MATH 320/321 (Real Analysis) Notes

Rio Weil

This document was typeset on June 12, 2021

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 for convenience. The structure of these notes is such that they are split into main text (the boxed elements) and side text (everything else). It is possible to solely read the main text for all of the material, but the additional discussion provided by the side text may be useful.

Contents

1 The Real and Complex Number Systems **2**
1.1 The Naturals, Integers, and Rationals . . . 2
1.2 Ordered Sets . . . 4
1.3 The Least Upper Bound Property . . . 5
1.4 Fields and Ordered Fields . . . 7
1.5 Consequences of the LUB Property . . . 10
1.6 Integer Roots of the Reals . . . 11
1.7 Construction of the Reals . . . 12
1.8 The Complex Field . . . 15
1.9 The Cauchy-Shwartz Inequality . . . 19
1.10 Euclidean Space . . . 21

2 Basic Topology **24**
2.1 Finite and Countable Sets . . . 24
2.2 Uncountable Sets . . . 27
2.3 Topology of Metric Spaces . . . 28
2.4 Closure and Relative Topology . . . 33
2.5 Compactness . . . 33
2.6 Compactness in $\mathbb{R}^k$ and the Cantor Set . . . 33

3 Numerical Sequences and Series **33**

4 Continuity **33**

5 Differentiation **33**

6 The Riemann-Stieltjes Integral **33**

7 Sequences and Series of Functions **33**

8 Some Special Functions **33**

9 Functions of Several Variables **33**

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 $\{(m, n) : m \in \mathbb{Z}, n \in \mathbb{N}\}$. 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 $\{(m, n) : m \in \mathbb{Z}, n \in \mathbb{N}\} / \sim$ 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. □

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 $A = \left\{p \in \mathbb{Q} : p > 0, p^2 < 2\right\}$, and $B = \left\{p \in \mathbb{Q} : p > 0, p^2 > 2\right\}$. 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). □

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 $S = \mathbb{Q}$, $E = A = \left\{p \in \mathbb{Q} : p > 0, p^2 > 2\right\}$ (as in Example 1.1(b)). Here, E is

bounded above, with $\beta = 2$ as one possible upper bound. to see this is the case, consider that if $p \in E$:

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

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

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. □

Theorem

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 $\alpha = \inf(E)$.

Proof

Let $E \subset S$ and $\alpha = \max(E)$. By definition α is an upper bound of E, and if $x < \alpha$ for some $x \in E$ then x is not an upper bound of E as it is not greater than $\alpha \in E$. The claim follows (with an identical proof for the minimum). □

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 $E_2 = \{r : \mathbb{Q}, r \leq 0\}$. 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 $E = \left\{\frac{1}{n} : n \in \mathbb{N}\right\}$. 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

$\mathbb{Z}$ 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

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

Proof

$\boxed{\Longrightarrow}$ 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, $\alpha = \inf(E)$.
$\boxed{\Longleftarrow}$ 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

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:

$$\begin{aligned} 0 + 0 &= 0 \quad 0 \cdot 0 = 1 \\ 0 + 1 &= 0 \quad 0 \cdot 1 = 0 \\ 1 + 1 &= 0 \quad 1 \cdot 1 = 1 \end{aligned}$$

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.

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

(M1): If $a, b \in G$, then $a \cdot b \in G$ (Closure)

(M3): For $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Associativity)

(M4): There exists $1 \in G$ such that $\forall x \in G$, $1 \cdot x = x$. (Identity)

(M5): $\forall x \in G$, 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 2×2 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:

A **ring** R 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 $x, y \in R$, then $x + y \in R$. (Closure under addition)

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

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

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

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

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

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

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

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

(D2): $(y + z) \cdot x = y \cdot x + z \cdot x$, $\forall x, y, z \in R$. (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, they will be the objects of interest 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. □

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.

1.5 Consequences of the LUB Property

We will use the least upper bound property and the fact that $\mathbb{R}$ has $\mathbb{Q}$ as a subfield to derive its properties.

Theorem 1.20: Archimedian Property, Density of Rationals/Irrationals in $\mathbb{R}$

(a) If $x, y \in \mathbb{R}$ and $x > 0$, then $\exists n \in \mathbb{N}$ such that $nx > y$.

(b) If $x, y \in \mathbb{R}$, and $x < y$, then $\exists p \in \mathbb{Q}$ such that $x < p < y$. ($\mathbb{Q}$ is dense in $\mathbb{R}$)

(c) If $x, y \in \mathbb{R}$, and $x < y$, then $\exists \alpha \in \mathbb{R} \setminus \mathbb{Q}$ such that $x < \alpha < y$. ($\mathbb{R} \setminus \mathbb{Q}$ is dense in $\mathbb{R}$)

Proof

(a) Let $A = \{nx : n \in \mathbb{N}\}$. Suppose for the sake of contradiction that the conclusion was false; then y is an upper bound of A. Then, $\alpha = \sup(A)$ exists by the LUB property of $\mathbb{R}$. Since $x > 0$, we then have that $\alpha - x < \alpha$ by the property of an ordered field. Hence, $\alpha - x$ is not an upper bound for A. Therefore, there exists some $m \in \mathbb{N}$ such that $mx > \alpha - x$. It then follows that $(m+1)x > \alpha$. We therefore have found $m + 1 = k \in \mathbb{N}$ such that $kx > \alpha$, contradicting α being the least upper bound of A. □

In order to prove (b) and (c), we first prove a stronger version of 1.20(a):

Lemma

If $x, y \in \mathbb{R}$ and $x > 0$, then there exists $n \in \mathbb{Z}$ such that $(n-1)x \leq y < nx$.

Proof

Suppose $y \geq 0$. Let $A = \{m \in \mathbb{N} : y < mx\} \subset \mathbb{N}$. By Theorem 1.20 (a), we have that $A \neq \emptyset$. Every non-empty subset of $\mathbb{N}$ has a smallest element (to see this, let $x \in A$, and define $A' = \{y \in A : y \leq x\}$. This is finite and nonempty and so has a smallest element, and the minimum element of this set will also be a lower bound and hence the minimum element of all of A), so let $n = \min(A)$. The claim holds for this n. The case for $y < 0$ is left as an exercise. □

Proof

(b) Since $y - x > 0$, by (a), $\exists n \in \mathbb{N}$ such that $1 < n(y - x)$. Furthermore, by the Lemma we have that $\exists m \in \mathbb{Z}$ such that $m - 1 \leq nx < m$ and hence $m \leq nx + 1$. From these inequalities we obtain that $nx < m \leq nx + 1 < ny$, and therefore $x < \frac{m}{n} < y$ for some $m \in \mathbb{Z}$, $n \in \mathbb{N}$. □

For the proof of part (c), we will use the result of Theorem 1.21 from the next section, specifically that there exists $s \in \mathbb{R} \setminus \mathbb{Q}$ such that $s > 0$ and $s^2 = 2$. We will call this $\sqrt{2}$.

Proof

(c) First, we have that $\sqrt{2} < 2$ as if $\sqrt{2} = 2$ then $(\sqrt{2})^2 = 2 = 2^2 = 4$ which is a contradiction, and if $\sqrt{2} > 2$ then $2 = \sqrt{2} \cdot \sqrt{2} > 2 \cdot 2 = 4$ by Rudin 1.18 which is yet again a contradiction. Thus, $\frac{\sqrt{2}}{2} < 1$.
Let $x, y \in \mathbb{R}$ such that $x < y$. By Theorem 1.20(b), there exists $p, q \in \mathbb{Q}$ such that $x < p < q < y$. Let $\alpha = p + \frac{\sqrt{2}}{2}(q - p)$. Then, we have that $p < \alpha < p + 1(q - p) < q$ and hence $x < p < \alpha < q < y$.
If $\alpha \in \mathbb{Q}$, then $\sqrt{2} = 2\left(\frac{\alpha - p}{q - p}\right) \in \mathbb{Q}$, which is a contradiction, so it follows that $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. □

1.6 Integer Roots of the Reals

In this section, we will prove that $\sqrt{2}$ exists and is an irrational number, but we will not use the fact that $\mathbb{R} \setminus \mathbb{Q}$ is dense in $\mathbb{R}$; this would of course be circular reasoning. The more general idea will be to prove that for any $n \in \mathbb{N}$, there exists $y \in \mathbb{R}$ such that $y = x^{1/n}$. Before this, we prove a lemma.

Lemma

If $0 < a < b$ and $n \in \mathbb{N}$, then $0 < b^n - a^n \leq nb^{n-1}(b - a)$

Note that a "Calculus proof" of this Lemma would be to let $f(x) = x^n$, and then

$$f(b) - f(a) = f'(c)(b - a) = nc^{n-1}(b - a) \leq nb^{n-1}(b - a)$$

Where we invoke the mean value theorem. But this obviously doesn't work as we have neither defined a derivative nor proven the mean value theorem. A proper proof would be:

Proof

Let $0 < a < b$. Then, we may factor $b^n - a^n$ such that:

$$b^n - a^n = (b - a)(b^{n-1} + ab^{n-2} + a^2b^{n-3} + \ldots + a^{n-2}b + a^{n-1})$$

The second factor is a sum of n terms, each positive, and in between 0 and b^{n-1}. ThereforE:

$$b^n - a^n \leq nb^{n-1}(b - a)$$

which proves the claim. □

We will now state the theorem formally:

Theorem 1.21: Integer Roots of the Reals

Let $x \in \mathbb{R}$, $x > 0$, and $n \in \mathbb{N}$. Then, there exists a unique $y \in \mathbb{R}$ such that $y > 0$ and $y^n = x$.

Note that somewhere in the proof, we will use the fact that $y \in \mathbb{R}$; this statement doesn't hold for rationals (see Example 1.1) so some property of the reals must come into play somewhere.

Proof

If $n = 1$, then the unique solution is $y = x$; we may therefore assume that $n \geq 2$.
Uniqueness: Suppose there exist two distinct numbers y_1, y_2 with $y_1 > 0, y_2 > 0$, and $y_1^n = y_2^n = x$. WLOG, suppose $0 < y_1 < y_2$. We then have that $0 < y_1^n < y_2^n$ which is a contradiction.
Existence: We prove existence in three steps.

1. We show that $E \neq \emptyset$. Let $E = \{t \in \mathbb{R} : t > 0, t^n < x\}$. If $x < 1$, then $x^n < x$, so $x \in E$. If $x \geq 1$, then $\left(\frac{1}{2}\right)^n < \frac{1}{2} < x$, so $\frac{1}{2} \in E$. Therefore, $E \neq \emptyset$.

2. We show that E is bounded above and has a supremum in $\mathbb{R}$. If $t > 1 + x$, then it follows that $t^n > t > x$, so $t \neq E$. Hence, $1 + x$ is an upper bound of E. By Theorem 1.19 (the LUB property of $\mathbb{R}$), it follows that $\sup(E) \in \mathbb{R}$ exists.

3. We show that $y = \sup(E)$ satisfies $y^n = x$. As $\mathbb{R}$ is an ordered field, one of $y^n < x$, $y^n = x$, or $y^n > x$ must be true; we show that the first and third are impossible.

   (a) Suppose $y^n < x$. We will obtain a contradiction by finding $h > 0$ such that $(y + h)^n < x$. (Why is this a contradiction? $y + h > y$, so if $(y + h)^n < x$, then $y + h \in E$, contradicting the fact that $y + h$ would be an upper bound of E). WLOG, suppose that $h < 1$. By the above Lemma, we have that:

   $$(y + h)^n - y^n \leq n(y + h)^{n-1}h \leq n(y + 1)^{n-1}h$$

   By choosing h sufficiently small, that is:

   $$h < \min\left\{1, \frac{x - y^n}{n(y + 1)^{n-1}}\right\}$$

   Then $n(y + 1)^{n-1}h < x^n - y^n$ from which it follows that $(y + h)^n - y^n < x^n - y^n$ and so $y + h < x$, which is the desired contradiction.

   (b) Suppose $y^n > x$. We will obtain a contradivction by finding $h > 0$ such that $(y - h)^n > x$. If this is true, then $y - h$ is an upper bound for E, contradicting the fact that y is the least upper bound for E. WLOG suppose that $h < 0$. Again applying the Lemma, we have that:

   $$y^n - (y - h)^n \leq ny^{n-1}h$$

   By choosing h sufficiently small, that is:

   $$h < \min\left\{1, \frac{y^n - x}{ny^{n-1}}\right\}$$

   It then follows that:

   $$y^n - (y - h)^n \leq ny^{n-1}h < y^n - x$$

   and hence $(y - h)^n > x$, which is the desired contradiction. □

1.7 Construction of the Reals

Theorem 1.19 says that there exists an ordered field that contains $\mathbb{Q}$ as a subfield. We now go about proving this statement. The construction is fairly technical and hence will be carried out in multiple steps. Some of the steps are left as exercises (one can refer to Rudin for the fully complete construction).

Step 1: Defining the elements of $\mathbb{R}$

The members of $\mathbb{R}$ will be proper subsets of $\mathbb{Q}$, called cuts. $\mathbb{R} = \{\text{all cuts}\}$.

Definition: Cuts

A **cut** is a proper subset $\alpha \subsetneq \mathbb{Q}$ with the three properties:

(I) $\alpha \neq \emptyset$

(II) If $p \in \alpha$, then $q \in \alpha \ \forall q < p$.

(III) If $p \in \alpha$, then $\exists r \in \alpha$ such that $p < r$.

Figure 2: Visualization of a cut α. The real number being described of this cut can be thought of as the number at the right boundary (the arrow).

In a sense, a cut gives us a way of discussing the real numbers (in the way we are familiar with them already) without referring to them directly; much like we could formally define/refer to rationals as equivalence classes of ordered pairs.
As a note, we could very well define cuts to be bounded below rather than above, and the following construction would still work out.

Step 2: $\mathbb{R}$ is an ordered set

We define $\alpha < \beta$ to mean $\alpha \subsetneq \beta$. We show that this makes $\mathbb{R}$ into an ordered set. First checking transitivity, we have that if $\alpha < \beta$ and $\beta < \gamma$ then $\alpha < \gamma$ by the fact that set inclusion is transitive. Furthermore, at most one of $\alpha < \beta$, $\alpha = \beta$, and $\beta < \alpha$ hold; to see this is the case, suppose the first two fail. Then, $\alpha \nsubseteq \beta$. Hence, $\exists p \in \alpha$ with $p \notin \beta$. If $q \in \beta$, $q < p$ and hence $q \in \alpha$ by (II), so $\beta \subset \alpha$, and since $\beta \neq \alpha$ it follows that $\beta \subsetneq \alpha$.

Step 3: $\mathbb{R}$ has the LUB property

We show that $\mathbb{R}$ has the LUB property. To see this is the case, let $A \subset \mathbb{R}$ with $A \neq \emptyset$, and suppose that there exists $\beta \in \mathbb{R}$ that is an upper bound for A. We will now define $\gamma = \bigcup_{\alpha \in A} \alpha$ and prove that $\gamma \in \mathbb{R}$ and $\gamma = \sup A$ (hence A has a supremum and $\mathbb{R}$ has the LUB property).
Since $A \neq \emptyset$, $\exists \alpha_0 \in A$, and since $\alpha_0 \neq \emptyset$ (as it is a cut) and $\alpha \subset \gamma$, it follows that $\gamma \neq \emptyset$. Next, we have that $\gamma \subset \beta$, since $\alpha \subset \beta$ for every $\alpha \in A$, and hence $\gamma \neq \mathbb{Q}$, that is, $\gamma \subsetneq \mathbb{Q}$. Hence γ satisfies property (I) of a cut.
Take $p \in \gamma$. Then $p \in \alpha_1$ for some $\alpha_1 \in A$. If $q < p$, then $q \in \alpha$ (as α is a cut) so $q \in \gamma$, satisfying property (II).
Next, choose $r \in \alpha_1$ such that $r > p$, then $r \in \gamma$ (as $\alpha_1 \subset \gamma$) and hence γ satisfies property (III). Hence γ is a cut, and $\gamma \in \mathbb{R}$.
Finally, we show that $\gamma = \sup A$. Clearly, $\alpha \leq \gamma$ for all $\alpha \in A$, as $\gamma = \bigcup_{\alpha \in A} \alpha$, so γ is an upper boun dof A. To show that it is the least upper bound, let $\delta < \gamma$ be a cut. Then, $\exists s \in \gamma$ such that $s \notin \delta$. Therefore, $\exists \alpha_2 \in A$ such that $s \in \alpha_2$; hence $\delta < \alpha_2$, so δ is not an upper bound for A, giving the desired result.

Step 4: Addition on $\mathbb{R}$

Definition: Addition

If $\alpha, \beta \in \mathbb{R}$, we define $\alpha + \beta = \{s + t : s \in \alpha, t \in \beta\}$. Showing that this is a cut is left as an exercise.

Definition: Zero

$0^* = \{s \in \mathbb{Q}\}$. Showing that this is a cut is left as an exercise.

We leave it as an exercise to show that the addition axioms (A1)-(A5) of a field are satisfied under this definition of addition on $\mathbb{R}$, with the 0 element as 0^* defined above.

Step 5: $\mathbb{R}$ satisfies the Ordered Field Property (i)

We verify that if $\alpha, \beta, \gamma \in \mathbb{R}$ and $\beta < \gamma$, then $\alpha + \beta < \alpha + \gamma$.
For every $s \in \alpha, t \in \beta$, we have that $t \in \gamma$ as β is a subset of γ by the definition of order on $\mathbb{R}$. Hence, $s + t \in \alpha + \beta$ implies $s + t \in \alpha + \gamma$. Therefore, $\alpha + \beta \subseteq \alpha + \gamma$ and hence $\alpha + \beta \leq \alpha + \gamma$.
We are then left to check that $\alpha + \beta \neq \alpha + \gamma$. To see that this is the case, if $\alpha + \beta = \alpha + \gamma$, then $\beta = \alpha + \beta - \alpha = \alpha + \gamma - \alpha = \gamma$ by the field axioms for addition. Therefore we obtain that $\beta = \gamma$, contradicting that $\beta < \gamma$. Hence the claim is proven.
As a remark, note that $0^* < \alpha \iff -\alpha < 0^*$.

Next we will define multiplication on $\mathbb{R}$. A first attempt would be $\alpha \cdot \beta = \{s \cdot t : s \in \alpha, t \in \beta\}$. However, this definition is incosistent with negative numbers from what we require multiplication to accomplish. $-1 \cdot -1$ would fail to be a cut (it would not contain any negative numbers and hence fail criteria (II)) and $-1 \cdot 1$ would yield the entirety of the rationals (again not a cut!)

Step 6: Positive Multiplication on $\mathbb{R}$

Definition: Positive Reals

We define $\mathbb{R}^+ = \{\alpha \in \mathbb{R} : \alpha > 0^*\}$

DefinitionMultiplication of Positive Reals

If $\alpha, \beta \in \mathbb{R}^+$, we define $\alpha \cdot \beta = \{r \cdot s : r \in \alpha, r > 0, s \in \beta, s > 0\} \cup \{t \in \mathbb{Q}, t \leq 0\}$. Equivalently, $\alpha \cdot \beta = \{p \in \mathbb{Q} :\leq r \cdot s : r \in \alpha, r > 0, s \in \beta, s > 0\}$. We leave it as an exercise to show that $\alpha \cdot \beta \in \mathbb{R}$, and moreover, $\alpha \cdot \beta \in \mathbb{R}^+$. Showing this second fact proves ordered field property (ii).

Definition: One

$1^* = \{r \in \mathbb{Q} : r < 1\}$. We again leave showing $1^* \in \mathbb{R}^+$ as an exercise.

Step 7: Multiplication on all of $\mathbb{R}$

Definition: Multiplication by zero

$\alpha \cdot 0^* = 0^* = 0^* \cdot \alpha$

Definition: Multiplication

We define general multiplication as below, where the $\cdot$ on the RHS represents the multiplication of positive reals as outlined in Step 5.

$$\alpha \cdot \beta = \begin{cases} (-\alpha) \cdot (-\beta) & \text{if } \alpha < 0^* \text{ and } \beta < 0^* \\ -\left((-\alpha) \cdot \beta\right) & \text{if } \alpha < 0^* \text{ and } \beta > 0^* \\ -\left(\alpha \cdot (-\beta)\right) & \text{if } \alpha > 0^* \text{ and } \beta < 0^* \end{cases}$$

We leave it as an exercise to show that the multiplicative axioms (M1)-(M5), as well as the distributive law (D) of a field are satisfied under this definition of multiplication on $\mathbb{R}$.

Up until this point, we have shown $\mathbb{R}$ is an ordered field with the LUB property; we last check that it contains $\mathbb{Q}$ as a subfield. Note that we do have to be a bit careful with what we mean here; $\mathbb{R}$ does not literally contain $\mathbb{Q}$; $\mathbb{R}$ is indeed a set of proper subsets of $\mathbb{Q}$. What we really mean is to associate every element of $\mathbb{Q}$ to an element of $\mathbb{R}$ such that the field structure is preserved.

Step 8: $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield

For each $r \in \mathbb{Q}$, associate the cut $r^* = \{p \in \mathbb{Q}, p < r^*\}$. We then leave as an easy exercise to verify that $r^* < s^* \iff r < s$, $r^* + s^* = r + s$, and $r^* \cdot s^* = r \cdot s$. This concludes the construction of the reals. □

Note that later on in the course, we will construct the real numbers in a different fashion; by considering Cauchy sequences modulo an equivalence relation. Also note that from here on out, it will suffice to have the standard/traditional picture of a "real number" in mind (i.e. infinite decimal expansions) and we will not have to really think about the real numbers as cuts; this was just necessary for the formal construction.

1.8 The Complex Field

Definition 1.24: The Complex Numbers

We define the set of **complex numbers** to be $\{(a,b) : a,b \in \mathbb{R}\}$, denoted by $\mathbb{C}$. For $x = (a,b) \in \mathbb{C}$ and $y = (c,d) \in \mathbb{C}$, we write $x = y$ if and only if $a = c$ and $b = d$ (note that this is a very different notion of equality compared to the rationals). We define the zero element to be $(0,0)$ and the one element to be $(1,0)$. We define addition of complex numbers such that:

$$x + y = (a,b) + (c,d) = (a + c, b + d)$$

And multiplication of complex numbers such that:

$$x \cdot y = (a,b) \cdot (c,d) = (ac - ba, ad + bc)$$

Theorem 1.25

The operations of $+$ and $\cdot$, as well as the zero/one elements defined above turn $\mathbb{C}$ into a field.

Proof

It suffices to verify the field axioms (A1)-(A5), (M1)-(M5), and (D) as discussed in 1.12. We will here show (M3), (M4), and (M5) and leave the rest as exercises.

(M3): Let $x, y, z \in \mathbb{C}$. We show that $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Let $x = (a, b), y = (c, d)$, and $z = (e, f)$. We then have that:

$$\begin{aligned}(x \cdot y) \cdot z &= (ac - bd, ad + bc) \cdot (e, f) \\ &= ((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e)\end{aligned}$$

We also have that:

$$\begin{aligned}x \cdot (y \cdot z) &= (a, b) \cdot (ce - df, cf + de) \\ &= (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)) \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf) \\ &= ((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e)\end{aligned}$$

So the claim is proven.

(M4): $(a, b)(1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b)$

(M5): Let $x \in \mathbb{C}$ such that $x \neq 0$. Then, $x = (a, b)$ where either $a \neq 0$ or $b \neq 0$ or both. Hence, $a^2 + b^2 > 0$. Then, let $\frac{1}{x} = (\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2})$. We then have that:

$$\begin{aligned}x\frac{1}{x} &= (a, b)\left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right) \\ &= \left(a\frac{a}{a^2 + b^2} - b\left(-\frac{b}{a^2 + b^2}\right), a\left(-\frac{b}{a^2 + b^2}\right) + b\left(\frac{a}{a^2 + b^2}\right)\right) \\ &= \left(\frac{a^2 + b^2}{a^2 + b^2}, -\frac{ab}{a^2 + b^2} + \frac{ab}{a^2 + b^2}\right) \\ &= (1, 0)\end{aligned}$$

Which proves the claim. □

Much like $\mathbb{Q}$ was a subfield of $\mathbb{R}$, $\mathbb{R}$ is a subfield of $\mathbb{C}$, and there exists a map ϕ from $\mathbb{R}$ to $\mathbb{C}$ that respects the field axioms, namely:

$$\begin{array}{rccc}\phi & : & \mathbb{R} & \longrightarrow & \mathbb{C} \\ & & x & \longmapsto & (x, 0)\end{array}$$

The theorem below shows that ϕ preserves the field structure:

Theorem 1.26

For $a, b \in \mathbb{R}$ we have that $(a, 0) + (b, 0) = (a + b, 0)$ and $(a, 0)(b, 0) = (ab, 0)$.

Definition 1.27: i

$i = (0, 1)$.

Theorem 1.28

$i^2 = -1$.

Theorem 1.29

If $a, b \in \mathbb{R}$, then $(a, b) = a + bi$.

Proof

Below are the trivial proofs for the above three theorems.

$$\begin{aligned}(a,0) + (b,0) &= (a+b, 0+0) = (a+b, 0)\\ (a,0) \cdot (b,0) &= (a \cdot b - 0 \cdot 0, a \cdot 0 + 0 \cdot b) = (ab, 0)\\ i^2 = i \cdot i &= (0,1) \cdot (0,1) = (-1, 0) = -1\\ a + bi &= (a,0) + b(0,1) = (a,0) + (0,b) = (a,b)\end{aligned}$$

A slightly odd question may be to ask whether $\mathbb{C}$ is a subfield of $\mathbb{R}$, i.e. does there exist $\psi : \mathbb{C} \mapsto \mathbb{R}$ such that $\psi(a + b) = \psi(a) + \psi(b)$ and $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$. As we will prove in Chapter 2, we do have that $|\mathbb{C}| = \left|\mathbb{R}^2\right| = |\mathbb{R}|$ (where $||$ denotes cardinality of the set, to be defined shortly), so there does exist a bijection (i.e. a function that is both injective/one-to-one and surjective/onto; we will define these terms precisely in the next chapter) between the two sets.

As a Lemma, we have that the only injective function $f : \mathbb{Q} \mapsto \mathbb{R}$ that satisfies $f(a + b) = f(a) + f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$ is $f(x) = x$. The proof of this is left as a homework problem (HW2). Therefore, it follows that the only injective function $g : \mathbb{Q} \times \{0\} \mapsto \mathbb{R}$ (where $\times$ denotes the Cartesian product) is given by $g((x, 0)) = x$. We now give a proof that $\mathbb{C}$ is not a subfield of $\mathbb{R}$.

Proof. Suppose then for the sake of contradiction that there exists an injective function $\psi : \mathbb{Q} \times \{0, 1\} \mapsto \mathbb{R}$. Such a function then must satisfy$\psi(i \cdot i) = \psi(-1) = -1$, and $\psi(i \cdot i) = \psi(i) \cdot \psi(i) = \psi((0, 1)) \cdot \psi((0, 1)) = 0 \cdot 0 = 0$ which is a contradiction. Hence, no such injection exists from $\mathbb{Q} \times \{0, 1\}$ to $\mathbb{R}$ and hence no such injection could exist from $\mathbb{C}$ ($\mathbb{R}^2$) to $\mathbb{R}$. Hence $\mathbb{C}$ is not a subfield of $\mathbb{R}$. □

Definition 1.30: Real/Imaginary Parts and Complex Conjugates

Let $z = a + bi \in \mathbb{C}$. Then, $\text{Re}(z) = a$ is the **real part** of z and $\text{Im}(z) = b$ is the **imaginary part** of z. The **complex conjugate** of z, denoted by $\bar{z}$, is defined as $\bar{z} = a - bi$.

Theorem 1.31

Let $z, w \in \mathbb{C}$. It then follows that:

(a) $\overline{z+w} = \bar{z} + \bar{w}$.

(b) $\overline{zw} = \bar{z} \cdot \bar{w}$.

(c) $z + \bar{z} = 2\,\mathrm{Re}(z)$, $z - \bar{z} = 2i\,\mathrm{Im}(z)$.

(d) $z\bar{z}$ is real and positive (except when $z = 0$).

Proof

We prove (d). We have that:

$$z\bar{z} = (a+bi)(a-bi) = a^2 + b^2$$

$a^2 + b^2 \geq 0$, and $a^2 + b^2 = 0 \iff a = 0, b = 0$ which proves the claim. □

Definition 1.32: Absolute Value

We define the **absolute value** $|z|$ of a complex number z as $|z| = \sqrt{z\bar{z}}$. Note that if $a \in \mathbb{R}$ and $z = (a, 0)$, then

$$|z| = \sqrt{a^2} = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

Hence if $a \in \mathbb{R}$, we can define $|a| = \big|(a, 0)\big|$.

Theorem 1.33

Let $z, w \in \mathbb{C}$.

(a) $|z| \geq 0$, $|z| = 0 \iff z = 0$.

(b) $|\bar{z}| = |z|$.

(c) $|z||w| = |zw|$.

(d) $\big|\mathrm{Re}(z)\big| \leq |z|$, $\big|\mathrm{Im}(z)\big| \leq |z|$.

(e) $|z + w| \leq |z| + |w|$.

Proof

We prove (d) and (e). Let $z, w \in \mathbb{C}$, with $z = a + bi$. For (d) we have that $\mathrm{Re}(z) = a$, so

$$\big|\mathrm{Re}(a)\big| = \sqrt{a^2} \leq \sqrt{a^2 + b^2} = |z|$$

And an equivalent proof follows for $\mathrm{Im}(z)$. For (e), we have that:

$$\begin{aligned}
|z+w|^2 &= (z+w)(\overline{z+w}) \\
&= z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} \\
&= |z|^2 + 2\,\mathrm{Re}(z\bar{w}) + |w|^2 \\
&\leq |z|^2 + 2\big|\mathrm{Re}(z\bar{w})\big| + |y|^2 && (|x| > x) \\
&= |z|^2 + 2|z\bar{w}| + |w|^2 && (1.33(d)) \\
&= |z|^2 + 2|z||\bar{w}| + |w|^2 && (1.33(c)) \\
&= |z|^2 + 2|z||w| + |w|^2 && (1.33(b)) \\
&= (|z| + |w|)^2
\end{aligned}$$

The claim follows by taking square roots on both sides. □

1.9 The Cauchy-Shwartz Inequality

Recall the summation notation:

$$x_1 + x_2 + \ldots + x_n = \sum_{j=1}^{n} x_i$$

Theorem 1.35: Cauchy-Shwartz Inequality

Let $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{C}$. We then have that:

$$\left|\sum_{j=1}^{n} a_j \bar{b}_j\right|^2 \leq \left(\sum_{j=1}^{n} \left|a_j\right|^2\right)\left(\sum_{j=1}^{n} \left|b_j\right|^2\right)$$

Note that in the above theorem, both the RHS and the LHS are real numbers (check!) so the equality makes sense (recall that there is no order on $\mathbb{C}$; in fact, it is impossible to define one).

A geometric interpretation of the above inequality is as follows. Let $\mathbf{a}, \mathbf{b}$ be vectors in $\mathbb{C}^n$. Then, $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{j=1}^{n} a_j \bar{b}_j$ is the inner product of $\mathbf{a}$ and $\mathbf{b}$. Then, the inequality says that $\big|\langle \mathbf{a}, \mathbf{b} \rangle\big|^2 \leq \langle \mathbf{a}, \mathbf{a} \rangle \cdot \langle \mathbf{b}, \mathbf{b} \rangle$.

Proof

Define $A = \sum_{j=1}^{n} \left|a_j\right|^2$, $B = \sum_{j=1}^{n} \left|b_j\right|^2$, and $C = \sum_{j=1}^{n} a_j \bar{b}_j$. If $B = 0$ (that is, all of the b_js are zero) then the LHS/RHS are both zero and we are done. So, let us assume that $B > 0$. Let $\lambda \in \mathbb{C}$, and we then have that:

$$\begin{aligned}
0 &\leq \sum_{j=1}^{n} \left|a_j + \lambda b_j\right|^2 \\
&= \sum_{j=1}^{n} (a_j + \lambda b_j)(\bar{a}_j + \bar{\lambda}\bar{b}_j) \\
&= \sum_{j=1}^{n} \left|a_j\right|^2 + \bar{\lambda} \sum_{j=1}^{n} a_j \bar{b}_j + \lambda \sum_{j=1}^{n} \bar{a}_j b_j + |\lambda|^2 \sum_{j=1}^{n} \left|b_j\right|^2 \\
&= A + \bar{\lambda} C + \lambda \bar{C} + |\lambda|^2 B
\end{aligned}$$

This inequality holds for any λ; it therefore holds for $\lambda = -\frac{C}{B}$, so:

$$\begin{aligned}
0 &\leq A - \frac{\bar{C}}{B} C - \frac{C}{B} \bar{C} + \frac{C\bar{C}}{B^2} B \\
&= A - \frac{|C|^2}{B}
\end{aligned}$$

So we therefore obtain that $|C|^2 \leq AB$ which is the desired inequality. □

A natural question given any inequality is when does equality hold; the answer turns out to be if the vectors are linearly independent, that is, at least one of $\mathbf{a} = \alpha\mathbf{b}$ and $\mathbf{b} = \beta\mathbf{a}$ ($\alpha, \beta \in \mathbb{C}$) hold. Note that we only require one of the two relations to hold; in the case that one of $\mathbf{a}, \mathbf{b}$ are $\mathbf{0}$ (the vector of all zeros) both equalities cannot be true. It is left as a homework problem to verify equality in the Cauchy-Shwartz inequality if and only if at least one of the two conditions holds (HW3).

1.10 Euclidean Space

Definition 1.36: Euclidean k-space

If $k \in \mathbb{N}$, define $\mathbb{R}^k$ as the set of k-tuples of real numbers:

$$\mathbb{R}^k = \{\mathbf{x} = (x_1, x_2, \ldots, x_k) : x_1, x_2, \ldots, x_k \in \mathbb{R}\}$$

We can then define vector addition as:

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k)$$

And scalar multiplication (for $\alpha \in \mathbb{R}$) to be:

$$\alpha\mathbf{x} = (\alpha x_1, \alpha x_2, \ldots, \alpha x_k)$$

These operations make $\mathbb{R}^k$ into a vector space over the real field. We can define the inner product over $\mathbb{R}^k$ to be:

$$(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y} = \sum_{j=1}^{k} x_j y_j$$

This allows us to define the norm of $\mathbf{x}$ to be:

$$|\mathbf{x}| = \sqrt{\mathbf{x} \cdot \mathbf{x}} = \left(\sum_{j=1}^{n} x_j^2 \right)^{1/2}$$

$\mathbb{R}^k$ with the above inner product and norm is called **Euclidean k-space**.

We briefly remark that the above inner product we defined agrees with the inner product we defined over $\mathbb{C}^k$; we can identify $r \in \mathbb{R}$ with $(r, 0) \in \mathbb{C}$, and hence recognize that $\mathbb{R}^k \subseteq \mathbb{C}^k$ where the imaginary part of each coordinate is zero. Then, for the inner product we get the exact same result, as $\bar{b}_j = b_j$ for any complex numbers with imaginary part zero. From this we can conclude that the Cauchy-Shwartz inequality also holds in $\mathbb{R}^k$.

Note that although the field $\mathbb{C}$ is $\mathbb{R}^2$ with multiplication defined as in Definition 1.24, in general vector multiplication on $\mathbb{R}^n$ is not well defined. That is, we cannot make $\mathbb{R}^n$ into a field in general; though we can make it into a vector space, which has slightly less structure.

One possibly familiar notion of vector multiplication in $\mathbb{R}^3$ is the cross product. For $\mathbf{x} = (x_1, x_2, x_3)$ and $\mathbf{y} = (y_1, y_2, y_3)$, the cross product is defined as:

$$\mathbf{x} \times \mathbf{y} = (x_2 y_3 - x_3 y_2, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1)$$

However, the cross product does not satisfy properties that would be necessary to make $\mathbb{R}^3$ a field. For one, it is not commutative, but anticommutative; $\mathbf{x} \times \mathbf{y} = -\mathbf{y} \times \mathbf{x}$. One might ask whether vectors in $\mathbb{R}^3$ have well-defind inverses, but even before that, there does not exist an identity vector in $\mathbb{R}^3$ under the cross product! In fact, $\mathbb{R}^3$ under vector addition and cross product multiplication can be viewed as a noncommutative ring without an identity.

Note that there is a more general notion of a "wedge product" between vectors in $\mathbb{R}^n$. We are in a sense very "lucky" that in $\mathbb{R}^3$, the wedge product of two vectors returns another vector in $\mathbb{R}^3$.

Theorem 1.37

Let $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^k$, and $\alpha \in \mathbb{R}$. Then:

(a) $|\mathbf{x}| \geq 0$

(b) $|\mathbf{x}| = 0 \iff \mathbf{x} = (0, \ldots, 0)$. This is often denoted as $\mathbf{0}$, the "zero vector".

(c) $|\alpha\mathbf{x}| = |\alpha||\mathbf{x}|$

(d) $|\mathbf{x} \cdot \mathbf{y}| \leq |\mathbf{x}||\mathbf{y}|$

(e) $|\mathbf{x} + \mathbf{y}| \leq |\mathbf{x}| + |\mathbf{y}|$

(f) $|\mathbf{x} - \mathbf{z}| \leq |\mathbf{x} - \mathbf{y}| + |\mathbf{y} - \mathbf{z}|$

(e) and (f) are often called "triangle inequalities"; a visual intuition for these inequalities is given in the following figure:

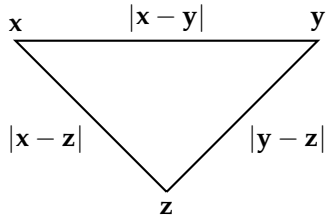

Figure 3: Visual picture for Theorem 1.37(f), drawn in $\mathbb{R}^2$. Suppose we started at $\mathbf{x}$ and wanted the shortest path to $\mathbf{z}$; we could try walking directly to $\mathbf{z}$, or we could try walking somewhere else first ($\mathbf{y}$) and then to $\mathbf{z}$. However, the theorem tells us that the direct path will always be shorter in Euclidean space.

Note that equality in part (f) arises if and only if $\mathbf{y}$ lies on the line segment between $\mathbf{x}$ and $\mathbf{z}$.

Proof

(a)-(c) are immediate, and (d) immediately follows from Theorem 1.35 (Cauchy-Shwartz). For (e), we have that:

$$\begin{aligned} |\mathbf{x} + \mathbf{y}|^2 &= (\mathbf{x} + \mathbf{y})(\mathbf{x} + \mathbf{y}) \\ &= |\mathbf{x}|^2 + 2\mathbf{x} \cdot \mathbf{y} + |\mathbf{y}|^2 \\ &\leq |\mathbf{x}|^2 + |2\mathbf{x} \cdot \mathbf{y}| + |\mathbf{y}|^2 \\ &\leq |\mathbf{x}|^2 + 2|\mathbf{x}||\mathbf{y}| + |\mathbf{y}|^2 \quad \text{(1.37(d))} \\ &= (|\mathbf{x}| + |\mathbf{y}|)^2 \end{aligned}$$

And the claim follows by taking square roots on both sides. For (f), substitute $\mathbf{x} \mapsto \mathbf{x} - \mathbf{y}$ and $\mathbf{y} \mapsto \mathbf{y} - \mathbf{z}$ into (e). □

Though we discuss the Euclidean norm here, it may also be of interest to consider/discuss other norms. One example is the L_1 norm (c.f. the norm discussed in Definition 1.36, which is the L_2 norm), which is the sum of the absolute values of each of the components. For $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ we have that:

$$|\mathbf{x}|_1 = |x_1| + |x_2| + \ldots + |x_n|, \quad |\mathbf{x} - \mathbf{y}|_1 = |x_1 - y_1| + |x_2 - y_2| + \ldots + |x_n - y_n|$$

The L_1 norm is often called the "Taxicab norm" or the "Manhattan norm" as the way it quantifies distance is akin to walking in discrete NSEW chunks; much like a taxi running through a grid-like New York City!

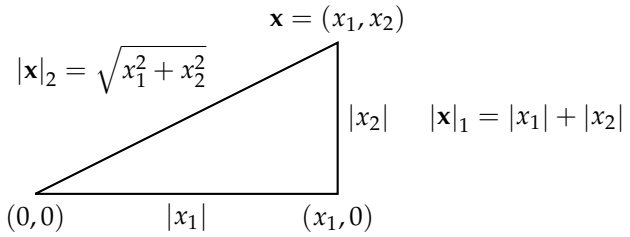

Figure 4: Visual comparison of the L_1 and L_2 norms in $\mathbb{R}^2$.

We are free to generalize this notion to the L_n norm, and we may also define the L_∞ norm, which for $\mathbf{x} \in \mathbb{R}^n$ is defined as:

$$|\mathbf{x}|_\infty = \max_i |x_i|$$

In general for any $\mathbf{x} \in \mathbb{R}^n$, we have that $|x|_1 \geq |x|_2 \geq |x|_3 \geq \ldots \geq |x|_\infty$. We note that we that we can generalize these norms to the cases where we have infinite components:

$$\|\mathbf{x}\|_p = \left(\sum_{i=1}^{\infty} |x_i|^p \right)^{1/p} < \infty \quad \|f\|_p \equiv \left(\int_S |f|^p \, \mathrm{d}\mu \right)^{1/p} < \infty$$

Which allow us to define norms for function spaces. However, a detailed discussion of these are beyond the scope of this course (to be covered in a later course in functional analysis!) Moreover, we haven't even defined what an infinite sum or integral are yet, which we will get to in later chapters.

2 Basic Topology

2.1 Finite and Countable Sets

This chapter is split into two portions; the first looks at counting, what it means for us to say that two sets have the same number of elements, and concludes with a classic theorem of Cantor concerning uncountable sets. The second part looks at the topology of metric spaces, before moving onto the topology of the real numbers.

Let us then begin with our discussion of counting. If we consider counting how many bananas there are on a table (say there are 10 bananas), then what we are formally doing is establishing a correspondence between each ball on the table with an element in the set $\{1, \ldots, 10\}$. When we refer to the number of elements in a set, it will be good to keep in mind that we are establishing functions between sets. Although we have been discussing functions with some frequency in the course already, we give a definition below for completeness.

Definition 2.1: Functions

Let A, B be sets. Then, a map that associates each element $x \in A$ with a unique element denoted as $f(x) \in B$ is a **function** $f : A \to B$. We then define A as the **domain** of f and the set $\{f(x) : x \in A\}$ as the **range**. For $E \subseteq A$, we call $f(E) = \{f(x) : x \in E\}$ the **image** of E under f. For $F \subseteq B$, we call $f^{-1}(B) = \{x \in A : f(x) \in B\}$ the **preimage** of F.

Definition 2.2: Injective/Surjective Functions

Let $f : A \mapsto B$ be a function. If for $x_1, x_2 \in A$ we have that $f(x_1) = f(x_2) \implies x_1 = x_2$ (or equivalently, $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$), then we say that f is **injective**, or **one-to-one**. If for all $y \in B$ there exists $x \in A$ such that $y = f(x)$, then we say that f is **surjective**, or **onto**. If a function is both injective and surjective, it is **bijective**.

Intuitively, we can think of injectivity as implying each element in B being reached at most once, and surjectivity implying that each element in B is reached at least once.

Definition 2.3: Cardinality & Equivalence

Let A, B be sets. We say that A, B have the same **cardinality** if there exists $f : A \mapsto B$ such that f is bijective. We can denote this as $A \sim B$ where $\sim$ indicates an **equivalence relation**. An equivalence relation has three properties:

(a) Reflexivity: $A \sim A$.

(b) Symmetry: If $A \sim B$ then $B \sim A$.

(c) Transitivity: If $A \sim B$ and $B \sim C$ then $A \sim C$.

As a point of notation, $|S|$ denotes the cardinality of the set S.

We get (a) from each set having a bijection to itself (i.e. the identity function), (b) from the fact that if there exists a bijection $f : A \mapsto B$, then there must exist an inverse $f^{-1} : B \mapsto A$, and (c) from if there exist bijections $f : A \mapsto B$ and $g : B \mapsto C$ then the composition $g \circ f : A \mapsto C$ will also be a bijection.

Definition 2.4: Countability

First, we denote $J_n = \{1, 2, 3, \ldots, n\}$ and $J = \mathbb{N} = \{1, 2, 3, \ldots\}$. Let A be a set. We say that A is **finite** if it has a finite number of elements, that is, there exists $n \in \mathbb{N}$ such that $A \sim J_n$. A set A is **infinite** if it is not finite, and we cannot put A in bijection with J_n for any $n \in \mathbb{N}$. We say that A is **countable**if $A \sim \mathbb{N}$, and **uncountable** otherwise.

Note that the above definition gives us a useful notion for what sets we can consider countable; if we can enumerate a set with the naturals, this yields a bijection with $\mathbb{N}$ and hence the set must be countable.

We here give some additional properties concerning cardinalities of sets, which may be useful:

- $|A| \leq |B| \iff \exists f : A \mapsto B$ such that f is injective
- $|A| \geq |B| \iff \exists f : A \mapsto B$ such that f is surjective
- $|A| \leq |B|$ and $|A| \geq |B| \implies |A| = |B|$

Example 2.5

$\mathbb{Z}$ is countable. To see this, consider the function:

$$f = \begin{cases} \frac{n}{2} & n \text{ is even} \\ -\frac{n-1}{2} & n \text{ is odd} \end{cases}$$

f is a bijection (check!) and hence $\mathbb{N} \sim \mathbb{Z}$.

The above example serves as a bit of a warning sign. Even though $\mathbb{N} \subsetneq \mathbb{Z}$ and $\mathbb{Z}$ has "more elements", we still find that the two sets have the same cardinality. A similar example is given by $\mathbb{N}$ and the set of all even natural numbers (which we may denote $2\mathbb{N}$); the bijection $f(n) : n \mapsto 2n$ between these two sets shows that $\mathbb{N} \sim 2\mathbb{N}$, even though $2\mathbb{N}$ is a strict subset of $\mathbb{N}$.

Theorem 2.8

A subset of a countable set is either finite or countable.

Proof

(Sketch) The countability of A implies that $A = \{a_1, a_2, a_3, a_4, a_5 \ldots\}$ (in other words, we can enumerate the elements using $\mathbb{N}$). Let $S \subseteq A$. Then, $S = \{a_1, \cancel{a_2}, a_3, a_4, \cancel{a_5}, \ldots\}$, that is, A with some (or none) of the elements removed. Now, we can rename all the elements with $a_1, a_2, \ldots$; what we have left is again an enumeration, so it is yet again (at most) countable.

One potentially useful fact is that if we have a set S and a function $f : \mathbb{N} \mapsto S$ such that f is surjective, then S is at most countable.

Proof. Let $T = \{n \in \mathbb{N} : f(n) \neq f(m), \forall m = 1, 2, \ldots, m\}$. We restrict $f : T \mapsto S$, then f is injective by constructive. It is still surjective, hence $T \sim S$. Since $T \subset \mathbb{N}$, by Theorem 2.8, S is finite or countable. □

Theorem 2.12

Let $E_1, E_2, \ldots$ be countable sets (i.e. we have a countable number of countable sets). Define $S = \bigcup_{n=1}^{\infty} E_n$. Then, S is countable.

Proof

Write $E_n = \{x_{n1}, x_{n2}, x_{n3}, \ldots\}$ (which we can do as each of the E_ns are countable). Then, we form an array:

$$\begin{array}{lcllll} E_1 & = & x_{11} & x_{12} & x_{13} & \cdots \\ E_2 & = & x_{21} & x_{22} & x_{23} & \cdots \\ E_3 & = & x_{31} & x_{32} & x_{33} & \cdots \\ \cdots & & & & & \end{array}$$

Then, we can re-number the elements along the diagonal lines (i.e. $x_{11}, x_{21}, x_{12}, x_{31}, x_{22}, x_{13}, \ldots$). This new enumeration corresponds to a countable set. From there, we let $T \subseteq \mathbb{N}$ be the remaining labels in the enumeration after removing the repeated elements from the sequence. Then, $T \sim S$, and hence S is at most countable. S cannot be finite as $E_1 \subseteq S$ and E_1 is not finite. Hence S is countable. $\square$

Corollary 2.13: $\mathbb{Q}$ is Countable.

- If A is countable, the set of n-tuples of $(a_1, \ldots a_n)$ is also countable for any $n \in \mathbb{N}$.
- $\mathbb{Q}$ is countable.

We defined $\mathbb{Q}$ as pairs of integers, but by the first part of the corollary (which follows immediately by application of Theorem 2.12) $\mathbb{Z}^2$ (the set of pairs of integers) has equal cardinality to $\mathbb{Z}$, and since $\mathbb{Q}$ is a subset of the set of pairs of integers, $\mathbb{Q}$ is countable.

From the discussion of today, we have established that $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$. Does $\mathbb{R}$ also have equal cardinality to these sets? Do infinite sets in general have the same cardinality? The answer turns out to be no for both of these questions. We will answer the first question in the next lecture (when we discuss Cantor diagonalization, a highlight of the course), but we can discuss the second statement now. First, we make a definition:

Definition: Power Sets

Let A be a set. Then, the **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

An interesting theorem then follows:

Theorem: Power Set Cardinality

Let A be a set. Then, $|A| < |\mathcal{P}(A)|$.

Proof

Suppose for the sake of contradiction that there exists a surjection $f : A \to \mathcal{P}(A)$ (this would imply that $|A| \geq \left|\mathcal{P}(A)\right|$, so by showing this is false, we obtain the desired result). Then, each element $x \in A$ gets mapped to some subset of A. We either have that x belongs to the subset that it gets mapped to, or it doesn't. Therefore, we can define a new subset $B \subseteq A$, such that:

$$B = \{x \in A : x \notin f(x)\}$$

In other words, the set of all xs that are not in the subset that they get mapped to by f. Since f is surjective, there must be an element $y \in A$ such that $f(y) = B$. One of $y \in B$, $y \notin B$ must be true. If $y \in B$, by construction of B we have that y is not in the subset that it gets mapped to by f, which is a contradiction. If $y \notin B$, by definition of B, $y \in B$ as it is not in the subset that it gets mapped to, yet again a contradiction. Therefore, we conclude that no $y \in A$ exists such that $f(y) = B$, and hence, no surjective f exists such that $f : A \to \mathcal{P}(A)$. Hence, $|A| < \left|\mathcal{P}(A)\right|$. □

An interesting consequence of this theorem is that for a countable set A, we then have that $\mathcal{P}(A)$ is an infinite set which has greater cardinality! For example, $|\mathbb{N}| < \left|\mathcal{P}(\mathbb{N})\right|$. Moreover, this gives rise to an infinite number of cardinalities in ascending order; $|\mathbb{N}| < \left|\mathcal{P}(\mathbb{N})\right| < \left|\mathcal{P}(\mathcal{P}(\mathbb{N}))\right| < \cdots$ and so on.

2.2 Uncountable Sets

Theorem 2.14: Existence of Uncountable Sets

Let $A = \{(b_1, b_2, \ldots), b_n \in \{0, 1\}\}$ be the set of binary sequences. Then, A is uncountable.

Proof

It suffices to show that every countable subset of A is a proper subset of A. Let $E \subset A$ be countable, and let $E = \left\{S^{(1)}, S^{(2)}, S^{(3)}, \ldots\right\}$. To show that E is a proper subset, we show that there exists a sequence $S \in A \setminus E$. To construct such an S, let us put the elements of E in an array.

$$\begin{aligned}
S^{(1)} &= \boxed{b_1^1} \quad b_2^1 \quad b_3^1 \quad \cdots \\
S^{(2)} &= b_1^2 \quad \boxed{b_2^2} \quad b_3^2 \quad \cdots \\
S^{(3)} &= b_1^3 \quad b_2^3 \quad \boxed{b_3^3} \quad \cdots
\end{aligned}$$

Then, define:

$$\tilde{b}_n^n = \begin{cases} 1 & \text{if } b_n^n = 0 \\ 0 & \text{if } b_n^n = 1 \end{cases}$$

I.e. $\tilde{b}_n^n$ is the bit flip of b_n^n. Then, let $S = (\tilde{b}_1^1, \tilde{b}_2^2, \tilde{b}_3^3, \ldots)$, that is, S is the sequence of bit-flipped diagonal elements of the original array. By construction, $S \neq S^{(k)}$ as for any $S^{(k)} \in E$ as S differs at the kth position. Hence, $S \notin E$ and therefore $E \subsetneq A$. □

The above proof is a very famous argument, invented by the mathematician George Cantor. The discovery that there exist sets with greater cardinality than $\mathbb{N}$ was initially quite controversial in the math community!

Corollary: $\mathbb{R}$ is Uncountable

$\mathcal{P}(\mathbb{N})$ (the power set of $\mathbb{N}$) is uncountable. $\mathbb{R}$ is uncountable.

Proof

Although we showed that $\mathcal{P}(\mathbb{N})$ was uncountable last lecture, we show this in an alternative way by considering a bijection between $\mathcal{P}(\mathbb{N})$ and the set A of binary sequences. To do this, consider that we can associate a subset $T \subset \mathbb{N}$, $T \in \mathcal{P}(\mathbb{N})$ with the sequence corresponding to:

$$b_n = \begin{cases} 1 & \text{if } n \in T \\ 0 & \text{if } n \notin T \end{cases}$$

Since A is uncountable, it follows that $\mathcal{P}(\mathbb{N})$ is uncountable. The second statement in the corollary follows (roughly) by considering $\mathbb{R}$ represented in binary, though this requires more justification than what we present here (we will show below that a subset of $\mathbb{R}$ is uncountable). □

Theorem

$[0,1] \subset \mathbb{R}$ is uncountable.

Proof

(Sketch) We construct a bijection from $[0,1]$ to A. Let $x \in [0,1]$, and let b_1 be the largest integer such that $N_1 = \frac{b_1}{2} \leq x$. Then, let $b_2 \in \{0,1\}$ be the largest integer such that $N_2 = \frac{b_1}{2} + \frac{b_2}{2^2} \leq x$. We can continue dividing $[0,1]$ in half in this way, approximating x by powers of 2 (a decimal expansion in binary). Then, let $E(x) = \{N_1, N_2, N_3, \ldots\}$. By construction, $E(x)$ is bounded above by x and nonempty. Hence, $\sup(E(x))$ exists and is unique, and in fact is equal to x (note that we are in essence constructing an "infinite series" where the sequence of partial sums is increasing and bounded, approaching x from the left). Doing this we can associate $(b_1, b_2, b_3, \ldots) \in A$ with every number $x \in [0,1]$ and therefore $[0,1] \sim A$. Hence $[0,1]$ is uncountable. □

2.3 Topology of Metric Spaces

In our investigation of topology, we will try to better understand distances between and neighbourhoods of points. To do so, we first introduce the notion of a metric space.

Definition 2.15: Metric Spaces

A set X is a **metric space** (whose elements we call points) with a **metric** $d : X \times X \mapsto \mathbb{R}$ such that for $x, y, z \in X$:

(a) $d(x,y) > 0$ if $x \neq y$; $d(x,x) = 0$;

(b) $d(x,y) = d(y,x)$ (d is symmetric);

(c) $d(x,z) \leq d(x,y) + d(y,z)$ (triangle inequality).

Example 2.16

$\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{R}^n, \mathbb{C}$ are all metric spaces with $d(x,y) = |x-y|$. Any subset $Y \subseteq X$ of a metric space is also a metric space, with the same metric.

Another example of a metric space is given below; note that this example can be generalized, in that any connected graph can be made into a metric space.

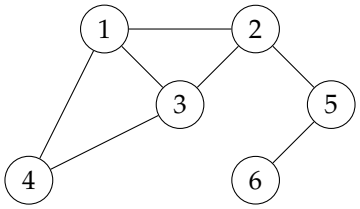

Figure 5: A graph-theoretic example of a metric space. Let $X = \{1,2,3,4,5,6\}$. Then, for $x, y \in X$, let $d(x,y)$ be the number of edges if the shortest path between x and y. Properties (a), (b) of a metric are immediately satisfied, and (c) follows from the property of the shortest path.

Definition 2.18: Neighbourhoods

A **neighbourhood** in a metric space X is a set $N_r(p) = \{q \in X : d(p,q) < r\}$ with $r > 0$.

Example

- In $\mathbb{R}$, $N_r(p)$ is the interval $(p-r, p+r)$ about midpoint p.
- In $\mathbb{R}^2$, $N_r(p)$ is the open disk about center p.
- In $\mathbb{R}^3$, $N_r(p)$ is the open ball about center p.
- In $\mathbb{R}^n$, $N_r(p)$ is the open hyperball about center p.

Definition 2.18: Interior Points

Let $E \subseteq X$. Then, p is an **interior point** of S if there is a neighbourhood $N_r(p)$ such that $N \subseteq E$.

Intuitively, an interior point of E is a point that is not on the boundary of E. As an example, in $\mathbb{R}^n$, if $E = \left\{y : |x-y| \leq 1\right\}$, then the interior points of E (which we can denote as E°) are $E^\circ = \left\{y : |x-y| < 1\right\}$. The idea is that there is always some finite distance to the boundary, so we can always fit a (perhaps small) open ball in. But this doesn't hold at the boundary!

Definition 2.18: Open Sets

A set $E \subseteq X$ is **open** if every point of E is an interior point of E.

Theorem 2.19

Every neighbourhood is an open set.

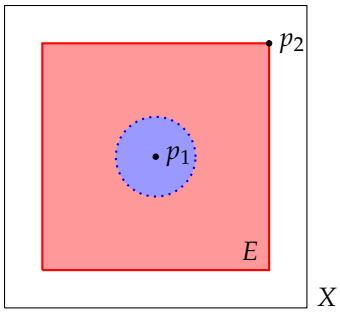

Figure 6: A visualation of an interior point. A set $E \subset X$ is pictured. p_1 is an interior point as there exists $N_r(p_1) \subset E$. p_2 is not an interior point as there does not exist a neighbourhood of p_2 that is entirely contained in E (it is on the boundary).

Proof

Consider a neighbourhood $E = N_r(p) \subseteq X$. Let $q \in E$. We will show that q is an interior point of E. Choose $s < r - d(p,q)$. Then, let $x \in N_s(q)$. By the triangle inequality:

$$d(x,p) \leq d(x,q) + d(q,p) < s + d(q,p) < r - d(p,q) + d(p,q) = r.$$

Hence, $d(x,p) < r$ and it follows that $x \in N_r(p)$. Hence, $N_s(q) \subset N_r(p)$ and q is an interior point of E. □

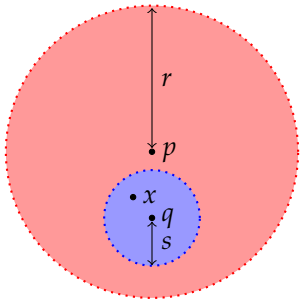

Figure 7: Visualization of the Sets/Points in Theorem 2.19

Definition 2.18: Limit Points/Isolated Points

Let $E \subseteq X$ and $p \in X$. Then, p is a **limit point** of E if every neighbourhood of p contains $q \in E$, $q \neq p$. If $p \in E$ and p is not a limit point of E, then p is an **isolated point** of E.

Example

Let $E = \left\{\frac{1}{n} : n \in \mathbb{N}\right\}$. Then, $\frac{1}{2}$ is not a limit point of E, as for $r < \frac{1}{4}$ $N_r(\frac{1}{2})$ does not contain any other points of E. On the other hand, 0 is a limit point of E. For any neighbourhood $N_r(0)$ of 0, $\frac{1}{N} \in N_r(0)$ for $N > \frac{1}{r}$. Note that 0 is the only limit point of E, and is not contained in E (indeed, there is no requirement that a limit point be contained in the set).

Theorem 2.20

If p is a limit point of E, then every neighbourhood of p contains an infinite number of $q \in E$.

Proof

(Sketch) Let $r_1 = 1$. Then, there exists $q_1 \in N_{r_1}(p)$ such that $q_1 \in E$ and $q_1 \neq p$ as p is a limit point of E by assumption. Let $r_2 = d(q_1, p)$. Then, there exists $q_2 \in N_{r_2}(p)$ such that $q_2 \in E$ and $q_2 \neq p$. We can repeat this process to get a (countably infinite) sequence of distinct points $q \in N_{r_1}(p)$, which proves the claim. □

Corollary

If $E \subseteq X$ is finite, then E has no limit points.

Definition 2.18: Closed Sets

A set $E \subseteq X$ is closed if every limit point of E is in E.

Note that with the above Corollary, we find that every finite set is (trivially) closed.

Definition 2.18: Complement

Let $E \subseteq X$. Then, the complement of E, denoted E^c is $E^c = \{x \in X : x \notin E\}$.

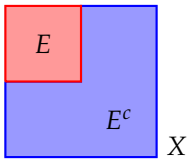

Figure 8: Visualization of a set E and its complement.

Theorem 2.23

A set $E \subseteq X$ is open if and only if E^c is closed.

Note that this theorem does not imply that all sets are closed or open; it is possible to have a set that is neither closed or open (such as $[0, 1) \subset \mathbb{R}$) and then its complement (with the former example, $(-\infty, 0) \cup [1, \infty]$) which is also neither closed nor open. As an additional note, we have that X (the entire metric space) and $\emptyset$ are both open and closed (which we may affectionately label as "clopen").

Proof

$\boxed{\Longrightarrow}$ Assume E is open. If E^c has no limit points, it is trivially closed, so suppose that there exists a limit point x of E^c. Suppose for the sake of contradiction that $x \notin E^c$. Then, $x \in E$. As E is open, x is an interior point of E, so there exists a neighbourhood $N_r(x) \subseteq E$. In particular, $N_r(x) \cap E^c = \emptyset$, contradicting the fact that x is a limit point of E^c. Hence, $x \in E^c$ and E^c is closed.
$\boxed{\Longleftarrow}$ Assume E^c is closed. Let $x \in E$. In particular, $x \notin E^c$, so x is not a limit point of E^c. So, there exists a neighbourhood $N_r(x)$ which contains no point of E^c, i.e. $N_r(x) \cap E^c = \emptyset$. It follows that $N_r(x) \subseteq E$, and hence x is an interior point of E. This argument applies to all points of E, hence E is open. □

Corollary

A set $F \subseteq X$ is closed if and only if F^c is open.

Let $F = E^c$ in Theorem 2.23 to realize the above Corollary.

Theorem 2.24

(a) For any collection $\{E_\alpha\}$ of open sets, $\bigcup_\alpha E_\alpha$ is open.

(b) For any collection $\{F_\alpha\}$ of closed sets, $\bigcap_\alpha F_\alpha$ is closed.

(c) For any finite collection $E_1, \ldots, E_n$ of open sets, $\bigcap_{i=1}^n E_i$ is open.

(d) For any finite collection $F_1, \ldots, F_n$ of closed sets, $\bigcup_{i=1}^n F_i$ is closed.

A point of notation; $\{E_\alpha\}$ can be finite, countable, or uncountable; the indices α are taken from an index set A which can be chosen to be of any cardinality.

Proof

(a) Suppose all sets in $\{E_\alpha\}$ are closed. Let $x \in \bigcup_\alpha E_\alpha$. Then, there exists α_0 such that $x \in E_{\alpha_0}$. Since E_{α_0} is open, there exists a neighbourhood $N_r(x)$ of x such that $N_r(x) \subseteq E_{\alpha_0} \subseteq \bigcup_\alpha E_\alpha$. Hence, $\bigcup_\alpha E_\alpha$ is open.

(b) Suppose all sets in $\{F_\alpha\}$ are open. To show that $\bigcap_\alpha F_\alpha$ is closed, we show that $\left(\bigcap_\alpha F_\alpha\right)^c$ is open (by Theorem 2.23). We have that $\left(\bigcap_\alpha F_\alpha\right)^c = \bigcup_\alpha F_\alpha^c$. As all F_α^c are open, by part (a) we have that $\bigcup_\alpha F_\alpha^c$ is also open. Hence $\bigcap_\alpha F_\alpha$ is closed.

(c) Suppose $E_1, \ldots, E_n$ are open. Let $x \in \bigcap_{i=1}^n E_i$, and then we have that $x \in E_i$ for all $i \in \{1, \ldots, n\}$. Hence, there exists r_i such that $N_{r_i}(x) \subseteq E_i$ as each of the E_is are open. Let $r = \min\{r_1, \ldots, r_n\}$ and then we have that $N_r(x) \subseteq N_{r_i}(x) \subseteq E_i$ for all E_i. Therefore, $N_r(x) \subseteq \bigcap_{i=1}^n E_i$ and $\bigcap_{i=1}^n E_i$ is open.

(d) Suppose $F_1, \ldots, F_n$ are closed. By Theorem 2.23 we have that $\bigcup_{i=1}^n F_i$ is closed if and only if $\left(\bigcup_{i=1}^n F_i\right)^c = \bigcap_{i=1}^n F_i^c$ is open. Since all F_i^cs are open, by part (c) $\bigcap_{i=1}^n F_i^c$ is open, and hence $\bigcup_{i=1}^n F_i$ is closed. □

Example 2.25

We consider some examples to see why the finiteness of the collections in parts (c)/(d) of the theorem are essential. Suppose $E_n = \left(-\frac{1}{n}, \frac{1}{n}\right) \subset \mathbb{R}$. These sets form a countably infinite collection of subsets of $\mathbb{R}$. We then consider that $\bigcap_{n=1}^{\infty} E_n = \{0\}$, which is not open; showing that openness is not preserved under infinite intersections. Next, consider $F_n = [0, 1 - \frac{1}{n}] \subset \mathbb{R}$, which form a countably infinite collection of closed sets in $\mathbb{R}$. We then have that $\bigcup_{n=1}^{\infty} F_n = [0, 1)$ which is not closed as 0 is not an interior point of the set. Hence, closedness is not preserved under infinite unions.

2.4 Closure and Relative Topology

2.5 Compactness

2.6 Compactness in $\mathbb{R}^k$ and the Cantor Set

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