Louis Meunier

Analysis I, II MATH254

Contents

1 Logic, Sets, and Functions

1.1 Mathematical Induction & The Naturals

The **natural numbers**, $\mathbb{N} = \{1, 2, 3, \ldots\}$, are specified by the 5 **Peano Axioms**:

(1) $1 \in \mathbb{N}$ [1]

(2) every natural number has a successor in $\mathbb{N}$

(3) 1 is not the successor of any natural number

(4) if the successor of x is equal to the successor of y, then x is equal to y [2]

(5) **the axiom of induction**

[1] using 0 instead of 1 is also valid, but we will use 1 here.

[2] axioms (2)-(4) can be equivalently stated in terms of a successor function $s(n)$ more rigorously, but won't here

The **Axiom of Induction** (AI), can be stated in a number of ways.

Axiom 1.1 (AI.i). *Let $S \subseteq \mathbb{N}$ with the properties:*

(a) $1 \in S$

(b) if $n \in S$, then $n + 1 \in S$ [3]

then $S = \mathbb{N}$.

[3] *(a)* is called the **inductive base**; *(b)* the **inductive step**. All AI restatements are equivalent in having both of these, and only differentiate on their specific values.

Example 1.1. *Prove that, for every* $n \in \mathbb{N}$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2} (\equiv (1))$

Proof (via AI.i). Let S be the subset of $\mathbb{N}$ for which (1) holds; thus, our goal is to show $S = \mathbb{N}$, and we must prove *(a)* and (b) of AI.i.

- by inspection, $1 \in S$ since $1 = \frac{1(1+1)}{2} = 1$, proving *(a)*
- assume $n \in S$; then, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ by definition of S. Adding $n + 1$ to both sides yields:

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) && (1) \\ &= (n+1)(\frac{n}{2} + 1) && (2) \\ &= \frac{(n+1)(n+2)}{2} && (3) \\ &= \frac{(n+1)((n+1)+1)}{2} && (4) \end{aligned}$$

Line (4) is equivalent to statement (1) (substituting n for $n+1$), and thus if $n \in S$, then $n+1 \in S$ and *(b)* holds. Thus, by AI.i, $S = \mathbb{N}$ and $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ holds $\forall n \in \mathbb{N}$. ■

Example 1.2. *Prove (by induction), that for every* $n \in \mathbb{N}$, $1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$.

Proof. Follows a similar structure to the previous example. Let S be the subset of $\mathbb{N}$ for which the statement holds. $1 \in S$ by inspection (*(a)* holds), and we prove *(b)* by assuming $n \in S$ and showing $n + 1 \in S$ (algebraically). Thus, by AI.i, $S = \mathbb{N}$ and the statement holds $\forall n \in \mathbb{N}$. ■

This can also be proven directly (Gauss' method).

Proof (Gauss' method). Let $A(n) = 1 + 2 + 3 + \cdots + n$. We can write $2 \cdot A(n) = 1 + 2 + 3 + \cdots + n + 1 + 2 + 3 + \cdots + n$. Rearranging terms (1 with n, 2 with $n - 1$, etc.), we can say $2 \cdot A(n) = (n+1) + (n+1) + \cdots$, where $(n+1)$ is repeated n times; thus, $2 \cdot A(n) = n(n+1)$, and $A(n) = \frac{n(n+1)}{2}$. ■

Axiom 1.2 (AI.ii)**.** *Let* $S \subseteq \mathbb{N}$ *s.t.*

(a) $m \in S$

(b) $n \in S \implies n + 1 \in S$

then $\{m, m+1, m+2, \ldots\} \subseteq S$.

Example 1.3. *Using AI.ii, prove that for $n \geq 2$, $n^2 > n+1$*

Proof. Again, very similar to the previous induction examples. Take S to be the subset of $\mathbb{N}$ for which the statement holds. *(a)* of AI.ii holds by inspection (where $m = 2$), and *(b)* holds by assuming $n \in S$ and showing that $n+1 \in S$. Thus, $S = \{2, 3, 4, \dots\}$, and the statement holds $\forall n \geq 2$. ∎

Axiom 1.3 (Principle of Complete Induction, AI.iii). *Let $S \subseteq \mathbb{N}$ s.t.*

(a) $1 \in S$

(b) if $1, 2, \dots, n-1 \in S$, *then* $n \in S$

then $S = \mathbb{N}$.

Finally, combing AI.ii and AI.iii;

Axiom 1.4 (AI.iv). *Let $S \subseteq \mathbb{N}$ s.t.:*

(a) $m \in S$

(b) if $m, m+1, \dots, m+n \in S$, *then* $m+n+1 \in S$

then $\{m, m+1, m+2, \dots\} \subseteq S$.

Theorem 1.1 (Fundamental Theorem of Arithmetic). *Every natural number n can be written as a product of one or more primes.* [4]

[4] 1 is not a prime number

Proof of Theorem 1.1. Let S be the set of all natural numbers that can be written as a product of one or more primes. We will use AI.iv to show $S = \{2, 3, \dots\}$.

- *(a)* holds; 2 is prime and thus $2 \in S$
- suppose that $2, 3, \dots, 2+n \in S$. Consider $2 + (n+1)$:
  - if $2 + (n+1)$ is *prime*, then $2 + (n+1) \in S$, as all primes are products of 1 and themselves and are thus in S by definition.
  - if $2 + (n+1)$ is *not prime*, then it can be written as $2 + (n+1) = a \cdot b$ where $a, b \in \mathbb{N}$, and $1 < a < 2 + (n+1)$ and $1 < b < 2 + (n+1)$. By the definition of S, $a, b \in S$, and can thus be written as the product of primes. Let $a = p_1 \cdot \dots \cdot p_l$ and $b = q_1 \cdot \dots \cdot q_j$, where the p's and q's are prime and $l, j \geq 1$. Then, $a \cdot b$ is a product of primes, and thus so is $2 + (n+1)$. Thus, $2 + (n+1) \in S$, and by AI.iv, $S = \{2, 3, 4, \dots\}$

∎

1.2 Extensions: Integers, Rationals, Reals

Consider the set of naturals $\mathbb{N} = \{1, 2, 3, \dots\}$. Adding 0 to $\mathbb{N}$ defines $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. We define the **integers** as the set $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, or the set of all positive and negative whole numbers.

Within $\mathbb{Z}$, we can define multiplication, addition and subtraction, with the neturals of 1 and 0, respectively. However, we cannot define division, as we are not guaranteed a quotient in $\mathbb{Z}$. This necessitates the **rationals**, $\mathbb{Q}$. We define

$$\mathbb{Q} = \{\frac{p}{q}, p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}.$$

On $\mathbb{Q}$, we have the familiar operations of multiplication, addition, subtraction and properties of associativity, distributivity, etc. We can also define division, as $\frac{\frac{p}{q}}{\frac{p'}{q'}} = \frac{pq'}{qp'}$.

We can also define a relation $<$ between fractions, such that

- $x < y$ and $y < z \implies x < z$
- $x < y \implies x + z < y + z$

$\mathbb{Q}$, together with its operations and relations above, is called an **ordered field**.

1.2.1 The Insufficiency of the Rationals

We can consider historical reasoning for the extension of $\mathbb{Q}$ to $\mathbb{R}$. Consider a right triangle of legs a, b and hypotenuse c. By the Pythagorean Theorem, $a^2 + b^2 = c^2$. Consider further the case there $a = b = 1$, and thus $c^2 = 2$. Does c exist in $\mathbb{Q}$?

Proposition 1.1. *$c^2 = 2$, $c \notin \mathbb{Q}$.*

Proof of Proposition 1.1. Suppose $c \in \mathbb{Q}$. We can thus write $c = \frac{p}{q}$, where[5] $p, q \in \mathbb{N}$, and p, q share no common divisors, ie they are in "simplest form". Notably, p and q cannot *both* be even (under our initial assumption), as they would then share a divisor of 2. We write

$$c = \frac{p}{q}$$
$$c^2 = 2 = \frac{p^2}{q^2}$$
$$2q^2 = p^2$$

$p \in \mathbb{N} \implies p^2 \in \mathbb{N}$, and thus p^2, and therefore[6] p, must be divisible by 2 ($\implies p$ even). Therefore, we can write $p = 2p_1, p_1 \in \mathbb{N}$, and thus $2q^2 = (2p_1^2)^2 \implies q^2 = 2p_1^2$. By the same reasoning, q must now be even as well, contradicting our initial assumption that p and q share no common divisors. Thus, $c \notin \mathbb{Q}$. ■

[5] Note that in the definition of $\mathbb{Q}$, p, q are defined to be in $\mathbb{Z}$; however, as we are using a

1.3 Sets & Set Operations

- $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- $\bigcup_{i=1}^{\infty} A_n = \bigcup_{n \in \mathbb{N}} A_n = \{x : x \in A_n \text{ for some } n \in \mathbb{N}\}$
- $\bigcap_{i=1}^{\infty} A_n = \bigcap_{n \in \mathbb{N}} A_n = \{x : x \in A_n \forall n \in \mathbb{N}\}$
- $A^C = \{x : x \in X \text{ and } x \notin A\}$[7]

[7] X is often omitted if it is clear from context.

Theorem 1.2 (De Morgan's Theorem(s)). *Let A, B be sets. Then,*

$$(a) \qquad (A \cap B)^C = A^C \cup B^C$$

and

$$(b) \qquad (A \cup B)^C = A^C \cap B^C.$$

Proof of Theorem 1.2. (b) *(A similar argument follows…)*

■

Proposition 1.2.

$$(a) \left(\bigcap_{n=1}^{\infty} A_n\right)^C = \bigcup_{n=1}^{\infty} A_n^C$$

$$(b) \left(\bigcup_{n=1}^{\infty} A_n\right)^C = \bigcap_{n=1}^{\infty} A_n^C$$

Proof of Proposition 1.2. Consider Proposition (b). Working from the left-hand side, we have

$$\begin{aligned} \left(\bigcup_{n=1}^{\infty} A_n\right)^C &= \{x : x \notin \bigcup A_n\} \\ &= \{x : x \notin A_n \forall\, n \in \mathbb{N}\} \\ &= \bigcap \{x : x \notin A_n\} \\ &= \bigcap A_n^C \end{aligned}$$

(a) can be logically deduced from this result. Consider the RHS, $\bigcup A_n^C$. Taking the complement:

$$\begin{aligned} \left(\bigcup A_n^C\right)^C &\overset{\text{via (b)}}{=} \bigcap A_n^{C^C} \\ &= \bigcap A_n \end{aligned}$$

Taking the complement of both sides, we have $\bigcup A_n^C = \left(\bigcap A_n\right)^C$, proving (a). ■

1.4 Functions

Definition 1.1. *Let A, B be sets. A* function f *is a rule assigned to each $x \in A$ a corresponding unique element $f(x) \in B$. We denote*

$$f : A \to B.$$

Definition 1.2. *The* domain *of a function $f : A \to B$, denoted Dom$(f) = A$. The* range *of f, denoted Ran$(f) = \{f(x) : x \in A\}$. Clearly, Ran$(f) \subseteq B$, though equality is not necessary.*

Example 1.4. *The function $f(x) = \sin x$, $f : \mathbb{R} \to [-1, 1]$. Here, Dom$(f) = \mathbb{R}$, and Ran$(f) =$ $[-1, 1]$.*

Example 1.5 (Dirichlet Function)**.** [8] $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \begin{cases} 1, x \in \mathbb{Q} \\ 0, x \notin \mathbb{Q} \end{cases}$. *Despite not having a true "explicit" formula, so to speak, this is still a valid function (under modern definitions).*

[8] Look up a graph of this function. Its beautiful. It's also interesting to note that its integral is simply 0.

1.4.1 Properties of Functions

Proposition 1.3. *Let $f : A \to B$, $C \subseteq A$, $f(C) = \{f(x) : x \in C\}$. We claim $f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$.*

Proof. We will prove this by showing (1) $\subseteq$ and (2) $\supseteq$.

(1) $y \in f(C_1 \cup C_2) \implies$ for some $x \in C_1 \cup C_2, y = f(x)$. This means that either for some $x \in C_1, y = f(x)$, or for some $x \in C_2, y = f(x)$. This implies that either $y \in f(C_1)$, or $y \in f(C_2)$, and thus y *must* be in their union, ie $y \in C_1 \cup C_2$.

(2) $y \in f(C_1) \cup f(C_2) \implies y \in f(C_1)$ or $y \in f(C_2)$. This means that for some $x \in C_1, y = f(x)$, or for some $x \in C_2, y = f(x)$. Thus, x *must* be in $C_1 \cup C_2$, and for some $x \in C_1 \cup C_2, y = f(x) \implies y \in f(C_1 \cup C_2)$.

(1) and (2) together imply that $f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$. ■

Example 1.6. *Let $A_n = 1, 2, \dots$ be a sequence of sets. Prove that $f(\bigcup_{n=1}^{\infty} A_n) = \bigcup_{n=1}^{\infty} f(A_n)$.*

Proof. Let $y \in f(\bigcup_{n=1}^{\infty} A_n)$. This implies that $\exists x \in \bigcup_{n=1}^{\infty} A_n$ s.t. $f(x) = y$. This implies that $x \in A_n$ for some n, and $y \in f(A_n)$ for that same "some" n, and thus y must be in the union of all possible $f(A_n)$, ie $y \in \bigcup f(A_n)$. This shows $\subseteq$, use similar logic for the reverse. ∎

Proposition 1.4. $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$ [9]

[9] NB: the reverse is not always true, ie these sets are not always equal; "lack" of equality is more "common" than not.

Proof. $y \in f(C_1 \cap C_2) \implies$ for some $x \in C_1 \cap C_2, y = f(x)$. This implies that for some $x \in C_1, y = f(x)$ **and** for some $x \in C_2, y = f(x)$. Note that this does *not* imply that these x's are the same, ie this reasoning is not reversible as in the previous union case. This implies that $y \in f(C_1)$ and $y \in f(C_2) \implies y \in f(C_1) \cap f(C_2)$. ∎

Example 1.7. *Prove that if $A_n, n = 1, 2, \dots, f(\bigcap_{n=1}^{\infty} A_n) \subseteq \bigcap_{n=1}^{\infty} f(A_n)$.*

Proof (Sketch). Use the same idea as in Example 1.6, but, naturally, with intersections. ∎

Example 1.8. *Take $f(x) = \sin x$, $A = \mathbb{R}, B = \mathbb{R}$, and take $C_1 = [0, 2\pi], C_2 = [2\pi, 4\pi]$. Then, $f(C_1) = [-1, 1]$, and $f(C_2) = [-1, 1]$. But $C_1 \cap C_2 = \{2\pi\}$; $f(\{2\pi\}) = \{\sin 2\pi\} = \{0\}$, and thus $f(C_1 \cap C_2) = \{0\}$, while $f(C_1) \cap f(C_2) = [-1, 1]$, as shown in Proposition 1.4.*

Definition 1.3 (Inverse Image of a Set). *Let $f : A \to B$ and $D \subseteq B$. The* inverse image *of D by F is denoted $f^{-1}(D)$*[10] *and is defined as*

$$f^{-1}(D) = \{x \in A : f(x) \in D\}.$$

[10] Note that this is **not** equivalent to the typical definition of an inverse *function*; f^{-1} may not exist

Example 1.9. $A = [0, 2\pi], B = \mathbb{R}, f(x) = \sin x, D = [0, 1]$.

$$f^{-1}(D) = \{x \in A : f(x) \in D\} = \{x \in [0, 2\pi] : \sin(x) \in [0, 1]\} = [0, \pi].$$

Proposition 1.5. *Given function f and sets D_1, D_2,*

(a) $f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$

(b) $f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$[11]

[11] Just see next proposition; if you really need convincing, just use 2 rather than ∞ as the upper limit of the unions/intersections and use the same proof.

Proposition 1.6. *Let $A_n, n = 1, 2, 3 \dots$. Then,*

(a) $f^{-1}(\bigcup_{n=1}^{\infty} A_n) = \bigcup_{n=1}^{\infty} f(A_n)$

(b) $f^{-1}(\bigcap_{n=1}^{\infty} A_n) = \bigcap_{n=1}^{\infty} f(A_n)$

Proof. [12]

(a)

$$\begin{aligned}
x \in f^{-1}(\bigcup_{n=1}^{\infty} A_n) &\iff f(x) \in \bigcup_{n=1}^{\infty} A_n \\
&\iff f(x) \in A_n \text{ for some } n \in \mathbb{N} \\
&\iff x \in f^{-1}(A_n) \text{ for some } n \in \mathbb{N} \\
&\iff x \in \bigcup_{n=1}^{\infty} f^{-1}(A_n)
\end{aligned}$$

(b)

$$\begin{aligned}
x \in f^{-1}(\bigcap_{n=1}^{\infty} A_n) &\iff f(x) \in \bigcap_{n=1}^{\infty} A_n \\
&\iff f(x) \in A_n \text{ for all } n \in \mathbb{N} \\
&\iff x \in f^{-1}(A_n) \text{ for all } n \in \mathbb{N} \\
&\iff x \in \bigcap_{n=1}^{\infty} f^{-1}(A_n)^{13}
\end{aligned}$$

■

[13]This is a "proof by definitions" as I like to call it.

[13]Similar proof can be used to prove Proposition 1.5, less generally.

Remark 1.1. *$f : A \to B$, $A_1 \subseteq A$. Given $f(A_1^C)$ and $f(A_1)^C$, there is **no general relation** between the two.*

For instance, take $A = [0, 6\pi], B = [-1, 2], C = [0, 2\pi]$, and $f(x) = \sin x$. Then, $f(C) = [-1, 1]$, and $f(C^C) = f([-1, 0)) = [-1, 1]$, but $f(C)^C = [-1, 1]^C = (1, 2]$, and $f(C^C) \neq f(C)^C$; in fact, these sets are disjoint.

Proposition 1.7. *Let $f : A \to B$ and let $D \subseteq B$. Then $f^{-1}(D^C) = [f^{-1}(D)]^C$.*

Proof.

$$f^{-1}(D^C) = \{x : f(x) \in D^C\} = \{x : f(x) \notin D\}$$

$$[f^{-1}(D)]^C = [\{x : f(x) \in D\}]^C = \{x : x \notin f^{-1}(D)\} = \{x : f(x) \notin D\}$$

■

1.5 Reals

Axiom 1.5 (Of Completeness)**.** *Any non-empty subset of $\mathbb{R}$ that is bound from above has at least one upper bound (also called the supremum).*

In other words; let $A \subseteq \mathbb{R}$ and suppose A is bounded from above (A has at a least upper bound). Then $\sup(A)$ exists.

Real numbers, algebraically have the same properties as the rationals; we have addition, multiplication, inverse of non-zero real numbers, and we have the relation $<$. All together, $\mathbb{R}$ is an ordered field.

Definition 1.4. *Let $A \subseteq \mathbb{R}$. A number $b \in \mathbb{R}$ is called an* ***upper bound*** *for A if for any $x \in A$, $x \leq B$.*

A number $l \in \mathbb{R}$ is called a ***lower bound*** *for A if for any $x \in A$, $x \geq l$.*

Definition 1.5 (The Least Upper Bound)**.** *Let $A \subseteq \mathbb{R}$. A real number s is called the* ***least upper bound*** *for A if the following holds:*

(a) s is an upper bound for A

(b) if b is any other upper bound for A, then $s \leq b$.

The least upper bound of a set A is unique, *if it exists; if s and s' are two least upper bounds, then by (a), s and s' are upper bound for A, and by (b), $s \leq s'$ and $s' \leq s$, and thus $s = s'$.*

This least upper bound is called the supremum *of A, denoted $\sup(A)$.*

Definition 1.6 (The Greatest Lower Bound)**.** *Let $A \subset \mathbb{R}$. A number $i \in \mathbb{R}$ is called the* ***greatest lower bound*** *for A if the following holds:*

(a) i is a lower bound for A

(b) if l is any other lower bound for A, then $i \geq l$.

If i exists, it is called the infimum *of A and is denoted $i = \inf(A)$, and is unique by the same argument used for $\sup(A)$.*

Proposition 1.8. *Let $A \subseteq \mathbb{R}$ and let s be an upper bound for A. Then $s = \sup(A)$ iff for any $\varepsilon > 0$, there exists $x \in A$ s.t. $s - \varepsilon < x$.*

Proof. We have two statements:

I. $s = \sup(A)$;

II. For any $\epsilon > 0$, $\exists x \in A$ s.t. $s - \epsilon < x$;

and we desire to show that I $\iff$ II.

- I $\implies$ II: Let $\epsilon > 0$. Then, since $s = \sup(A)$, $s - \epsilon$ *cannot* be an upper bound for A (as s is the least upper bound, and thus $s - \epsilon < s$ cannot be an upper bound at all). Thus, there exists $x \in A$ such that $s - \epsilon < x$, and thus if I holds, II must hold.

- II $\implies$ I: suppose that this does not hold, ie II holds for an upper bound s for A, but $s \neq \sup(A)$. Then, there exists some upper bound b of A s.t. $b < s$. Take $\epsilon = s - b$. $\epsilon > 0$, and since II holds, there exists $x \in A$ such that $s - \epsilon < x$. But since $s - \epsilon = b$ and thus $b < x$, then b cannot be an upper bound for A, contradicting our initial condition. So, if II $\implies$ I does *not* hold, we have a "impossibility", ie a value b which is an upper bound for A which cannot be an upper bound, and thus II $\implies$ I.

■

Proposition 1.9. *Let $A \subseteq \mathbb{R}$ and let i be a lower bound for A. Then $i = \inf(A) \iff$ for every $\epsilon > 0$ there exists $x \in A$ s.t. $x < i + \epsilon$.*[14]

[14]Use similar argument to proof of previous proposition.

Remark 1.2. *Axiom 1.5 can also be expressed in terms of infimum. Define $-A = \{-x : x \in A\}$. Then, if b is an upper bound for A, then $b \geq x \forall x \in A$, then $-b \leq -x \forall x \in A$, ie -b is a lower bound of $-A$. Similarly, if l is a lower bound for A, $-l$ is an upper bound for $-A$.*

Thus, if A is bounded from above, then

$$-\sup(A) = \inf(-A),$$

and if A is bounded from below,

$$-\inf(A) = \sup(-A).$$

Axiom 1.6 (AC (infimum))**.** *Let $A \subseteq \mathbb{R}$; if A bounded from below, $\inf(A)$ exists.*

Definition 1.7 (max, min)**.** *Let $A \subseteq \mathbb{R}$. An $M \in A$ is called a* maximum *of A if for any $x \in A$, $x \leq M$. M is an upper bound for A,* ***but also*** *$M \in A$.*

If M exists, then $M = \sup(A)$; M is an upper bound, and if b any other upper bound, then $b \geq M$, because $M \in A$, and thus $M = \sup(A)$.

NB: $M = \max(A)$ ***need not*** *exist, while $\sup(A)$ must exist. Consider $A = [0, 1)$; $\sup(A) = 1$, but there exists no $\max(A)$.*

The same logic exists for the existence of minimum vs infimum (consider $(0, 1)$, with no maximum nor minimum).

Theorem 1.3 (Nested interval property of $\mathbb{R}$). *Let $I_n = [a_n, b_n] = \{x : a_n \leq x \leq b_n\}, n = 1, 2, 3\dots$ be an infinite sequence of bounded, closed intervals s.t.*

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots I_n \supseteq I_{n+1} \supseteq \dots$$

Then, $\bigcap_{n=1}^{\infty} I_n \neq \varnothing$ (note that this does not *hold in $\mathbb{Q}$).*

Proof. [15] We have $I_n = [a_n, b_n], I_{n+1} = [a_{n+1}, b_{n+1}], \dots$. And the inclusion $I_n \supseteq I_{n+1}$. $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n, \forall n \geq 1$. So, the sequence a_n (left-end) is increasing, and the sequence b_n (right-end) is decreasing.

We also have that for any $n, k \geq 1$, $a_n \leq b_k$. We see this by considering two cases:

- Case 1: $n \leq k$, then $a_n \leq a_k$ (as a_n is increasing), and thus $a_n \leq a_k \leq b_k$.
- Case 2: $n > k$, then $a_n \leq b_n \leq b_k$ (again, as b_n is decreasing).

Let $A = \{a_n : n \in \mathbb{N}\}$. Then, A is bounded from above by *any* b_k (as in our inequality we showed above). Let $x = \sup(A)$, which must exist by Axiom 1.5.

Note that as a result, $x \geq a_n$ for all n, and for all k, $x \leq b_k$, as x is the lowest upper bound and must be $\leq$ all other upper bounds, and so for all $n \geq 1$, $a_n \leq x \leq b_n$, ie $x \in I_n \forall n \geq 1$, and thus $x \in \bigcap_{n=1}^{\infty} I_n$ and so $\bigcap_{n=1}^{\infty} \neq \varnothing$. ■

[15] Sketch: show that the left-end points are increasing and the right-end points are decreasing. Show either that all the left-end points are bounded from above or that all the right-end points are bounded from below. As a result, there exists a sup/inf (depending on which end you choose) of the set of all the right/left points. For the sup case, all upper bounds must be $\geq$ sup, and thus the sup is in all I_n, and thus in their intersect, and thus the intersect is not empty.

Remark 1.3. *The proof above emphasized the left-end points; it can equivalently be proven via the right-end points, and using $y = \inf(\{b_n : n \in \mathbb{N}\}) = \inf(B)$, rather than $\sup(A)$, and showing that $y \in \bigcap I_n$.*

Remark 1.4. *Note too that, if $x = \sup(A)$ and $y = \inf(B)$, then $x, y \in \bigcap_{n=1}^{\infty} I_n$; in fact, $\bigcap_{n=1}^{\infty} I_n = [x, y]$.*

Remark 1.5. *The intervals I_n* must *be closed; if not, eg $I_n = (0, \frac{1}{n})$, then $\bigcap_{n=1}^{\infty} I_n = \varnothing$.*

1.6 Density of Rationals in Reals

Proposition 1.10 (Archimedean Property). *(a) For any $x \in \mathbb{R}$, there exists a natural number n s.t. $n > x$.*

(b) For any $y \in \mathbb{R}$ satisfying $y > 0$, $\exists n \in \mathbb{N}$ such that $\frac{1}{n} < y$.

Remark 1.6. *(a) states that $\mathbb{N}$ is not a bounded subset of $\mathbb{R}$.*

Remark 1.7. *(b) follows from (a) by taking $x = \frac{1}{y}$ in (a), then $\exists n \in \mathbb{N}$ s.t. $n > \frac{1}{y} \implies \frac{1}{n} < y$, and thus we need only prove (a).*

Remark 1.8. *Recall that $\mathbb{Q}$ is an ordered field (operations $+, \cdot$ and a relation $<$). $\mathbb{Q}$ can be extended to a larger ordered field with extended definitions of these operations/relations, such that it contains elements that are larger than any natural numbers (ie, not bounded above). This is impossible in $\mathbb{R}$ due to AC.*

Proof. Suppose (a) not true in $\mathbb{R}$, ie $\mathbb{N}$ is bounded from above in $\mathbb{R}$. Let $\alpha = \sup \mathbb{N}$, which exists by AC.

Consider $\alpha - 1$; since $\alpha - 1 < \alpha$, $\alpha - 1$ is not an upper bound of $\mathbb{N}$. So, there exists some $n \in \mathbb{N}$ s.t. $\alpha - 1 < n$; then, $\alpha < n + 1$ where $n + 1 \in \mathbb{N}$, and thus α is also not an upper bound, as there exists a natural number that is greater than α. This contradicts the assumption that $\alpha = \sup \mathbb{N}$, so (a) must be true. ∎

Theorem 1.4 (Density). *Let $a, b \in \mathbb{R}$ s.t. $a < b$. Then, $\exists x \in \mathbb{Q}$ s.t. $a < x < b$.*

Remark 1.9. *If you take $a \in \mathbb{R}$ and $\epsilon > 0$, then by the theorem, $\exists x \in \mathbb{Q}$ where $x \in (a - \epsilon, a + \epsilon)$. So any real number can be approximated arbitrarily closely (via choose of ϵ) by a rational number.*

Proof. Since $b - a > 0$, by (b) of Proposition 1.10, $\exists n \in \mathbb{N}$ s.t. $\frac{1}{n} < b - a$, ie $na + 1 < nb$.

Let $m \in \mathbb{Z}$ s.t. $m - 1 \leq na < m$. Such an integer must exists since $\bigcup_{m \in \mathbb{Z}} [m-1, m) = \mathbb{R}$, the family $[m-1, m), m \in \mathbb{Z}$ makes partitions of $\mathbb{R}$. Then, $na < m$ gives that $a < \frac{m}{n}$. On the other hand, $m - 1 \leq na$ gives $m \leq na + 1 < nb$. So $\frac{m}{n} < b$ and it follows that $\frac{m}{n}$ satisfies $a < \frac{m}{n} < b$. ∎

In the proof, we used the claim:

Proposition 1.11. *If $z \in \mathbb{R}$, then there exists $m \in \mathbb{Z}$ s.t. $m - 1 \leq z < m$.*

Proof. Let S be a non-empty subset of $\mathbb{N}$. Then S has the least element; $\exists m \in S$ s.t. $m \leq n, \forall n \in S$.

We can assume $z \geq 0$; if $0 \leq z < 1$, then we are done (take $m = 1$), and assume that $z \geq 1$. Let now $S = \{n \in \mathbb{N} : z < n\}, \neq \varnothing$ by Proposition 1.10, (a). Let m be the least element of S. It exists by Well-Ordering Property; then, since $m \in S$, $z < m$. But, we also have $m - 1 \leq z$, otherwise, if $z < m - 1$ then $m - 1 \in S$ and then m is not the least element of S. Thus, we have $m - 1 \leq z < m$, as required. ∎

Theorem 1.5. *The set J of irrationals is also dense in $\mathbb{R}$. That is, if $a, b \in \mathbb{R}, a < b$, $\exists$ irrational y s.t. $a < y < b$ (noting that $J = \mathbb{R} \setminus \mathbb{Q}$).*

Proof. Fix $y_0 \in \mathbb{J}$. Consider $a - y_0, b - y_0$. $a - y_0 < b - y_0$, and by density of rationals, $\exists x \in \mathbb{Q}$ s.t. $a - y_0 < x < b - y_0$. Then, $a < y_0 + x < b$; let $y = x + y_0$, and we have $a < y < b$.

Note that y cannot be rational; if $y \in \mathbb{Q}$, $y = x + y_0 \implies y - x = y_0$, and since $x \in \mathbb{Q}$, $y - x \in \mathbb{Q} \implies y_0 \in \mathbb{Q}$, contradicting the original choice of $y_0 \notin \mathbb{Q}$. Thus, $y \in J$. ∎

Theorem 1.6. *$\exists$ a unique positive real number α s.t. $\alpha^2 = 2$.*

Proof. We show both uniqueness, existence:[16]

Uniqueness: if $\alpha^2 = 2$ and $\beta^2 = 2, \alpha \geq 0, \beta \geq 0$, then $0 = \alpha^2 - \beta^2 = (\alpha - \beta)(\alpha + \beta) > 0$, and so $\alpha - \beta = 0 \implies \alpha = \beta$.

- Existence: consider the set $A = \{x \in \mathbb{R} : x \geq 0 \text{ and } x^2 < 2\}$. A is not empty as $1 \in A$. The set of A is bounded above by 2, since if $x \geq 2$, then $x^2 \geq 4 > 2$, so $x \notin A$. So, by AC, $\sup A$ exists; let $\alpha = \sup A$. We will show that $\alpha^2 = 2$, by showing that both $\alpha^2 < 2$ and $\alpha^2 > 2$ are contradictions.

  - $\alpha^2 < 2$
    For any $n \in \mathbb{N}$ we expand

$$\left(\alpha + \frac{1}{n}\right)^2 = \alpha^2 + \frac{2\alpha}{n} + \frac{1}{n^2} \leq \alpha^2 + \frac{2\alpha + 1}{n},$$

    noting that $\frac{1}{n^2} \leq \frac{1}{n}$ for $n \geq 1$.
    Let $y = \frac{2-\alpha^2}{2\alpha+1}$, which is strictly positive. By Proposition 1.10, $\exists n_0 \in \mathbb{N}$ s.t.

$$\frac{1}{n_0} < \frac{2-\alpha^2}{2\alpha+1} \text{ or } \frac{2\alpha+1}{n_0} < 2 - \alpha^2.$$

    Substituting this n_0 into our inequality, we have

$$\left(\alpha + \frac{1}{n_0}\right)^2 \leq \alpha^2 + \frac{2\alpha+1}{n_0} < \alpha^2 + 2 - \alpha^2 = 2.$$

    Since $\alpha + \frac{1}{n_0}$ is positive, $\alpha + \frac{1}{n_0} \in A$. But, since $\alpha = \sup A$, $\alpha + \frac{1}{n_0} \leq \alpha$, which is impossible, so $\alpha^2 < 2$ cannot be true.
  - $\alpha^2 > 2$
    Take $n \in \mathbb{N}$;

$$\left(\alpha - \frac{1}{n}\right)^2 = \alpha^2 - \frac{2\alpha}{n} + \frac{1}{n^2} > \alpha^2 - \frac{2\alpha}{n}.$$

    Now, let $y = \frac{\alpha^2-2}{2\alpha}$; $y > 0$, and by Proposition 1.10, $\exists n_0 \in \mathbb{N}$ s.t.

$$\frac{1}{n_0} < \frac{\alpha^2-2}{2\alpha}, \text{ or } \frac{2\alpha}{n_0} < \alpha^2 - 2.$$

    Substituting this n_0, we have

$$\left(\alpha - \frac{1}{n_0}\right)^2 > \alpha^2 - \frac{2\alpha}{n_0} > \alpha^2 + 2 - \alpha^2 = 2.$$

    So for any $x \in A$, we have $\left(\alpha - \frac{1}{n_0}\right)^2 > 2 > x^2$. $\alpha - \frac{1}{n_0} > 0$, and $x > 0$, since $x \in A$. Then, $\left(\alpha - \frac{1}{n_0}\right)^2 > x^2$ gives that $\alpha - \frac{1}{n_0} > x$.
    So, $\alpha - \frac{1}{n_0} > x$ for all $x \in A$. So $\alpha - \frac{1}{n_0}$ is an upper bound for A, but since $\alpha = \sup A$, $\alpha - \frac{1}{n_0} \geq \alpha$ ie $\alpha \geq \alpha + \frac{1}{n_0}$, which is impossible. So $\alpha^2 > 2$ cannot be true.

  Thus, $\alpha^2 = 2$.

■

Remark 1.10. *A similar argument gives that for any $x \in \mathbb{R}$, $x \geq 0$, $\exists! \alpha \in \mathbb{R}$, $\alpha \geq 0$ such that $\alpha^2 = x$. This x is called the* square root *of x, denoted $\alpha = \sqrt{x}$.*

Remark 1.11. *For any natural number $m \geq 2$ and $x \geq 0$, $\exists! \alpha \in \mathbb{R}, \alpha \geq 0$ s.t. $\alpha^m = x$. The proof is similar, and we call α the m-th root of x.*

Remark 1.12. *Our last proof also gives that $\mathbb{Q}$ cannot satisfy AC. Suppose it does, ie any set in $\mathbb{Q}$ bounded from above has a supremum $\in \mathbb{Q}$. Then, consider $B = \{x \in \mathbb{Q} : x \geq 0 \text{ and } x^2 < 2\}$; set $\alpha = \sup B$. The exact same proof can be used, but we will not be able to find an upper bound in $\mathbb{Q}$.*

[16] Proof sketch: uniqueness is clear. Existence follows from showing that α^2 cannot be either $<$ or $>$ 2. This is done by contradiction, taking some number slightly larger/smaller than α for the $<$ / $>$ resp., then showing that this number cannot be greater/less than α. In the $<$ case, we show that $\alpha + \frac{1}{n_0}$ for a particular n_0 must be in A, and so α cannot be $\sup A$ and thus a contradiction is reached. For the $>$ case, we need slightly different logic (really, more algebra), and get to another contradiction, this time by showing that $\alpha - \frac{1}{n_0}$ is an upper bound for A by our assumption, contradicting.

1.7 Cardinality

Definition 1.8. *Let $f : A \to B$.*

1. *f injective (one-to-one) if $a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$*
2. *f surjective (onto) if for any $b \in B \exists a \in A$ s.t. $f(a) = b$.*
3. *f bijective if both.*

Definition 1.9 (Composition). *If $f : A \to B, g : B \to C$, the* composite map *$h = g \circ f$ is define by $h(x) = g(f(x))$. Note that $h : A \to C$.*

Example 1.10. *Consider functions f, g.*

1. *If f, g injective, so is $h = g \circ f$*
2. *If f, g bijective, then so is h*
3. *If $\exists E \subseteq C$, then $h^{-1}(E) = f^{-1}(g^{-1}(E))$*

Definition 1.10. *The inverse function[17] is defined only for bijective map $f : A \to B$. $y \in B$, $f^{-1}(y) = x$ where $x \in A$ s.t. $f(x) = y$.*

[17] Not the same as the inverse *image* of a set by a function, which is defined for any function.

Example 1.11.
1. *$A = \mathbb{R}, B = (0, \infty), f(x) = e^x$. f is a bijection, and $f^{-1}(y) = \ln y, y \in (0, \infty)$.*
2. *$A = (-\frac{\pi}{2}, \frac{\pi}{2}, B = \mathbb{R})$. $f(x) = \tan x, f^{-1}(y) = \arctan y$*

Definition 1.11 (Equal Cardinalities). *Let A, B be two sets. We say A, B have the same cardinality, denote $A \sim B$ if there exists a function $f : A \to B$.*

Example 1.12. *Let $E = \{2, 4, 6, \dots\}$ (even natural numbers). Define $f : \mathbb{N} \to E$ by $f(n) = 2n$. Thus, f is a bijection, and $\mathbb{N} \sim E$.*[18]

[18]See these independent notes for more.

Theorem 1.7. *The relation $\sim$ is a relation of equivalence.*

1. $A \sim A$
2. *if $A \sim B$, then $B \sim A$*
3. *if $A \sim B$ and $B \sim C$, then $A \sim C$*

Definition 1.12 (Countable). *A set A is* countable *if $\mathbb{N} \sim A$.*

Remark 1.13. *According to this, finite sets are not countable; this is just a convention. Sometimes, we say a set is countable if it is finite or to above definition holds, where we say that a set is* countably infinite *if it is infinite and countable.*

Other times, finite sets are treated separately than countable sets.

Theorem 1.8. *Suppose that $A \subseteq B$.*

1. *If B is finite or countable, then so is A*
2. *If A is infinite and uncountable, then so is B*

Definition 1.13 (Cartesian Product). *If A, B sets, $A \times B = \{(a, b) : a, b \in A, B\}$.*

Proposition 1.12. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$*; there exists a bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.*

Proposition 1.13. *Let A be a set. The following are equivalent statements:*

(a) *A is finite or a countable set;*

(b) *there exists a surjection from $\mathbb{N}$ onto A;*

(c) *there exists a injection from A into $\mathbb{N}$.*

Proof. We proceed by proving that each statement implies the next (and thus are equivalent).

- (a) $\implies$ (b): Suppose A is finite and has $\mathbb{N}$ elements. Then there exists a bijection $h : \{1, 2, \ldots n\} \to A$. We now define a map $f : \mathbb{N} \to A$, by setting

$$f(m) = \begin{cases} h(m) & \text{if } m \leq n \\ h(n) & \text{if } m > n \end{cases}.$$

  f is surjective, and thus (b) holds. If (a) countable, $\exists$ bijection $f : \mathbb{N} \to A$, and any bijection is a surjection, so (b) also holds.

- (b) $\implies$ (c): Let $h : \mathbb{N} \to A$ be a surjection, whose existence is guaranteed by (b). Then, for any $a \in A$, the set

$$h^{-1}(\{a\}) = \{m \in \mathbb{N} : h(m) = n\} \neq \varnothing,$$

  since h is a surjection. Then, by the well-ordering property of $\mathbb{N}$, the set $h^{-1}(\{a\})$ has a least element.
  If n is the least element of $h^{-1}(\{a\})$, we set $f(a) =$. This defines a function

$$f : A \to \mathbb{N},$$

  and we aim to show that f is injective, ie that $f(a_1) = f(a_2) \implies a_1 = a_2$.
  Suppose $f(a_1) = f(a_2) = n$. Then, n is the least element of $h^{-1}(\{a_1\})$ and of $h^{-1}(\{a_2\})$, and in particular, $h(n) = a_1$ and $h(n) = a_2$, and thus $a_1 = a_2$ and so f is indeed injective.

- (c) $\implies$ (a): Let $f : A \to \mathbb{N}$ be an injection, whose existence is guaranteed by (c). Consider the range of f, ie

$$f(A) = \{f(a) : a \in A\}.$$

  Since f an injection, f is a bijection between A and $f(A)$.
  Otoh, $f(A) \subseteq \mathbb{N}$, and so by Theorem 1.8, $f(A)$ is either finite or countable, and there exists a bijection between A and some set that is either fininte or countable. Thus, A must also be finite or countable, and so (a) holds.

■

Theorem 1.9. *Let $A_n, n = 1, 2, \ldots$ be a sequence of sets such that each A_n is either finite or countable. Then, their union*

$$A = \bigcup_{n=1}^{\infty} A_n$$

is also either finite or countable.

Proof. We will use (a) $\iff$ (b) from Proposition 1.13 to prove this.

Since each A_n finite or countable, by (a) $\implies$ (b), there exists a surjection

$$\varphi_n : \mathbb{N} \to A_n.$$

Now, let $h : \mathbb{N} \times \mathbb{N} \to A$, (the union) by setting

$$h(n, m) = \varphi_n(m).$$

We aim to show that h is also surjective.
If $a \in \bigcup_{n=1}^{\infty} A_n$, then $a \in A_n$ for some $n \in \mathbb{N}$. Since $\varphi_n : \mathbb{N} \to A_n$ is a surjection, there exists an $m \in \mathbb{N}$ s.t. $\varphi_n(m) = a$. By definition of h, we have

$$h(n, m) = a,$$

and thus h is a surjection.

By Proposition 1.12, there exists a bijection $f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$, and we can define the composite map

$$h \circ f : \mathbb{N} \to A \, (= \cup_{n=1}^{\infty} A_n),$$

which is a surjection as both h, f are surjections. So, there exists a surhjection from $\mathbb{N} \to A$, and by Proposition 1.13, (b) $\implies$ (a), and thus $A = \bigcup_{n=1}^{\infty} A_n$ is also finite our countable.

■

Remark 1.14. *If $A = \bigcup_{n=1}^{\infty} A_n$, where each A_n is either finite or countable, and at least one A_n is countable, then A is countable.*

Remark 1.15. *If $A_1, \dots, A_n$ are finitely many finite or countable sets then their union $A_1 \cup \dots \cup A_n$ is also finite or countable (essentially just previous proof where we use n instead of ∞ for the upper limit of the union...).*

Theorem 1.10. *The set $\mathbb{Q}$ of rational numbers is countable.*

Proof. We write

$$\mathbb{Q} = A_0 \cup A_1 \cup A_2,$$

where $A_0 = \{0\}$, $A_1 = \{\frac{m}{n} : m, n \in \mathbb{N}\}$, and $A_2 = \{-\frac{m}{n} : m, n \in \mathbb{N}\}$.
Let us show that A_1 is countable; define

$$h : \mathbb{N} \times \mathbb{N} \to A, \, f(m, n) = \frac{m}{n}.$$

h is clearly a surjection; if $f : \mathbb{N} \to \mathbb{N}\times\mathbb{N}$ is a bijection, then by Proposition 1.12, $h\circ f : \mathbb{N} \to A_1$ is a surjection. By Proposition 1.13, A_1 is countable.
We prove that A_2 countable in essentially the same way.
Then, $A_0 \cup A_1 \cup A_2$ is also countable, as it is the union of countable sets, and thus $\mathbb{Q}$ is also countable. ■

Theorem 1.11. *The set $\mathbb{R}$ of real numbers is uncountable.*[19]

Proof. We will argue by contradiction; suppose $\mathbb{R}$ is countable, then show that the nested interval property (Theorem 1.3) of the real line fails.
Let $f : \mathbb{N} \to \mathbb{R}$ be a bijection, setting $f(1) = x_1, f(2) = x_2, \dots, f(n) = x_n, \dots$; we can then

[19]Proof sketch: by contradiction. Assume that a bijection exists, and show that it cannot be a surjection by the previous props/thms. Specifically, carefully construct nested in-

list the elements of $\mathbb{R}$ as $\mathbb{R} = \{x_1, x_2, x_3, \dots, x_n, \dots\}$.
We can now construct a sequence $I_n, n \in \mathbb{N}$ of bounded, closed intervals, such that I_1 does not contain x_1.
If $x_2 \notin I_1$, then $I_2 = I_1$. If $x_2 \in I_1$, then divide I_1 into four equal closed intervals.
Call the leftmost/rightmost of these intervals I_1' and I_1'' respectively. We know that $x_2 \in I_1$, so we must have that either $x_2 \notin I_1'$ or $x_2 \notin I_1''$ If $x_2 \notin I_1'$, then $I_2 = I_1'$. If $x_2 \notin I_1''$, then $I_2 = I_1''$.
Thus, we have constructed I_1, I_2 s.t.

$$I_1 \supseteq I_2 \text{ and } x_1 \notin I_1, x_2 \notin I_2.$$

Consider x_3; if $x_3 \notin I_2$, then $I_3 = I_2$. If $x_3 \in I_2$, we repeat the "dividing" process as before. Since $x_3 \in I_2$, either $x_3 \notin I_2'$ or $x_3 \notin I_2''$. If $x_3 \notin I_2'$, $I_3 = I_2'$. Else, if $x_3 \notin I_2''$, $I_3 = I_2''$.
We have now that

$$I_1 \supseteq I_2 \supseteq I_3 \text{ and } x_1 \notin I_1, x_2 \notin I_2, x_3 \notin I_3,$$

and we can continue this construction to obtain an infinite sequence of bounded, closed intervals I_n s.t.

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq I_{n+1} \supseteq \cdots,$$

and for each n, $x_n \notin I_n$.
Consider the intersection of all these I_n's,

$$\bigcap_{n=1}^{\infty} I_n.$$

For every m, $x_m \notin I_m$, so for every $m \in \mathbb{N}, x_m \notin \bigcap_{n=1}^{\infty} I_n$, and so $\mathbb{R} = \{x_1, x_2, \dots x_m, \dots\}$ has an empty intersection with this intersection, ie

$$\mathbb{R} \cap \left(\bigcap_{n=1}^{\infty} I_n \right) = \varnothing.$$

Otoh, $\bigcap_{n=1}^{\infty} I_n \subseteq \mathbb{R}$, so we must have that $\bigcap_{n=1}^{\infty} I_n = \varnothing$ contradicting the nested interval property of the real line which states that this intersection must not be empty. We thus have a contradiction, and our assumption that $\mathbb{R}$ countable fails. [20] ∎

[20] Note that Theorem 1.3 is built upon the Axiom of Completeness, a "fact" of $\mathbb{R}$ (what makes it "distinct" from $\mathbb{Q}, \mathbb{N}$, etc). Thus, we are really just using AC, with some abstractions sts.

Proposition 1.14. *The set J of all irrational numbers in $\mathbb{R}$ is uncountable.*

Proof. We have that $\mathbb{R} = \mathbb{Q} \cup J$. If J countable, then $\mathbb{R}$ would also be countable as the union of two countable sets (as we showed $\mathbb{Q}$ countable in Theorem 1.10). $\mathbb{R}$ uncountable, so J is also uncountable. ∎

Proposition 1.15. *Any bounded non-empty open interval $(a, b) \in \mathbb{R}$ is uncountable.*

Proof. We will construct a bijection $f : (a, b) \to \mathbb{R}$ so that $(a, b) \sim \mathbb{R}$. Since $\mathbb{R}$ is uncountable, so must (a, b). ∎

2 Appendix

2.1 Tutorials

2.1.1 Tutorial I (Sept 13)

1. We say n odd if $\exists k, n = 2k+1$. Prove that the product of two odds is odd.

   Proof. Take two odd integers, $n_1 = 2k+1$ and $n_2 = 2j+1$. The product $n_1 \times n_2 = (2k+1)(2j+1) = 4kj + 2(k+j) + 1$. We have, then

   $$\underbrace{4kj + 2(k+j)}_{\text{even}} + 1.$$

   Even + odd = odd, thus odd. ■

2. **Proof by Contrapositive:** $P \implies Q \equiv \neg Q \implies \neg P$. Let $q \in \mathbb{Q}$. Prove: If $x \in \mathbb{R} \setminus \mathbb{Q}$, then $q + x$ is irrational.

   Proof (contrapositive). Let $q + x$ be rational. The sum of rationals is rational, and thus $q, x \in \mathbb{Q}$, and thus $x \notin \mathbb{R} \setminus \mathbb{Q}$. ■

3. **Proofs by Induction**

   (a) Prove that $1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.

   . Let P_n be the statement that $1^3 + \cdots = \left(\frac{n(n+1)}{2}\right)^2$. P_0 holds as $1 = \frac{(1)(2)}{2}^2 = 1$. Let P_n hold:

   $$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

   Adding $(n+1)^3$ to both sides:

   $$1^3 + 2^3 + \cdots + n^3 + (n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3$$

   Focusing on the RHS:

   $$\begin{aligned}\left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 &= (n+1)^2\left(\frac{n^2}{4} + (n+1)\right)\\ &= (n+1)^2\left(\frac{n^2+4n+4}{4}\right)\\ &= (n+1)^2\left(\frac{(n+2)^2}{4}\right)\\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2 && \equiv P_{n+1}\end{aligned}$$

Thus, by AI, P_n holds for all $n \in \mathbb{N}$. ■

(b) We have an 8×8 checker board. We remove the top-left and bottom-right squares. Prove that the remaining board cannot be covered by 2×1 dominoes.

Proof. Note that every domino must cover a black square and a white square. However, the board is missing 2 white squares (say). Thus, there are 62 squares (32 black, 30 white), and we would need *exactly* 31 dominos (62/2). Each requires 1 black, 1 white tile, and thus we will run out of white squares before we reach our 31 dominos, and thus we cannot cover the board. ■

(c) Take F_n to represent the nth Fibonacci number. Let $\varphi = \frac{1+\sqrt{5}}{2}$. Show that $F_n > \varphi^{n-2} \forall n \geq 3$.

Proof. Let P_n represent the "truth" of the given statement. $P_3 : F_3 = F_2 + F_1 = 1 + 1 = 2$. $\varphi^1 = \varphi$; clearly $2 > \frac{1+\sqrt{5}}{2}$. Note that we should also prove P_4, P_5 for use in our induction.
$P_4 : (\frac{1+\sqrt{5}}{2})^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} < 3$.
$P_5 : (\frac{1+\sqrt{5}2}{)}^3 \cdots < 5$
Take P_{n-1}, P_n to hold, ie $F_{n-1} > \varphi^{n-3}$ and $F_n > \varphi^{n-2}$.

$$
\begin{aligned}
F_{n+1} = F_n + F_{n-1} &> \varphi^{n-2} + \varphi^{n-3} \\
&= \varphi^{n-3}(\underbrace{\varphi + 1}_{=\varphi^2}) \\
&= \varphi^{n-1},
\end{aligned}
$$

as desired, Noting that $\varphi + 1 = \frac{1+\sqrt{5}}{2} + 1 = \frac{1+\sqrt{5}+2}{2} = \ldots \varphi^2$. ■

(d) $a_1 = 1, a_2 = 8, a_n = a_{n-1} + 2a_{n-2}$. Prove $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$.

Proof. $a_1 = 1 = 3 \cdot 2^0 + 2(-1)^1 = 3 - 2 = 1$ $a_2 = 8 = 3 \cdot 2^1 + 2(-1)^2 = 6 + 2 = 8$ So, P_1, P_2 holds. Assume P_n, P_{n+1} holds. Then, we have $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ and so:

$$
\begin{aligned}
a_{n+1} &= 3 \cdot 2^{n-1} + 2(-1)^n + 2 \cdot \left(3 \cdot 2^{n-2} + 2(-1)^{n-1}\right) \\
&= \cdots = 3 \cdot 2^n + 2(-1)^{n+1}
\end{aligned}
$$

Thus, proven. ■

4. Show $A \setminus (B \setminus A) = A$.

Proof. Let $x \in A \setminus (B \setminus A)$. x must be in A, but not $B \setminus A$. Thus, x is in A, but not in B. Thus, LHS $\subseteq$ RHS.

Let $x \in A$. Thus, $x \notin B \setminus A$, and thus $x \in A \setminus (B \setminus A)$, and so $A \subseteq A \setminus (B \setminus A)$. Thus, LHS = RHS.

■

5. $A_n = \{nk : k \in \mathbb{N}\}, n \geq 2$. Find $\bigcup_{n=2}^{\infty} An \bigcap_{n=2}^{\infty} A_n$.

.

$$\bigcup_{n=2}^{\infty} A_n = \bigcup \{2k, 3k, 4k, \dots\} = \{n : n \geq 2, n \in \mathbb{N}\} = \mathbb{N} \setminus \{1\}$$

$$\bigcap_{n=2}^{\infty} A_n = \varnothing \textit{ consider just } n = 2, n = 3 \text{ cases...}$$

■

2.2 Important

Figure 1: Important!