Analysis-02

Yifan Wei

May 11, 2018

"There is no Royal Road to geometry"

Euclid

Preparation

1. Exercise 1 in Analysis-01

   From now on we will call $S/\sim$ *the quotient set of* S *over* $\sim$.

2. Exercise 2 in Analysis-01

   This indicates surjections and injections are *quasi-invertible*, and it's not difficult to see bijections are always invertible. And the *image* of A under $f : A \to B$ is
   $$f(A) := \{y \in B | \exists x \in A, y = f(x)\}.$$

1 Cardinality of sets

It's good to know that the set $\mathbb{N}$ of natural numbers(ordered in the usual sense) has a ***well-ordering principle***, that is, every subset of it has a minimal element. This is not a new property and can be deduced from the definition of natural numbers.

1.1 Equipollence

Bijections are important relations between sets. An example is when we're enumerating elements of certain set, what we're doing is constructing a bijection from this set to a subset of $\mathbb{N}$.

But here is a natural question that everyone may ask:

"*Can all sets be enumerated?*"

Unfortunately this is not true. To make this clear, we can define a special relation between sets called ***equipollence***.

Definition 1.1 (Equipollence)**.** Two sets A and B are said to be equipollent **iff**(short for *if and only if*) there is a bijection from A to B. This relation is denoted by $A \leftrightarrow B$.

It's a good exercise to show this relation satisfies all the requirements to be an equivalence relation.

1. (Reflexivity) For every set A, define a function $f := \{(x, x)|x \in A\}$. This is a bijection because it's both surjective and injective.
2. (Symmetry) If $f := \{(x, y)|x \in A, y \in B\}$ is the bijection from A to B, define $g := \{(x, y)|(y, x) \in f\}$.
3. (Transitivity) For bijections $f : A \to B, g : B \to C$, define $h := \{(x, y)|\exists y \in B, (x, y) \in f, (y, z) \in g\}$.

And this shocking fact:

Theorem 1.1. *S is never equipollent with $P(S)$.*

Proof. The case when S is $\emptyset$ is trivial. Suppose $f : S \to P(S)$ is a bijection. Define $E := \{x|x \notin f(x)\}$. Since f is a bijection, there must be an element y in S such that $E = f(y)$. If $y \in E$, then $y \in f(y)$, then y cannot be an element of E. However, if $y \notin E$, then $y \notin f(y)$, then y does belong to E. Such inconsistency was led by a false precondition, so f can't be a bijection. □

1.2 Classification of sets

Since equipollence is an equivalence relation, then all the sets we're studying can be classified into different classes(unions of some equivalent classes). If Peano's natural numbers are concerned, we have:

1. **Finite sets**

   Set equipollent with $\{1, 2, 3, ..., n\}$, for certain $n \in \mathbb{N}$. For such a set S we can say it has ***cardinality*** of n, denoted by $Card(S) = n$ or $|S| = n$. Note that when we use the definition of von Neumann, $|S| = n$ is the same to $S \leftrightarrow n$. (Usually it's convenient to say an empty set has cardinality of 0 and define it to be a finite set.)

2. **Infinite sets**

   (a) **Countable sets**

   Those who are equipollent with $\mathbb{N}$ (having the cardinality of $\mathbb{N}$).

   (b) **Uncountable sets**

   Set which is neither finite nor countable. For example $P(\mathbb{N})$ is an uncountable set.

The cardinality of $\mathbb{N}$ is denoted by $\aleph_0$(read as *aleph-naught* or *aleph-zero*, the first letter of Hebrew alphabet), and the cardinality of $P(\mathbb{N})$ is denoted by $2^{\aleph_0}$.

In fact we can assign each equivalent class a **cardinal number**, but the comparison of cardinal numbers is a little tricky. If we follow our instinct to say $|A| \geq |B|$ when there is a surjection from A to B. We will have no problem to show this relation is reflexive and transitive, but it's hard to prove its antisymmetry property whose proof is known as Schröder-Bernstein Theorem(Actually we've already assumed it when we are considering the order of natural numbers). The well-known continuum hypothesis(CH) states that there is no set S whose cardinality is between $\aleph_0$ and $2^{\aleph_0}$.

Why the name of this hypothesis is *continuum*? That's the topic of the next section, the ***Real Numbers***!

2 The set of Real Numbers is the *continuum*

Q:What is $\mathbb{R}$?
A:The completion of $\mathbb{Q}$!

2.1 The integers and rational numbers

Things will be interesting when we later come to *group*s and *ring*s. But I think it's useful to establish these "boring" definitions and properties now.

2.1.1 Addition & Multiplication

Addition and multiplication of natural numbers can be defined inductively, respectively. (Using von Neumann's definition of successor: $n^+ := n \cup \{n\}, 1 := 0^+$)

1. **Addition:**

   $n + 0 := n$,
   $m + n^+ := (m + n)^+$.

2. **Multiplication:**

   $n \cdot 1 := n$,
   $n \cdot m^+ := n \cdot m + n$.

They're all **binary operation**s on $\mathbb{N}$, that is, functions from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. However both of these functions are pretty *delicate*, they satisfy(A for addition, M for multiplication):

1. **Associativity**:

   $A(a, A(b, c)) = A(A(a, b), c)$, ($a + (b + c) = (a + b) + c$),
   $M(a, M(b, c)) = M(M(a, b), c)$, ($a \cdot (b \cdot c) = (a \cdot b) \cdot c$).

2. **Commutativity**:

   $A(a,b) = A(b,a)$, ($a + b = b + a$),
   $M(a,b) = M(b,a)$, ($a \cdot b = b \cdot a$).

3. **Distributivity**:

   $M(a, A(b,c)) = A(M(a,b), M(a,c))$, ($a \cdot (b + c) = a \cdot b + a \cdot c$)

   We read this as M is distributive over A (on both sides).

Another important property is each of them preserves order ($x \leq y$ meas $x \subseteq y$):

$$a \leq b, c \leq d \Rightarrow a + c \leq b + d,$$

$$a \leq b, c \leq d \Rightarrow a \cdot c \leq b \cdot d.$$

2.1.2 Integers

The set of integers $\mathbb{Z}$ (Z for German *Zahlen*) is the quotient set $\mathbb{N} \times \mathbb{N}/\sim$ with an equivalence relation defined as:

$$(a,b) \sim (c,d) \Leftrightarrow a + d = c + b.$$

And we extend addition and multiplication to equivalent classes(use $\langle a,b \rangle$ denote the class equivalent to (a,b)):

$$\langle a,b \rangle \oplus \langle c,d \rangle := \langle a + c, b + d \rangle,$$

$$\langle a,b \rangle \otimes \langle c,d \rangle := \langle a \cdot c + b \cdot d, a \cdot d + b \cdot c \rangle,$$

with the extended order $\leq$:

$$\langle a,b \rangle \leq \langle c,d \rangle \Leftrightarrow b + c \leq a + d.$$

This extension makes all *equations* of the form: $a + x = b$, solvable and with exactly *one* solution in $\mathbb{Z}$. Actually there can be many different $\mathbb{Z}$s such as the usually $\pm\mathbb{N}$, but they are all *isomorphic* to the above one, roughly speaking, there is only one *structure* of integers though we can use different forms to represent its elements.

2.1.3 Rational Numbers

The construction of $\mathbb{Q}$ is here.

It's an ordered *field*.

We have a measure of magnitude on $\mathbb{Q}$, the absolute value $|\cdot|$:

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

And the fact that $\mathbb{Q}$ is *dense*:

$$\forall x, y \in \mathbb{Q}, \text{ if } x < y \text{ then } \exists z \in \mathbb{Q},\ x < z < y.$$

But the rational numbers has a fatal defeat, they can't represent a straight line! Such as the length of the diagonal of a square.

Dedekind find the most profound essence of the continuity of a straight line is that:

"*If all points of the straight line fall into two classes such that every point of the first class lies to the left of every point of the second class, then there exists one and only one point which produces this division of all points into two classes, this severing of the straight line into two portions.*"

If we put rational numbers on a line, there will be many holes (see **Problem 1**), in a word rational numbers are discontinuous.

2.2 The *completion* of rational numbers

The key point is to assign those sequences which should have a limit a limit.

We say a space is complete when every Cauchy sequence has a limit in that space. Analogous to the construction of integers, we follow these steps to construct a desired continuum call Real Numbers:

Definition 2.1 (Cauchy sequence)**.** A Cauchy sequence (a_n) is a sequence of rational numbers that satisfies Cauchy's criterion, i.e. $\forall \epsilon \in \mathbb{Q} > 0$, $\exists N \in \mathbb{N}$, such that $\forall m, n > N$, $|a_m - a_n| < \epsilon$. Denote the set of all Cauchy sequence as $Cau(\mathbb{Q})$.

Definition 2.2 (Infinitesimal sequence)**.** An infinitesimal sequence (a_n) is a sequence such that $\forall \epsilon > 0$, $\exists N \in \mathbb{N}$, $\forall n > N$, $|a_n| < \epsilon$. (Notice that such a sequence is automatically a Cauchy sequence.)

Definition 2.3 (Equivalence of Cauchy sequences)**.** Two Cauchy sequences (a_n) and (b_n) are equivalent iff their difference $(c_n := a_n - b_n)$ is an infinitesimal sequence. We can still denote this specific equivalence relation by $\sim$.

And finally,

Definition 2.4 (Real Numbers)**.** The set of real numbers $\mathbb{R}$ is the quotient set $Cau(\mathbb{Q})/\sim$.

Through this set of definitions we can easily extend operations on $\mathbb{Q}$ to $\mathbb{R}$ once we use certain equivalent classes as bridges. For example, the (strict) ordering of real numbers is defined as: $x < y$ iff $\exists (a_n) \in x, (b_n) \in y$, $\exists N \in \mathbb{N}$, $\exists \epsilon \in \mathbb{Q} > 0$, such that, $\forall n > N$, $|a_n - b_n| \geq \epsilon$.

And the absolute value $|\cdot|$, exactly the same form:

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

Addition and multiplication can be found at exercise.

Of course there are other ways to construct real numbers such as through Dedekind cuts.

2.3 Supreme & Infimum

Definition 2.5 (Bounded sets)**.** A bounded set S of real numbers is a set that the magnitude of its elements are bounded by a real number. That is: $\exists B \in \mathbb{R}$, $\forall x \in S$, $|x| \leq B$. Such B is called a bound of S.

However usually we will meet sets which is only bounded above or bounded below. (Guess their definitions!)

An important property of $\mathbb{R}$ is that any bounded above(below) sets has a least(greatest) upper(lower) bound, called the *supreme* (*infimum*), denoted by $\sup S$ ($\inf S$). This property is called the *least-upper-bound property*.

3 Exercise

1. Modify the proof of theorem 1.1 given in the text to show there is no surjection from S to $P(S)$ as well as no injection from $P(S)$ to S.

2. Prove that if there if an infinite set S and a injection from S to $\mathbb{N}$, then S is countable.

3. The well-known fundamental theorem of arithmetic states that a natural number can be factored into a unique product of powers of prime numbers. Use this fact to prove:

   (a) Finite Cartesian product of $\mathbb{N}$ is countable.
   (**Hint:** Use $f(a_1, a_2, ..., a_n) := \prod_{i=1}^{n} p_i^{a_i}$, where p_i is the ith prime)

   (b) The set of all finite arrays is countable.

4. Prove if C is countable and $\forall i \in C$ S_i is countable, then

$$\bigcup_{i \in C} S_i \text{ is countable.}$$

   (**Hint:** show when S_is are disjoint the union is equipollent to $\mathbb{N} \times \mathbb{N}$)

5. Prove $\mathbb{Z}$ and $\mathbb{Q}$ are countable.

   (**Hint:** Write rational numbers in fractions and use Exercise 3 and 2)

6. Prove $Cau(\mathbb{Q})$ is closed under addition:

$$(a_n) + (b_n) := (c_n := a_n + b_n),$$

   and multiplication:

$$(a_n)(b_n) := (c_n := a_n b_n).$$

   Now try to give the definition of addition and multiplication of real numbers.

7. Prove there exists an identity element for addition:

$$\exists e_0 \in \mathbb{R},\ \forall x \in \mathbb{R},\ x + e_0 = x,$$

and exactly one additive inverse for each element:

$$\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x + y = e_0.$$

From now on we will call e_0 zero(0). And denote the additive inverse of x by $-x$.

8. Prove there exists an identity element for addition:

$$\exists e_1 \in \mathbb{R},\ \forall x \in \mathbb{R},\ xe_1 = x,$$

and exactly one multiplicative inverse for each non-zero element:

$$\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x + y = e_1.$$

And we will call e_1 one(1),and write the multiplicative inverse of x as $\frac{1}{x}$ or x^{-1}.

9. Prove that if (a_n) is a Cauchy sequence, then if we rearrange the position of its terms, it will be an equivalent Cauchy sequence, i.e. prove for any bijective $f : \mathbb{N} \to \mathbb{N}$

$$\forall (a_n) \in Cau(\mathbb{Q}),\ (a_n) \sim (a_{f(n)}).$$

10. Prove any Cauchy sequence can be rearranged into a bounded monotone sequence.

11. Prove any bounded monotone sequence is a Cauchy sequence. And use this fact to prove the least-upper-bound propety of real numbers.

4 Problem

1. Follow these steps to construct a Cauchy sequence of rational numbers which has no limit in $\mathbb{Q}$:

   (a) $\forall q \in \mathbb{Q}$, if $q > 0$ and $q^2 > 2$, then define $p := \frac{q}{2} + \frac{1}{q}$, show that $p^2 > 2$ and $p < q$.

   (b) $\forall q \in \mathbb{Q}$, if $q > 0$ and $q^2 < 2$, then define $p := -\frac{q^2}{4} + q + \frac{1}{2}$, show that $p^2 < 2$ and $p > q$.

   (c) Set $a_0 = 1$, define $a_{n+1} := \frac{a_n}{2} + \frac{1}{a_n}$. Use (a) to prove this sequence is a Cauchy sequence and use (b) to prove this sequence has no limit in $\mathbb{Q}$. (Why we need such an example?)

2. Follow these steps to show the cardinality of $\mathbb{R}$ is $2^{\aleph_0}$

   (a) Define "natural numbers" on $\mathbb{R}$ to be all the finite successive addition of 1 to 0. Write symbolically, define

   $$n := \sum_{k=1}^{n} 1.$$

   (Can you see the difference between two ns on both sides?)
   Prove the *Archimedean property* on $\mathbb{R}$:

   $$\forall a, b \in \mathbb{R},\ \exists n \in \mathbb{N},\ |a| < n|b|.$$

   (nx means $\sum_{k=1}^{n} x$)

   (b) One step further, prove that we can assign each real number a greatest integer below it, this is the so called *floor function*.

   (c) Now we can assign each real number r a *binary expansion* (a_n):

   $$a_0 := \lfloor r \rfloor,\ a_{n+1} := \begin{cases} 0 & , a_n + \frac{1}{2} > r, \\ 1 & , a_n + \frac{1}{2} \leq r. \end{cases}$$

   Prove this expansion is unique for every r.

   (d) If we construct a subset of $\mathbb{N}$ according to the binary expansion like this:

   $$S := \{n \in \mathbb{N} | a_{n+1} = 1\}.$$

   Prove this provide an injection from $\mathbb{R}$ to $\mathbb{Z} \times P(\mathbb{N})$.
   Use the sequence $(s_n := \sum_{k=0}^{n} a_k 2^{-k})$ to show there is an injection from $\mathbb{Z} \times P(\mathbb{N})$ to $\mathbb{R}$ then from Schröder-Bernstein Theorem we conclude that $\mathbb{R}$ is equipollent to $\mathbb{Z} \times P(\mathbb{N})$. To prove the cardinality of $\mathbb{Z} \times P(\mathbb{N})$ is $2^{\aleph_0}$ is an interesting exercise left to you. Remember you can use Schröder-Bernstein Theorem freely, or, maybe you can come up with very neat solution without referring to the famous theorem? Try it!

Because of this result, people call $2^{\aleph_0}$ the cardinality of *continuum*.