Math 320: Chapter 1

rctcwyvrn

September 2020

1 Common sets

- Natural numbers $\mathbb{N}$ (Rudin uses $\mathbb{J}$)
  - Set notation $\{1, 2, 3, 4, \ldots\}$
  - Closed under addition and multiplication
  - Not closed under subtraction (might get a negative number)
- Integers $\mathbb{Z}$
  - Set notation $\ldots - 3, -2, -1, 0, 1, 2, 3, 4, \ldots$
  - Closed under subtraction and addition
  - But not under division
- Rationals $\mathbb{Q}$
  - Set notation: $\left\{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}\right\}$
    - Where $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ iff $m_1 * n_2 = m_2 * n_1$
    - Our intuitive idea of division
  - Alternative we could define $\mathbb{Q}$ in a more straightforward way
    - Define $\mathbb{Q}$ as the set of ordered pairs $\{(m, n) : m \in \mathbb{Z}, n \in \mathbb{N}\}$
    - We also need to make sure the equivalent fractions are accounted for
    - where (m_1, n_1) is equivalent to (m_2, n_2) (ie $(m_1, n_1) \sim (m_2, n_2)$) if $m_1 n_2 = m_2 n_1$
  - Closed under addition, subtraction, multiplication, and division (if divisor is non-zero)
  - Question: Are the rationals sufficient for everything we want to do in real analysis (in calculus)?
    - Can we do things in calculus?
    - Can we take limits? (and have them work properly?)
  - Nope! (note: the name of this course is **real** analysis, not **rational** analysis

– The problem is that the rationals have holes, they're not "filled in all the way" like the reals are

Example: Holes in the rationals

(Rudin 1.1a) We want to show that there's a number we can't reach in the rationals ($\sqrt{2}$). $\nexists p \in \mathbb{Q} : p^2 = 2$

Proof:

By contradiction: Suppose that $\exists p \in \mathbb{Q} : p^2 = 2$. Then since p is rational, we can write $p = \frac{m}{n}$, $m \in \mathbb{Z}$, $n \in \mathbb{N}$.

- WLOG we may suppose that m and n are not both even (because if not then we could just divide both by 2 and have a new m and n and repeat until this statement is true)
  - Q: How can we be sure that this dividing by 2 will eventually end? (More explicitly, how many times do we need to do it?)
- We have $2 = p^2 = \frac{m^2}{n^2}$

$$2 = \frac{m^2}{n^2} \tag{1}$$
$$m^2 = 2n^2 \tag{2}$$

- So m must be even
- Ie $m = 2k$ for some odd integer k

$$2n^2 = m^2 \tag{3}$$
$$2n^2 = (2k)^2 \tag{4}$$
$$n^2 = 2k^2 \tag{5}$$

- So n must be even, but we said that one of them had to be odd.
- Contradiction!

Example:

(Rudin 1.1b)

- Let $A = \left\{p \in \mathbb{Q} : p > 0, p^2 < 2\right\}$
- Let $B = \left\{p \in \mathbb{Q} : p > 0, p^2 > 2\right\}$
- Consider the area where the two sets meet. We know that they meet at $\sqrt{2}$, which is not a rational.
- So we know that the set of rationals has little holes in it, like $\sqrt{2}$ which make us unable to use limits, which are important for real analysis

Then:

- $\forall p \in A, \exists q \in A : p < q$ (A does not have a largest element)
- Similarly B does not have a smallest element ($\forall p \in B, \exists q \in B : q < p$

Proof:

First one

- Consider arbitrary $p \in A$. Try $q = \frac{2p+2}{2+p}$
- Check $q \in \mathbb{Q}$, the denominator is non-zero and rational, so the result is rational.
- Check $q > 0$, both numerator and denominator are positive
- Check $q^2 < 2$.

$$\begin{aligned} q^2 &= \frac{(2p+2)^2}{(2+p)^2} && (6) \\ &= \frac{2(p^2-2)}{(p+2)^2} + 2 && (7) \end{aligned}$$

- The fraction is less than zero, because the numerator is negative ($p^2 < 2$ because $p \in A$), so $q^2 < 2$)
- Check that $p < q$. Well $q = p + \frac{2-p^2}{2+p}$, which is positive, so $q > p$

Second one

- Exercise (Try the exact same choice of q)

Q: Where did that q come from? (Think calculus)

Q: Why do we care so much that there is $q^2 = 2$, but don't care that there isn't a $q^2 = -1$?

1.1 Ordered Sets

Definition: Set order

An **order** **(<)** on a set S is a relation st

- Every pair of distinct elements $x, y \in S$, exactly one of $x < y$, $x > y$, $x = y$ is true
- Transitivity: For $x, y, z \in S$, $x < y$ $y < z$ implies $x < z$

Definition: Ordered set

A pair $(S, <)$ of an order and a set (duh)

- Notation: Just S if the order is obvious from the context

Example: Ordered sets

With ordering $x < y$ if $y - x$ is positive

- $S = \mathbb{N}$
- $S = \mathbb{Z}$
- $\mathbb{Q}$, $\mathbb{R}$ etc

Example: English set

S as the set of English words, $<$ is the dictionary order (by letters)

- "a" $<$ "aa" $<$ "ab" $<$ "b"

Notation:

- $x < y$ and $y > x$ are the same
- $x \leq y$ means $x < y$ or $x = y$

Definition: Bounded above

Let S be an ordered set and E be a subset of S ($E \subset S$)

We say E is **bounded above** if there exists an element $\theta \in S : \forall x \in E : x \leq \theta$

θ is an **upper bound(ub)** of E

- Note: This requires a "universal bounding set" or else the idea of being bounded above doesn't make sense

Example:

Let $S = \mathbb{Q}$ with the standard ordering. Let $E = A$ (from the last section, $0 < a$, $a^2 < 2$)

- Then E is bounded above by $p = 2$ (or really any element $p > \sqrt{2}$)

For $p \in E$, check $2 - p$

$$\begin{aligned} 2 - p &= \frac{4 - p^2}{(2 + p)} \qquad (8) \\ &> \frac{4 - 2}{2 + p} \qquad (9) \\ &> 0 \qquad (10) \end{aligned}$$

Example:

Let $S = A$ and $E = A$ (not a proper subset), in this case E is not bounded above

- We know that for any element $\theta \in E$ there exists another element in E that is larger (from last lecture)

Definition: Bounded below

Let S be an ordered set, $E \subset S$. E is **bounded below** if $\exists \beta \in S : \forall x \in E : \beta \leq x$

- β is called a **lower bound (lb)**

1.2 Least upper bounds and greatest lower bounds

Definition: Least upper bound (LUB)

Let S be an ordered set, subset E bounded above. If $\exists \alpha \in S$ such that

- α is a UB for E
- If $\gamma < \alpha$, then γ is NOT a UB for E

Then α is called the **least upper bound (LUB)** or **supremum**

- Notation: $\alpha = sup(E)$

Remark: Why can we say that α is THE supremum? How do we know that it's unique?

Definition: Greatest lower bound (GLB)

Similarly the **greatest lower bound** or **infenum** is the element α (if it exists) st

- α is a LB for E
- $\gamma > \alpha$ then gamma is not a LB for E
- Notation: $\alpha = inf(E)$

Example:

Let $S = \mathbb{Q}$ with the normal ordering. $E = \left\{\frac{1}{n} : n \in \mathbb{N}\right\}$

- What is the supremum? $sup(E) = 1$
- What is the infenum? $inf(E) = 0$

Things to check:

- Are they rational (in the universal set S)? Well yes
- Are they a UB/LB? Yes
- The hard part: Prove that they are the greatest/least lower/upper bound (todo)

Note:

- E contains its supremum, but not its infenum

Definition: Least upper bound property (LUB property)

An ordered set S has the LUB property if $\forall E \subset S$ where E is not the empty set, and E is bounded above, then E has a least upper bound (in S)

- All subsets of S that are bounded above, have a LUB

There is also a parallel definition for the **greatest upper bound property**.

Example:

Does $\mathbb{Z}$ have the LUB property?

What about $\mathbb{Q}$?

- How would you go about proving it?
  - Not having the statement is more straightforward because you can just find a counter-example
  - Considering arbitrary subsets is more difficult

1. I think the answers are yes and no.

Theorem:

(Rudin 1.11) Let S be an ordered set.

- S has the LUB property $\iff$ S has the GLB property

Proof:

Forward:

Let S be an ordered set with the LUB property. (WTS S has the GLB property).

Let $E \subset S$ with E nonempty and bounded below (assumptions for the GLB property) (wts E has an infenum)

Let $L = \{x \in S : \text{x is a LB for } E\}$. L is non-empty because E is bounded below

If $y \in E$, then y is an UB for L. (Because all elements of L are less than all elements of E). Since E is non-empty, L is bounded above.

So now we have set $L \subset S$ that is non-empty and bounded above, because S has the LUB property, L has supremum α. Claim that this α is the infenum of E.

$\alpha \leq x : \forall x \in E$, hence α is a lower bound for E, so α is an element of L (why?)

- $\forall \gamma \in S$, $\gamma < \alpha$ implies γ is not an upper bound of L.
- Since all values in E are upper bounds of L, $\gamma \notin E$.
- So since being less than α implies it is not in E, it follows that $\forall x \in E : \alpha \leq x$

Since α is the supremum of L, $\alpha \geq \gamma : \forall \gamma \in L$. Since L is the set of all upper bounds of E, we get that α is the greatest lower bound of E

$\square$

Backward: (exercise, should be very similar)

Remark: General proof notes:

- Use the structure and values that we have access to to generate the desired values. Ie use facts about bounded above/below, use the LUB property to get a solid value in S, the supremum of L.
- The fact that we know so little about S and E makes things easier, because there only are so many things you can try to create values from

1.3 Fields and ordered fields

Definition: Fields

A **field** is a set F along with two operations $(+, \cdot)$ such that the following properties (**the field axioms**)

Addition

1. $x, y \in F$ implies $x + y \in F$ (Closed under addition)
2. Commutative: $x + y = y + x$
3. Associative: $(x + y) + z = x + (y + z)$
4. Additive identity: $\exists 0 \in F$ st $\forall x \in F : 0 + x = x$
5. Additive inverse: $\forall x \in F : \exists y \in F : x + y = 0$. Notation: $y = -x$

Multiplication

1. $x, y \in F$ implies $x \cdot y \in F$ (Closed under multiplication)
2. Commutative: $x \cdot y = y \cdot x$
3. Associative: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
4. Multiplicative identity: $\exists 1 \in F$ st $1 \neq 0$ and $\forall x \in F : 1 \cdot x = x$
5. Multiplicative inverse: $\forall x \in F : x \neq 0 \implies \exists y \in F : x \cdot y = 0$. Notation: $y = x^{-1}$ or $y = \frac{1}{x}$
6. Distributive: $x \cdot (y + z) = x \cdot y + x \cdot z$

Little exercises

- Show that 0 is unique
- Show that 1 is unique

Example: Fields

$\mathbb{Q}$ is a field. $\mathbb{Z}$ is not a field (no multiplicative inverses)

Example:

$F = \{0, 1\}$ is a field.

- Let $1 + 1 = 0$, define everything else as expected
- (So this is really just $\mathbb{Z}/2\mathbb{Z}$)
- Notation: This set is called F_2 (isn't this $GF(2)$?)
- Note: Consider these as bits, then $+$ is XOR and $\cdot$ is AND

Note that 2 is a prime, and this generalizes for any prime p

Let $F_p = \{0, 1, \ldots p - 1\}$ where addition and multiplication are mod$p$. This is a field when p is prime

- For more properties of fields: Rudin prop 1.14, 1.15, 1.16

Now we have fields and we have ordered sets, so the logical next step is ordered fields.

Definition: Ordered fields

An **ordered field** is a field F that is also an ordered set with the properties

1. $x, y, z \in F$ $y < z$, then $x + y < x + z$
2. $x, y \in F$, $x > 0$ and $y > 0$ then $x \cdot y > 0$ (Note that we're combining the additive identity 0, and the multiplication operator)

Example:

- $\mathbb{Q}$ is an ordered field.
- What about F_2? Can you define an ordering such that it makes an ordered set? No! (prove by exhaustion since there are only two orderings)

Proof:

1. Let $0 < 1$. But $0 < 1$ but $1 + 0 < 1 + 1 = 0$ does not hold (property 1)
2. Let $1 < 0$, but $0 = 1 + 1 < 0 + 1 = 1$ does not hold (again property 1)

Theorem:

(Rudin 1.19) $\exists$ an ordered field that has the LUB property and that contains $\mathbb{Q}$ as a subfield, call this field $\mathbb{R}$

- What does that $\exists$ mean in this context? It means that we can create $\mathbb{R}$ from the pieces we already know $\mathbb{Q}, \mathbb{Z}, \mathbb{N}$ etc
- We say that there exists a field $\mathbb{R}$ but is it unique? No, but the idea is that they all have the same properties (and I assume are isomorphic?) so we only consider there to be one $\mathbb{R}$
- (I assume a subfield is just a subset of F with addition and multiplication are closed and the field axioms hold)

1.4 Consequences of the LUB property

We specified that $\mathbb{R}$ in the last theorem would have the LUB property, what properties of $\mathbb{R}$ do we get from that?

Theorem:

(Rudin 1.20) Three properties

1. $x, y \in \mathbb{R} : x > 0$, then $\exists n \in \mathbb{N} : nx > y$ (Archimidean property)
2. $x, y \in \mathbb{R} : x < y$ then $\exists p \in \mathbb{Q} : x < p < y$ (Rationals are 'dense' in $\mathbb{R}$)
3. $x, y \in \mathbb{R} : x < y$, then $\exists r \in \mathbb{R} \setminus \mathbb{Q} : x < r < y$ ($\mathbb{R}$ without $\mathbb{Q}$ is 'dense' in $\mathbb{R}$

Proof: A from Rudin 1.20

Proof (A) Let $A = \{nx : n \in \mathbb{N}\}$
If the conclusion is false then $\forall a \in A : a \leq y$, y would be an upper bound for A.

$\mathbb{R}$ has the LUB property, so $\alpha = \sup A$ would exist. WTS that this is a contradiction (A has no supremum) by finding $k \in \mathbb{N} : kx > \alpha$.

We know that $x > 0$ which implies $\alpha - x < \alpha$, so $\alpha - x$ is not an upper bound of A (because α is the supremum).
$\implies \exists m \in \mathbb{N} : mx > \alpha - x$
$\implies (m + 1)x > \alpha$ which is a contradiction, since an element of A is greater than the supremum

Next, prove a stronger version of (A) to help with the later proofs

(A*) If $x, y \in \mathbb{R} : x > 0$ then $\exists n \in \mathbb{Z} : (n - 1)x \leq y < nx$

Proof: A*

Case 1: $y \geq 0$. Let $A = \{m \in \mathbb{N} : y < mx\}$ (set of natural numbers). From A we know that A is nonempty.

Every nonempty subset of $\mathbb{N}$ has a smallest element (exercise). Let $n = min(A)$. Check that n fits the inequality that we want.

- $y < nx$ because it is an element of A
- $(n-1)x \leq y$ because it is the minimum element of A, so any smaller naturals m must not be in A, and thus be $mx \leq y$

Case 2: $y < 0$ exercise

Proof: The $\mathbb{Q}$ is dense in $\mathbb{R}$ (statement B)

Since $y - x > 0$, by (A) $\exists n \in \mathbb{N} : n(y - x) > 1$ (choose $x = y - x$, $y = 1$ for the theorem).

By (A*) $\exists m \in \mathbb{Z} : m - 1 \leq nx < m$ (choose $x = 1$, $y = nx$ for the theorem)
$\implies nx < m \leq nx + 1$

Now from $n(y - x) > 1$ we have
$\implies nx < m \leq nx + 1 < ny$

Divide both sides by n, we get
$\implies x < \frac{m}{n} < y$

Proof: Statement C

Borrow a fact from next lecture: $\exists s \in \mathbb{R} \setminus \mathbb{Q} : s > 0, s^2 = 2$, call $s = \sqrt{2}$. Proof will be next lecture, and it won't depend on statement C.

- $\sqrt{2} < 2$. This isn't obvious, since all we know is that the square of $\sqrt{2}^2 = 2$. The cases $\sqrt{2} = 2$ and $\sqrt{2} > 2$ both don't make sense, so $\sqrt{2} < 2$
  - Rudin 1.18: $a < b \implies a^2 < b^2$

Thus $0 < \sqrt{2}/2 < 1$, use this as a starting point to build the irrational number between x, y

By (B) $\exists p \in \mathbb{Q} : x < p < y$. Repeat with p and y, $\exists q \in \mathbb{Q} : x < p < q < y$

Let $\alpha = p + \frac{\sqrt{2}}{2}(q - p)$

- Is between p and q because it's a number less than 1 ($\frac{\sqrt{2}}{2}$) times the delta between p and q
  - $p < \alpha < p + 1(q - p) = q$. So we have $x < p < \alpha < q < y$
- Is not rational because $\sqrt{2}$
  - If α was rational, then we could write $\sqrt{2} = 2(\frac{\alpha - p}{(q-p)})$, which implies $\sqrt{2} \in \mathbb{Q}$, which is a contradiction

$\square$