Splash 2013: Constructing the Real Numbers

Linh Nguyen
lvnguyen@mit.edu

1 Why real numbers?

Suppose we only know rational number.
Projectile example: $y = 20 - 10x^2$, solve for x. Is there solution on $\mathbb{Q}$? If one has a timer, he may try to approximate the time with multiple trails, and find that the resulting sequence comes very close to a number. Nevertheless, there's no rational number satisfying that condition.

Theorem: There's no rational number q such that $q^2 = 2$
That shows $\mathbb{Q}$ is incomplete, even though it is dense. In fact, one can prove that between any intervals [a,b] there is *infinitely* many rational numbers. In fact, the famous theorem by Cantor (1874?) shows that, given any interval [a,b], the *probability* of choosing a rational number is 0. It doesn't mean we will never be able to choose a rational number in the interval; it means in the long run, the will be far more irrational numbers are chosen rather than rational numbers.

That requires a more powerful set: the real number, to accomodate for all the missing stones from Q.

2 Basic ingredients

Instead of building directly from $\mathbb{Q}$, it's best to work abstractly. The advantage is that, we know for sure what we assume and what we don't assume. Real numbers possess many unique properties (such as metric space, compactness, etc.), and sometimes it's confusing whether a property comes from which.

2.1 Ordered set

Definition: An *order* in S is a relation, often denoted by <, satisfying two properties
- For any $x, y \in S$, exactly one of three conditions holds: $x < y, x = y, y < x$ (the last one is sometimes written as $y > x$, but we haven't defined >!)
- If $x < y$ and $y < z$, then $x < z$
The notation $\leq$ is also used to indicate $x < y$ or $x = y$.

Definition: An ordered set is a set S with a defining order
- $\mathbb{Q}$ is an ordered set: define $r < s$ if $s - r$ is a positive number
- $\mathbb{C}$ is an ordered set: define $a + bi < c + di$ if $a < c$, or $a = c$ and $b < d$. This is often called the *dictionary order*, and most of the sets can be forced to be this order.

You may notice in a finite ordered set, you can always find the largest and smallest element. However, in an infinite set, this is often not the case. We need another useful definition

Definition: Suppose $E \subset S$ and E is not empty. If there is a number $b \in S$ such that $x \leq b$ for every $x \in S$, we call b be an *upper bound* of S.

Definition: Suppose $E \subset S$ and E is not empty. The number $b \in S$ is called the *least upper bound* of S if it satisfies two properties
- b is an upper bound of E

- There's no $c < b$ such that c is an upper bound of E.
Denote $b = \sup E$ (comes from the word supremum). Similarly, we have the concept of *infimum*.

Example: The set $G = \{0, 1/2, 2/3, 3/4, ..\}$ obviously has no largest element, but is bounded above by any element $x \geq 1$. In fact, we can show $\sup G = 1$. Also, the supremum/infimum can coincide with the minimum/maximum of the set; for example, $\inf G = 0$ which is also the smallest element of G.

Definition: An ordered set S has the *least upper bound property*, if for any $E \subset S$, E is bounded above, $\sup E$ exists and is in S.
The set $\mathbb{Q}$ does not have the least upper bound property: take the set $\{x \in \mathbb{Q}; x^2 < 2\}$

2.2 Field

A field is a set F, equipped with two operations: addition and multiplication, satisfying the following axioms
A: Addition axioms
- A1: If $x \in F, y \in F$ then $x + y \in F$
- A2: Commutative: $x + y = y + x$ (sometimes it is called an abelian group with addition operation)
- A3: Associative: $(x + y) + z = x + (y + z)$
- A4: F contains an element 0: $0 + x = x + 0 = x$ for all $x \in F$
- A5: For every $x \in F$ there exists an element $y \in F$ such that $x + y = 0$. This element is often denoted as $(-x)$.

M: Multiplication axioms
- M1: If $x, y \in F$ then $xy \in F$
- M2: Commutative: $xy = yx$
- M3: Associative: $(xy)z = x(yz)$
- M4: Identity: F contains element 1 such that $1x = x1 = x$ for any $x \in F$
- M5: Inverse: for $x \in F$ and $x \neq 0$ there exists an element $y \in F$ such that $xy = yx = 1$. This is often denoted as $1/x$ or x^{-1}

D: Distributive law (linking addition and multiplication together)
- D1: $x(y + z) = xy + xz$ for all $x, y, z \in F$

From these basic axioms, we can prove all the main property that you would expect for a field. I will describe a few (without proof), those are interested may consult the Rudin's book:
- If $x + y = x + z$ then $y = z$. Corollary: ff $x + y = x$ then $y = 0$ - The element 0 and 1 is unique
- If $x \neq 0$ and $y \neq 0$ then $xy \neq 0$

2.3 Ordered field

Definition: An ordered field is a field F, equipped with an order satisfying two conditions:
- If $y < z$ then $x + y < x + z$
- If $x > 0, y > 0$ then $xy > 0$
Note: $\mathbb{C}$ is not an ordered field. One standard mistake is to "force" it to be a field by dictionary order. That results in an ordered set, but not ordered field (proof).

3 Dedekind's construction

We start from $\mathbb{Q}$ and we want to construct $\mathbb{R}$ while keeping all the properties of an ordered field, and we need to show the least upper bound property. But we need to be careful that we don't assume any properties of $\mathbb{R}$. For example, here's one faulty example: $X_{\sqrt{2}} = \{y \in \mathbb{Q}; y < \sqrt{2}\}$. What's wrong? We don't have $\sqrt{2}$, let alone saying its position! Of course, after we construct it will automatically fit in. But right now, it's a logical fault!

3.1 Cut

The elements of $\mathbb{R}$ will be subsets α of $\mathbb{Q}$ satisfying the following conditions
1. α is not empty and is not $\mathbb{Q}$
2. If $x \in \alpha$, then $y \in \alpha$ for all $y < x$
3. If $x \in \alpha$, then $x < y$ for some $y \in \alpha$
Condition 1 eliminates "infinity" element; condition 2 guarantees all elements less than x is included; condition 3 guarantees α has no largest element.

3.2 Order

Definition of order: $a < b$
$\alpha < \beta$ if $\alpha \subset \beta$
Check it is an ordered set.
Step 3: Least upper bound property
Step 4: Definition for addition
$\alpha + \beta$ is the set of all sums $r + s$ for $r \in \alpha$ and $s \in \beta$
Define $0*$ is the set of negative rational numbers. Show properties of $\alpha + \beta$
Step 5: First condition for ordered field
If $\alpha + \beta < \alpha + \gamma$ then $\beta < \gamma$ **Step 6:** Multiplication, part 1
We may try directly the above definition as we did in addition. But trouble occurs (example: $(-2).(-2)$ will include all positive numbers). Therefore, it's necessary to detour, starting with multiplication on positive numbers.
Define $\alpha\beta$ be the set of all $p \leq rs$ for $r \in \alpha, s \in \beta, r \geq 0, s \geq 0$
Define 1^* be the set of all $q < 1$ **Step 7:** Multiplication, part 2
It finishes both multiplication and distribution law
Step 8: Association with $\mathbb{Q}$
We shall show $\mathbb{Q}$ is actually a subset of $\mathbb{R}$ by associating each member of Q a corresponding set of R. Phew!