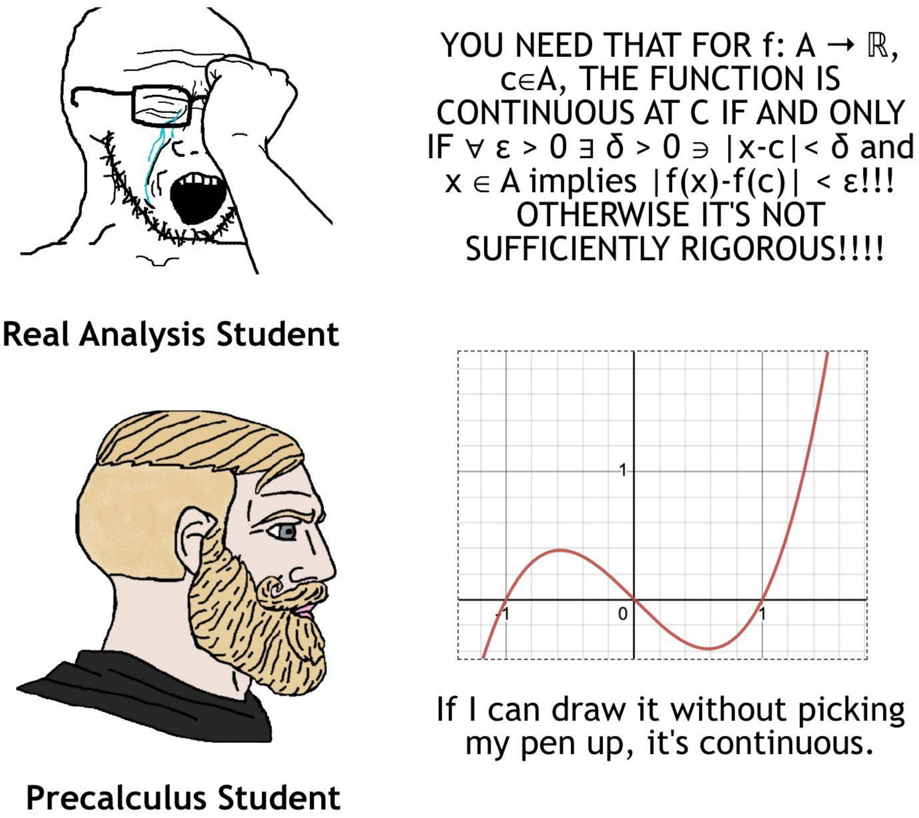
Fantuan's Academia

Fantuan's Math Notes series

Notes on Mathematical Analysis

Author: Jingxuan Xu


YOU NEED THAT FOR f: A → ℝ, c∈A, THE FUNCTION IS CONTINUOUS AT C IF AND ONLY IF ∀ ε > 0 ∃ δ > 0 ∋ |x-c|< δ and x ∈ A implies |f(x)-f(c)| < ε!!! OTHERWISE IT'S NOT SUFFICIENTLY RIGOROUS!!!!
Real Analysis Student
1
-1
0
1
If I can draw it without picking my pen up, it's continuous.
Precalculus Student

May 13, 2024

Contents

All the Sections with * are hard sections and can be skipped without losing coherence.

This note is referenced on **Understanding Analysis** by Stephen Abbott [1], **Principles of Mathematical Analysis** by Walter Rudin [2], **Analysis I** by Terence Tao [3], and MTH 117,118 notes of XJTLU.

Part I

Part I: The Real Line

Chapter 1

Real Numbers

1.1 Why Analysis?

Analysis, simply saying, is a course about 'rigorous calculus'. Somebody may ask then: "why we need another course about calculus?". Indeed, basic calculus concepts and various computing skills are introduced in Year I Calculus course. However, regarding calculus as a pure math object, it should maintain its full rigor. If we apply calculus in the real world problems without knowing where they came from and what is their constraints to be correctly applied, some pathological things will happen, as listed below.

Example 1.1.1. *Infinite Series*
Consider the divergent infinite series

$$S = 1 + 2 + 4 + 8 + 16 + \cdots \tag{1.1}$$

If we multiply it by 2,

$$2S = 2 + 4 + 8 + 16 + \cdots \tag{1.2}$$

Subtract (1.1) from (1.2), we will have the ridiculous result

$$S = -1$$

Example 1.1.2. *Interchanging Integrals*
We always change the order of double integral to make calculation easier. But, can we always do that in any cases? Consider

$$\int_0^\infty \int_0^1 \left(e^{-xy} - xye^{-xy}\right) \, \mathrm{d}y \, \mathrm{d}x$$

If we directly compute this, we can get,

$$\int_0^\infty \int_0^1 \left(e^{-xy} - xye^{-xy}\right) \, \mathrm{d}y \, \mathrm{d}x = \int_0^\infty \left[ye^{-xy}\right]_{y=0}^1 \, \mathrm{d}x = \int_0^\infty e^{-x} \, \mathrm{d}x = \left[-e^{-x}\right]_0^\infty = 1$$

However, if we change the order of integral

$$\int_0^1 \int_0^\infty \left(e^{-xy} - xye^{-xy}\right) \,\mathrm{d}x \,\mathrm{d}y = \int_0^1 \left[xe^{-xy}\right]_{x=0}^{\infty} \mathrm{d}y = \int_0^1 (0-0) \,\mathrm{d}y = 0$$

We arrive different answers!

Example 1.1.3. *Reordering Infinite Series*
Consider the alternating harmonic series

$$S = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots$$

We know that this infinite series converges at some point. Therefore, nothing similar as Example 1.1.1 could happen here. However, if we do the following computation:

$$\begin{array}{rl} \frac{1}{2}S = & \frac{1}{2} - \frac{1}{4} + \frac{1}{6} - \frac{1}{8} + \frac{1}{10} - \frac{1}{12} + \frac{1}{14} - \frac{1}{16} + \cdots \\ S = & 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \frac{1}{8} + \frac{1}{9} - \frac{1}{10} + \frac{1}{11} - \frac{1}{12} + \frac{1}{13} - \frac{1}{14} + \frac{1}{15} - \frac{1}{16} + \cdots \\ \hline \end{array}$$

$$\frac{3}{2}S = \left(1 + \frac{1}{3}\right) - \frac{1}{2} + \left(\frac{1}{5} + \frac{1}{7}\right) - \frac{1}{4} + \left(\frac{1}{9} + \frac{1}{11}\right) - \frac{1}{6} + \left(\frac{1}{13} + \frac{1}{15}\right) - \frac{1}{8} + \cdots$$

We see that $\frac{3}{2}S$ is just a reordering of our initial infinite series (with two positive terms following one negative term)! Therefore, we just change the convergent point by simply reordering the infinite series.
This doesn't make sense! Since by intuition, reordering the terms in an algorithm will not change its result. However, you see here, the situation changes in the infinite case.

As showed above, we indeed need this course to make analysis as a much more rigorous math topic than Year I Calculus. To get started, we will first talk about real numbers.

1.2 From Rational to Irrational Numbers

The simplest number system we can call to our mind is the **Natural Numbers**

$$\mathbb{N} = \{0, 1, 2, 3, 4, \cdots\}$$

Obviously, this number system is based on counting. It is enough for the simple use of counting things. However, this number system is not closed under subtraction (i.e., one natural number subtracts another natural number may not result in a natural number). Therefore, we introduce the **Integer Numbers**

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

This number system is still not complete since it is not closed under division. For example, $3 \div 5$ is not in the list. We further introduce the **Rational Numbers**

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

Back to Pythagoras's era (500-400 BC), he only believes the existance of rational numbers, and so did his followers in Pythagoreanism, except for one: Hippasus of Metapontum. After Pythagoras announced his famous Pythagorean Theorem, Hippasus directly used this theorem to discover $\sqrt{2}$: an irrational number!

Consider a right-angled triangle with two right-angled edges of length 1. Then by Pythagorean Theorem, length of the hypotenuse z should satisfy

$$z^2 = 1^2 + 1^2 = 2$$

We denote this number as $\sqrt{2}$, for which the square of it is 2. It seems that we cannot write this number in the form of a rational number. And indeed, we can prove that it is not a rational number.

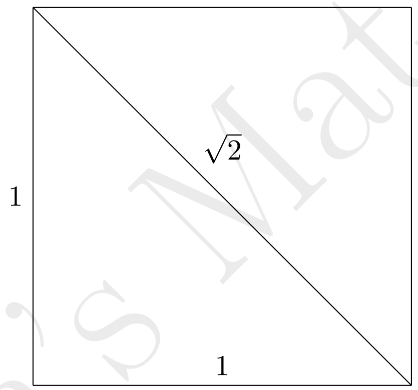


Figure 1.1: Pythagorean Theorem and $\sqrt{2}$

Proposition 1.2.1: Irrationality of $\sqrt{2}$

$\sqrt{2}$ is not a rational number.

Proof. We prove by contradiction. Suppose $\sqrt{2}$ is a rational number, then it can be written as

$$\sqrt{2} = \frac{p}{q}, \quad q \neq 0, p, q \in \mathbb{Z}, p, q \text{ are relatively prime}$$

Multiply by q on both sides and take square, we have

$$2q^2 = p^2$$

Because $2q^2$ is an even number (even number times a number must equal to an even number), p^2 is an even number. Therefore, p itself is an even number (if p is odd, then p^2 is odd, which is a contradiction). Hence, we can write p as

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

Substitute this in the previous equation, we have

$$2q^2 = 4k^2 \quad \Longrightarrow \quad q^2 = 2k^2$$

By the same arguement, we can also conclude that q is an even number. Then, p and q would have a common factor 2, which is a contradiction with our assumption that p, q are relatively prime. □

Therefore, there is another kind of number except for rational numbers! This was a big shock for people during Pythagoras's time, and the discovery of $\sqrt{2}$ is called **'The First Mathematical Crisis'**. Since this discovery broke the belief of Pythagoreanism, Hippasus, who discovered this, was drowned at sea by Pythagoras's followers.

Fortunately, now we fully accept that there is 'irrational numbers'. Nobody would be sentenced to death for acknowledging the existence of irrational numbers. Rational and Irrational numbers together, are called **Real Numbers**, denoted by $\mathbb{R}$.

But, how we should construct real numbers from rational numbers? Could we construct a procedure just like what we did for extending integers to rational numbers? In section 1.8* we will introduce an elegant method, and another method would be introduced later in Chapter 2. Since these construction processes are hard, we should now temporarily just believe that there is indeed a set of numbers called real numbers. In next section we will state the axiom that real numbers should behave.

1.3 Axiom of Completeness I: Supremum Property

One of the most important property of real number is: **It is complete**. The rigorous definition of completeness would be introduced later. Heuristically, completeness of real numbers means that 'All points on the real line are described by real numbers".

Consider rational numbers, they are 'almost everywhere' on the real line, i.e., there is no such a rational number a that is 'closest' to the rational number b. Indeed, suppose there is a b that is 'closest' to a, then, the rational number $\frac{a+b}{2}$ is 'closer' to a, which is a contradiction. This property is called **dense**, and will be introduced later.

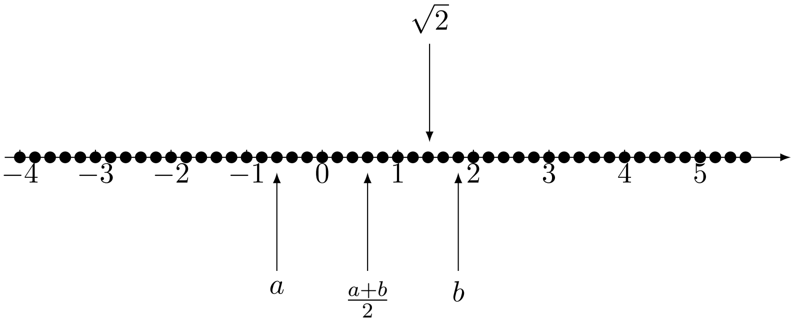


Figure 1.2: Rational Numbers $\mathbb{Q}$ is dense in Real Line $\mathbb{R}$

Even if $\mathbb{Q}$ is dense in $\mathbb{R}$, there are infinite many small 'holes' on the line that was not represented by any of the rational numbers. For example, the point at the distance of $\sqrt{2}$ from the origin, as showed in Figure 1.2. Completeness then means that these holes are exactly 'filled' by 'irrational numbers', so that each point on the line is represented by a unique real number.

To transform these discussions into mathematical language, we first introduce some simple definitions. In this whole note I will denote 'such that' by 's.t.' for simplicity.

Definition 1.3.1: Bounded Above/Bounded Below, Lower/Upper Bound

- A set $A \subseteq \mathbb{R}$ is **bounded above** if

$$\exists\, b \in \mathbb{R}, \text{ s.t. } \forall\, a \in A \implies a \leqslant b$$

The number b is called an **upper bound** for A.

- A set $A \subseteq \mathbb{R}$ is **bounded below** if

$$\exists\, l \in \mathbb{R}, \text{ s.t. } \forall\, a \in A \implies l \leqslant a$$

The number l is called an **lower bound** for A.

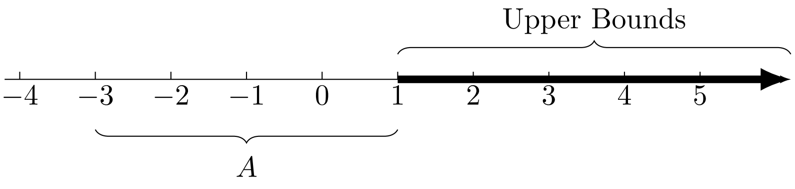


Figure 1.3: A set bounded above

Note that upper bound and lower bound of a set A may not be unique. In fact, if $A \subseteq \mathbb{R}$ is bounded above, upper bounds are always not unique. However, there would sometimes exist a 'least upper bound', which is the most important subject towards the construction of completeness axiom.

Definition 1.3.2: Supremum/Infimum

- A real number s is called the **supremum (least upper bound)** of a set $A \subseteq \mathbb{R}$ if

  1. s is an upper bound for A.
  2. For any upper bound b of A, we have $s \leqslant b$.

  This is denoted by $s = \sup A$. If $s \in A$, it is also the **maximum** of A.

- A real number l is called the **infimum (greatest lower bound)** of a set $A \subseteq \mathbb{R}$ if

  1. l is a lower bound for A.
  2. For any lower bound b of A, we have $b \leqslant l$.

  This is denoted by $l = \inf A$. If $l \in A$, it is also the **minimum** of A.

Note that although upper bound is not unique for sets, Supremum, if exists, is unique.

Proposition 1.3.3: Uniqueness of Supremum

A set $A \subseteq \mathbb{R}$ can have at most one supremum.

Proof. Suppose s_1, s_2 are suprema of a set A. Regard s_1 as an upper bound and s_2 as the supremum, we will arrive $s_2 \leqslant s_1$. Regard s_1 as the supremum and s_2 as an upper bound we will arrive $s_1 \leqslant s_2$. Therefore, $s_1 = s_2$. □

Now we should have all tools for the construction of our completeness theorem. This theorem would be seen as an **axiom**, i.e., no need to be proved and it is raised by nature, so that it is an inherent property of the set of real numbers. (In Section 1.8* we will use an elegant method to prove this axiom)

Axiom 1.3.4: Supremum Property

Every nonempty set of real numbers that is bounded above has a supremum.

Why this axiom expresses the completeness of real numbers? We consider a counterexample. Suppose we only have rational number system. Then consider the set $A = (0, \sqrt{2}) \cap \mathbb{Q}$. If the supremum s is less than $\sqrt{2}$, say $s = \sqrt{2} - \epsilon \in \mathbb{Q}$. Then there would be a number $k = \sqrt{2} - \frac{\epsilon}{2} \in A$, such that $k > s$, which is a contradiction to the definition of supremum. Similarly, we can derive that the supremum also cannot be larger than $\sqrt{2}$. Since $\sqrt{2} \notin \mathbb{Q}$, we conclude that this set A, in rational number system, has no supremum.

Therefore, the rational number system $\mathbb{Q}$ does not have this supremum property. It's only for real number system! Actually, this is the first **Axiom of Completeness for real numbers** in this note. In later chapter there would be more, and we will later on examine the relashionships between these Axiom of Completeness.

Note: We state the axiom of completeness only regarding to supremum. There is no need to assert that infimum exists as part of the axiom. To see this, let A be nonempty and bounded below, define B as

$$B = \{b \in \mathbb{R} : \text{ } b \text{ is a lower bound for } A\}$$

Then we will get $\sup B = \inf A$, by the definition of supremum and infimum. For set A, we can then state the axiom of completeness with respect to the set B, i.e., with respect to the supremum.

To conclude this section, a characterization of supremum would be stated below. This is an EXTREMELY USEFUL TOOL since sometimes it is very difficult to work on supremum directly using its definition.

Proposition 1.3.5: Characterization of Supremum

Let $s \in \mathbb{R}$ and set $A \subseteq \mathbb{R}$. $s = \sup A$ if and only if

- s is an upper bound of A.
- $\forall \epsilon > 0, \exists\, a \in A, \text{ s.t. } s - \epsilon < a$.

Proof.
($\Longrightarrow$) Suppose $s = \sup A$. Then, s is indeed an upper bound by definition. Also, $s - \epsilon$ is not an upper bound for any $\epsilon > 0$, since $s - \epsilon < s$. Therefore, by definition, there exists $a \in A$, such that $s - \epsilon < a$.
($\Longleftarrow$) Suppose s satisfy the conditions stated in the proposition. Then by the second condition, any number smaller than s is not an upper bound. Therefore, s is the least upper bound. □

1.4 Properties of real numbers

There are many applications of the Axiom of Completeness. We will first introduce the important **Archimedean Property**, which states how $\mathbb{N}$ behaves inside $\mathbb{R}$.

Theorem 1.4.1: Archimedean Property

- For any $x \in \mathbb{R}$, there exists an $n \in \mathbb{N}$ satisfying that $n > x$.
- For any $y > 0$, there exists an $n \in \mathbb{N}$ satisfying that $\frac{1}{n} < y$

Proof.

1. To prove the first statement, we assume that there exists $x \in \mathbb{R}$ such that for all $n \in \mathbb{N}$ we have $n \leqslant x$. This is equivalent to say that, $\mathbb{N}$ is bounded above. By Supremum Property, supremum exists. Let $\alpha = \sup \mathbb{N}$. Then $\alpha + 1 \in \mathbb{N}$. This contradicts the definition of supremum since $\alpha + 1 > \alpha = \sup \mathbb{N}$. Thus, we arrive a contradiction.
2. The second statement follows from (1) by letting $x = 1/y$.

□

Note: It seems that there is no need to prove the statement (1) in Archimedean Property. It just said that $\mathbb{N}$ is unbounded, and we know that as a common sense. However, it is worth noting that as a proper extension of $\mathbb{Q}$ (i.e., a set contains $\mathbb{Q}$ and not equal to $\mathbb{Q}$), the Archimedean Property is very unique for $\mathbb{R}$. Indeed, there **does exist** a proper extension of $\mathbb{Q}$ such that it is bounded (called the Extended-Real Numbers). Discussing this number system will go far out from the scope of this note. You should look for detailed explanation in my Real Analysis note. Now we see how $\mathbb{Q}$ and $\mathbb{R}\backslash\mathbb{Q}$ behaves inside $\mathbb{R}$.

Proposition 1.4.2: $\mathbb{Q}$ is dense in $\mathbb{R}$

For any $a, b \in \mathbb{R}$, $a < b$, there exists $r \in \mathbb{Q}$ such that $a < r < b$.

Proof. We need to produce $m, n \in \mathbb{Z}, n \neq 0$ such that $r = \frac{m}{n}$ and

$$a < \frac{m}{n} < b$$

The first thing we need to do is to choose sufficiently large n so that a 'step length' $\frac{1}{n}$ is less than the length of $b - a$, so that there would be some point of the form $\frac{m}{n}$ locating between the two points, as showed in the Figure 1.4.

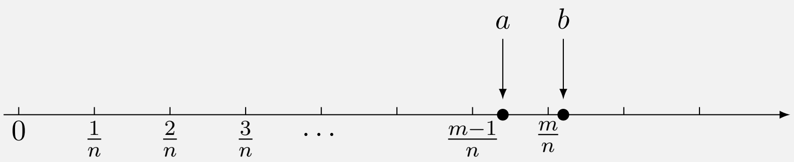


Figure 1.4: Choose sufficiently small step so that $\frac{m}{n}$ is between a and b

By Archimedean Property, we can actually take $n \in \mathbb{N}$ such that

$$\frac{1}{n} < b - a$$

Now, as showed in the picture, we need to choose $m \in \mathbb{Z}$ so that

$$\frac{m-1}{n} \leqslant a < \frac{m}{n} \quad \Longrightarrow \quad m - 1 \leqslant na < m$$

The only thing left is that to prove $\frac{m}{n} < b$. To do this, we see that

$$m \leqslant na + 1 < n\left(b - \frac{1}{n}\right) + 1 = nb$$

Therefore, the proposition is proved. □

We can use the same strategy to see that irrational number is also dense in $\mathbb{R}$. Before doing that, we need to prove some lemma about properties of operations in rational and irrational numbers.

Lemma 1.4.3: Operations in $\mathbb{Q}$ and $\mathbb{R}\backslash\mathbb{Q}$

1. If $a, b \in \mathbb{Q}$, then $a + b, ab \in \mathbb{Q}$.
2. If $a \in \mathbb{Q}, b \in \mathbb{R}\backslash\mathbb{Q}$, then $a + t, at(a \neq 0) \in \mathbb{R}\backslash\mathbb{Q}$

Proof.

1. Since $a, b \in \mathbb{Q}$, we have $a = \frac{m}{n}$, $b = \frac{r}{q}$ for $m, n, r, q \in \mathbb{Z}, n, q \neq 0$. Therefore,

$$a + b = \frac{mq + nr}{nq} \in \mathbb{Q}, \quad ab = \frac{mr}{nq} \in \mathbb{Q}$$

since $mq + nr, nq, mr \in \mathbb{Z}$.

2. Since $a \in \mathbb{Q}$, we have $a = \frac{m}{n}$ where $m, n \in \mathbb{Z}$, $n \neq 0$. Suppose $a + t \in \mathbb{Q}$, then we can write

$a+t = \frac{r}{q}, r, q \in \mathbb{Z}, q \neq 0$. Then,

$$t = (a+t) - a = \frac{r}{q} - \frac{m}{n} = \frac{rn - mq}{qn} \in \mathbb{Q}$$

which is a contradiction. Similarly, we can also see that $at \notin \mathbb{Q}$ (when $a \neq 0$). □

Proposition 1.4.4: $\mathbb{R} \backslash \mathbb{Q}$ is dense in $\mathbb{R}$

For any $a, b \in \mathbb{R}, a < b$, there exists a $t \in \mathbb{R} \backslash \mathbb{Q}$ such that $a < t < b$.

Proof. As in Proposition 1.4.2, we first choose $n \in \mathbb{N}$ such that

$$\frac{1}{n} < b - a$$

Then, we choose $m \in \mathbb{Z}$ such that

$$m + \sqrt{2} - 1 \leqslant na < m + \sqrt{2}$$

Obviously, we have $a < \frac{m+\sqrt{2}}{n}$. Also,

$$m + \sqrt{2} \leqslant na + 1 < n\left(b - \frac{1}{n}\right) + 1 = nb$$

Thus, $a < \frac{m+\sqrt{2}}{n} < b$. Since $m, \frac{1}{n} \in \mathbb{Q}$, $\sqrt{2} \in \mathbb{R} \backslash \mathbb{Q}$, by Lemma 1.4.3, we have $\frac{m+\sqrt{2}}{n} \in \mathbb{R} \backslash \mathbb{Q}$. The statement is proved. □

At this stage we have proved that $\sqrt{2}$ is not a rational number. But, we have not proved that it is a real number. Below we will prove this. Why we need to prove this obvious thing? Indeed, you will see from the prove below that the main theorem used is Supremum Property. Therefore, this inherent property of real numbers asserts that those irrational numbers we encounter often are all real numbers.

Proposition 1.4.5: $\sqrt{2}$ is a real number

There exists a real number $\alpha \in \mathbb{R}$ such that $\alpha^2 = 2$.

Proof. Consider the set

$$T = \{t \in \mathbb{R} : t^2 < 2\}$$

Set $\alpha = \sup T$.

- Suppose $\alpha^2 < 2$. Let $n \in \mathbb{N}$ be arbitrary, then

$$\left(\alpha + \frac{1}{n}\right)^2 = \alpha^2 + \frac{2\alpha}{n} + \frac{1}{n^2} < \alpha^2 + \frac{2\alpha}{n} + \frac{1}{n} = \alpha^2 + \frac{2\alpha + 1}{n}$$

  If we choose $n \in \mathbb{N}$ such that

$$\frac{1}{n} < \frac{2 - \alpha^2}{2\alpha + 1}$$

  The existence of this n is promised by Archimedean Property. Note that $n > 0$ since we assume that $\alpha^2 < 2$. We would get

$$\left(\alpha + \frac{1}{n}\right)^2 < \alpha^2 + \frac{(2\alpha + 1)(2 - \alpha^2)}{2\alpha + 1} = 2$$

  Therefore, $\alpha + \frac{1}{n} \in T$, which means that α is not an upper bound, which is a contradiction to that $\alpha = \sup T$.

- Suppose $\alpha^2 > 2$. Similarly, we can write

$$\left(\alpha - \frac{1}{n}\right)^2 = \alpha^2 - \frac{2\alpha}{n} + \frac{1}{n^2} > \alpha^2 - \frac{2\alpha}{n}$$

  If we choose $n \in \mathbb{N}$ such that

$$\frac{1}{n} < \frac{\alpha^2 - 2}{2\alpha}$$

  Again, the existance is promised by Archimedean Property. Then we would have

$$\left(\alpha - \frac{1}{n}\right)^2 > \alpha^2 - \alpha^2 + 2 = 2$$

  This shows that $\alpha - \frac{1}{n}$ is an upper bound of T, which means that α is not the least upper bound, i.e., not the supremum. This is a contradiction to the assumption that $\alpha = \sup T$.

By Supremum Property, the supremum of T exists. Then, it can only be $\sqrt{2}$. Since the supremum of a set is a real number (which is promised in Supremum Property), we finally arrive that $\sqrt{2}$ is actually a real number. □

1.5 Axiom of Completeness II: Nested Interval Property

Another famous Axiom of Completeness of real numbers is called the **(Cantor) Nested Interval Property**. It says that for any nested closed interval sequence, the intersection of these intervals is not empty. Here is what all these words mean.

Axiom 1.5.1: Nested Interval Property

For each $n \in \mathbb{N}$, construct a closed interval $I_n = [a_n, b_n]$, where $a_n, b_n \in \mathbb{R}$. Assume $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$. Then, the intersection of these nested intervals

$$\bigcap_{n=1}^{\infty} I_n \neq \emptyset$$

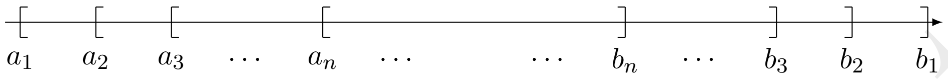


Figure 1.5: Nested Intervals

Actually, this axiom can be derived from Supremum Property, as showed below.

Proof. Consider the set

$$A = \{a_n : n \in \mathbb{N}\}$$

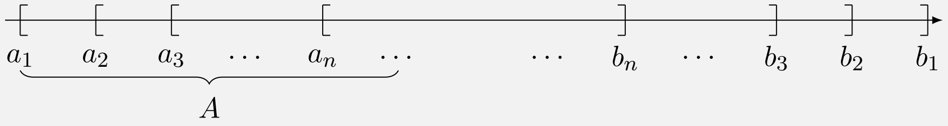


Figure 1.6: Nested Intervals with set A

We can see that each b_n is served as an upper bound for the set $[a_n, b_n]$, for every $n \in \mathbb{N}$. Set $x = \sup A$. Then $a_n \leqslant x$ for every n since x is the upper bound. Also, $b_n \geqslant x$ for every n since b_n are upper bounds and x is the supremum. Therefore we get,

$$\forall n \in \mathbb{N}, a_n \leqslant x \leqslant b_n$$

Hence, $x \in \bigcap_{n=1}^{\infty} I_n \neq \emptyset$. □

Can we, inversely, get Supremum Property from Nested Interval Property? The answer is no! Therefore, there is some 'strong' axioms and some 'weak' axioms. In this case, Supremum Property is 'strong' and Nested Interval Property is 'weak', since we can go from Supremum Property to Nested Interval, but not the reverse direction.

But, why we can't? In the 'proof' below I will show you a **circular reasoning**, indicating that we can only go from Nested Interval Property to Supremum Property if Archimedean Property exists.

Note: This is not a prove, but just a reasoning process.

Suppose Nested Interval Property is true. We want to prove Supremum Property. Let A be a nonempty set which is bounded above. Denote $\alpha = \sup A$. Choose $a \in A$ and b such that b is an upper bound of A. Then, consider the intervals $[a, \frac{a+b}{2}]$ and $[\frac{a+b}{2}, b]$. Then, α is at least in one of these two intervals. Choose an interval that contains it. Continue bisecting this interval as we did at the last step. Again, the supremum would contain in one of the intervals. Choose that interval. $\cdots\cdots$

After n steps, the length of the chosen interval would be $\frac{b-a}{2^n}$. The only thing we are left to do is to prove that $\frac{b-a}{2^n}$ converges to 0 (The rigorous definition of limit would be introduced in Chapter 2, here you can just recall what you have learnt in Year I Calculus). However, the proof of this statement needs Archimedean Property, since we want for every $\epsilon > 0$, we can find a $n \in \mathbb{N}$ such that $\frac{b-a}{2^n} < \epsilon$. This is equivalent to what is said in the second statement of Archimedean Property. Recall how Archimedean Property is derived. Yes, it is derived from Supremum Property! So we cannot directly use Archimedean Property if we assume we don't know Supremum Property and want to prove it. This is an example of **circular reasoning**, and in result, we have no way deriving Supremum Property from Nested Interval Property.

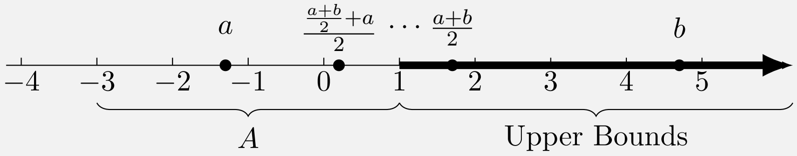


Figure 1.7: Bisecting intervals to approximate supremum

Therefore, we get the relationship between Supremum Property and Nested Interval Property. The relation is visually displayed below in Figure 1.8.

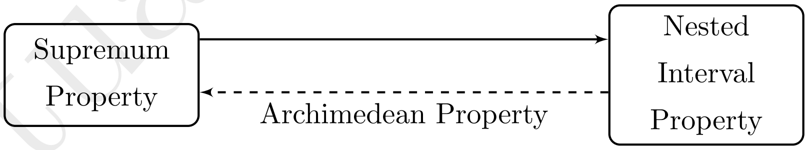


Figure 1.8: Relation between Axiom of Completeness

This graph would be further expanded when we encounter more and more Axiom of Completeness.

1.6 'Size of Infinity': Cardinality

Does infinity also have different 'sizes'? You may ask after seeing this section title. The answer is yes! We all know that there are infinitely many rational numbers and irrational numbers, and it seems that both of them are ‘almost everywhere’ on the real line. However, in this section we will introduce a surprising result: There are ‘much more’ irrational numbers than rational numbers!

Before we discuss this result, we need to first talk about the way of comparing two ‘infinite sizes’. Let’s start with finite one. To compare the number of elements in two finite sets, it is easy, just count them. For example, $A = \{1, 2, 3, 4\}$ and $B = \{5, 6, 7, 8\}$. They all have 4 elements, and naturally, have the same size. To extend this into infinite case, we need to use **bijective maps**.

Definition 1.6.1: Cardinality

Two sets A, B have the same **Cardinality** if there exists a bijective map $f : A \to B$ such that each element of A is mapped one-to-one and onto an element of B. Dented as $A \sim B$.

Then, the cardinality of a set just discribes the ‘size’ of that set. Let’s see some examples first.

Example 1.6.2: $\mathbb{N}$ ***has the same cardinality as the set of even numbers***

This is weird at first glance, since intuitively the set of even numbers is a proper subset of $\mathbb{N}$, and they could not have the same size. Denote the set of even numbers as

$$E = \{2, 4, 6, 8, \cdots\}$$

Then we can construct a bijective map $f : \mathbb{N} \to E$ by $f(n) = 2n, \forall\, n \in \mathbb{N}$.

$$\begin{array}{rcccccccc} \mathbb{N}: & 1 & 2 & 3 & 4 & \cdots & n & \cdots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots \\ E: & 2 & 4 & 6 & 8 & \cdots & 2n & \cdots \end{array}$$

Example 1.6.3: $\mathbb{N} \sim \mathbb{Z}$

We can construct a bijective map $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(n) = \begin{cases} \dfrac{n-1}{2}, & \text{if } n \text{ is odd} \\ -\dfrac{n}{2}, & \text{if } n \text{ is even} \end{cases}$$

$$\begin{array}{rcccccccc} \mathbb{N}: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots \\ \mathbb{Z}: & 0 & -1 & 1 & -2 & 2 & -3 & 3 & \cdots \end{array}$$

In the two examples above, we see that we correspond elements of some set with natural numbers $1, 2, 3, 4, \cdots$, just as we are counting them in some order. This is such an important case that we gave it a name.

Definition 1.6.4: Countable/Uncountable Set

A set is A is called

- **Finite** if the number of elements in A is finite.
- **Countable** if $A \sim \mathbb{N}$.
- **Uncountable** if it is infinite and not countable.

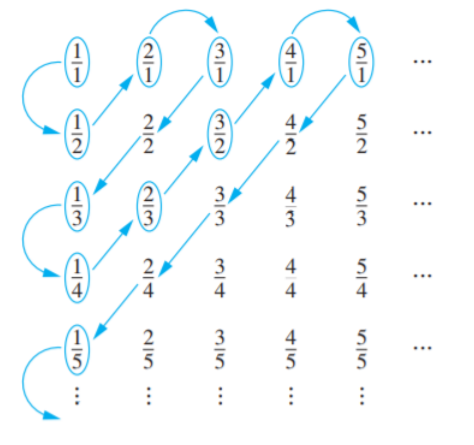
We can see from Example 1.6.2 and 1.6.3 that E and $\mathbb{Z}$ are countable sets. What does uncountable set looks like? **The next theorem is central for this section.** It says that $\mathbb{R}$ has a somewhat ‘bigger’ size than $\mathbb{Q}$.

Theorem 1.6.5: Countability of $\mathbb{Q}$, Uncountability of $\mathbb{R}$

1. $\mathbb{Q}$ is a countable set.
2. $\mathbb{R}$ is an uncountable set.

Proof.

1. There are two popular ways of proving that $\mathbb{Q}$ is countable. I will show both of them.
   METHOD I: Arrage all the rational numbers in an infinite matrix such that mth row and nth column corresponds to the number $\frac{n}{m}$. Then, assign natural numbers to them ‘meanderingly’, as showed below. If there is a number that has the same value with some number that has been assigned, we delete it. For example, $\frac{1}{1}$ is assigned 1, $\frac{1}{2}$ is assigned 2, $\frac{2}{1}$ is assigned 3, $\frac{3}{1}$ is assigned 4, $\frac{2}{2}$ is deleted since it has the same value with $\frac{1}{1}$, and $\frac{1}{3}$ is assigned 5...... Continuing this fashion, we will have a bijective map from positive rational numbers to natural numbers.



With this, we can further map 0 to 0 and map negative rational numbers to negative integers. Then, this whole map is a bijective map from $\mathbb{Q}$ to $\mathbb{Z}$. Since there also exists biject map from $\mathbb{Z}$ to $\mathbb{N}$, we have $\mathbb{N} \sim \mathbb{Q}$.

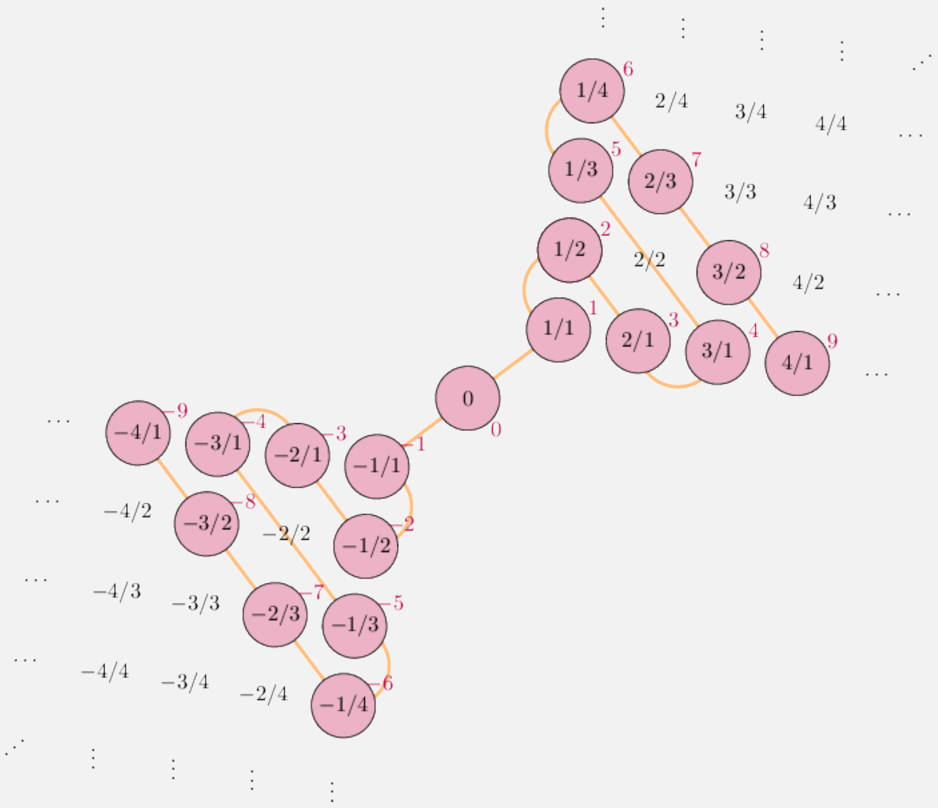
METHOD II: Set $A_1 = \{0\}$, and for all $n \geqslant 2$, set

$$A_n = \left\{ \pm\frac{p}{q} : p, q \in \mathbb{N} \text{ are relatively prime with } p + q = 0 \right\}$$

For example,

$$A_2 = \left\{ \frac{1}{1}, -\frac{1}{1} \right\}, \quad A_3 = \left\{ \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1} \right\}, \quad A_4 = \left\{ \frac{1}{3}, -\frac{1}{3}, \frac{3}{1}, -\frac{3}{1} \right\}, \cdots$$

Each A_n is finite and every rational number appears in exactly one of these sets. Therefore, we can construct the bijective map by listing the elements in each A_n.



2. The main theorem used in this proof is the **Nested Interval Property**. We will prove by contradiction. Suppose there exists a bijective function $f : \mathbb{N} \to \mathbb{R}$. Then, each real number can be assigned to a natural number. Therefore, we can denote x_i as the real number being assigned

to the natural number i, and write $\mathbb{R}$ as

$$\mathbb{R} = \{x_1, x_2, x_3, x_4, \cdots\}$$

Now, consider the set $[0, 9]$. We can divide it into 3 parts: $[0, 3] \cup [3, 6] \cup [6, 9]$. Then, x_1 can at most belong to two of them. Choose the interval that x_1 does not belong to, denote it as I_1.

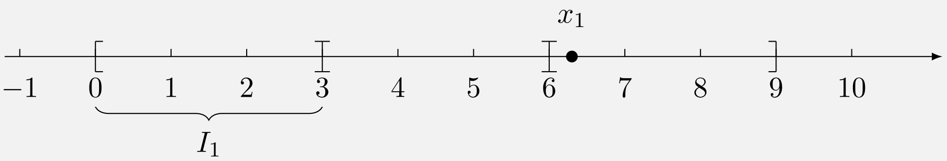


Figure 1.9: Construction Process of Nested Intervals, I

Then, we can divide I_1 into 3 equal parts just as the previous step. Again, x_2 can at most belong to one of these three intervals. Choose the one that x_2 does not belong to, and call it I_2. Continuing this fashion, for I_n, we divide it into 3 equal parts, and choose the interval that x_{n+1} does not belong to, call it I_{n+1} $\cdots$.

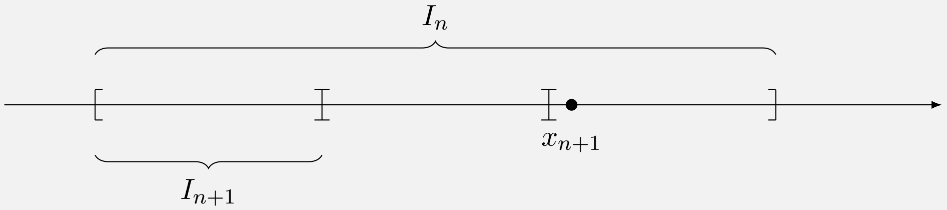


Figure 1.10: Construction Process of Nested Intervals, II

Using this procedure, we can produce nested intervals I_n such that

$$I_{n+1} \subseteq I_n, \forall\, n \in \mathbb{N}, \text{ and } \quad x_n \notin I_n$$

Therefore,

$$x_n \notin \bigcap_{n=1}^{\infty} I_n, \forall\, n \in \mathbb{N}$$

This shows that

$$\bigcap_{n=1}^{\infty} I_n = \emptyset$$

which is a contradiction to the Nested Interval Property. □

Therefore, $\mathbb{R}$ is a 'bigger' set than $\mathbb{N}$! There does exist uncountable sets. In examples before, we have seen some other sets that is countable. In the next few examples, we will see what does uncountable sets look like.

Example 1.6.6: $(-1, 1) \sim \mathbb{R}$

Here we can construct the function $f : (-1, 1) \to \mathbb{R}$ by

$$f(x) = \frac{x}{x^2 - 1}$$

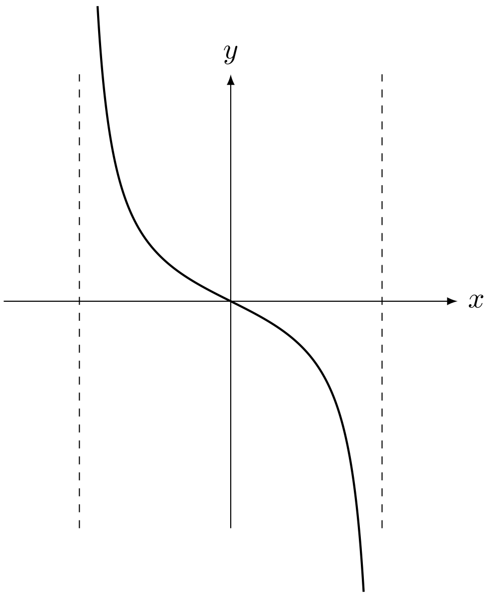


Figure 1.11: function $f(x) = \frac{x}{x^2-1}$

Example 1.6.7: $(a, b) \sim \mathbb{R}$

To extend the result from Example 1.6.6 to the case for every $a, b \in \mathbb{R}$, we can just do linear transformation on the function f in that example. Set

$$-1 < kx + c < 1, k > 0$$

We have

$$\frac{-1 - c}{k} < x < \frac{1 - c}{k}$$

Therefore, we can set

$$a = \frac{-1 - c}{k}, \quad b = \frac{1 - c}{k}$$

To get

$$k = \frac{2}{b-a}, \quad c = \frac{a+b}{a-b}$$

Thus

$$g(x) = f\left(\frac{2x}{b-a} + \frac{a+b}{a-b}\right)$$

will map (a, b) to the whole space $\mathbb{R}$.

Example 1.6.8: $(a, \infty) \sim \mathbb{R}$

We can construct the function $f : (a, \infty) \to \mathbb{R}$ by

$$f(x) = \log(x - a)$$

Example 1.6.9: $[0, 1) \sim (0, 1)$

This one is interesting. It seems very easy. However, if you try that, it is not. Let us consider one famous paradox in mathematics: **Hilbert's paradox of the Grand Hotel**. There is a hotel with countably infinitely many rooms in the hotel, and the hotel is full. Then, some travellers come and want a room. The reception just send a call to everybody in the room: For person who live in room n, just move to the room $n + 1$, and the room 1 would be available for this traveller. Weird! Since we seem to create a new empty room from nowhere.

This problem is just the same. We need to move some countable set accordingly to make a new room for this new comer 0. Therefore, we can construct the bijective function $f : [0, 1) \to (0, 1)$ like

$$f(x) = \begin{cases} 1/2, & \text{if } x = 0 \\ 1/4, & \text{if } x = \dfrac{1}{2} \\ 1/8, & \text{if } x = \dfrac{1}{4} \\ 1/16, & \text{if } x = \dfrac{1}{8} \\ \dots \\ x, & \text{otherwise} \end{cases}$$

Now we should be familiar with countable sets and uncountable sets. In Chapter 1.7* we will further go into n-dimensions, to see that $\mathbb{R}$ are also uncountable sets, of the same cardinality with $\mathbb{R}$.

Finally, to end this section, we will see that whether the set of irrational numbers is countable or uncountable. Before doing that, let's prove some theorems about the properties of countable sets.

Theorem 1.6.10: Subsets and Unions of countable sets

1. If $A \subseteq B$, B is countable, then, A is either countable or finite.

2. If $A_1, A_2, ..., A_m$ are countable, then,
$$\bigcup_{n=1}^{m} A_n$$
is countable.

3. If A_n is countable for each $n \in \mathbb{N}$, then,
$$\bigcup_{n=1}^{\infty} A_n$$
is countable.

Proof.

1. Let B be a countable set. Then, there exists bijective map $f : \mathbb{N} \to B$. Let $A \subsetneq B$ be an infinite subset of B. We must show that A is countable.
We now start to define a bijective map from $\mathbb{N}$ to A. Let
$$n_1 = \min\{n \in \mathbb{N} : f(n) \in A\}, \text{ Set } g(1) = f(n_1)$$
$$n_2 = \min\{n \in \mathbb{N}\backslash\{1, 2, \cdots, n_1\} : f(n) \in A\}, \text{ Set } g(2) = f(n_2)$$
$$n_3 = \min\{n \in \mathbb{N}\backslash\{1, 2, \cdots, n_2\} : f(n) \in A\}, \text{ Set } g(3) = f(n_3)$$
$$\vdots$$
Inductively, as we can easily verify, that this function is bijective from $\mathbb{N}$ to A.

2. We first prove that this is true for two countable sets, A_1, A_2. Let $B_2 = A_2\backslash A_1$. Then, A_1 and B_2 is disjoint, and $A_1 \cup A_2 = A_1 \cup B_2$. Therefore, we only need to prove that $A_1 \cup B_2$ is countable. By statement 1 above, we can see that $B_2 = A_2\backslash A_1 \subseteq A_2$ is countable or finite. First suppose that B_2 is countable. Then, we can write both sets in the enumerated form
$$A_1 = \{a_1, a_2, a_3, \cdots\}$$
$$B_2 = \{b_1, b_2, b_3, \cdots\}$$
Since they are disjoint, we can write their union as
$$A_1 \cup B_2 = \{a_1, b_1, a_2, b_2, a_3, b_3, \cdots\}$$

A bijective map then can be constructed as $f : \mathbb{N} \to A_1 \cup B_2$ such that

$$f(n) = \begin{cases} a_{\frac{n}{2}}, & \text{if } n \text{ is even} \\ b_{\frac{n+1}{2}}, & \text{if } n \text{ is odd} \end{cases}$$

Now suppose B_2 is finite. This time

$$A_1 = \{a_1, a_2, a_3, \cdots\}$$

$$B_2 = \{b_1, b_2, b_3, \cdots, b_m\}$$

Since they are disjoint, we can write their union as

$$A_1 \cup B_2 = \{b_1, b_2, b_3, \cdots, b_m, a_1, a_2, a_3, \cdots\}$$

A bijective map then can be constructed as $f : \mathbb{N} \to A_1 \cup B_2$ such that

$$f(n) = \begin{cases} b_n, & \text{if } n \leqslant m \\ a_{n-m}, & \text{if } n > m \end{cases}$$

We have proved that $A_1 \cup A_2$ is countable. Now if A_3 is countable, we can directly see that,

$$A_1 \cup A_2 \cup A_3 = (A_1 \cup A_2) \cup A_3$$

is countable. Inductively, we have

$$\bigcup_{n=1}^{m} A_n$$

is countable if $A_1, \cdots, A_m$ are countable sets.

3. Suppose A_n is countable for all $n \in \mathbb{N}$. Then each set can be written as

$$A_n = \{a_{n1}, a_{n2}, a_{n3}, \cdots\}$$

We can arrange the elements into a infinite matrix

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots \\ \vdots & \vdots & \vdots & \cdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Then, we can assign each element a natural number just as what we did in the proof of Theorem 1.6.5. This constructs a bijective map. □

Here is an interesting fact derived from the theorem: We can have a countable collection of disjoint open intervals, such as $(0,1),(1,2),(2,3),\cdots$ However, **we cannot have an uncountable collection of disjoint open intervals**. Suppose for contradiction, there is such a collection. Each open interval must contain a rational number (since $\mathbb{Q}$ is dense in $\mathbb{R}$). Then, for each interval, we can randomly select a rational number that is contained in it. This constructs a biject map from these intervals to a subset of $\mathbb{Q}$. By the first statement in the previous theorem, the number of intervals must be countable.

Let's go back to the topic. Naturally from the theorem proved above, we can have the result:

Corollary 1.6.11: $\mathbb{R}\backslash\mathbb{Q}$ is uncountable

The set of irrational numbers, $\mathbb{R}\backslash\mathbb{Q}$, is uncountable.

Proof. Suppose $\mathbb{R}\backslash\mathbb{Q}$ is countable. Then, by Theorem 1.6.10, the union $\mathbb{R}=\mathbb{R}\backslash\mathbb{Q}\cup\mathbb{Q}$ is countable since $\mathbb{Q}$ is countable, which contradicts the fact that $\mathbb{R}$ is uncountable. □

There are 'more' irrational numbers than rational numbers! Even if they are all dense in the real line. Indeed, this kind of pattern is what you will always encounter down the road of matheamtics study. The 'pathological' mathematical objects are far more than the well-behaved ones. For example, there are more discontinuous functions than continuous ones. There are more transcendental numbers than algebraic numbers......

1.7* Aleph Numbers and Continuum Hypothesis

This section is a hard section and can be skipped without losing coherence.

1.7.1* Cantor's Diagonalization Method

In 1891, Cantor offered another elegant proof of the fact that $\mathbb{R}$ is uncountable. This method is called **Cantor's Diagonalization Method**. It uses the **decimal representations** for real numbers.

Definition 1.7.1: Decimal Representation

A decimal representation of a non-negative real number r is its expression as a sequence of symbols consisting of decimal digits traditionally written with a single separator:

$$r = b_k b_{k-1} \cdots b_0 . a_1 a_2 a_3 \cdots , \quad b_i, a_j \in \{0, 1, 2, 3, \cdots, 9\}, i \in \{1, 2, 3, \cdots, k\}, j \in \mathbb{N}$$

and it represents the infinite sum

$$r = \sum_{i=0}^{k} b_i 10^i + \sum_{i=1}^{\infty} \frac{a_i}{10^i}$$

For the rigorous definition of Infinite sum, see Chapter 2. **Here is a problem, each real number has at least one decimal representation. Some real number has two decimal representation. The mapping from decimal representation to real numbers is not bijective**. To solve this problem, we observe that **a real number has two such representations if and only if one has a trailing infinite sequence of 0, and the other has a trailing infinite sequence of 9**. To make the mapping into a bijection, we will ban the use of decimal representations with a trailing infinite sequence of 9.
Now we state the Cantor's proof.

Proof. **CANTOR'S DIAGONALIZATION METHOD**
We have already seen that $(0, 1) \sim \mathbb{R}$. If we can prove that $(0, 1)$ is uncountable, we are done.
We prove by contradiction. Suppose there exists a bijective function $f : \mathbb{N} \to (0, 1)$. Then, for each $m \in \mathbb{N}$, $f(m)$ is a real number that has decimal representation

$$f(m) = .a_{m1} a_{m2} a_{m3} \cdots$$

where $a_{mn} \in , \mathbb{1}, , \cdots , .$ The bijective correspondence is summarized below as a table

$$\begin{array}{ccccccccc}
\mathbb{N} & & (0,1) & & & & & & \\
1 & \longleftrightarrow & f(1) & = & .\mathbf{a_{11}} & a_{12} & a_{13} & a_{14} & \cdots \\
2 & \longleftrightarrow & f(2) & = & .a_{21} & \mathbf{a_{22}} & a_{23} & a_{24} & \cdots \\
3 & \longleftrightarrow & f(3) & = & .a_{31} & a_{32} & \mathbf{a_{33}} & a_{34} & \cdots \\
4 & \longleftrightarrow & f(4) & = & .a_{41} & a_{42} & a_{43} & \mathbf{a_{44}} & \cdots \\
\vdots & & \vdots & & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Then, every decimal representation of numbers in $(0, 1)$ would appear somewhere in the table. However, we can define a real number $x \in (0,1)$ with decimal representation of $x = .b_1b_2b_3\cdots$ such that

$$b_n = \begin{cases} 1, & \text{if } a_{nn} \neq 1 \\ 2, & \text{if } a_{nn} = 1 \end{cases}$$

Then, $x \neq f(1)$ because $a_{11} \neq b_1$. $x \neq f(2)$ because $a_{22} \neq b_2$. $x \neq f(3)$ because $a_{33} \neq b_3 \cdots$ Therefore, we have for each $n \in \mathbb{N}$, $x \neq f(n)$, which is a contradiction. □

Note: This proof cannot be used on $\mathbb{Q}$ since, as we know from junior or high school, that rational numbers have infinite-repeating decimals, and the construction for x would lead to a real number.

This kind of method can be used not only on the proof of the fact that $\mathbb{R}$ is an uncountable set. Let's see another example.

Example 1.7.2: Set of infinite $0-1$ sequence is uncountable

Let

$$S = \{(a_1, a_2, a_3, \cdots) : a_n = 0 \text{ or } 1\}$$

S is uncountable.

Proof. Suppose it is countable. We can then write elements in S as $S = \{x_1, x_2, x_3, \cdots\}$, $x_n = (a_{n1}, a_{n2}, a_{n3}, \cdots)$, where $a_{nm} = 0$ or 1. Then, we can construct a similar table as in Cantor's Diagonalization Method. Now consider an infinite sequence

$$b_n = \begin{cases} 0, & \text{if } a_{nn} = 1 \\ 1, & \text{if } a_{nn} = 0 \end{cases}$$

It is not in the list, which is a contradiction. □

1.7.2* Schröder-Bernstein Theorem, Cardinality of Real Space $\mathbb{R}^n$

Sometimes it is very difficult to find a bijective function between two sets A and B with the same cardinality. However, it is almost always easy to find a injective function from A to B, and another injective function from B to A. Does this imply that there exists a bijective function? Yes! And it is called the **Schröder-Bernstein Theorem**.

Theorem 1.7.3: Schröder-Bernstein Theorem

Suppose there exists injective function $f : X \to Y$ and another injective function $f : Y \to X$. Then, there exists a bijective function from X to Y, hence $X \sim Y$.

Proof. There are many versions of proof of this theorem. The most famous one is presented by a 19-year old student, Bernstein, who was in Cantor's Seminar. Almost simultaneously, Schröder presents another proof.

To make this proof clear and well-structured, I will separate them into several STEPS. The basic idea is to partition X and Y into components

$$X = A \cup A' \text{ and } Y = B \cup B'$$

with $A \cap A' = \emptyset$ and $B \cap B' = \emptyset$, in such way that f maps A surjectively onto B, and g maps B' surjectively onto A'

STEP I: Set $A_1 = X \backslash g(Y)$. If $A_1 = \emptyset$ then $g(Y) = X$, g is bijective, then we are done. So, assume $A_1 \neq \emptyset$. Inductively define a sequence of sets by letting $A_{n+1} = g(f(A_n))$. We will show that $\{A_n : n \in \mathbb{N}\}$ is pairwise disjoint collection of subsets of X.

We first show that $A_1 \cap A_k = \emptyset$. This is obvious since $A_1 = X \backslash g(Y)$ and $A_k = g(f(k-1)) \in g(Y)$.

Now we turn to prove more general case that $A_j \cap A_k = \emptyset$. Define $h(x) = g(f(x))$. Because both f and g are injective, we have h is injective as well. Note that

$$h(A \cap B) = h(A) \cap h(B)$$

This can be proved by the following details:

($\Longrightarrow$) Suppose $x \in h(A \cap B)$, since h is injective, there exists unique $y \in A \cap B$ such that $h(y) = x$. Since $y \in A$ and $y \in B$, we have $x = h(y) \in h(A) \cap h(B)$. This shows that $h(A \cap B) \subseteq h(A) \cap h(B)$.

($\Longleftarrow$) Suppose $x \in h(A) \cap h(B)$, then $x \in h(A)$ and $x \in h(B)$. Since h is injective, there exists unique $y \in X$ such that $x = h(y)$. This means that $y \in A$ and $y \in B$. Thus, $y \in A \cap B, x = h(y)$. We conclude that $x \in h(A \cap B)$. Therefore, $h(A \cap B) \supseteq h(A) \cap h(B)$.

Denote $h^2 = h \circ h$, and inductively denote h^k as the kth composition of h. Note that h^k is injective. Therefore, we have

$$A_{j+1} \cap A_{k+1} = h^k(A_{j-k}) \cap h^k(A_1) = h^k(A_{j-k} \cap A_1) = h^k(\emptyset) = \emptyset, \quad j, k \in \mathbb{N}$$

STEP II: Now we prove that $\{f(A_n) : n \in \mathbb{N}\}$ is a pairwise disjoint collection of subsets of Y. This is easy. Since f is injective, we have $f(A_j) \cap f(A_k) = f(A_j \cap A_k) = f(\emptyset) = \emptyset$.

STEP III: Now we let $A = \bigcup_{n=1}^{\infty} A_n$ and $B = \bigcup_{n=1}^{\infty} f(A_n)$. Note that since A_n are pairwise disjoint,

$$f(A) = f\left(\bigcup_{n=1}^{\infty} A_n\right) = \bigcup_{n=1}^{\infty} f(A_n) = B$$

Therefore, f maps A surjectively onto B.

STEP IV: We finally show that for $A' = X\backslash A$ and $B' = X\backslash B$, we have g maps B' surjectively onto A'. To prove this, we need to show that $g(B') = A'$. We prove both directions by contradiction.
($\Longrightarrow$) To prove $g(B') \subseteq A'$, suppose for contradiction that there exists $b' \in B'$ such that $g(b') \in A$. Since $A_1 \cap g(Y) = \emptyset$, we must have $g(b') \notin A_1$, thus $g(b') \in A\backslash A_1$. Note that

$$g(B) = g\left(\bigcup_{n=1}^{\infty} f(A_n)\right) = \bigcup_{n=1}^{\infty} g(f(A_n)) = \bigcup_{n=1}^{\infty} A_{n+1} = A\backslash A_1$$

We have $g(b') \in g(B)$. This means that there exists $b \in B$ such that $b' \neq b$ (this is because $B \cap B' = \emptyset$), and $g(b') = g(b)$, which is a contradiction to the injectivity of g.
($\Longleftarrow$) To prove $g(B') \supseteq A'$, suppose for contradiction that there exists $a' \in A'$ such that $a' \notin g(B')$. Immediately, because $A' \in g(Y)$, we have $a' \in g(B)$ (since $a' \notin g(B')$). This will contradict the fact that $a' \in A'$ since $g(B) = A\backslash A_1 \subseteq A$.
STEP V: Now we know that $f : A \to B$ and $g : B' \to A'$ are bijective functions. Define

$$l(x) = \begin{cases} f(x), & \text{if } x \in A \\ g^{-1}(x), & \text{if } x \in A' \end{cases}$$

This is a bijective function from X to Y. □

You see from this proof another fact in mathematics: Some theorems that seem to be easily structured can be very hard to prove.
Let's see some applications of this theorem. The very important one is that we can use Schröder-Bernstein Theorem to prove that $\mathbb{R}^n$ has the same cardinality with $\mathbb{R}$.

Example 1.7.4: $\mathbb{R}^n \sim \mathbb{R}$

Let us first consider the interval $(0, 1)$. Let

$$S = \{(x, y) : 0 < x, y < 1\}$$

The function $f : (0, 1) \to S$, where $f(x) = (x, x)$ maps $(0, 1)$ injectively into S, but not surjective. Now we want to find an injective function from S to $(0, 1)$. Recall the decimal representation of real numbers. We construct the map in the following way: Let $(x, y) \in S$, such that

$$x = .a_1a_2a_3\cdots, \quad y = .b_1b_2b_3\cdots$$

Let

$$z = .a_1b_1a_2b_2a_3b_3\cdots$$

We define $g : S \to (0,1)$ by $g(x,y) = z$. This is then an injective function, because the decimal representation is unique for each real number. By Schröder-Bernstein Theorem, there exists a bijective map from $(0,1)$ to S, thus $(0,1) \sim S$.

Now, if we define the function $h : S \to \mathbb{R}^2$ by

$$h(x,y) = \left(\frac{x}{x^2-1}, \frac{y}{y^2-1}\right)$$

We see from Example 1.6.6 that this function is bijective. Therefore, we have

$$\mathbb{R} \sim (0,1) \sim S \sim \mathbb{R}^2$$

Inductively, we can also have

$$\mathbb{R} \sim \mathbb{R}^n$$

This is actually a surprising result. We have $\mathbb{Q}$ is countable and $\mathbb{R}$ is uncountable, since we can think $\mathbb{Q}$ as a set of 'countable points', but $\mathbb{R}$ as a complete real 'line'. This jump from '1-dimensional' to '2-dimensional' space intuitively explained why $\mathbb{R}$ is a much bigger set. However, this intuition does not work for dimensions more than this. Hyper-Eulidean Spaces in all dimensions have the same cardinality! Then, a question would raise naturally: Would there be a set, that is even larger than $\mathbb{R}$? The answer is yes, and will be discussed in the next subsection.

1.7.3* Cantor's Theorem

In the same paper where Cantor published his Diagonalization Method, he also stated the proof of **Cantor's Theorem**, which says that **the power set of a set is strictly 'larger' than the original set**.

For those who don't know what is a power set, the power set of A is the collection of all subsets of A. For example, $A = \{1,2,3\}$, the power set is then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. In finite case, it is easy to see that for a finite set with n elements, the power set of it has 2^n elements. Therefore, in finite case, it is obvious that there is no surjective function from original set to its power set. However, what is surprising, is that this is also true in infinite case.

Theorem 1.7.5: Cantor's Theorem

Given any set A, there does not exist a function $f : A \to \mathcal{P}(A)$ that is surjective.

Proof. Assume for contradiction, that $f : A \to \mathcal{P}(A)$ is surjective. Note that for each element $a \in A$, $f(a)$ is a *subset* of A. (This proof is super tortuous, please follow very carefully!)
Surjective means that for each $y \in \mathcal{P}(A)$, there exists $a \in A$, such that $f(a) = y$. To arrive a contradiction, we will produce a set $B \subseteq A$ such that it is not equal to $f(a)$ for any $a \in A$.

For each $a \in A$, consider $f(a) \subseteq A$. We will conclude all a in a set B such that $f(a)$ does not contain a. In precise,

$$B = \{a \in A : a \notin f(a)\}$$

Now, because f is surjective, there must be some $a' \in A$ such that $f(a') = B$.

- If $a' \in B$, then $a' \notin f(a')$ by the definition of B. Since $f(a') = B$, we have $a' \notin B$, which is a contradiction.
- If $a' \notin B$, then $a' \in f(a')$ by the definition of B. Since $f(a') = B$, we have $a' \in B$, which is a contradiction.

Therefore, we have a contradiction, f cannot be surjective. □

This theorem will directly mean that, the cardinality of $\mathcal{P}(\mathbb{R})$ is larger than the cardinality of $\mathbb{R}$. We find an even larger set than $\mathbb{R}$! Moreover, we will have a full spectrum of cardinalities, such that $\mathcal{P}(\mathcal{P}(\mathbb{R}))$ is larger than $\mathcal{P}(\mathbb{R})$, and $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R})))$ is larger than $\mathcal{P}(\mathcal{P}(\mathbb{R}))\cdots$ and there does not exist a 'largest set'. Thus, statement like 'Let U be a set of all possible things' would become a paradox, because we can immediately find a larger set by constructing the power set of U.

To see the most important application of this theorem, let's first prove that $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$.

Example 1.7.6: $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$

Define $f : \mathcal{P}(\mathbb{N}) \to S$, where

$$S = \{(a_1, a_2, a_3, \cdots) : a_n = 0 \text{ or } 1\}$$

by $f(A) = (a_1, a_2, a_3, \cdots)$ where $a_i = 0$ if $i \notin A$ and $a_i = 1$ if $i \in A$, for each $i \in \mathbb{N}$. This is a bijective map, thus $\mathcal{P}(\mathbb{N}) \sim S$. Recall Example 1.7.2, we have proved that $S \sim \mathbb{R}$. Therefore, $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$.

The cardinality of natural numbers and real numbers are so important, so they have a fancy name.

Definition 1.7.7: Aleph Number

1. The cardinality of natural number is called **Aleph 0**, and is denoted as $\aleph_0$.
2. The cardinality of real numbers is called **Aleph 1**, and is dentoed as $\aleph_1$, where $2^{\aleph_0} = \aleph_1$.

The more rigorous definition of aleph numbers would be stated in my Set Theory note. A question would naturally raise: Is there any other aleph numbers between $\aleph_0$ and $\aleph_1$? Cantor published a hypothesis that there is no such aleph number.

Conjecture 1.7.8: Continuum Hypothesis

There does not exist an aleph number c such that

$$\aleph_0 < c < \aleph_1$$

This connected back to the time of **'The Third Mathematical Crisis'**, when Bertrand Russell (1872-1970) stated his famous **'Russell's Paradox'**. It says that

$$\text{Let } R = \{x : x \notin x\}, \text{ then } R \in R \Longleftrightarrow R \notin R$$

A lively example of this is called **Barber Paradox**. The barber is the "one who shaves all those, and those only, who do not shave themselves". The question is, does the barber shave himself? If the barber shaves himself, then himself becomes the group of people who shaves themselves, so he cannot shave himself. If he doesn't, then he must shave himself because he shaves all those who do not shave themselves. A statement cannot be simultaneously right and wrong!

After few decades, there was a system of axiom constructed in set theory, called 'ZFC system', excluded the situation which Russell presented, and ended the Third Mathematical Crisis. Is that the end? No! **Kurt Gödel** (1906-1978) then stated his famous **Incompleteness Theorem**, which said that even in ZFC system, mathematics is not complete, i.e., there exists a theorem that we cannot prove it right or wrong.

What does this story relate to Continuum Hypothesis? Indeed, Continuum Hypothesis is one of the theorem that is 'undecidable', where it can be accepted or rejected without making any logical contradictions. Whether continuum Hypothesis is true or not, will be never known to us. To intuitively explain why this happens, you can go back to see the proof of Cantor's Theorem, which arrives the contradiction in the way like 'If $a \in B$, then $a \notin B$ and if $a \notin B$, then $a \in B$', which is a similar kind of paradox!

1.8* The Dedekind Cuts: Completion from $\mathbb{Q}$ to $\mathbb{R}$

This section is a hard section and can be skipped without losing coherence.

We refer the Supremum as an ‘axiom’, meaning that there is nothing to be proved. The real numbers were defined simply as an extension of the rational numbers in which bounded sets have supremum. No attempt was made to demonstrate that such extension is possible. Now, in this advanced section, we will actually prove that such extension exist.

1.8.1* Cut

We begin this chapter pretended that we don’t know there exists a thing called ‘real number’, and we assume we know all the familiar addition, multiplication and order rule for rational numbers. The goal is to extend rational numbers into a larger set so that Supremum Property holds.

Definition 1.8.1: Cut

A subset A of the rational numbers is called a **cut** if

1. $A \neq \emptyset$ amd $A \neq \mathbb{Q}$.
2. If $r \in A$, then for all $q \in \mathbb{Q}$ such that $q < r$, we have $q \in A$.
3. A does not have a maximum. i.e., if $r \in A$, then there exists $s \in A$ with $r < s$.

This is the main tool used in constructing real numbers in this chapter. Let’s see some examples of cut.

Example 1.8.2: Examples of Cuts

1. Fix $r \in \mathbb{Q}$. The set $C_r = \{t \in \mathbb{Q} : t < r\}$ is a cut.
2. $T = \{t \in \mathbb{Q} : t^2 < 2 \text{ or } t < 0\}$ is a cut.
3. $U = \{t \in \mathbb{Q} : t^2 \leqslant 2 \text{ or } t < 0\}$ is a cut. The proof of statement 3 in the definition of cut for U can follow the pattern in proof of Proposition 1.4.5.
4. **Counterexample:** $S = \{t \in \mathbb{Q} : t \leqslant 2\}$ is not a cut since it has maximum 2.

All the verification of 3 properties of cut above are easy, and thus are omitted here. Now we define our goal: The set of real numbers.

Definition 1.8.3: Real Number in Dedekind Cut Sense

The real numbers $\mathbb{R}$ is the set of all cuts in $\mathbb{Q}$.

You may ask: what? we define real numbers as sets! This looks very weird at first. The most intuitive (but heuristic) explanation to this weird definition is that, we can construct a bijection from each cut to each real number such that for a cut A, it is mapped to a real number on the 'cut point'. For example, for the cut T above, it is mapped to the real number $\sqrt{2}$. (**Note:** Since we assume at first we don't know real numbers, including $\sqrt{2}$, this explanation is just heuristic one.) This bijection is called a **isomorphism** if and only if the algebraic structure on $\mathbb{R}$ we defined above is the same as the set of real numbers in our common sense. Then the two sets are called **isomorphic**. If two sets are isomorphic, they are essentially the same, with just different notations.

Now we discuss exactly which algebraic structures $\mathbb{R}$ should obtain. Before that, we need to know what is a 'structure'.

1.8.2* Field and Ordering

Definition 1.8.4: (Binary) Operation

Given a set F, an **operation** on F is a function $f : F \times F \to F$.

For example, the 'addition' operation on rational numbers takes $(2, 3) \in \mathbb{Q} \times \mathbb{Q}$ to the element $5 \in \mathbb{Q}$. The 'multiplication' operation on rational numbers takes $(2, 3) \in \mathbb{Q} \times \mathbb{Q}$ to the element $6 \in \mathbb{Q}$. With this, we can define what is a field.

Definition 1.8.5: Field

A triple $(F, +, \times)$, where F is a set and $+, \times$ are two arbitrary operations, is a **field** if

- Commutativity: $x + y = y + x$ and $x \times y = y \times x$, $\forall\, x, y \in F$.
- Associativity: $(x + y) + z = x + (y + z)$ and $(x \times y) \times z = x \times (y \times z)$, $\forall\, x, y, z \in F$.
- Identity: There exists $0 \in F$ and $1 \in F$ such that $x + 0 = x$ and $x \times 1 = x$ for all $x \in F$.
- Inverse: Given $x \in F$, there exists $-x \in F$ such that $x + (-x) = 0$. If $x \neq 0$, there exists an element $x^{-1} \in F$ such that $x \times x^{-1} = 1$.
- Distributive Property: $x \times (y + z) = x \times y + x \times z$, $\forall\, x, y, z \in F$.

Note: If you are the first time encountering these definitions, note that the $+$ and $\times$ notation need not to represent addition and multiplication. As long as there are two operations on the set that satisfies these 5 properties correspondingly, it is a field. For example, sometimes in functional spaces, the function composition $\circ$ would take the position of $\times$.

Example 1.8.6: Examples of Fields

$\mathbb{Q}$ is a field, $\mathbb{N}$ and $\mathbb{Z}$ are not field, as you can verify.

Definition 1.8.7: (Binary) Relation

A **relation** on F is a subset of $F \times F$.

This definition is very abstract. However, the following definition would give a strict example of this.

Definition 1.8.8: Ordering/Ordered Field

An **Ordering** on a set F is a relation, represented by $\leqslant$, with properties

- At least one of the $x \leqslant y$ and $y \leqslant x$ is true, $\forall x, y \in F$.
- If $x \leqslant y$ and $y \leqslant x$, then $x = y$, $\forall x, y \in F$.
- If $x \leqslant y$ and $y \leqslant z$, then $x \leqslant z$, $\forall x, y, z \in F$.

A field F is called an **ordered field** if F is endowed with an ordering such that

- If $y \leqslant z$, then $x + y \leqslant x + z$, $\forall x, y, z \in F$.
- If $0 \leqslant x$, $0 \leqslant y$, then $0 \leqslant x \times y$, $\forall x, y \in F$.

Since $\mathbb{Q}$ is a field, and has an ordering on it, our goal now is to construct addition, multiplication, and ordering on $\mathbb{R}$, such that it is ordered, and it is a field.

1.8.3* Algebra on $\mathbb{R}$

We first define an ordering on $\mathbb{R}$.

Definition 1.8.9: Ordering on $\mathbb{R}$

Let $A, B \in \mathbb{R}$ be two cuts. Define $A \leqslant B$ to mean $A \subseteq B$.

Proof. Now we need to prove this definition satisfies the 3 properties of an ordering.

1. Suppose $A \nsubseteq B$. We need to prove that $B \subseteq A$. If $A \nsubseteq B$, there exists $a \in A$ such that $a \notin B$. This means that $\forall b \in B, b < a$. Then, by the second property in definition of cut, we have $\forall b \in B$, $b \in A$. This means that $B \subseteq A$.
2. If $A \subseteq B$ and $B \subseteq A$, then $A = B$ by definition of equality of set.
3. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$ by the property of set.

Therefore, this definition satisfy the properties of ordering. □

Further, we define an addition on $\mathbb{R}$.

Definition 1.8.10: Addition on $\mathbb{R}$

Let $A, B \in \mathbb{R}$ be cuts. Define

$$A + B = \{a + b : a \in A,\, b \in B\}$$

We first need to prove that $A + B \in \mathbb{R}$, i.e., $A + B$ is indeed a cut.

Proof. We need to go through the three properties of cuts.

- Since A, B are cuts, by property 1 of cut, $A, B \neq \emptyset$. Therefore, we can find $a \in A$ and $b \in B$, then $a + b \in A + B$. Thus $A + B \neq \emptyset$.

  Since A, B are cuts, by property 1 of cut, $A, B \neq \mathbb{Q}$. Therefore, we can find $a' \notin A$ and $b' \notin B$, then for all $a \in A$ and $b \in B$, we have $a < a'$, $b < b'$. Therefore, for all $a + b \in A + B$, we will have $a + b < a' + b'$. Thus $a' + b' \notin A + B$. We have $A + B \neq \mathbb{Q}$.

- To prove property 2 of cut, let $a + b \in A + B$ be arbitrary and let $s \in \mathbb{Q}$ satisfy $s < a + b$. Then, $s - b < a$, which implies that $s - b \in A$ because A is a cut. Then,

  $$s = (s - b) + b \in A + B$$

  Since s is arbitrary, we have for every $s \in \mathbb{Q}$ that $s < a + b$, we also have $s \in A + B$.

- To prove property 3, since A, B are cuts, for $a \in A, b \in B$, we can find $a' \in A, b' \in B$ such that $a < a', b < b'$. Then, for each $a + b \in A + B$, we can find $a' + b' \in A$ such that $a + b < a' + b'$.

Therefore, $A + B$ is indeed a cut. □

Then, we need to prove that this definition satisfies the related properties in the field, and also the ordering field property 1.

Proof.

- We first prove the **Commutativity**. Obviously,

  $$A + B = \{a + b : a \in A,\, b \in B\} = \{b + a : a \in A,\, b \in B\} = B + A$$

- Then, we prove the **Associativity**. Obviously,

$$(A+B)+C = \{(a+b)+c : a \in A,\, b \in B, c \in C\} = \{a+(b+c) : a \in A,\, b \in B, c \in C\} = A+(B+C)$$

- Next, we prove the existence of **Identity**, define

$$O = \{p \in \mathbb{Q} : p < 0\}$$

We want to prove that this is served as the identity.
($\Longrightarrow$) Let $a + o \in A + O$ where $a \in A$ and $o \in O$. Then $o < 0$. Therefore, $a + o < a$. By property of cut, $a + o \in A$. Thus $A + O \subseteq A$.
($\Longleftarrow$) Let $a \in A$. Then by property of cut, we can find $a < a' \in A$. Define $s = a - a' < 0$. We have $s \in O$. Then, $a = s + a' \in A + O$. Thus, $A \subseteq A + O$.
In conlcusion, we have $A = A + O$, proving that O is the identity.

- Now, we prove the existance of **Inverse**. This is a little bit more difficult than the identity, since the normal definiton of $-A$ would not be a cut. We alternatively, define

$$-A = \{r \in \mathbb{Q} : \text{ there exists } t \notin A \text{ with } t < -r\}$$

This is just like a 'reflection' of the 'cut point' with respect to the origin.

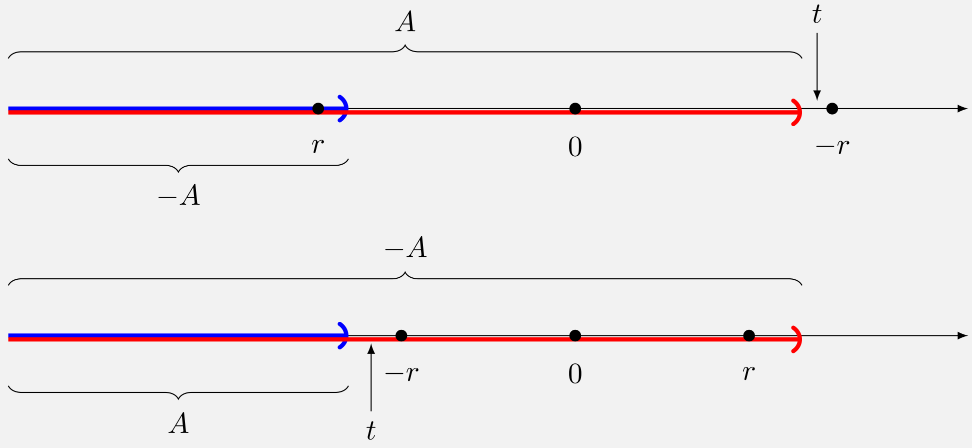


Figure 1.12: A and its inverse

We first need to prove that $-A$ is indeed a cut.

1. To prove the first property of cut, since A is a cut, we can find $t \notin A$, and since $\mathbb{Q}$ is unbounded, we can find some $-r \in \mathbb{Q}$ such that $t < -r$. Thus, $-A \neq \emptyset$.

Let $a \in A$. Then for all $t \notin A$, we have $t > a$. Thus $-a \notin -A$ since if it is, then $t < -(-a) = a$, which is a contradiction. Therefore, $-A \neq \mathbb{Q}$.

2. To prove the second property of cut, let $r \in -A$ and let $q < r$. Then, $t < -r < -q$ for the $t \notin A$ such that $t < -r$. Hence, by definition of $-A$, $q \in -A$.
3. To prove the third property of cut, let $r \in -A$ and let $t \notin A$ such that $t < -r$. Let $q = \frac{t-r}{2}$, we have $t < q < -r$. Thus, $-q \in -A$ and $-q > r$. There is no maximum.

After this, we need to prove that this indeed defines an inverse.
($\Longrightarrow$) If $a \in A$ and $r \in -A$, then there exists $t \notin A$ with $t < -r$. Since $t \notin A$, we have $t > a$. Then, $a + r < a - t < 0$, hence $a + r \in O$. This shows that $A + (-A) \subseteq O$.
($\Longleftarrow$) Now, let $o \in O$. We would like to find $a \in A$ and $r \in -A$ satisfying $o \leqslant a + r$. This would imply $O \subseteq A + (-A)$. Since $o \in \mathbb{Q}$, and $o < 0$, let $o = -p/q$ where $p, q \in \mathbb{N}, q \neq 0$. We first prove the lemma:
For any cut A and $n \in \mathbb{N}$, we can find $z \in A$ where

$$\frac{z}{n} \in A \quad \text{and} \quad \frac{z+1}{n} \notin A$$

To do this, start with $a \in A$ and $a' \notin A$. Find $N, M \in \mathbb{Z}$ such that

$$\frac{N}{n} < a \quad \text{and} \quad \frac{M}{n} > a'$$

Clearly $N/n \in A$ and $M/n \notin A$. Therefore, there must exist a transition point z such that the lemma holds.
Now if we let $a = \frac{n}{2q} \in A$ and $\frac{n+1}{2q} \notin A$, then $r = -\frac{n+2}{2q} \notin A$, and

$$a + r = -\frac{1}{q} \geqslant -\frac{p}{q} = o$$

Therefore, $O \subseteq A + (-A)$. In conclusion, $A + (-A) = O$.

- Finally, we prove the **first property of ordering field**.

Let $Y \subseteq Z$. Let $x \in X$ and $y \in Y$. Since $Y \subseteq Z$, we have $y \in Z$ either. This implies $x + y \in X + Z$. Thus, $X + Y \subseteq X + Z$. □

Note: We cannot simply define the inverse as

$$-A = \{r \in \mathbb{Q} : -r \notin A\}$$

which would be the first thought of most people. The counterexample is that for $A = \{t \in \mathbb{Q} : t < -2\}$,we will have $-A = \{t \in \mathbb{Q} : t \leqslant 2\}$, which is not a cut. Therefore, we need the additional 't' in the definiton of inverse to avoid this situation.

Now, we define a multiplication in $\mathbb{R}$. This is also difficult because negative set times negative set would be positive. Therefore, we first consider the case of $A \geqslant O$ and $B \geqslant O$.

Definition 1.8.11: Multiplication on $\mathbb{R}$, positive case

Given $A \geqslant O$ and $B \geqslant O$, define the product

$$AB = \{ab : a \in A, b \in B \text{ with } a, b \geqslant 0\} \cup O$$

Similarly, we need to first prove that the definition indeed results in a cut.

Proof.

- choose $-1 \in O$. Then, $-1 \in AB$, we have $AB \neq \emptyset$. Since A, B are cuts, choose $a' \notin A$,$b' \notin B$, then for all $a \in A, b \in B$, we have $a' > a, b' > b$. Also, $a', b' > 0$ since otherwise it will be in O. Thus, for all $r \in AB$, $a'b' > r$. This indicates that $AB \neq \mathbb{Q}$.
- Suppose $r \in AB$, let $q < r$. If $r < 0$ then $q < r < 0$, we have $q \in AB$. If $r > 0$, $r = ab$ for some $a \in A$ and $b \in B$ with $a, b \geqslant 0$. If $q < 0$, then obviously $q \in AB$. If $q > 0$, we have $\frac{q}{b} < \frac{r}{b} = a$, thus $\frac{q}{b} \in A$. This would indicate that $q = \frac{q}{b} b \in AB$.
- Let $r \in AB$. If $r < 0$ then obviously $\frac{r}{2} \in AB$ and $r < \frac{r}{2} \in AB$. If $r > 0$ then, $r = ab$ for some $a \in A, b \in B, a, b, \geqslant 0$. Sonce A, B are cuts, we could find $a' \in A$ and $b' \in B$ with $a' > a$ and $b' > b$. Then $a'b' \in AB$ and $a'b' > ab$. There is no maximum.

Therefore, AB is indeed a cut. □

After defining this, we can accordingly define the negative cut cases such that

$$AB = \begin{cases} -[A(-B)], & \text{if } A \geqslant O \text{ and } B < O \\ -[(-A)B], & \text{if } A < O \text{ and } B \geqslant O \\ (-A)(-B), & \text{if } A < O \text{ and } B < O \end{cases}$$

We can accordingly, prove that these are cuts, and prove the commutativity, associativity, distributive property, and the second property of the ordering field. However, we will not do it here since it will be way tedious. The proving pattern is just like that for addition. Just note that the multiplicative identity is

$$I = \{t \in \mathbb{Q} : t < 1\}$$

and the multiplicative inverse for the positive cut A (defined in Definition 1.8.11) is defined as

$$A^{-1} = \left\{ a \in \mathbb{Q} : \text{ there exists } t \notin A \text{ with } t < \frac{1}{a} \right\} \cup \{0\} \cup O$$

1.8.4* Rediscover Supremum Property

After proving that $\mathbb{R}$ satisfies all the **Ordered Field** Property, we finally, prove the **Supremum Property**, which we see as an axiom throughtout the first chapter.

Note that now, since we define real numbers as cuts, 'a set of real numbers' would be a collection of cuts (set of sets). For these collections we will denote them using the calligraphy font, such as $\mathcal{A}$. Obviously, for a set $\mathcal{A}$ which is nonempty and bounded above, the desired supremum would be the union of all cuts $A \in \mathcal{A}$

$$S = \bigcup_{A \in \mathcal{A}} A$$

Now we prove that S is indeed a cut.

Proof.

- Let $A \in \mathcal{A}$, and $a \in A$. Then $a \in S$. Thus $S \neq \emptyset$. Now let B be a bound on $\mathcal{A}$, let $b' \notin B$. Since for any $s \in S$, we will have $s \in A$ for some $A \in \mathcal{A}$, and $A \leqslant B$ for all A, we have $s \in B$. This will indicate that $b' > s$. Thus, $b' \notin S$, $S \neq \mathbb{Q}$.
- Consider arbitrary $s \in S$ with $s \in A \in \mathcal{A}$. Then, for any $q < s$ we have $q \in A$, thus $q \in S$.
- Continuing the proof of property 2, we can also find a $a \in A$ such that $s < a$. There is no maximum.

Therefore, S is indeed a cut. □

Finally, we prove that S is the supremum for $\mathcal{A}$.

Proof. First, S is indeed an upper bound since for all $a \in A$, we have $a \in S$. Second, let B be an upper bound for $\mathcal{A}$. Now for any $s \in S$ with $s \in A \in \mathcal{A}$, we have $A \leqslant B$, so $s \in B$. Therefore, $S \leqslant B$, S is indeed a supremum! □

We are not finished yet. Since this construction of $\mathbb{R}$ as a set of cuts, is a completely different notation from that of rational numbers. We are doing an extension, meaning that $\mathbb{Q}$ should be a subfield of $\mathbb{R}$.

However, note that if we write all rational numbers as 'rational cuts'

$$Q = \{t \in \mathbb{Q} : t < r, r \in \mathbb{Q}\}$$

This would be an **isomorphism** from rational numbers to rational cuts, and indeed, we can easily verify that the set of all rational cuts is an ordered field (just re-prove all the ordering field properties before, using the sets of all rational cuts).

In conclusion, our result is:

Theorem 1.8.12: Extension of $\mathbb{Q}$ to $\mathbb{R}$

There exists an ordered field in which every nonempty set that is bounded above has a supremum. In addition, this field contains $\mathbb{Q}$ as a subfield.

Chapter 2

Infinite Sequences and Series

2.1 Limit of a Sequence

The first important mathematical object we need to analysis in this chapter is **sequences**.

Definition 2.1.1: Sequence

A **sequence** is a function whose domain is $\mathbb{N}$.

Considering the definition, we can reasonably write a sequence in the form of $(a_1, a_2, a_3, \cdots)$ where a_i is the element that $i \in \mathbb{N}$ maps to. We always denote it as $(a_n)_{n\in\mathbb{N}}$, or simply, (a_n).

Note: Sometimes sequences will start not with x_1, but with x_{n_0} where $n_0 > 1$, $n_0 \in \mathbb{N}$. This does not matter much, because we are only interested in how the sequence behaves at the infinite 'tail', i.e., the **limit**.

Definition 2.1.2: Convergence of a Sequence

A sequence (a_n) **converges** to a real number a if,

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \text{ s.t. } n > N \Longrightarrow |a_n - a| < \epsilon$$

We denote this as $\lim_{n\to\infty} a_n = a$.

This is **the** most important mathematical languange in analysis, called ϵ-δ language, or ϵ-N in this case. To fully understand the meaning of this definition, we first fix an ϵ, and by the definition, there exists a point, where all of the terms in the sequence after this point should be in the ϵ-range centered at a.

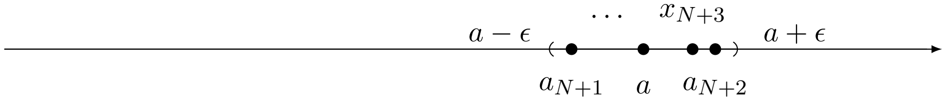


Figure 2.1: Definition of convergence

The critical point is that, we can choose all ϵ, regardless how small it is, we can always find N such that, all the points after are ‘approaching’ the limit a, and they can never jump out this ϵ range.

Definition 2.1.3: Divergence of a Sequence

A sequence that does not converge is said to **diverge**.

Note: We cannot identify divergence by the negation of the definition of convergence, i.e.,

$$\exists\, \epsilon > 0, \text{ s.t. } \forall\, N \in \mathbb{N}, \text{ s.t. } \exists\, n > N \Longrightarrow |a_n - a| \geqslant \epsilon$$

since by this statement, the sequence may converge, just not converges to the point a.

We can easily see that the limit of a sequence must be unique.

Proposition 2.1.4: Uniqueness of Limit

The limit of a sequence is unique.

Proof. Suppose a, a' are limits of a sequence (a_n). Then, by definition,

$$\text{Fix } \epsilon > 0, \exists\, N_1 \in \mathbb{N}, \text{ s.t. } n > N_1 \Longrightarrow |a_n - a| < \frac{\epsilon}{2}$$

$$\text{Fix } \epsilon > 0, \exists\, N_2 \in \mathbb{N}, \text{ s.t. } n > N_2 \Longrightarrow |a_n - a'| < \frac{\epsilon}{2}$$

Therefore, for current fixed ϵ and $n > \max\{N_1, N_2\}$, we have

$$|a - a'| = |a - a_n + a_n - a'| \leqslant |a - a_n| + |a_n - a'| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

This is true for arbitrary ϵ. Therefore, $a = a'$. □

The proof of convergence using definition can generally follow these steps:

- ‘Let $\epsilon > 0$ be arbitrary’.
- Demonstrate a choice for $N \in \mathbb{N}$. This step usually requires some work on draft paper, to see which N is suitable. Note that N may (and commonly will) depend on ϵ.
- Assume $n > N$, show that $|a_n - a| < \epsilon$.

Example 2.1.5: Prove convergence using definition

Prove that

$$\lim \frac{2n^2}{n^3+3} = 0$$

Things that will appear on your draft paper:

$$\left|\frac{2n^2}{n^3+3} - 0\right| = \frac{2n^2}{n^3+3} < \frac{2n^2}{n^3} = \frac{2}{n} < \epsilon$$

it seems that $N = \frac{2}{\epsilon}$ would be a good choice.

Things that will appear on your answer sheet:

Proof. Let ϵ be arbitrary. Let $N = \frac{2}{\epsilon}$. Assume $n > N$. Then,

$$\left|\frac{2n^2}{n^3+3} - 0\right| = \frac{2n^2}{n^3+3} < \frac{2n^2}{n^3} = \frac{2}{n} < \frac{2}{2}\epsilon = \epsilon$$

Therefore, by definition, the sequence converges to 0. □

2.2 Properties of Limit

We first see that every convergent sequence are bounded. To rigorously state this, we need to define what is 'bounded'.

Definition 2.2.1: Bounded Sequence

A sequence (x_n) is bounded if there exists $M > 0$ such that $|x_n| \leqslant M$ for all $n \in \mathbb{N}$.

Proposition 2.2.2: Boundedness of Convergence Sequence

Every convergent sequence is bounded.

Proof. Suppose (x_n) converges to l. Then, fix $\epsilon = 1$, we have

$$\exists\, N \in \mathbb{N}, \text{ s.t. } n \geqslant N \implies |x_n - l| < 1$$

This means that for all $n \geqslant N$

$$|x_n| \leqslant |x_n - l| + |l| < |l| + 1$$

For the terms before N, since there are only finite terms, there must be a maximum. Let

$$M = \max\{|x_1|, |x_2|, \cdots, |x_{N-1}|, |l| + 1\}$$

We can conclude that $|x_n| \leqslant M$ for all $n \in \mathbb{N}$. □

Next, we state **Algebraic Limit Theorem**, which shows that limit of sequences behave very well under addition, multiplication and division.

Proposition 2.2.3: Algebraic Limit Theorem

Let $\lim a_n = a$ and $\lim b_n = b$. Then,

1. $\lim(ca_n) = ca, \forall\, c \in \mathbb{R}$
2. $\lim(a_n + b_n) = a + b$
3. $\lim(a_n b_n) = ab$
4. $\lim(a_n/b_n) = a/b$, provided $b \neq 0$

Proof.

1. When $c = 0$, it is trivial. So suppose $c \neq 0$. Since $\lim a_n = a$, we have

$$\forall\, \epsilon > 0, \exists\, N \in \mathbb{N},\ \text{s.t. } n > N \Longrightarrow |a_n - a| < \frac{\epsilon}{|c|}$$

Then we have for $n > N$,

$$|ca_n - ca| = |c||a_n - a| < |c|\frac{\epsilon}{|c|} = \epsilon$$

which shows our desired result.

2. Since $\lim a_n = a$ and $\lim b_n = b$, we have

$$\forall\, \epsilon > 0, \exists\, N_1 \in \mathbb{N},\ \text{s.t. } n > N_1 \Longrightarrow |a_n - a| < \frac{\epsilon}{2}$$

$$\forall\, \epsilon > 0, \exists\, N_2 \in \mathbb{N},\ \text{s.t. } n > N_2 \Longrightarrow |b_n - b| < \frac{\epsilon}{2}$$

Let $N = \max\{N_1, N_2\}$. Then, for $n > N$, we will have

$$|(a_n + b_n) - (a + b)| \leqslant |a_n - a| + |b_n - b| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

3. This is a little bit harder. The goal is to find an N such that for all $n > N$ we have $|a_n b_n - ab| < \epsilon$. Note that

$$|a_n b_n - ab| = |a_n b_n - ab_n + ab_n - ab| \leqslant |a_n b_n - ab_n| + |ab_n - ab| = |b_n||a_n - a| + |a||b_n - b|$$

Since b_n converges, by Proposition 2.2.2, it is bounded. Therefore, $|b_n| \leqslant M$ for some M and for all $n \in \mathbb{N}$. Then if we choose N_1 and N_2 such that

$$\forall \epsilon > 0, \exists N_1 \in \mathbb{N}, \text{ s.t. } n > N_1 \Longrightarrow |a_n - a| < \frac{\epsilon}{2M}$$

$$\forall \epsilon > 0, \exists N_2 \in \mathbb{N}, \text{ s.t. } n > N_2 \Longrightarrow |b_n - b| < \frac{\epsilon}{2|a|}$$

and let $N = \max\{N_1, N_2\}$. Then for all $n > N$, we have

$$|a_n b_n - ab| \leqslant |b_n||a_n - a| + |a||b_n - b| < M\frac{\epsilon}{2M} + |a|\frac{\epsilon}{2|a|} = \epsilon$$

4. We can prove this statement if only if we can prove

$$(b_n) \longrightarrow b \quad \text{implies} \quad \left(\frac{1}{b_n}\right) \longrightarrow \frac{1}{b}$$

since we can then get the desired result from (3). The goal is to find N such that for all $n > N$ we have $\left|\frac{1}{b_n} - \frac{1}{b}\right| < \epsilon$. Note that

$$\left|\frac{1}{b_n} - \frac{1}{b}\right| = \frac{|b - b_n|}{|b||b_n|}$$

We know $|b - b_n|$, so we need to control the size of $\frac{1}{|b||b_n|}$. **This is a very important trick**. Now we are not concerning about the upper bound of b_n, we are concerning the lower bound. The trick is to use the convergence relation between (b_n) and b to construct desired inequality. Since $(b_n) \to b$, we can fix $\epsilon = \frac{|b|}{2}$, then

$$\forall \epsilon > 0, \exists N_1 \in \mathbb{N}, \text{ s.t. } n > N_1 \Longrightarrow |b_n - b| < \frac{|b|}{2}$$

Further simplify this relationship, we have for all $n > N_1$,

$$|b_n| = |(b_n - b) + b| > ||b_n - b| - |b|| = |b| - |b_n - b| > \frac{|b|}{2}$$

where the first inequality is by inverse triangular inequality. Therefore, if we choose N_2 such that

$$\forall \epsilon > 0, \exists N_2 \in \mathbb{N}, \text{ s.t. } n > N_2 \Longrightarrow |b_n - b| < \frac{\epsilon|b|^2}{2}$$

and let $N = \max\{N_1, N_2\}$. Then for all $n > N$ we have

$$\left|\frac{1}{b_n} - \frac{1}{b}\right| = \frac{|b - b_n|}{|b||b_n|} < \frac{\epsilon|b|^2}{2}\frac{1}{|b|\frac{|b|}{2}} = \epsilon$$

This shows the desired result. □

Next, we show **Order Limit Theorem**, which shows that the limit preserves the order of two related elements.

Proposition 2.2.4: Order Limit Theorem

Let $\lim a_n = a$ and $\lim b_n = b$. Then,

1. If $a_n \leqslant b_n$ for all $n \in \mathbb{N}$, then $a \leqslant b$
2. If $c \in \mathbb{R}$, and $a_n \leqslant c$ for all $n \in \mathbb{N}$, then $a \leqslant c$. Similarly, if $b_n \geqslant c$ for all $n \in \mathbb{N}$, then $b \geqslant c$

Proof.

1. For every $\epsilon > 0$ we can find $N \in \mathbb{N}$ such that for all $n > N$, we have

$$\forall\, \epsilon > 0, \exists\, N \in \mathbb{N},\ \text{s.t. } n > N \Longrightarrow a_n - a > -\epsilon$$

$$\forall\, \epsilon > 0, \exists\, N \in \mathbb{N},\ \text{s.t. } n > N \Longrightarrow b_n - b < \epsilon$$

Therefore, we can get

$$a - b \leqslant a - b + (b_n - a_n) = (b_n - b) - (a_n - a) < \epsilon - (-\epsilon) = 2\epsilon$$

where the first inequality hold because $a_n \leqslant b_n$. Therefore,

$$b > a - 2\epsilon$$

Since this holds for all $\epsilon > 0$, we have $b \geqslant a$.

2. Take $a_n = c$ or $b_n = c$, we can prove the second argument.

□

The **most useful** corollary of Proposition 2.2.4 is the famous **Squeeze Theorem**.

Corollary 2.2.5: Squeeze Theorem

If $x_n \leqslant y_n \leqslant z_n$ for all $n \in \mathbb{N}$, and $\lim x_n = \lim z_n = l$, then $\lim y_n = l$.

2.3 Completeness and Convergence

2.3.1 Axiom of Completeness III: The Monotone Convergence Theorem

Here we consider the third form of Axiom of Completeness of Real Number: Monotone Convergence Theorem. To state this, we first define what is a monotone sequence.

Definition 2.3.1: Monotone Sequence

A sequence (a_n) is **increasing** if $a_n \leqslant a_{n+1}$ for all $n \in \mathbb{N}$ and **decreasing** if $a_n \geqslant a_{n+1}$ for all $n \in \mathbb{N}$. A sequence is **monotone** if it is increasing or decreasing.

Now we state the theorem.

Theorem 2.3.2: Monotone Convergence Theorem (MCT)

If a sequence is monotone and bounded, then it converges. Specifically, if it is increasing, then it converges to the supremum of elements. If it is decreasing, then it converges to the infimum of elements.

Proof. Let (a_n) be monotone and bounded. Assume (a_n) is increasing, and the decreasing case can be handled similarly. We let

$$s = \sup\{a_n : n \in \mathbb{N}\}$$

We will then prove that $\lim a_n = s$. Let $\epsilon > 0$. Because s is the least upper bound, $s - \epsilon$ then, is not the upper bound. Then, there exists a point s_N in the sequence such that $s - \epsilon < a_N$. Since a_n is increasing, we have if $n \geqslant N$, we have $a_N \leqslant a_n$. Hence,

$$s - \epsilon < a_N < a_n \leqslant s < s + \epsilon$$

for all $n > N$, as desired. □

Actually, we could have used the MCT in place of Supremum Property as our starting axiom for building a proper theory of real numbers. Intuitively, for a nonempty set which is bounded above, there must exist a increasing bounded sequence in it, and it converges by MCT. The limit is then the supremum. One of the proof is stated below.

Proof. □

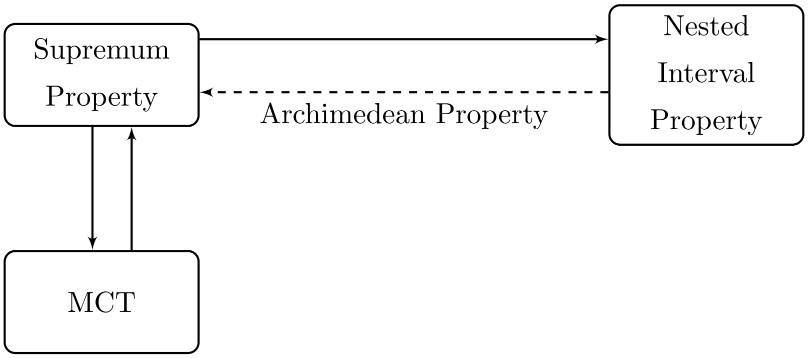


Figure 2.2: Relation between Axiom of Completeness

2.3.2 Axiom of Completeness IV: Bolzano-Weierstrass Theorem

A very important terminology in analysis is **subsequence**. A sequence can be divergent with some of its subsequence converges.

Definition 2.3.3: Subsequence

Let (a_n) be a sequence of real numbers, and let $n_1 < n_2 < n_3 < \cdots$ be an increasing sequence of natural numbers. Then the sequence

$$(a_{n_1}, a_{n_2}, a_{n_3}, \cdots)$$

is called a **subsequence** of (a_n), denoted by (a_{n_k}), where $k \in \mathbb{N}$.

Obviously, from intuition, if a sequence converges, then its subsequences also converge.

Proposition 2.3.4: Convergence of Subsequence

Subsequences of a convergent sequence converge to the same limit as the original sequence.

Proof. Assume $(a_n) \to a$, let (a_{n_k}) be a subsequence. Given $\epsilon > 0$, there exists N such that $|a_n - a| < \epsilon$ whenever $n \geqslant N$. Because $n_k \geqslant k$ for all k, the same N will suffice for the subsequence. □

Note that not all sequences contain a convergent subsequence. Consider $(a_n) = (1, 2, 3, 4, \cdots)$, there is no subsequence contained in it. However, for bounded sequence, the situation is changed.

Theorem 2.3.5: Bolzano-Weierstrass Theorem

Every bounded sequence contains a convergent subsequence.

Proof. □

Chapter 3

Topology on the Real Line

Chapter 4

Continuity of Functions on $\mathbb{R}$

Part II

PART II: Calculus on the Real Line

Part III

PART III: Metric Space

Part IV

PART IV: Calculus on the Real Space

Bibliography

[1] Abbott, S. (2015). *Understanding analysis.* Springer.

[2] Rudin, W. (1953). *Principles of mathematical analysis.*

[3] Tao, T. (2006). *Analysis i*, volume 1. Springer.