<div style="border:1px solid black; padding:10px;">

MATH 320/321 (Real Analysis) Notes

Rio Weil

This document was typeset on May 13, 2021

</div>

Introduction

This set of notes is transcribed from UBC's MATH 320/321 (Real Variables I/II) sequence. The course covers the first 9 chapters of Rudin's "Principles of Mathematical Analysis" with occasional omissions & additions. The numbering of the definitions/theorems/examples will follow that used in Rudin to make following along with the textbook convenient. The structure of these notes is such that it is split into the main text (the boxed elements) and side text (everything else). It is possible to read just the main text for the main ideas without loss of continuity, but the additional discussion of the side text may be useful.

Contents

1   The Real and Complex Number Systems

1.1   The Naturals, Integers, and Rationals

We begin by a review of number systems which are already familiar.

Definition: The Natural Numbers

The **Naturals**, denoted by $\mathbb{N}$, is the set $\{1, 2, 3, \ldots\}$.

For $x, y, \in \mathbb{N}$, we have that $x + y \in \mathbb{N}$ and $xy \in \mathbb{N}$, so the naturals are closed under addition and multiplication. However, we note that it is not closed under subtraction; take for example $2 - 4 = -2 \notin \mathbb{N}$.

Definition: The Integers

The **Integers**, denoted by $\mathbb{Z}$, is the set $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

The integers are closed under addition, multiplication, and subtraction. However, it is not closed under division; for example, $1/2 \notin \mathbb{Z}$.

Definition: The Rationals (informal)

The **Rationals**, denoted by $\mathbb{Q}$, can be defined as $\left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}$, where $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ are identified if $m_1 n_2 = m_2 n_1$.

We note that unlike the naturals/integers, the rationals do not have as obvious of a denumeration. This above is a good definition if we already have the same rigorous idea of what a rational number is in our mind; i.e. it works because we have a shared preconceived understanding of a rational number.

If this is not the case, it may help to define the rational numbers more rigorously/formally (even if the definition may be slightly harder to parse). As a second attempt at a definition, we can say that $\mathbb{Q}$ is the set of ordered pairs $\big\{(m, n) : m \in \mathbb{Z}, n \in \mathbb{N}\big\}$. However, this is not quite enough as we need a notion of equivalence between two rational numbers (e.g. $(1, 2) = (2, 4)$). Hence, a complete and rigorous definition would be:

Definition: The Rationals (formal)

The **Rationals**, denoted by $\mathbb{Q}$, is the set $\big\{(m, n) : m \in \mathbb{Z}, n \in \mathbb{N}\big\} / \sim$ where $(m_1, n_1) \sim (m_2, n_2)$ if $m_1 n_2 = m_2 n_1$.

Under the formal definition, the rationals are a set of equivalence classes of ordered pairs, under the equivalence relation $\sim$. We note that the rationals are closed under addition, subtraction, multiplication, and division.

This formal definition might be slightly harder to parse, so it might be useful to consider an example with a similar flavour. Consider the set $X = \{m \in \mathbb{Z}\} / \sim$ such that $m_1 \sim m_2$ if $m_1 - m_2$ is divisible by 12. This is "clock arithmetic", with equivalence classes $[0], [1], [2], \ldots$ for each hour on an analog clock. A fun side note: If instead of 12 we picked a prime number, we would get a field (we will discuss what this is in a later lecture)!

Note that under this definition, $(1, 2)$ and $(2, 4)$ are different representations of the same rational number. With this definition, we would define addition such that $(m_1, n_1) + (m_2, n_2) = (m_1 n_2 + m_2 n_1, n_1 n_2)$. Note that $(2m_1, 2n_2) + (m_2, n_2) = (2m_1 n_2 + 2m_2 n_1, 2n_1 n_2)$ and we can identify $(m_1 n_2 + m_2 n_1, n_1 n_2)$ with $(2m_1 n_2 + 2m_2 n_1, 2n_1 n_2)$. If we choose different representations when we do addition, we might get a different representation in our result, but it will represent the same rational number regardless of the choice of representations we originally chose to do the addition.

A natural question then becomes if the rationals are sufficient for doing all of real analysis. Certainly, it seems as we have a number system that is closed under all our basic arithmetic operations; but is this enough? For example, are we able to take limits just using the rationals? The answer turns out to be no (they are insufficient!) and the following example will serve as one illustration of this fact.

> **Example 1.1: Incompleteness of the Rationals**
>
> There exists no $p \in \mathbb{Q}$ such that $p^2 = 2$.

We proceed via proof by contradiction. Recall in that these types of proof, we start with a certain wrong assumption, follow a correct/true line of reasoning, reach an eventual absurdity, and therefore conclude that the original assumption was mistaken.

> **Proof**
>
> Let us then suppose for the contradiction that there exists $p = \frac{m}{n}$ with $p^2 = 2$. We then have that not both m, n are even, and hence at least one is odd. Then, we have that $2 = p^2 = \frac{m^2}{n^2}$ and hence $m^2 = 2n^2$, so m^2 is even, implying m is even. So, let us write $m = 2k$ for $k \in \mathbb{Z}$. Then, $(2k)^2 = 4k^2 = 2n^2$, and hence $2k^2 = n^2$. Therefore, n^2 is even and hence n is even. m and n are therefore both even, a contradiction. We conclude that no such p exists. $\square$

Why can we conclude that not both m, n are even in the above proof? This is the case as if m, n we both even, then we could write $m = 2m'$, $n = 2n'$ for some m', n', and then $p = \frac{m}{n} = \frac{2m'}{2n'} = \frac{m'}{n'}$ which we can continue until either the numerator or denominator is odd. A natural question to consider is how to prove that this process of reducing fractions will eventually conclude. The resolution is to invoke the fundamental theorem of arithmetic, and write m, n in terms of their unique prime factorization. We are then able to cancel out factors of 2 from the numerator/denominator until at least one is odd.

We note that this example leads us to conclude that the rationals have certain "holes" in them. This is concerning, as there are sequences of rational numbers that tend to $\sqrt{2}$. Conversely, its not as concerning that there is no rational number x such that $x^2 = -1$, as there is no such sequence of rational numbers that is "close to" i (note that both $\sqrt{2}$ and i have not yet been defined, but this will come shortly).

> **Example 1.1: Incompleteness of the Rationals**
>
> Let $A = \{p \in \mathbb{Q} : p > 0, p^2 < 2\}$, and $B = \{p \in \mathbb{Q} : p > 0, p^2 > 2\}$. Then, $\forall p \in A, \exists q \in A$ such that $p < q$, and $\forall p \in B, \exists q \in B$ such that $q < p$.

Figure 1: Visualization of sets A and B. We note that $\sqrt{2}$ has not been defined in our formalism yet, but from our prior mathematical intuition it would be what goes in the "hole" of the rationals.

For the proof of this statement, we consider playing a 2 person game. One person is $\forall$, one person is $\exists$, and we consider if one person has a winning strategy. $\forall$ goes first, and then $\exists$ goes next, having seen the choice that $\forall$ has made. Then, we check if indeed $p < q$. If $p < q$, then $\exists$ wins. If $p \not< q$, then $\forall$ wins.

> **Proof**
>
> Let $p \in A$. Then, let $q = \frac{2p+2}{2+p}$. Since $p \in \mathbb{Q}$, it follows that $2p + 2 \in \mathbb{Q}$ and $2 + p \in \mathbb{Q}$ so $q \in \mathbb{Q}$. Furthermore, we have that $2p + 2 > 0$ and $2 + p > 0$, so $q > 0$. We also have that:
>
> $$q^2 = \frac{(2p+2)^2}{(2+p)^2} = 2 + \frac{2(p^2-2)}{(p+2)^2} < 2$$
>
> Where the inequality follows from the fact that $p^2 < 2$ and hence $(p^2 - 2) < 0$. It therefore follows that $q \in A$. Finally, we have that:
>
> $$q = p + \frac{2 - p^2}{2 + p} > p$$
>
> so $q > p$, completing the proof of the first part of the claim. The second part is left as an exercise (we note that the same q can be used). $\qquad\square$

The number $q = \frac{2p+2}{2+p}$ seems to be pulled out of a hat, but actually comes from a fairly geometric picture (the secant method of approximating roots). Discussion on this topic can be found here: https://math.stackexchange.com/questions/141774/choice-of-q-in-baby-rudins-example-1-1.

1.2 Ordered Sets

Over the next couple sections, we will be discussing certain properties of sets that will give us a better understanding of the real numbers, and allow us to construct them.

> **Definition 1.5: Order**
>
> An **order** $<$ on a set S is a relation with the following properties:
>
> (i) For every pair $x, y \in S$, exactly one of $x < y$, $x = y$, or $y < x$ is true.
>
> (ii) For $x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.
>
> A point on notation; We note that $x > y$ means $y < x$, and $x \leq y$ means $x < y$ or $x = y$.

> **Definition 1.6: Ordered Sets**
>
> An ordered set is a pair $(S, <)$. We may write just S if the order can be inferred by the context.

A familiar (and useful) set of examples is $S = \mathbb{N}$ or $S = \mathbb{Z}$ or $S = \mathbb{Q}$. For these three sets, we have that $x < y$ if $y - x$ is positive. For another example, consider the set S of english words; then the order $<$ can be the dictionary/lexographic order.

> **Definition 1.7: Upper & Lower Bounds**
>
> Let S be an ordered set and $E \subset S$ (note that here, $E \subset S$ is a non-strict subset, and $E \subsetneq S$ is a strict subset). E is **bounded above** if there exists an element $\beta \in S$ such that $\forall x \in E$, $x \leq \beta$. Any such β is an **upper bound** of E. Similarly, we say that E is **bounded below** if there exists an element $\alpha \in S$ such that $\forall x \in E$, $\alpha \leq x$. In this case, α is a **lower bound** of E.

As an example, one can take $S = \mathbb{Q}$, $E = A = \{p \in \mathbb{Q} : p > 0, p^2 > 2\}$ (as in Example 1.1). Here, E is bounded above, with $\beta = 2$ as one possible upper bound. to see this is the case, consider that if $p \in E$:

$$2 - p = \frac{4 - p^2}{2 + p} > \frac{4 - 2}{2 + p} > 0$$

4

However, if we take $S = A$, $E = A$, then E is not bounded above as we saw in the example. There is no upper bound of A in A. In general, this example reveals the subtle point that "the upper bound of a set" is ill-defined; we need to specify $E \subset S$.

1.3 The Least Upper Bound Property

Definition 1.8: Least Upper Bound & Greatest Lower Bound

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

  (i) α is an upper bound for E

  (ii) If $\gamma < \alpha$, then γ is not an upper bound for E

The α is the **least upper bound**, or **supermum** of E. This can be denoted as $\alpha = \sup(E)$. Analogously, the **greatest lower bound**, or **infimum** of E (denoted $\alpha = \inf(E)$) is an element $\alpha \in S$ (if it exists) such that:

  (i) α is a lower bound for E

  (ii) If $\gamma > \alpha$, then γ is not an upper bound of E.

Theorem: Uniqueness of supremum/infimum

If the supremum/infimum of $E \subset S$ exist, they are unique.

Proof

Let $E \subset S$. Suppose that there exist α_1, α_2 such that $\alpha_1 = \sup(E)$ and $\alpha_2 = \sup(E)$. If $\alpha_1 < \alpha_2$, as α_1 is an upper bound of E, this contradicts the fact that α_2 is the least upper bound of E. We reach an identical contradiction if $\alpha_2 < \alpha_1$. Therefore we conclude that $\alpha_1 = \alpha_2$ and the supremum of E is unique (if it exists). The proof for the infimum is analogous. $\square$

Theorem: Equivalence of maximum and supremum

If $E \subset S$ has a maximum element α (that is, an element such that $x < \alpha$ for all $x \in E$) then $\alpha = \sup(E)$. Similarly, if E has a minimum element α, then $\alpha = \inf(E)$. The proof is left as an exercise.

Example 1.9

  (a) Consider again the sets $A, B \subset \mathbb{Q}$ from example 1.1. A is bounded above by any element in B, and the upper bounds of A are exactly the elements of B. Since B has no smallest member, A does not have a least upper bound in $\mathbb{Q}$.

  (b) Let $E_1, E_2 \subset \mathbb{Q}$ such that $E_1 = \{r : \mathbb{Q}, r < 0\}$ and $E_2 = \{r : \mathbb{Q}, r \le 0\}$. Then $\sup(E_1) = \sup(E_2) = 0$. Note that this example shows that the supremum can either be contained or not contained in the set; $0 \notin E_1$ but $0 \in E_2$.

  (c) Let $E \subset \mathbb{Q}$ such that $E = \{\frac{1}{n} : n \in \mathbb{N}\}$. Then $\sup(E) = 1$ and $\inf(E) = 0$. This is proven below.

Proof

$\sup(E) = 1$ immediately follows from the equivalence of the maximum and supremum as proven above. To see that $\inf(E) = 0$, first note that 0 is a lower bound for E as all of the elements of E are positive. To see that it is the lower bound, take any $x > 0$. Then, we have that for any $n > \frac{1}{x}$, $\frac{1}{n} < x$ and hence x is not an upper bound of E. This proves the claim. □

Definition 1.10: The LUB/GUB Property

An ordered set S has the **least upper bound property** if for every $E \subset S$, if $E \neq \emptyset$ and E is bounded above, then E has a least upper bound (that is, $\sup(E)$ exists in S). Similarly, an ordered set S has the **greatest lower bound property** if for every $E \subset S$, if $E \neq \emptyset$ and E is bounded below, then E has a greatest lower bound.

We will show in the next theorem that these properties are actually equivalent; before then, we briefly consider two examples.

Example: $\mathbb{Z}$ and $\mathbb{Q}$

$\mathbb{Z}$ has the least upper bound property, while $\mathbb{Q}$ does not.

Proof

For the first claim, consider any nonempty $E \subset \mathbb{Z}$ that is bounded above. Choose any $x \in E$. Since $\mathbb{Z}$ is bounded above, there exist finitely many elements that are greater than x. Take the maximum of these finitely many elements. This maximum is also the maximum of E, so it is the supremum of E. Therefore $\mathbb{Z}$ has the LUB property as claimed.

The second claim immediately follows from Example 1.9(a). □

Theorem 1.11: Equivalence of LUB/GUB properties

Let S be an ordered set. Then S has the LUB property if and only if it has the GUB property.

Proof

$\boxed{\implies}$ Let S be an ordered set with the LUB property. Let $E \subset S$ with $E \neq \emptyset$, with E bounded below. Let $L = \{x \in S : x \text{ is a lower bound of } E.\}$. $L \neq \emptyset$ as E is bounded below (and hence has at least one lower bound). If $y \in E$, then y is an upper bound for L. Since E is nonempty, L is therefore bounded above. Since S has the LUB property, then $\sup(L)$ must exist. Let us call this α. Then, $\alpha \leq x \; \forall x \in E$ (as if $\gamma < \alpha$, then γ is not an upper bound of L and hence $\gamma \neq E$). Hence, α is a lower bound for E and hence $\alpha \in L$. Since $\alpha = \sup(L)$ and α is an upper bound for L, we have that $\alpha \geq \gamma \; \forall \gamma \in L$. Thus, $\alpha = \inf(E)$.

$\boxed{\impliedby}$ Left as an exercise. □

1.4 Fields and Ordered Fields

Definition 1.12: Fields

A field F is a set with two binary operations, $+$ and $\cdot$ (addition and multiplication) such that the following axioms are satisfied:

(A1): If $x, y \in F$, then $x + y \in F$. (Closure under addition)

(A2): $x + y = y + x$ for all $x, y \in F$. (Commutativity of addition)

(A3): $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$. (Associativity of addition)

(A4): $\exists 0 \in F$ such that $\forall x \in F$, $0 + x = x$. (Additive identity)

(A5): $\forall x \in F$, $\exists y$ such that $x + y = 0$. We can denote $y = -x$. (Additive inverse)

(M1): If $x, y \in F$, then $x \cdot y \in F$. (Closure under multiplication)

(M2): $x \cdot y = y \cdot x$ for all $x, y \in F$.

(M3): $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in F$. (Associativity under multiplication)

(M4): $\exists 1 \in F$ such that $1 \neq 0$ and $\forall x \in F$, $1 \cdot x = x$. (Multiplicative identity)

(M5): $\forall x \in F$, exists $y \in F$ such that $x \cdot y = 1$. We can denote $y = \frac{1}{x}$. (Multiplicative inverse)

(D): $x \cdot (y + z) = x \cdot y + x \cdot z$, $\forall x, y, z \in F$. (Distributive law)

Note that A3/M3 show that $x + y + z$ and $x \cdot y \cdot z$ are well defined in a mathematical sense; however, associativity may not hold for computers that do math with finite precision!

Theorem: Uniqueness of Identities and Inverses

The additive/multiplicative identities given by (A4)/(M4) and the additive/multiplicative inverses given by (A5)/(M5) are unique.

Proof

Let F be an ordered field. Suppose that there exist $0_1, 0_2 \in F$ such that $0_1 + x = x$ and $0_2 + x = x$ for all $x \in F$. We then have that:

$$\begin{aligned}
0_1 + 0_2 &= 0_1 + 0_2 \\
0_1 + 0_2 &= 0_2 + 0_1 && \text{(A2)} \\
0_2 &= 0_1 && \text{(Property of additive identity)}
\end{aligned}$$

Which shows that the additive identity is unique. The remaining proofs are left as an exercise. □

Some easy (and familiar) consequences of the field axioms can be found in Rudin 1.14-1.16. Instead of repeating those here, we will discuss some examples.

The rationals form a field (under the usual notions of addition/multiplication), but the integers do not, as there are no multiplicative inverses (e.g. there exists no integer $x \in \mathbb{Z}$ such that $2 \cdot x = 1$). The simplest

example of a field is $F = \{0, 1\}$, with the relations:

$$0 + 0 = 0 \quad 0 \cdot 0 = 1$$
$$0 + 1 = 0 \quad 0 \cdot 1 = 0$$
$$1 + 1 = 0 \quad 1 \cdot 1 = 1$$

This field is often called $\mathbb{F}_2$ or F_2, and is useful in computer science (where bits can take on two states, 0 or 1). As a slight tangent, a byte (8 bits) can be considered an element of an 8-dimensional vector space over the field $\mathbb{F}_2$, where + would be the XOR operator and $\cdot$ would be the AND operation.

A generalization of the above example is $\mathbb{F}_p$ or F_p, for a prime number p. This field would consist of the elements $0, 1, \ldots, p-1$. The addition and multiplication are carried out mod p. An interesting result is that in general, finite fields must have cardinality of some prime power.

Note that a field cannot have a single element; the field axioms (A4) and (M4) require the existence of distinct additive and multiplicative identities, which a singleton set cannot satisfy.

Although algebra is not the focus of this course, it may be interesting to briefly think about sets with less structure than a field. We start by considering a group.

Definition: Groups

A **group** G is a set with a binary operation $(a, b) \mapsto a \cdot b$ such that the following axioms are satisfied:

(i) If $a, b \in G$, then $a \cdot b \in G$ (Closure)

(ii) For $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associativity)

(iii) There exists $1 \in G$ such that $\forall x \in G$, $1 \cdot x = x$. (Identity)

(iv) $\forall x \in G$, there exists $y \in G$ such that $x \cdot y = 1$. (Inverse)

We note that $\mathbb{Z}$ is a group under addition, but not under multiplication (due to lack of multiplicative inverses). We can also consider the set of 2x2 matrices with integer entries:

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z} \right\}$$

G is again a group under matrix addition, but not under matrix multiplication (as not every matrix in G is invertible). If we restricted G to be the set of $2x2$ invertible matrices, in this case it could form a group under matrix multiplication. A set with slightly more structure than a group (though not quite as structured as a field) is a ring:

Definition: Rings

A **rings** G is a set with two binary operations $(a, b) \mapsto a + b$ and $(a, b) \mapsto a \cdot b$ such that the following axioms are satisfied:

(A1): If $x, y \in F$, then $x + y \in F$. (Closure under addition)

(A2): $x + y = y + x$ for all $x, y \in F$. (Commutativity of addition)

(A3): $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$. (Associativity of addition)

(A4): $\exists 0 \in F$ such that $\forall x \in F$, $0 + x = x$. (Additive identity)

(A5): $\forall x \in F$, $\exists y$ such that $x + y = 0$. We can denote $y = -x$. (Additive inverse)

(M1): If $x, y \in F$, then $x \cdot y \in F$. (Closure under multiplication)

(M3): $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in F$. (Associativity under multiplication)

(M4): $\exists 1 \in F$ such that $1 \neq 0$ and $\forall x \in F$, $1 \cdot x = x$. (Multiplicative identity)

(D1): $x \cdot (y + z) = x \cdot y + x \cdot z$, $\forall x, y, z \in F$. (Left distributivity)

(D2): $(y + z) \cdot x = y \cdot x + z \cdot x$, $\forall x, y, z \in F$. (Right distributivity)

Rings have the same axioms as fields under addition, but multiplication is not necessarily commutative (this is why an additional distributivity axiom is added), and multiplicative inverses are not required. We note that $\mathbb{Z}$ and G are both rings under their respective operations of addition and multiplication.

For the remainder of this course, we will really only be discussing fields; however, groups and rings will come up again and again in abstract algebra courses!

Definition 1.17: Ordered Field

An **Ordered field** is a field F that is also an ordered set, such that the following axioms are satisfied:

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

(ii) If $x, y \in F$ and $x > 0, y > 0$, then $x \cdot y > 0$.

Some properties of ordered fields are discussed in Rudin 1.18. We will again refer the reader to the discussion in the textbook for these properties, and here consider some examples.

$\mathbb{Q}$ is an ordered field, with the familiar order of $a > b$ if $a - b > 0$. A question may arise if $\mathbb{F}_2$ is an ordered field. A priori fields do not have order, but is it possible to impose an order on this set such that it is an ordered field? The answer turns out to be no.

Proof. It suffices to show that both possible orderings leads to a contradiction. Suppose $0 < 1$. Then, $1 = 0 + 1 < 1 + 1 = 0$ which is a contradiction. Suppose instead that $1 < 0$. Then, $0 = 1 + 1 < 1 + 0 = 1$ which again is a contradiction. $\square$

Theorem 1.19: Existence of $\mathbb{R}$

There exists an ordered field $\mathbb{R}$ which has the LUB property and contains $\mathbb{Q}$ as a subfield.

What does it mean for $\mathbb{Q}$ to be a subfield? It means that there exists an injective function $\mathbb{Q} \mapsto \mathbb{R}$ that respects the properties of an ordered field.

This field $\mathbb{R}$ happens to be exactly the set of real numbers we are familiar with. However, a natural question is "what does it mean that there exsits a field?" It turns out that we can define the reals based on the definitions we have made already. One further question might be that could there not exists several fields with the above property; however, taking the appropriate view, we will find that there is a unqiue such field.

2 Basic Topology

3 Numerical Sequences and Series

4 Continuity

5 Differentiation

6 The Riemann-Stieltjes Integral

7 Sequences and Series of Functions

8 Some Special Functions

9 Functions of Several Variables