Rudin Textbook Notes

Arjun

January 9, 2024

It begins!

1

The rational numbers are inadequate, both as a field and an unordered set.

Example 1.1. There is no rational number p such that $p^2 = 2$.

Proof. For the sake of contradiction, assume that $p^2 = 2$ has a rational solution, $\frac{a}{b}$,where a and b are integers such that $\gcd(a, b) = 1$. Therefore, we can take the square root of both sides as so:

$$\sqrt{2} = \frac{a}{b}$$

Through algebraic manipulation, we then get

$$2a^2 = b^2$$

This means b must be even, and so b^2 is divisible by 4. This means a must also be even. Contradiction, as we assumed that $\gcd(a, b) = 1$. $\square$

Now, something more interesting: let A be the set of positive rationals p such that $p^2 < 2$, and B be the set of positive rationals p such that $p^2 > 2$.

Proposition 1.1. There is NO largest element in A.

Proof. We have some rational p such that $p^2 < 2$. Now, define a new rational q such that $q = p - \frac{p^2-2}{p+2} = \frac{2(p+1)}{(p+2)}$. Why do we define a rational like so? Well, for one, $q > p$, because $\frac{p^2-2}{p+2}$ is less than zero. Also, $q^2 - 2 = \frac{2(p^2-2)}{(p+2)^2} < 0$. Therefore, for some arbitrary rational p such that $p^2 < 2$, we have found another rational q such that $q > p$ and $q^2 < 2$. $\square$

Proposition 1.2. There is NO smallest element in B.

Proof. Very similar proof. We have some rational p such that $p^2 > 2$. Now, define a new rational q such that $q = p - \frac{p^2-2}{p+2} = \frac{2(p+1)}{(p+2)}$. Why do we define a rational like so? Well, for one, $q < p$, because $\frac{p^2-2}{p+2}$ is greater than zero. Also, $q^2 - 2 = \frac{2(p^2-2)}{(p+2)^2} > 0$. Therefore, for some arbitrary rational p such that $p^2 > 2$, we have found another rational q such that $q < p$ and $q^2 > 2$. $\square$

The reason we went through this whole process is to show that even though, say, there's a rational between any two rationals, there are still gaps that the rationals have. That's where the real numbers come into play!
To talk about these gaps, it's necessary to talk about bounds, first.

Definition 1.1. Suppose S is an ordered set, and $E \subset S$. If there exists a $\beta \in S$ such that $x \leq \beta \ \forall x \in S$, then β is an **upper bound** of E. A similar definition for **lower bound**.

This is a good definition, but an upper/lower bound for a set is NOT unique. In other words, there can be multiple, if not an infinite number of upper/lower bounds for a set. Is there a way to define a unique bound? Yes!

Definition 1.2. Suppose S is an ordered set, and $E \subset S$ is bounded above. Suppose there is an element $\alpha \in S$ with the following properties:

(i) α is an upper bound of E.

(ii) If $x < \alpha$, then x is **not** an upper bound of E.

Then α is the least upper bound of E, also known as the **supremum** of E, and we can say $\alpha = \sup E$.
A similar definition can be made for the greatest lower bound of E (assuming E is bounded below), or the **infimum** of E, so we can say $\gamma = \inf E$.

A natural question that may arise is WHEN a supremum or infimum of a set even exists. For instance, the set $\{p \in \mathbb{Q} \mid p^2 < 2\}$ has no least upper bound (or in other words, the supremum doesn't exist). This is where the following definition arises:

Definition 1.3. An ordered set S has the **least-upper-bound property** if any non-empty subset of S that's bounded above has a supremum that exists in S.

A similar definition can be made for the greatest-lower-bound property, and it turns out that every ordered set with one of these properties also has the other property. This leads to the following important theorem, which highlights a close relation between greatest lower bounds and least upper bounds:

Theorem 1.1. Suppose that S is an ordered set with the least-upper-bound property, $B \subset S$, B is non-empty, and B is bounded below. Let L be the set of all lower bounds of B. Then

$$\alpha = \sup L$$

exists in S, and $\alpha = \inf B$. In other words, $\inf B$ exists in S.

Proof. Since we know that our subset B is bounded below, L is certainly not empty. In fact, since L consists of all $y \in S$ such that $y \leq x \ \forall x \in B$, it is also true that every $x \in B$ is an upper bound of L. This means that L is bounded above, and since our ordered set S has the least-upper-bound property, the supremum of L indeed exists, call it α.
If $\gamma < \alpha$, then since α is the supremum of L, γ is not an upper bound of L, so $\gamma \notin B$. Therefore, an element of B CANNOT be less than α. Rather, all elements of B must be greater than or equal to α. So, since L is the set of all lower bounds of B, and α is indeed a lower bound of B, $\alpha \in L$.
Now, since α is an upper bound of L, if $\beta > \alpha$, then $\beta \notin L$. With this, we have shown that α is a lower bound of B (since $\alpha \in L$), and if $\beta > \alpha$, then $\beta \notin L$. These are all the qualifications for a value to be an infimum, and so we can therefore say that $\alpha = \inf B$. $\square$

At this point, Rudin goes into field axioms for addition and multiplication (as well as the distributive law that ties both addition and multiplication together). We shall jot down the axioms here, but we won't go into the various remarks and propositions about these axioms.

Definition 1.4. A **field** is a set F with two operations, called *addition* and *multiplication*, which satisfy the following "field axioms":

1. Addition Axioms
   - (A1) Addition is closed: if $x \in F$ and $y \in F$, then the sum $x + y \in F$.
   - (A2) Addition is commutative: $x + y = y + x$ for all $x, y \in F$.
   - (A3) Addition is associative: $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$.
   - (A4) Existence of the identity element: F contains an element 0 such that $0 + x = x$ for all $x \in F$.
   - (A5) Existence of the inverse elements: For every $x \in F$, there exists an element $-x \in F$ such that $x + (-x) = 0$.
2. Multiplication Axioms
   - (M1) Multiplication is closed: if $x \in F$ and $y \in F$, then the product $xy \in F$.
   - (M2) Multiplication is commutative: $xy = yx$ for all $x, y \in F$.
   - (M3) Multiplication is associative: $(xy)z = x(yz)$ for all $x, y, z \in F$.
   - (M4) Existence of the identity element: F contains an element $1 \neq 0$ such that $1x = x$ for all $x \in F$.
   - (M5) Existence of the inverse elements: For every **non-zero** $x \in F$, there exists an element $\frac{1}{x} \in F$ such that $x \cdot \frac{1}{x} = 1$.
3. Distributive Law
   - (D1) $x(y + z) = xy + xz$ holds for all $x, y, z \in F$.

While the addition and multiplication axioms are rather disjoint from each other, the distribute law ties them both together. We can also define some sense of order for a field with the following definition.

Definition 1.5. An **ordered field** is a field F which is also an ordered set, such that

(i) $x + y < x + z$ if $x, y, z \in F$ and $y < z$.

(ii) $xy > 0$ if $x \in F$, $y \in F$, $x > 0$, and $y > 0$.

With all these definitions made, we can now focus on the core idea of this chapter, which is the existence of the real numbers, as well as how they are constructed. The proof is rather long and tedious, but essential. Get hyped!

Theorem 1.2. There exists an ordered field $\mathbb{R}$, called the **Real Numbers**, which has the least-upper-bound property. Moreover, $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield ($\mathbb{Q} \subset \mathbb{R}$, and each field share the same addition and multiplication operations).

Proof. We will be constructing $\mathbb{R}$ from $\mathbb{Q}$, and this construction will be divided into several steps.

Step 1: The elements $\mathbb{R}$ will constructed by taking specific subsets of $\mathbb{Q}$. These subsets are referred to as **cuts**. By definition, a cut is any set $\alpha \subset \mathbb{Q}$ with the following properties:

(i) α is neither the empty set, nor the entire set $\mathbb{Q}$.

(ii) If $p \in \alpha$, and $q \in \mathbb{Q}$, then if $q < p$, $q \in \alpha$.

(iii) If $p \in \alpha$, then $p < r$ for some $r \in \alpha$. In other words, α has no maximum element.

Step 2: Since we are defining $\mathbb{R}$ to be these cuts, we know that $\mathbb{R}$ is a set (because a set is essentially a collection objects, the official definition is omitted in these notes for now). However, we must show a stronger statement, that $\mathbb{R}$ is actually an ordered set (whose definition, yet again, is omitted for now, and will be added later).

$\square$