$. By Properties 2 and 3, we have

$$\sup(cA) = \sup(-dA) = -\inf(dA) = -d\inf(A) = c\inf(A)$$

and $\inf(cA) = \inf(-dA) = -\sup(dA) = -d\sup(A) = c\sup(A)$. ∎

Supremum and Infimum of Real Valued Functions.

For a function $f : X \to \mathbb{R}$, let

$$\sup_{x\in X} f(x) = \sup\{f(x) : x \in X\} \quad \text{and} \quad \inf_{x\in X} f(x) = \inf\{f(x) : x \in X\}.$$

Note that if $f, g : X \to \mathbb{R}$, then

$$\{f(x) + g(x) : x \in X\} \subseteq \{f(x) : x \in X\} + \{g(x) : x \in X\},$$

and the equality may not hold. (Example?)

<u>Property 5</u>. Let X be a set and let $f,\, g : X \to \mathbb{R}$. Then

(i) $\sup\limits_{x\in X}\big(f(x)+g(x)\big) \;\le\; \sup\limits_{x\in X} f(x) \;+\; \sup\limits_{x\in X} g(x).$

(ii) $\inf\limits_{x\in X}\big(f(x)+g(x)\big) \;\ge\; \inf\limits_{x\in X} f(x) \;+\; \inf\limits_{x\in X} g(x).$

In both (i) and (ii), the strict inequalities can hold.

<u>*Proof*</u>. **(i)** Let $a = \sup\limits_{x\in X} f(x)$ and $b = \sup\limits_{x\in X} g(x)$. Then $\forall x \in X$, $f(x) \le a$ and $g(x) \le b$, and hence $f(x)+g(x) \le a+b$. Therefore, $\sup\limits_{x\in X}\big(f(x)+g(x)\big) \le a+b = \sup\limits_{x\in X} f(x) \;+\; \sup\limits_{x\in X} g(x)$.

(ii) It can be proved similarly.

Let $f,\, g : [0.1] \to \mathbb{R}$ be given by $f(x) = x$ and $g(x) = -x$. Then

$$\sup_{x\in[0.1]}\big(f(x)+g(x)\big) \;=\; \inf_{x\in[0.1]}\big(f(x)+g(x)\big) \;=\; 0,$$

$$\sup_{x\in[0.1]} f(x) \;=\; 1, \quad \inf_{x\in[0.1]} f(x) \;=\; 0, \quad \sup_{x\in[0.1]} g(x) \;=\; 0, \;\text{ and }\; \inf_{x\in[0.1]} g(x) \;=\; -1.$$

In this case, we have the strict inequalities in (i) and (ii). ■

Chapter Two Basic Topology

We will cover the first three parts of this chapter in the book.

Part 1: Finite, Countable and Uncountable Sets

Definition 1. Let A and B be sets. If $\exists$ a bijection $h : A \to B$, then we say that A and B have the same cardinal number (or the same cardinality), and we write $A \sim B$ (or $\text{card}(A) = \text{card}(B)$, or $|A| = |B|$).

- "$\sim$" is an equivalence relation on any family of sets:

  (i) $A \overset{id_A}{\sim} A$;

  (ii) $A \overset{h}{\sim} B \implies B \overset{h^{-1}}{\sim} A$;

  (iii) $(A \overset{h}{\sim} B) \wedge (B \overset{g}{\sim} C) \implies A \overset{g \circ h}{\sim} C$.

For $n \in \mathbb{N}$, we let $\mathbb{N}_n = \{1, \cdots, n\}$. E.g., $\mathbb{N}_3 = \{1, 2, 3\}$

Definition 2. We say that

1) A is finite if $A = \emptyset$ or $A \sim \mathbb{N}_n$ for some $n \in \mathbb{N}$;
2) A is infinite if A is not finite;
3) A is countable if $A \sim \mathbb{N}$;
4) A is at most countable if A is either finite or countable;
5) A is uncountable if A is neither finite nor countable.

Examples. **(i)** $A = \{m \in \mathbb{Z} : m^2 < 10\} = \{0, \pm 1, \pm 2, \pm 3\}$ is a finite set.

(ii) $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all infinite sets.

(iii) $\mathbb{N} \subsetneqq \mathbb{Z}$, but $\mathbb{Z} \sim \mathbb{N}$ and hence $\mathbb{Z}$ is countable. E.g., the following $\mathbb{N} \to \mathbb{Z}$ is a bijection:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & \cdots \end{array}$$

Let X be a set. By a sequence in X, we mean a function $f : \mathbb{N} \to X$.

In this case, we use $\{x_n\}$ or (x_n) for f, where $x_n = f(n)$, called the n^{th} term $(n = 1, 2, \cdots)$.

When f is one-to-one, $\{x_n\}$ is called a sequence with distinct terms.

Relations Between Sequences and Countable Sets.

$\{x_n\}$ is a sequence with distinct terms $\implies$ $A = \{x_n : n \in \mathbb{N}\}$ is a countable set.

Conversely, A is countable $\implies$ $\exists$ a bijection $h : \mathbb{N} \to A$

$\implies$ A is given by a sequence with distinct terms ($A = \{x_n : n \in \mathbb{N}\}$ with $x_n = h(n)$).

- Therefore, when the set X is given, we get a one-to-one correspondence

$$\{\text{ all countable subsets of } X\,\} \longleftrightarrow \{\text{ all sequences with distinct terms in } X\,\}.$$

Theorem 1 (Theorem 2.8). Let A be a countable set and let E be an infinite subset of A. Then E is also countable.

$E \subseteq \mathbb{Z}$

Proof. Write elements of A as a sequence of distinct terms: $x_1, x_2, x_3, \cdots$.

Let n_1 be the smallest $m \in \mathbb{N}$ such that $x_m \in E$. Then $\{m \in \mathbb{N} : m > n_1 \text{ and } x_m \in E\} \neq \emptyset$ since E is infinite. Let n_2 be the smallest element of the above set. Inductively, we can get $n_1 < n_2 < n_3 < \cdots$ such that $E = \{x_{n_1}.x_{n_2}, x_{n_3}, \cdots\}$; that is, $\mathbb{N} \sim E$ via $k \mapsto x_{n_k}$.

Therefore, E is countable. ■

Definition 3. We define

$\text{card}(A) \leq \text{card}(B)$ if $\exists$ an injection $A \to B$,

and $\text{card}(A) < \text{card}(B)$ if $\text{card}(A) \leq \text{card}(B)$ but $\text{card}(A) \neq \text{card}(B)$.

Fact 1. $A \subseteq B \implies \text{card}(A) \leq \text{card}(B)$.

Fact 2. If $A \neq \emptyset$, then $\text{card}(A) \leq \text{card}(B) \iff \exists$ a surjection $B \to A$. (Proof?)

The theorem below is very powerful for proving $\text{card}(A) = \text{card}(B)$.

Cantor-Bernstein Theorem. Let A and B be sets such that $\text{card}(A) \leq \text{card}(B)$ and $\text{card}(B) \leq \text{card}(A)$. Then $\text{card}(A) = \text{card}(B)$. $\to$ Easier than finding bijection

Proofs of this theorem can be seen from internet (e.g., www.youtube.com/watch?v=IkoKttTDuxE).

We use $\aleph_0$ (aleph zero) to denote card$(\mathbb{N})$.

- We can prove the following:

  1) A is finite $\iff$ card$(A) < \aleph_0$;

  2) A is infinite $\iff$ card$(A) \geq \aleph_0$;

  3) A is countable $\iff$ card$(A) = \aleph_0$;

  4) A is at most countable $\iff$ card$(A) \leq \aleph_0$;

  5) A is uncountable $\iff$ card$(A) > \aleph_0$.

Therefore, $\aleph_0$ is the smallest infinite cardinal number.

Theorem 2 (Theorem 2.12). Let $\{E_n\}$ be a sequence of countable sets and let $S = \bigcup_{n=1}^{\infty} E_n$. Then S is countable.

Proof. Since $E_1 \subseteq S$, we have card$(S) \geq$ card$(E_1) = \aleph_0$ by Fact 1. We only need show that card$(S) \leq \aleph_0$ due to Cantor-Bernstein Theorem. We write

$$\begin{array}{ll} E_1\colon & x_{11},\ x_{12},\ x_{13},\ x_{14},\ \cdots \\ E_2\colon & x_{21},\ x_{22},\ x_{23},\ x_{24},\ \cdots \\ E_3\colon & x_{31},\ x_{32},\ x_{33},\ x_{34},\ \cdots \\ E_4\colon & x_{41},\ x_{42},\ x_{43},\ x_{44},\ \cdots \\ & \cdots \qquad \cdots \end{array}$$

Then we can list elements of S as

$$\underbrace{x_{11}},\ \underbrace{x_{21},\ x_{12}},\ \underbrace{x_{31},\ x_{22},\ x_{13}},\ \underbrace{x_{41},\ x_{32},\ x_{23},\ x_{14}},\ \cdots,$$

where we can have $x_{ij} = x_{mn}$. In this way, S is the range of a sequence (i.e., $\exists$ a surjection $\mathbb{N} \to S$). Therefore, by Fact 2, we get card$(S) \leq \aleph_0$. $\blacksquare$

Corollary 1. If A and B are countable sets, then $A \times B$ is countable. (Proof?)

Fact 3. For any at most countable set E, there exists a countable set E' such that $E \subseteq E'$.

Corollary 2. Let A be a set that is at most countable. Suppose for each $a \in A$, B_a is an at most countable set. Then $S = \bigcup_{a \in A} B_a$ is at most countable.

Proof. By Fact 3, $\exists$ a countable set A' such that $A \subseteq A'$. For each $\gamma \in A'$, choose a countable set C_γ such that $B_\gamma \subseteq C_\gamma$ when $\gamma \in A$. Let $T = \bigcup_{\gamma \in A'} C_\gamma$. Then $S \subseteq T$, and T is countable by Theorem 2. So, $\text{card}(S) \leq \text{card}(T) = \aleph_0$. Therefore, S is at most countable. ■

Corollary 3. If $A_1, \cdots, A_n$ are countable sets, then $A = A_1 \times \cdots \times A_n$ is countable, where $A_1 \times \cdots \times A_n = \{(a_1, \cdots, a_n) : a_1 \in A_1, \cdots, a_n \in A_n\}$.

Proof. We use PMI to this corollary. First, the assertion is true when $n = 1$.

Assume that $A_1 \times \cdots \times A_{n-1}$ is countable.

Then by Corollary 1, we have $A = (A_1 \times \cdots \times A_{n-1}) \times A_n$ is countable. ■.

Corollary 4. The set $\mathbb{Q}$ of rational numbers is countable.

Proof. For each $r \in \mathbb{Q}$, write $r = \frac{p_r}{q_r}$, where $p_r, q_r \in \mathbb{Z}$ and $q_r \neq 0$. Then $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$, $f(r) = (p_r, q_r)$, is injective. Thus $\text{card}(\mathbb{Q}) \leq \text{card}(\mathbb{Z} \times \mathbb{Z}) = \aleph_0$ (by Corollary 1).

On the other hand, since $\mathbb{N} \subseteq \mathbb{Q}$, we have $\text{card}(\mathbb{Q}) \geq \aleph_0$.

Therefore, $\text{card}(\mathbb{Q}) = \aleph_0$; that is $\mathbb{Q}$ is countable. ■

Theorem 3 (Theorem 2.14). Let A be the set of all sequences $\{x_n\}$ such that x_n is either 0 or 1 (i.e., A is the set of all functions $\mathbb{N} \to \{0, 1\}$). Then A is uncountable.

Proof. Clearly, A is infinite. Assume that A is countable. Then elements of A can be listed as $s_1, s_2, s_3, \cdots$. Write

$$
\begin{array}{ll}
s_1: & x_{11}, x_{12}, x_{13}, x_{14}, \cdots \\
s_2: & x_{21}, x_{22}, x_{23}, x_{24}, \cdots \\
s_3: & x_{31}, x_{32}, x_{33}, x_{34}, \cdots \\
s_4: & x_{41}, x_{42}, x_{43}, x_{44}, \cdots \\
 & \cdots \quad \cdots
\end{array}
$$

For $n \in \mathbb{N}$, let $x_n = \begin{cases} 0 & x_{nn} = 1, \\ 1 & x_{nn} = 0. \end{cases}$ Then $s = \{x_n\} \in A$ but $\forall n$, $s \neq s_n$, a contradiction.

Therefore, A is uncountable. ■

The above idea of proof was first used by Cantor and is called Cantor's diagonal process. Using this process, we can prove that the interval $(0,1)$ is uncountable.

Fact 4. The interval $(0,1)$ is uncountable, and hence $\mathbb{R}$ is uncountable.

Proof. First we note that each $x \in (0,1)$ can be expressed uniquely as $x = 0.t_1t_2\cdots$, where $t_i \in \{0,1,2,\cdots 9\}$ and there are infinitely many $t_i \neq 0$. E.g., 0.25 is expressed as $0.24999\cdots$.

Clearly, $(0,1)$ is infinite. Assume that $(0,1)$ is countable. Then elements of $(0,1)$ can be listed as $x_1,\ x_2,\ x_3,\ \cdots$. We Write

$$\begin{aligned}
x_1 &= 0.\,t_1^1\,t_2^1\,t_3^1\,t_4^1\ \cdots \\
x_2 &= 0.\,t_1^2\,t_2^2\,t_3^2\,t_4^2\ \cdots \\
x_3 &= 0.\,t_1^3\,t_2^3\,t_3^3\,t_4^3\ \cdots \\
x_4 &= 0.\,t_1^4\,t_2^4\,t_3^4\,t_4^4\ \cdots \\
\cdots & \quad \cdots
\end{aligned}$$

For $n \in \mathbb{N}$, let $q_n = \begin{cases} 2 & \text{if } t_n^n = 1, \\ 1 & \text{if } t_n^n \neq 1. \end{cases}$ Then $x = 0.\,q_1\,q_2\,q_3\ \cdots \in (0,1)$ but $\forall n,\ x \neq x_n$, a contradiction. Therefore, $(0,1)$ is uncountable.

Since $(0,1) \subseteq \mathbb{R}$, we have that $\mathbb{R}$ is also uncountable. ■

Chapter Two Basic Topology

Part 2: Metric Spaces

In mathematics, space = set + structure(s).

Definition 4. Let X be a set. A function $d : X \times X \to [0, \infty)$ is called a metric (or distance) on X if

i) $\forall x, y \in X$, $d(x, y) = 0 \iff x = y$;

ii) $\forall x, y \in X$, $d(x, y) = d(y, x)$;

iii) $\forall x, y, z \in X$, $d(x, z) \leq d(x, y) + d(y, z)$. (Triangle inequality)

In this case, (X, d) is called a metric space.

Examples. **(1)** For $x, y \in \mathbb{R}$, $d(x, y) = |x - y|$ defines a metric on $\mathbb{R}$.

More general, for $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n) \in \mathbb{R}^n$, $d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$ is a metric on $\mathbb{R}^n$. With is metric, $\mathbb{R}^n$ is called the n-dimensional Euclidean space.

(2) Similarly, $d(x, y) = |x - y|$ defines a metric on $\mathbb{C}$.

(3) On the set $\mathbb{R}^n$ $(n > 1)$, the following are other distance functions which are all "equivalent to" the Euclidean metric d:

$$\text{for } 1 \leq p < \infty,\ d_p(x, y) = \Big(\sum_{i=1}^{n} |x_i - y_i|^p \Big)^{1/p}; \quad d_\infty(x, y) = \max_{1 \leq i \leq n} |x_i - y_i|.$$

It is clear that the Euclidean metric in (1) is just d_2.

(4) Let X be a set. Define $d : X \times X \to [0, \infty)$ by $d(x, y) = \begin{cases} 1 & \text{if } x \neq y, \\ 0 & \text{if } x = y. \end{cases}$ Then d is a metric on X, and (X, d) is called a discrete metric space.

(5) Let (X, d) be a metric space and $Y \subseteq X$. Let d_Y be the restriction of d to $Y \times Y$ (i.e., $d_Y(y_1, y_2) = d(y_1, y_2)$ for all $y_1, y_2 \in Y$). Then d_Y is a metric on Y, and Y with this metric is called a subspace of X.

Some Concepts on Metric Spaces.

Let (X, d) be a metric space, $x \in X$, and $r > 0$.

(i) Define $B(x, r) = \{y \in X : d(x, y) < r\}$, called the open ball centred at x with radius r, or the r-neighborhood of x.

E.g., in $\mathbb{R}$, $B(x, r) = (x - r, x + r)$.

A general neighborhood of x is a subset U of X such that $B(x, r) \subseteq U$ for some $r > 0$.

E.g., in $\mathbb{R}$, $[x - r, x + r)$, $[x - r, x + 2r]$, etc. are all neighborhoods of x.

Exercise. For $p = 1, 2, \infty$, on $(\mathbb{R}^2, d_p)$, compare the sets $B\big((0,0), 1\big)$.

(ii) A subset G of X is called open if $\forall x \in G$, $\exists r > 0$, $B(x, r) \subseteq G$.

E.g., in $\mathbb{R}$, the interval $(0, 1)$ is open, but the interval $[0, 1)$ is not open.

$\emptyset$ and X are open in X.

(iii) Let $E \subseteq X$. x is called a limit point of E (or, cluster point, or accumulation point) if $\forall r > 0$, $B(x, r) \cap E$ contains $y \neq x$ (that is, $\big(B(x, r) - \{x\}\big) \cap E \neq \emptyset$).

We let E' = the set of all limit points of E.

E.g., in $\mathbb{R}$, 0 is a limit point of $E = (0, 1)$ though 0 is not in $(0, 1)$. In this case, $E' = [0, 1]$. Also in $\mathbb{R}$, if $E = \{0, 1\}$, then $E' = \emptyset$.

(iv) A subset E of X is called closed if $E' \subseteq E$.

E.g., in $\mathbb{R}$, the set $\{0, 1\}$ is closed but $(0, 1)$ is not closed.

$\emptyset$ and X are closed in X.

Theorem 4 (Theorem 2.19). Let (X, d) be a metric space, $x \in X$ and $r > 0$. Then $B(x, r)$ is open in X.

Proof. Let $y \in B(x, r)$. We need find $\varepsilon > 0$ such that $B(y, \varepsilon) \subseteq B(x, r)$.

Let $\varepsilon = r - d(x, y)$. Then $\varepsilon > 0$ since $y \in B(x, r)$. Now $\forall z \in B(y, \varepsilon)$, we have

$$d(z, x) \leq d(z, y) + d(y, x) < \varepsilon + d(y, x) = r,$$

and thus $z \in B(x, r)$. Therefore, $B(y, \varepsilon) \subseteq B(x, r)$. Hence, $B(x, r)$ is open. ∎

Theorem 5 (Theorem 2.23). Let E be a subset of a metric space (X, d). Then

(i) E is open $\iff$ $X - E$ is closed;

(ii) E is closed $\iff$ $X - E$ is open.

Proof. **(i)** "$\Longrightarrow$". Suppose E is open. We need prove that $(X - E)' \subseteq X - E$.

Let $x \in (X - E)'$. Then $\forall r > 0$, $\big(B(x, r) - \{x\}\big) \cap (X - E) \neq \emptyset$, which is equivalent to $B(x, r) - \{x\} \nsubseteq E$. So, $\forall r > 0$, $B(x, r) \nsubseteq E$, and thus $x \in E$ (since E is open). That is, $x \in X - E$. Therefore, we obtain that $(X - E)' \subseteq X - E$, and hence $X - E$ is closed.

"$\Longleftarrow$". Suppose $X - E$ is closed. We need prove that $\forall x \in E$, $\exists r_0 > 0$, $B(x, r_0) \subseteq E$.

Let $x \in E$. Then $x \notin (X - E)'$, since $(X - E)' \subseteq X - E$. Thus $\exists r_0 > 0$ such that $\big(B(x, r_0) - \{x\}\big) \cap (X - E) = \emptyset$; that is, $B(x, r_0) - \{x\} \subseteq E$. Since $x \in E$, $B(x, r_0) \subseteq E$. Therefore, we prove that E is open.

(ii) Replacing E by $X - E$ in (i), we get $X - E$ is open $\iff$ $X - (X - E) = E$ closed. ■

In a metric space (X, d), the "closed" ball centred at x with radius r is defined by

$$B[x, r] = \{y \in X : d(x, y) \leq r\}.$$

Corollary 5. $B[x, r]$ is closed.

Proof. By Theorem 5, we only need prove that $X - B[x, r]$ is open.

Let $z \in X - B[x, r]$. Then $d(z, x) > r$. Let $\varepsilon = d(z, x) - r$. Then $r > 0$. We prove below that $B(z, \varepsilon) \subseteq X - B[x, r]$.

Let $y \in B(z, \varepsilon)$. Then $d(y, z) < \varepsilon = d(z, x) - r$, or $d(z, x) - d(y, z) > r$. Since

$$d(z, x) \leq d(z, y) + d(y, x),$$

we obtain that

$$d(y, x) \geq d(z, x) - d(z, y) > r.$$

Hence, $y \in X - B[x, r]$. Therefore, we have $B(z, \varepsilon) \subseteq X - B[x, r]$.

Therefore, we prove that $X - B[x, r]$ is open. ■

Theorem 6 (Theorem 2.24). Let (X, d) be a metric space.

(i) If $\{G_\alpha\}$ is a family of open sets in X, then $\bigcup_\alpha G_\alpha$ is open in X.

(ii) If $G_1, \cdots, G_n$ are open sets in X, then $\bigcap_{i=1}^n G_i$ is open in X.

Remark 1. The above (i) and (ii) together with "$\emptyset$, X are open" are used as the definition of a topology on X.

Proof. **(i)** Let $x \in \bigcup_\alpha G_\alpha$. Then $x \in G_{\alpha_0}$ for some α_0. Since G_{α_0} is open, $\exists r > 0$ such that $B(x, r) \subseteq G_{\alpha_0} \subseteq \bigcup_\alpha G_\alpha$. Therefore, we obtain that $\bigcup_\alpha G_\alpha$ is open.

(ii) Let $x \in \bigcap_{i=1}^n G_i$. Then for each $1 \le i \le n$, $\exists r_i > 0$ such that $B(x, r_i) \subseteq G_i$. Let $r = \min\{r_1, \cdots, r_n\}$. Then $r > 0$ and $B(x, r) \subseteq G_i$ for all $1 \le i \le n$. Hence, $B(x, r) \subseteq \bigcap_{i=1}^n G_i$. Therefore, we prove that $\bigcap_{i=1}^n G_i$ is open. ∎

By Theorems 5 and 6 together with DeMorgan's Laws, we have the following corollary on closed sets.

Corollary 6. Let (X, d) be a metric space.

(i) If $\{F_\alpha\}$ is a family of closed sets in X, then $\bigcap_\alpha F_\alpha$ is closed in X.

(ii) If $F_1, \cdots, F_n$ are closed sets in X, then $\bigcup_{i=1}^n F_i$ is closed in X.

Note that $\emptyset$ and X are both open and closed (called clopen). Therefore, $\emptyset$ is the smallest open set and X is the largest open set, and $\emptyset$ is the smallest closed set and X is the largest closed set.

Question. For any $\emptyset \subseteq E \subseteq X$, does E have the largest open/closed subset, and does E have the smallest open/closed superset?

E.g., $(0,1)$ does not have largest closed subset; $[0,1]$ does not have smallest open superset.

<u>Definition 5</u>. Let $E \subseteq X$. The <u>closure</u> of E is the set $\overline{E} = E \cup E'$.

An element x of X is called an <u>interior point</u> of E if $\exists r > 0$, $B(x,r) \subseteq E$. The <u>interior</u> of E is the set E° of all interior points of E.

- By definition, we have $\underline{E^\circ \subseteq E \subseteq \overline{E}}$.

<u>Characterizations of Closure and Closed Sets</u>.

Comparing with $x \in E' \iff \forall r > 0, \big(B(x,r) - \{x\}\big) \cap E \neq \emptyset$ (definition), we have

(I) $x \in \overline{E} \iff \forall r > 0, B(x,r) \cap E \neq \emptyset$.

<u>*Proof*</u>. Since $\overline{E} = E \cup E'$, we have $x \in \overline{E} \implies \forall r > 0, B(x,r) \cap E \neq \emptyset$.

Conversely, suppose that $\forall r > 0$, $B(x,r) \cap E \neq \emptyset$. If $x \in E$, then $x \in \overline{E}$; if $x \notin E$, then $\forall r > 0$, $\big(B(x,r) - \{x\}\big) \cap E = B(x,r) \cap E \neq \emptyset$, that is, $x \in E' \subseteq \overline{E}$. So, in both cases, we have $x \in \overline{E}$. $\blacksquare$

(II) $\overline{E}$ is always closed.

<u>*Proof*</u>. To prove that $\overline{E}$ is closed, we need show that $\overline{E}' \subseteq \overline{E}$.

Let $x \in \overline{E}'$. Then $\forall r > 0$, $\big(B(x,r) - \{x\}\big) \cap \overline{E} \neq \emptyset$.

Assume that $x \notin \overline{E}$. Then, by (I), $\exists r_0 > 0$ such that $B(x,r_0) \cap E = \emptyset$. Since $B(x,r_0)$ is open, we have $B(x,r_0) \cap E' = \emptyset$. It follows that

$$B(x,r_0) \cap \overline{E} = B(x,r_0) \cap (E \cup E') = \big(B(x,r_0) \cap E\big) \cup \big(B(x,r_0) \cap E'\big) = \emptyset,$$

contradicting to $\big(B(x,r_0) - \{x\}\big) \cap \overline{E} \neq \emptyset$. Therefore, $x \in \overline{E}$. Hence, we have $\overline{E}' \subseteq \overline{E}$. $\blacksquare$

(III) $\overline{E} = \bigcap\{F : E \subseteq F \subseteq X \text{ and } F \text{ is closed}\}$, and hence $\overline{E}$ is the smallest closed set in X containing E.

<u>*Proof*</u>. Since $\overline{E}$ is closed, we have that $\bigcap\{F : E \subseteq F \subseteq X \text{ and } F \text{ is closed}\} \subseteq \overline{E}$.

Conversely, if $E \subseteq F \subseteq X$ and F is closed, then by (I), $\overline{E} \subseteq \overline{F} = F$. Hence, we have

$$\overline{E} \subseteq \bigcap\{F : E \subseteq F \subseteq X \text{ and } F \text{ is closed}\}.$$

Therefore, $\overline{E} = \bigcap\{F : E \subseteq F \subseteq X \text{ and } F \text{ is closed}\}$, and $\overline{E}$ is the smallest closed set in X containing E. $\blacksquare$

By (II) and the definition of closure, we have the following

(IV) E is closed $\iff E = \overline{E} \iff \overline{E} \subseteq E$.

Theorem 7 (Theorem 2.28). Let $E \subseteq \mathbb{R}$ be non-empty and bounded above. Then we have $\sup(E) \in \overline{E}$. Similarly, if $E \subseteq \mathbb{R}$ is non-empty and bounded below, then $\inf(E) \in \overline{E}$.

Proof. Let $y = \sup(E)$. To get $y \in \overline{E}$, we need show that

$$\forall \varepsilon > 0, \ B(y, \varepsilon) \cap E \ = \ (y - \varepsilon, y + \varepsilon) \cap E \ \neq \ \emptyset.$$

Let $\varepsilon > 0$. Then $\exists x \in E$, $y - \varepsilon < x$. On the other hand, we have $x \leq y < y + \varepsilon$. Therefore, $x \in (y - \varepsilon, y + \varepsilon) \cap E$, and hence $(y - \varepsilon, y + \varepsilon) \cap E \neq \emptyset$. ■

Characterizations of Interior and Open Sets.

Parallel to the results on the closure $\overline{E}$ and closed sets, we have the followings on the interior E° and open sets.

(V) $E^\circ \ = \bigcup \{G : G \subseteq E \text{ and } G \text{ is open}\}$, and hence E° is the largest open subset of E.

(VI) E is open $\iff E = E^\circ \iff E \subseteq E^\circ$.

Definition 6. Let X be a metric space, $E \subseteq X$ and $x \in X$. x is called a boundary point of E if $\forall r > 0$, $B(x, r) \cap E \neq \emptyset$ and $B(x, r) \cap (X - E) \neq \emptyset$. We use ∂E to denote the set of all boundary points of E, called the boundary of E.

By (I), we have

(VII) $\partial E \ = \ \overline{E} \cap \overline{(X - E)}$. Therefore, ∂E is closed.

(VIII) $\overline{E} \ = \ E \cup \partial E$.

By the definition of E° and ∂E, we have

(IX) $E^\circ \ = \ E - \partial E \ = \ \overline{E} - \partial E$.