Math Remark
Algebraic Structure

X

ElegantLATEX Program

Update: February 12, 2025

Contents

1   Number System

Without talking some basic knowledge of Mathmatics logic, we generally define the object we want to study: Number System is a set of "number" and equipped by certain opreations. Here "number" is not necessary a real number like 1,2,3 we face daily in caculation, later we will aware that "number is actually a represent of a system, or using the language of the category, a normal system like $\mathbb{N}$ is just a represent object we choose in a category $Cat(\mathbb{N})$ (The collection of the system same as $\mathbb{N}$).

The main goal of this part is to construct the different number system begin from the natural number $\mathbb{N}$, the procedure often can be found in the textbook and the exercise, and the extension of distinct system inspire us to define the new algebra object.

1.1   From $\mathbb{N}$ to $\mathbb{Z}$

The common idea is to add a new element -1 to the system such that

$$1 + (-1) = 0$$

which refers to the completion of the unit of $\mathbb{N}$. We should notice that $\mathbb{Z}$ is a typical commutative ring with 1 identity, by comparison $(\mathbb{N}, +)$ is even not an abelian group, so by add a new element to the system we can clearly get the another "direction", which means $\{0, -1, -2, ...\}$ also forms a number system like $\mathbb{N}$ loosely speaking. we can caulate that $-2 = (-1) + (-1)$ by

$$2 + (-1) + (-1) = 1 + 1 + (-1) + (-1) = 0$$

so we can define that $-k$ is the sum of k same number -1.

Here we reconsider the negative number from the inspiration of the substraction, we can know that

$$-1 = 1 - 2 = 2 - 3 = 3 - 4 = ...$$

and

$$1 = 2 - 1 = 3 - 2 = 4 - 3 = ...$$

so we can define a binary relation on $\mathbb{N} \times \mathbb{N}$ by

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

In fact we should notice that we want to write $a - b = c - d$, but we do not still define substraction formally, so we do the change. we can define that the relation is equivalent, which is easily to verify:

- **reflexivity:** $(a, b) \sim (a, b) \iff a + b = b + a$.

- **Symmetry:**

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

- **transitivity:**

$$(a, b) \sim (c, d) \wedge (c, d) \sim (e, f) \iff a + d = b + c \wedge c + f = d + e$$
$$\iff a + (d + c) + f = b + (c + d) + e$$
$$\iff a + f = b + e$$
$$\iff (a, b) \sim (e, f)$$

Hence we can use this equiavlence relation to construct the intger.

Proposition 1.1 *Suppose $X = \mathbb{N} \times \mathbb{N}$, and we put $[a, b]$ to be the equiavlence class of the class containning $(a, b) \in X$, then following result can be verified:*
(1) the following operation is well-defined.

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

$$[a, b] \cdot [c, d] = [ac + bd, ad + bc]$$

(2) the system $(X/\sim, +, \cdot)$ form a commutative ring with multiplicative identity.

(3) The map $f : \mathbb{N} \to \mathbb{Z}, n \mapsto [n, 0]$ is injective and additives

$$f(n + m) = f(n) + f(m)$$

(4) If $X_+ = \{[n, 0] : n \in \mathbb{N}\}$ and $X_- = \{[0, n] : n \in \mathbb{N}\}$, then

$$X/\sim = X_+ + X_-$$

Proof. (1) For any $(x, y) \in [a, b]$ and $(x', y') \in [c, d]$, we define the addition by

$$(x, y) + (x', y') = (x + x', y + y')$$

then we have

$$x + b = y + a \wedge x' + d = y' + c$$

add them togther we get

$$(x + y) + (b + d) = (x' + y') + (a + c)$$

which implies $(x + x', y + y') \sim (a + c, b + d)$, and then clearly $[a, b] + [c, d] \subset [a + c, b + d]$. The proof can be finished here because that the caculation will always

be in the $[a+c, b+d]$, so we just need to check the corresponding caculation is really an injective then the definition will be well, but let us finish another direction, because it refers to the properties of natural number.

Mutually, if $(x,y) \in [a+c, b+d]$, then we have

$$x + b + d = y + a + c$$

By the choice of the element in class $[a,b]$, we can always find (i,j) such that $i \leq a$ and $j \leq b$, one thing should be pointed that we do not use substraction, usually we fix j such that $y + j \geq x$, which can be ensured by Archimedean Property , i.e. $\mathbb{N}$ is not bounded. and then i will be founded by **the properties of additive group**. hence here we can write down

$$(x,y) = (i,j) + (x_i, y_j)$$

we do not write $x_i = x - i$ and $y_j = y - j$ to prevent the abuse of the substraction. Finally, we can get two equation

$$i + x_i + b + d = j + y_j + a + c$$

$$i + b = j + a$$

then we can use the cancellation law of the group to get $(x_i, y_j) \sim (c, d)$, which finish our proof. ∎

Remark We finish our definition, and formally we define the integer is such a ring which is an quotient set,

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$$

and we denote $[0,0]$ by 0, denote $[1,0]$ by 1. And $[a,b]$ is called a positive number if $a > b$, and we denote it by $a - b$, which is the solution of $a = b + x$, otherwise we call $[a,n]$ a negiative number with the notation $-(a - b)$. More directly, if $n \in \mathbb{N} - \{0\}$, we have the simialrly notation in $\mathbb{Z}$ by

$$n = [n,0] \qquad -n = [0,n]$$

then we will have some basic properties as following

- $-(-a) = a$ or $a + (-a) = 0$
- $(-a)b = a(-b) = -ab$

By some verification, we can use these symbols to replace the equivalence class to refers the element in the integer ring, i.e. we finish the construction of the integer.

2 From ℚ to ℝ: Completion

In this section we will talk about the construction of real number, there are many equivalent ways to define real number, they are all same we will see that later. The flaw of the rational number is that it is not complet, or intuitively it can be seen as a line with too many holes in it. Convergence and limit theory is the core of the analysis, we are interested in what value a sequence convergs to, for example:

$$\lim_{n \to \infty} (1 + \frac{1}{n})^n = e$$

clearly, it is a sequence of ℚ but it converges to an irrational number. Moreover, we can consider Fibonacci number given by recurrence $F_{n+2} = F_{n+1} + F_n$, then we define s sequnece in ℚ by $a_n = \frac{F_{n+1}}{F_n}$, then it will converges to the golden ratio $\frac{1+\sqrt{5}}{2}$. Although the two example gives the limit of the seqence, but the fact is that we do not have the number in the rational number system we had! Hence some problem confuse the people in the time when the axiomatic system of number fields or even the real number system had not yet been established.

Now Let us construct the real number from the point of view: **any sequence of ℚ with the good characteristic of convergence can find a limit in the system.** Here

the sequence is just **Cauchy sequence**.

Definition 2.1 *A sequence (x_n) in $\mathbb{Q}$ is called a **Cauchy sequence** if for every rational $\varepsilon > 0$, there exists an integer $N \in \mathbb{N}$ such that for all $m, n \geq N$, we have*

$$|x_n - x_m| < \varepsilon.$$

Moreover, it is called to converges to L in $\mathbb{Q}$ if for every rational $\varepsilon > 0$, there exists an integer N N such that for all $n \geq N$, we have

$$|x_n - L| < \varepsilon$$

This is a type of sequence which tends to level off at the tail, so has a good feature to be convergent to some value. Now we denote the set of all sequence of $\mathbb{Q}$ be Q, then we can define a relation in it by

$$(a_n)_{n \in \mathbb{N}} \sim (b_n)_{n \in \mathbb{N}} \iff (a_n - b_n)_{n \in \mathbb{N}} \text{ converges to } 0$$

The relation is clearly equiavlent, the transitivity is given by the triangle inequality, that nuaturally the properties of absolute value (generally a norm). We use $[a_n]$ denote the class of equivalence of the sequnece $(a_n)_{n \in \mathbb{N}}$, now we need to define the algebra

operation in it, respectively we define:

$$[a_n] + [b_n] := [a_n + b_n]$$

$$[a_n] \cdot [b_n] := [a_n \cdot b_n]$$

where the opreations in bracket is the operation we defined in Q, so $a_n + b_n$ and $a_n \cdot b_n$ is again a sequnce of $\mathbb{Q}$. The definition is well-defined, on the one hand, sum of two cauchy sequence is still cauchy, so $a_n + b_n$ is exactly in some class of equivalence, and we just choose it to be the represent. on the other hand, the product is not very clear, we notice that

$$|a_n b_n - a_m b_m| = \frac{1}{2}|(a_n - a_m)(b_n + b_m) + (a_n + a_m)(b_n - b_m)|$$

easily we can know that cauchy sequence must be bounded, so there exists M, M' such that

$$|a_n b_n - a_m b_m| \le M|a_n - a_m| + M'|b_n - b_m|$$

so we can just choose $n, m \ge \max\{N_a, N_b\}$, which is implied by two cauchy sequence, and simialrly we choose $a_n \cdot b_n$ to be the represent.

Proposition 2.1 *Let $\mathbb{R} = Q/\sim$, under above definition, $(\mathbb{R}, +, \cdot)$ is a field.*

Proof. It is just the boring verification, you can choose to do it or just trust the result, here I do it.

we let the class $[0]$ denote the sequence $a_n = 0$ for any n, then it will be the additive identity and it denote all sequence converging to zero, since for any sequence $(b_n)_{n \in \mathbb{N}}$, we have $b_n + 0 = b_n$, so it has an inverse $-b_n$. And the multiplicative identity is $[1]$, it is the class of the sequence with 1 as all element, it will denote all sequence convering to 1. Then for any sequence $(b_n)_{n \in \mathbb{N}}$ not in $[0]$, we have $b_n \cdot 1 = b_n$, so $[b_n] \cdot [1] = [b_n]$, and the existence of its multiplicative inverse is a little complex since not necessary all b_n are not zero. We firstly prove a properties of the cauchy sequence:

Lemma 2.2 *For any cauchy sequence not converging to zero, there exists at most finite term having the different sign with the other term. and we call a cauchy sequence is poistive (negiative) if almost term is positive (negative).*

For a cauchy sequence $(a_n)_{n \in \mathbb{N}}$, $\epsilon_1 > 0$ implies an integer N_1 such that $|a_n - a_m| < \epsilon_1$ for any $n, m \geq N_1$. It is not converges to zero, then there exists a lower bound $c > 0$ which implies an intger N_2 such that any $n_0 \geq N_2$, $|a_{n_0}| > c$. so we just take $N_2 = N_1$ such that for any $n \geq N_1$

$$||a_n| - |a_{n_0}|| \leq |a_n - a_{n_0}| < \epsilon_1$$

and then

$$|a_n| \geq -\epsilon_1 + |a_{n_0}| > c - \epsilon_1 > 0$$

so we just take $\epsilon_1 = c/2$, which finish the proof of the lemma.

so we just need to construct a new sequence $(\bar{a}_n)$, for any $n \geq N_1$, $\bar{a}_n = a_n$ and for any $n < N_1$, $\bar{a}_n = a_{N_1}$, then $a_n \neq 0$ for any integer, so the sequence will be equiavlent to (a_n) and then sure $[a_n] = [\bar{a}_n]$, so the multiplicative inverse will be $[\frac{1}{\bar{a}_n}]$.

Finally notice that associative law and distributive law is inherit the rational number, so we finish our proof. ∎

Now we will consider the representative of the field to simplify the notation. We firstly notice that if a sequence converges to some q in $\mathbb{Q}$, then the sequence will clearly be equiavlent to a constant sequence $(q)_{n\in\mathbb{N}}$, so we just embed $\mathbb{Q}$ in $\mathbb{R}$ by $q = [q]$. But for the representative for irrational number, sometimes we really can choose a algebra symbol like $\pi, e, \sqrt{2}\ldots$, but these symbol actually refer to a non-constant sequence in $\mathbb{Q}$, or we say that we use rational number to apporximate it. When n really be ∞, something changes and the apporixmation will really be a new number which can not be contained in the system of rational number.