Rudin Textbook Notes

Arjun

January 13, 2024

It begins!

Chapter 1: The Real and Complex Number Systems

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 $\gcd(a, b) = 1$. □

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 $q^2 < 2$. □

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 $q^2 > 2$. □

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 $\alpha = \inf B$. □

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

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

Step 1: The elements 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.

From this point on in this construction, p, q, and r will denote rational numbers, while α, β, and γ will denote cuts.

Step 2: Since we are defining R to be these cuts, we know that 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, namely that R is actually an ordered set (whose definition, yet again, is omitted for now, and will be added later).

Firstly, we define $\alpha < \beta$ to mean that α is a proper subset of β. (Will fill out rest of the proof later)

Step 3: We not must show that the ordered set R has the least-upper-bound property. This requires us to show that a nonempty subset of R that's bounded above by some $\beta \in R$, so say some set A, has a well-defined supremum.

We can define γ to be the union of all $\alpha \in A$, where α is some cut. This means $p \in \gamma$ if and only if $p \in \alpha$ for some $\alpha \in A$. Our goal now is to prove that $\gamma \in R$, and that γ is indeed the supremum of A.

To prove that $\gamma \in R$, we need to verify that γ satisfies the three properties from Step 1.

Since A is a nonempty set, this means there exists an $\alpha_0 \in A$ that is nonempty. Since $\alpha \subset \gamma$, γ is therefore non-empty. Also, since $\alpha \subset \beta$ for all $\alpha \in A$, this means that $\gamma \subset \beta$, since γ is the defined to be the union of all $\alpha \in A$. So, since γ is a proper subset of β, which could be at most $\mathbb{Q}$, we can be sure that $\gamma \neq \mathbb{Q}$. Therefore, the first property is satisfied. ✓

Pick some $p \in \gamma$. This means $p \in \alpha_i$ for some $\alpha_i \in A$. If $q < p$, then $q \in \alpha_i$ (by properties of a cut). Therefore, since $q \in \alpha_i$, $q \in \gamma$. This satisfies the second property. ✓

Now, choose some rational number $r \in \alpha_i$ such that $r > p$ (we know r exists because α_i is a cut). Since $\alpha_i \subset \gamma$, $r \in \gamma$. This satisfies the third property. ✓

With these three properties being satisfied, we can therefore say that

$\gamma \in R$, as it is indeed a cut.
We now need show that γ is the supremum of A.
Firstly, every $\alpha \in A$ is a subset of γ since γ is defined to be the union of all α, so γ is an upper bound. Now, suppose we have some $\delta < \gamma$. Since δ is a proper subset of γ, that means there is some $s \in \gamma$ such that $s \notin \delta$. Since $s \in \gamma$, that means $s \in \alpha_j$ for some $\alpha_j \in A$. Since α_j and δ are both cuts, and there's a rational number that's present in α_j but not in δ, then $\delta \subset \alpha_j$. Hence, δ is not an upper bound for A. This gives us the desired result of $\gamma = \sup A$.

Step 4: At this point, we shown that the ordered set R has the last-upper-bound property. It will take some work to show that R is actually an ordered field, the first step being to show that R is a field, with the right addition and multiplication definitions.
It's important to realize that at this point, all the elements of R are cuts, so we need to define addition via these cuts. So, if $\alpha, \beta \in R$, we can define $\alpha + \beta$ to be the set of all the sums $r + s$, where $r \in \alpha$ and $s \in \beta$. In order to see whether or not this is a valid addition operation, we need to figure out whether all the addition axioms from the definition of a field holds. Before this, we define 0^* to be the set of all the negative rational numbers (this is a cut, and therefore a member of R). This cut will play the role of 0, the identity element.

(A1) We show that $\alpha + \beta$ is a cut (the three properties from Step 1 hold).

1) $\alpha+\beta$ is nonempty, due to both α and β being nonempty. Furthermore, take some $r' \notin \alpha$ and $s' \notin \beta$. This means that $r'+s' > r+s$ (for any $r \in \alpha$ and $s \in \beta$). Therefore, $r'+s' \notin \alpha+\beta$, so $\alpha+\beta \neq \mathbb{Q}$. This satisfies the first property. ✓

2) Pick some $p = r + s$, where $r \in \alpha$ and $s \in \beta$. If $q < p$, then $q < r + s \Rightarrow q - s < r$, so $q - s \in \alpha$. So, $q = (q - s) + s \in \alpha + \beta$, which satisfies the second property. ✓

3) Choose some $t \in \alpha$ such that $t > r$. That means $p < t + s$, and $t + s \in \alpha + \beta$, so we have showed that an element larger than p is in $\alpha + \beta$, which satisfies the third property. ✓

This ultimately satisfies the closure property for $\alpha + \beta$.

(A2) Just like how $\alpha + \beta$ is the set of all $r + s$, with $r \in \alpha$ and $s \in \beta$, we can say $\beta + \alpha$ is the set of all $s + r$. $r + s = s + r$ for all rationals r and s, so $\alpha + \beta = \beta + \alpha$, which satisfies the commutativity property.

(A3) This is the associativity property, and it has very similar reasoning to the commutativity property above.

(A4) We have to show that $\alpha + 0^* = \alpha$ for any $\alpha \in R$. Say $r \in \alpha$ and $s \in 0^*$, then $r + s < r$ (remember that 0^* is the set of all negative rationals), so $r + s \in \alpha$. This means that $\alpha + 0^* \subseteq \alpha$. Now, pick some $p, r \in \alpha$ such that $r > p$. This mean that $p - r \in 0^*$. So, $p = r + (p - r) \in \alpha + 0^*$, which indicates that $p \in \alpha + 0^*$. Thus, $\alpha \subseteq \alpha + 0^*$, and we conclude that $\alpha = \alpha + 0^*$.

(A5) Now, we must show that every element contains an inverse. Firstly, recall that the inverse for some element means that when added to that element, the sum is the additive identity. So, for some cute α, another cut β is the additive inverse of α if $\alpha + \beta = 0^*$. Therefore, fix some $\alpha \in R$. We can define β to be the set of all rational p such that there exists a rational $r > 0$ where $-p - r \notin \alpha$. This is a strange set, but let's make an example: if we say α is the cut of all the rationals less than 2, then β will be the set of all the rationals less than -2. Therefore, $\alpha + \beta$ will essentially become the cut of all the rationals less than 0, so 0^*.

In order to rigorously show that $\alpha + \beta = 0^*$, we must first show that β is indeed a cut in the first place (or in other words, that $\beta \in R$), so we must show that β satisfies the three properties of a cut.

Firstly, if we say $s \notin \alpha$, and if we then define $p = -s - 1$, then $-p - 1 = s + 1 - 1 = s \notin \alpha$ (so $r = 1$), which means $p \in \beta$, implying that β is not empty. Furthermore, if we say $q \in \alpha$, notice that $-q$ cannot be in β, because if it was, then that would mean there exists a positive rational r such that $q - r \notin \alpha$. However, since α is a cut, this cannot be. Hence, $b \neq \mathbb{Q}$. This satisfies the first property.

Next, assume that $p \in \beta$, which means $-p - r \notin \alpha$, for some positive r. If we then suppose $q < p$, then $-q > -p$, so $-q - r > -p - r$, and therefore $-q - r \notin \alpha$, implying that $q \in \beta$, which satisfies the second property.

Finally, say that $t = p + \frac{r}{2}$. That means $t > p$, and $-t - \frac{r}{2} = -p - r \notin \alpha$, so $t \in \beta$. This satisfies the third property. Hence, we can therefore say that $\beta \in R$.

Now that β has been proven to be a valid cut, we must show that it is the inverse of α (so $\alpha + \beta = 0^*$). This means we must show each set is a subset of the other.

Assume we have $q \in \alpha$ and $s \in \beta$. If $s \in \beta$, then there exists a rational $r > 0$ such that $-s - r \notin \alpha$. This leads to $-s \notin \alpha$, because if it was in α, then that would contradict the fact that there exists a rational $r > 0$ such that $-s - r \notin \alpha$ (remember, if some rational is in a cut, then all rationals lower than it is also in the cut). Therefore, $q < -s$, so $q + s < 0$, indicating that $\alpha + \beta \subseteq 0^*$.

Conversely, pick some $v \in 0^*$, and then define w to be $-\frac{v}{2}$, a positive number. By the archimedean property of the rationals (this property is defined and proven later on in the notes), there is an integer n such that $nw \in \alpha$, but $(n+1)w \notin \alpha$. Remember, our goal is to show that $v \in \alpha + \beta$, and currently, we have our component for α. For β, we can first define $p = -(n+2)w$. The reason we define this as so is because $p \in \beta$, since $-p - w = (n+2)w - w = (n+1)w \notin \alpha$.

In other words, there exists a positive rational r, namely w, such that $-p-r \notin \alpha$. Therefore, we now have, surprisingly enough, that $nw+p = nw-(n+2)w = -2w = v$, so $v = nw+p \in \alpha+\beta$, which means $0^* \in \alpha+\beta$. This ultimately shows that $\alpha+\beta = 0^*$, which means β is indeed the additive inverse for α, and we will denote this inverse as $-\alpha$ from now on.

□