Analysis

Otto Martinwall

2022

Contents

Chapter 1

Proof Techniques

1.1 Mathematical Induction

Axiom 1.1. (Well-Ordering Property of $\mathbb{N}$). If S is a nonempty subset of $\mathbb{N}$, then there exists an element $m \in S$ such that $m \leq k$ for all $k \in S$.

Theorem 1.2 (Principle of Mathematical Induction)**.** Let $P(n)$ be a statement that is either true or false for each $n \in \mathbb{N}$. Then $P(n)$ is true for all $n \in \mathbb{N}$, provided that

1. $P(1)$ is true, and

2. for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

Proof. This will be a proof by contradiction, using the tautology "$(p \Rightarrow q) \Leftrightarrow [(p \quad \wedge \sim q) \Rightarrow c]$", where "$\sim$" denotes negation and "$c$" is a false statement. Suppose that (a) and (b) hold, but $P(n)$ is false for some $n \in \mathbb{N}$. Let

$$S = \{n \in \mathbb{N} : P(n) \text{ is false}\}.$$

Then S is not empty and the well-ordering property guarantees the existence of an element $m \in S$ that is a least element of S. Since $P(1)$ is true by (1), $1 \notin S$, so that $m > 1$. It follows that $m-1$ is also a natural number, and since m is the least element in S, we must have $m-1 \notin S$.

But since $m-1 \notin S$, it must be that $P(m-1)$ is true. We now apply (2) with $k = m-1$ to conclude that $P(k+1) = P(m)$ is true. this implies that $m \in S$, which contradicts our original choice of m. We conclude that $P(n)$ must be true for all $n \in \mathbb{N}$. $\square$

A more general form of mathematical induction is

Theorem 1.3. Let $m \in \mathbb{N}$ and let $P(n)$ be a statement that is either true or false for each $n \geq m$. Then $P(n)$ is true for all $n \geq m$, provided that

1. $P(m)$ is true, and
2. for each $k \geq m$, if $P(k)$ is true, then $P(k+1)$ is true.

Proof. The proof will use the original principle of induction. For each $r \in \mathbb{N}$, let $Q(r)$ be the statement "$P(r+m-1)$ is true.". Then from (1) we know that $Q(1)$ holds. Now let $j \in \mathbb{N}$ and suppose that $Q(j)$ holds. That is, $P(j+m-1)$ is true. Since $j \in \mathbb{N}$,

$$j + m - 1 = m + (j - 1) \geq m$$

, so by (2), $P(j+m)$ must be true. Thus $Q(j+1)$ holds and the induction step is verified. We conclude that $Q(r)$ holds for all $r \in \mathbb{N}$.

Now if $n \geq m$, let $r = n - m + 1$, so that $r \in \mathbb{N}$. Since $Q(r)$ holds, $P(r+m-1)$ is true. But $P(r+m-1)$ is the same as $P(n)$, so $P(n)$ is true for all $n \geq m$. $\square$

Chapter 2

Set Theory

2.1 Ordered Pairs

Definition 2.1 (Ordered Pair). The **ordered pair** (a, b) is the set whose members are $\{a\}$ and $\{a, b\}$. In symbols we have

$$(a, b) = \{\{a\}, \{a, b\}\}$$

This definition ensures that order matters. To show this, this theorem and its proof should suffice.

Theorem 2.2 (Ordered Pair Theorem). [a]

$$(a, b) = (c, d) \leftrightarrow a = c, b = d$$

[a] this is a made up name by me

Proof. If $a = c$ and $b = d$, then

$$(a, b) = \{\{a\}, \{a, b\} = \{\{c\}, \{c, d\}\} = (c, d)$$

Conversely, suppose that $(a, b) = (c, d)$. Then by our definition we have $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. We wish to conclude that $a = c$ and $b = d$. To this end we consider two cases, depending on whether $a = b$ or $a \neq b$.

If $a = b$, then $\{a\} = \{a, b\}$, so $(a, b) = \{\{a\}\}$. Since $(a, b) = (c, d)$, we then have

$$\{\{a\}\} = \{\{c\}, \{c, d\}\}.$$

The set on the left has only one member, $\{a\}$. Thus the set on the right can have only one member, so $\{c\} = \{c, d\}$, and we can conclude that $c = d$. But then

$\{\{a\}\} = \{\{c\}\}$, so $\{a\} = \{c\}$ and $a = c$. Thus $a = b = c = d$.

On the other hand, if $a \neq b$, then from the preceding argument it follows that $c \neq d$. Since $(a, b) = (c, d)$, we must have

$$\{a\} \in \{\{c\}, \{c, d\}\},$$

which means that $\{a\} = \{c\}$ or $\{a\} = \{c, d\}$. In either case we have $c \in \{a\}$, so $a = c$. Again, since $(a, b) = (c, d)$, we must also have

$$\{a, b\} \in \{\{c\}, \{c, d\}\}.$$

Thus $\{a, b\} = \{c\}$ or $\{a, b\} = \{c, d\}$. But $\{a, b\}$ has two distinct members and $\{c\}$ has only one, so we must have $\{a, b\} = \{c, d\}$. Now $a = c$, $a \neq b$, and $b \in \{c, d\}$, which implies that $b = d$. □

Definition 2.3 (Cartesian Product)**.** If A and B are sets, then the **Cartesian product** (or **cross product**) of A and B, written $A \times B$, is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$. In symbols,

$$A \times B = \{(a, b) : (a \in A) \wedge (b \in B)\}.$$

2.2 Relation

Definition 2.4 (Relation). Let A and B be sets. A **relation between** A **and** B is any subset R of $A \times B$. We say that an element a in A is **related** by R to an element b in B if $(a, b) \in \mathrm{R}$, and we often denote this by writing "$a\mathrm{R}b$". The first set A is referred to as the **domain** of the relation and denoted by dom R. If $B = A$, then we speak of a relation $\mathrm{R} \subseteq A \times A$ being a **relation on A**.

Definition 2.5 (Equivalence Relation). A relation R on a set S is an **equivalence relation** if it has the following properties for all $x, y, z \in S$:

- **Reflexive property:** $x\mathrm{R}x$
- **Symmetric property:** $x\mathrm{R}y \leftrightarrow y\mathrm{R}x$
- **Transitive property:** $(x\mathrm{R}y \wedge y\mathrm{R}z) \rightarrow x\mathrm{R}z$

An example for a **equivalence relation** is the relation "is parallel to" when considering all lines in the plane, if we agree that a line is parallel to itself.

Definition 2.6 (Equivalence Class). Given an equivalence relation R on a set S, the **equivalence class** with respect to R of $x \in S$ is the set

$$E_x = \{y \in S : y\mathrm{R}x\}$$

Example. Let $S = \{a : a \text{ lives in Sweden}\}$, which is the set of all people living in Sweden. Also, let a equivalence relation on this set be

$$R = \{(a, b) \in S \times S : a \text{ was born in the same year as } b\}.$$

Then

$$E_x = \{y \in S : y\mathrm{R}x\}$$

is the set of all people living in Sweden who was born during the same year as some person x who is also living in Sweden. $\diamond$

Theorem 2.7. Two equivalence classes on the same set S with the same equivalence relation R must be disjoint or equal.

Proof. Let R be an equivalence relation on a set S, and let E_x and E_y be two equivalence classes with respect to R of $x \in S$. Suppose that they overlap, then there exists some $w \in E_x \cap E_y$. For all $x' \in E_x$ we have $x'\mathrm{R}x$, and because $w \in E_x$,

$w\text{R}x$, and by symmetry, $x\text{R}w$. Also, $w \in E_y$ so $w\text{R}y$. By using transitivity, $x'\text{R}x$ and $x\text{R}w$ and $w\text{R}y$ implies that $x'\text{R}y$, which means that $x' \in E_y$ and that $E_x \subseteq E_y$.

Conversely, for all $y' \in E_y$ we have $y'\text{R}y$, and because $w \in E_y$, $w\text{R}y$, and by the symmetry property, $y\text{R}w$. Also, $w \in E_x$ so $w\text{R}x$. By using the transitivity property, $y'\text{R}y$ and $y\text{R}w$ and $w\text{R}x$ implies that $y'\text{R}x$ and that $E_y \subseteq E_x$. Since $E_x \subseteq E_y$ and $E_x \supseteq E_y$, it must be that $E_y = E_x$. $\square$

Definition 2.8. A **partition** of a set S is a collection P of nonempty subsets of S such that

- Each $x \in S$ belongs to some subset $A \in \text{P}$.
- For all $A, B \in \text{P}$, if $A \neq B$, then $A \cap B = \emptyset$.

A member of P is called a **piece** of the partition.

Example. Two equivalence classes on the same set S with the same equivalence relation R who are not equal (and therefore disjoint) are two pieces of a partition P on the set S. $\diamond$

2.3 Functions

Definition 2.9 (Function between two sets). Let A and B be sets. A **function** from A to B is a nonempty relation $f \subseteq A \times B$ that satisfies the following two conditions:

1. *Existance*: $\forall a \in A, \exists b \in B \ni (a, b) \in f$
2. *Uniqueness*: $([(a, b) \in f] \wedge [(a, c) \in f]) \Rightarrow (b = c)$

A is called the **domain** of f and is denoted by dom f. B is referred to as the **codomain** of f. We may write $f : A \to B$ to indicate that f has domain A and codomain B. The **range** of f, denoted rng f, is the set of

$$\operatorname{rng} f = \{b \in B : \exists a \in A \ni (a, b) \in f\}$$

The domain of a function is either obtained from context or it is stated explicitly. Unless told otherwise, whenever a function is specified by a formula, possibly like this

$$f(x) = 3x^2 - 5,$$

then the domain of f is assumed to be the largest possible subset of $\mathbb{R}$ for which the formula will result in a real number.

2.3.1 Properties of Functions

Definition 2.10 (Surjection). A function $f : A \to B$ is called **surjective** (or is said to map A **onto** B) if $B = \text{rng } f$. A surjective function is also referred to as a **surjection**.

Definition 2.11 (Injection). A function $f : A \to B$ is called **injective** (or **one-to-one**) if, for all a and a' in A, $f(a) = f(a')$ implies that $a = a'$. An injective function is also referred to as an **injection**.

Definition 2.12 (Bijection). A function $f : A \to B$ is called **bijective** or a **bijection** if it is both surjective and injective.

If a function is bijective, then it is particularly well behaved.

Definition 2.13 (Image and pre-image). Suppose that $f : A \to B$ and that $C \subseteq A$, then the subset $f(C) = \{f(x) : x \in C\}$ of B is called the **image** of C in B.

If we let $D \subseteq B$, then the subset $f^{-1}(D) = \{x \in A : f(x) \in D\}$ of A is called the **pre-image** of D in A, or f inverse of D.

Remark. In the second case where $D \subseteq B$ and $f^{-1}(D) = \{x \in A : f(x) \in D\}$, it must not be that rng f includes all of D, because D must not be a subset of A.

Theorem 2.14. Suppose that $f : A \to B$. Let $C \subseteq A$ and let $D \subseteq B$. Then the following hold:

1. $C \subseteq f^{-1}[f(C)]$
2. $f[f^{-1}(D)] \subseteq D$

Proof. We begin with case 1.

Suppose that $f : A \to B$, and that $C_1 \subseteq A$ and $C_2 \subseteq A$, and that $C_1 \cap C_2 = \emptyset$ and that $f(C_1) = f(C_2)$. Then $f^{-1}[f(C_1] = C_1 \cup C_2$, which must contain more members than C_1. Therefore, $C \subseteq f^{-1}[f(C)]$ as was to be prooven.[a]

For case 2, suppose that $f : A \to B$ and $D \subseteq B$. Let $D_1 = \{d \in D : \exists a \in A \ni f(a) = d\}$, and let $D_2 = \{d \in D : \forall a \in A, f(a) \neq d\}$. This implies that $D = D_1 \cup D_2$ and $D_1 \cap D_2 = \emptyset$. The definition of D_1 also means that $f[f^{-1}(D_1)] = D_1$. Also, because of the definition of D_2, $f^{-1}(D) = f^{-1}(D_1 \cup D_2) = f^{-1}(D_1)$ since

$f^{-1}(D_2) = \emptyset$.

Since $f[f^{-1}(D_1)] = D_1 = f[f^{-1}(D)]$ and $D_1 \cap D_2 = \emptyset$, it must be that $f[f^{-1}(D)] \subseteq D$ because D has equal or more members than D_1. □

[a] if f were injective (which it isn't in the proof) then $C = f^{-1}[f(C)]$, which is shown in the proof of 2.15.

Theorem 2.15. Suppose that $f : A \to B$. Let $C \subseteq A$ and $D \subseteq B$. Then the following hold:

1. If f is injective, then $f^{-1}[f(C)] = C$.
2. If f is surjective, then $f[f^{-1}(D)] = D$.

Proof. We begin with case 1.

Suppose that $f : A \to B$, and that $C_1 \subseteq A$ and $C_2 \subseteq A$, and that $f(C_1) = f(C_2)$. Then $f^{-1}[f(C_1)] = C_1 \cup C_2$. Since f is injective, and $f(C_1) = f(C_2)$, it must be that $C_1 = C_2$, and therefore $f^{-1}[f(C_1)] = C_1$.

For case 2, suppose that $f : A \to B$ and $D \subseteq B$. Let $D_1 = \{d \in D : \exists a \in A \ni f(a) = d\}$, and let $D_2 = \{d \in D : \forall a \in A, f(a) \neq d\}$. This implies that $D = D_1 \cup D_2$ and $D_1 \cap D_2 = \emptyset$. The definition of D_1 also means that $f[f^{-1}(D_1)] = D_1$. Since f is surjective, $D_2 = \emptyset$, which means that $D = D_1$ since $D_1 \cup D_2 = D_1$, and therefore $f[f^{-1}(D_1)] = D_1$ implies that $f[f^{-1}(D)] = D$. □

2.3.2 Composition Function

Definition 2.16 (Composition Function). Suppose that $f : A \to B$ and $g : B \to C$, then $\forall a \in A, f(a) \in B$, and since $f(a)$ is an object in B, $g(f(a)) \in C$. This is called the **composition** of f and g.

$$g \circ f = g(f(a)), \quad \forall a \in A$$

In terms of ordered pairs,

$$g \circ f = \{(a, c) \in A \times C : [\exists b \in B \ni (a, b) \in f] \wedge [(b, c) \in g]\}$$

Theorem 2.17. Let $f : A \to B$ and $g : B \to C$. Then

1. f and g are surjective $\Rightarrow g \circ f$ is surjective.
2. f and g are injective $\Rightarrow g \circ f$ is injective.
3. f and g are bijective $\Rightarrow g \circ f$ is bijective.

Proof. Case 1:

Since g is surjective, rng $g = C$, which means that $\forall c \in C, \exists b \in B \ni g(b) = c$. Now since f is surjective, $\exists a \in A \ni f(a) = b$. But then $(g \circ f)(a) = g(f(a)) = g(b) = c$, so $g \circ f$ is surjective.

Case 2:

Suppose that $b' = f(a') \in B$ and $b = f(a) \in B$, and that $g(b') = g(b) \in C$. This implies that $b' = b$ since g is injective, which means that $f(a') = f(a)$, but because f too is injective, this implies that $a' = a$. This results in that $g(f(a')) = g(f(a)) \Rightarrow a' = a$, so by definition, $g \circ f$ is injective.

Case 3:

By the result of case 1 and 2, if f and g are bijective, then $g \circ f$ is bijective. □

2.3.3 Inverse function

To extend the idea of pre-image from 2.13, we can define a **inverse function**.

Definition 2.18 (Inverse Function). Suppose that $f : A \to B$. The **inverse function** of f is the function f^{-1} given by

$$f^{-1} = \{(y, x) \in B \times A : (x, y) \in f\}$$

Remark. If $f : A \to B$ is bijective, then $f^{-1} : B \to A$ is bijective.

Definition 2.19 (Identity Function). A function defined on a set A that maps each element in A onto itself is called the **identity function** on A, and is denoted by i_a.

Remark. If $f : A \to B$ and f is bijective, then

- $f^{-1} \circ f = i_A$,
- $f \circ f^{-1} = i_B$.

Theorem 2.20. Let $f : A \to B$ and $g : B \to C$ be bijective. Then the composition $g \circ f : A \to C$ is bijective and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. By theorem 2.17 we know that $g \circ f$ is bijective, so there exists an inverse $(g \circ f)^{-1}$. We are asked to verify the equality of the two functions $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$, as sets of ordered pairs. To this end, suppose $(c, a) \in (g \circ f)^{-1}$. By the definition of an inverse function, this means $(a, c) \in g \circ f$. The definition of composition implies that

$$\exists b \in B \ni [(a, b) \in f] \wedge [(b, c) \in g].$$

Since f and g are bijective, this means that $(b, a) \in f^{-1}$ and $(c, b) \in g^{-1}$. That is, $f^{-1}(b) = a$ and $g^{-1}(c) = b$. But then,

$$(f^{-1} \circ g^{-1})(c) = f^{-1}(g^{-1}(c)) = f^{-1}(b) = a \tag{2.1}$$

so that $(c, a) \in (f^{-1} \circ g^{-1})$ and $(g \circ f)^{-1} \subseteq (f^{-1} \circ g^{-1})$.

To the other end, suppose that $(c, a) \in (f^{-1} \circ g^{-1})$. The definition of composition implies that

$$\exists b \in B \ni [(c, b) \in g^{-1}] \wedge [(b, a) \in f^{-1}].$$

This implies that $(b, c) \in g$ and that $(a, b) \in f$ and therefore $(a, c) \in g \circ f$. Since both f and g are bijective, there must exist an inverse $(g \circ f)^{-1}$ such that $(c, a) \in (g \circ f)^{-1}$.

Now, since $(c, a) \in (f^{-1} \circ g^{-1})$ implies that $(c, a) \in (g \circ f)^{-1}$, and $(c, a) \in (g \circ f)^{-1}$ implies that $(c, a) \in (f^{-1} \circ g^{-1})$, it must be that $(g \circ f)^{-1} = (f^{-1} \circ g^{-1})$. $\square$

2.4 Cardinality

Definition 2.21 (Set Equivalence). Two sets S and T are called **set equivalent**, and we write $S \sim T$, if there exists a bijective function from S onto T.

This definition ensures that if two sets are set equivalent, they contain the same number of elements, since a bijective function between them will set up a one-to-one correspondence between the elements of each set.

Definition 2.22 (Finite or Infinite Set). A set S is said to be **finite** if $S = \emptyset$ or if there exists $n \in \mathbb{N}$ and a bijection $f : \{1, 2, \ldots, n\} \to S$.[a] If a set is not finite, it is said to be **infinite**.

[a] Moving forward, we will make use of the set $I_n = \{1, 2, \ldots, n\}$.

Definition 2.23. The **cardinal number** of the set $I_n = \{1, 2, \ldots, n\}$ is n, and if $S \sim I_n$, we say that S **has n elements**. The cardinal number of $\emptyset$ is taken to be 0. If a cardinal number is not finite, it is called **transfinite**.

Definition 2.24. A set S is said to be **denumerable** if there exists a bijection $f : \mathbb{N} \to S$. If a set is finite or denumerable, it is called **countable**. If a set is not countable, it is **uncountable**. The cardinal number of a denumerable set is denoted by $\aleph_0$.

Remark. Against our intuition from finite sets, if E is the set of all even natural numbers, then $\mathbb{N} \sim E$, because if $f(n) = 2n$, then $f : \mathbb{N} \to E$ is bijective. Therefore, both $\mathbb{N}$ and E has the cardinal number $\aleph_0$ even though $E \subset \mathbb{N}$.

Example. $\mathbb{Z}$, the set of all integers, is denumerable since $f : \mathbb{N} \to \mathbb{Z}$ is bijective if

$$f(n) = \begin{cases} 0 \text{ if } n = 1 \\ \frac{n}{2} \text{ if } n \text{ is even} \\ \lceil -\frac{n}{2} \rceil \text{ if } n \text{ is odd} \end{cases}$$

because this leads to that

$$\begin{aligned} &f(1) \to 0 \\ &f(2) \to 1 \\ &f(3) \to (-1) \\ &f(4) \to 2 \\ &f(5) \to (-2) \\ &\vdots \end{aligned}$$

So for any $b \in \mathbb{Z}$, there exists a $a \in \mathbb{N}$ such that $f(a) = b$, which implies that f is surjective, and there is also a one to one correspondence between the two sets so f is injective, and therefore bijective. $\diamond$

Notation. For any nonempty finite set S, there exists a bijection $f : I_n \to S$ for some $n \in \mathbb{N}$. Therefore, we use this function to count the members as $f(1), f(2), f(3), \ldots, f(n)$. Letting $f(k) = s_k$ we can write $S = \{s_1, s_2, \ldots, s_n\}$. We can also do this for any denumerable set T, since because it is denumerable, there exists a bijection $g : \mathbb{N} \to T$, so we can use $g(k) = t_k$ to write $T = \{t_1, t_2, t_3, \ldots\}$.

Lemma 2.25. Every subset of a finite set is finite.

Proof. — NOT DONE $\square$

Theorem 2.26. Let S be a countable set and let $T \subseteq S$. Then T is countable.

Proof. If T is finite, then we are done. Thus we may assume that T is infinite. This implies that S is infinite[a], so S is denumerable (since it is countable and infinite). Therefore, there exists a bijection $f : \mathbb{N} \to S$ and we can write S as a list of distinct members

$$S = \{s_1, s_2, s_3, \ldots\}$$

where $f(n) = s_n$. Now let

$$A = \{n \in \mathbb{N} : s_n \in T\}.$$

Since A is a nonempty subset of $\mathbb{N}$, the *Well-Ordering Property of* $\mathbb{N}$ implies that A has a least member, say a_1. Similarly, the set $A \backslash \{a_1\}$ has a least member, say a_2. In general, having chosen $a_1, \ldots, a_k$, let a_{k+1} be the least member in $A \backslash \{a_1, \ldots, a_k\}$. Essentially, if we select from our listing of S those terms that are in T and keep them in the same order, then a_n is the subscript of the nth term in this new list.

Now define a function $g : \mathbb{N} \to \mathbb{N}$ by $g(n) = a_n$. Since T is infinite, g is defined for every $n \in \mathbb{N}$. Since $a_{n+1} \notin \{a_1, \ldots, a_n\}$, g must be injective[b]. Thus tje composition $f \circ g$ is also injective. Since each element of T is somewhere in the listing of S, $g(\mathbb{N})$ includes all the subscripts of terms in T. Thus $f \circ g$ is a bijection from $\mathbb{N}$ onto T and T is denumerable. $\square$

[a]This implication is true by lemma 2.25

[b]I suppose that this is a small proof by induction that g is injective? This proof is not mine and is taken from *Analysis with an Introduction to Proof.*

Theorem 2.27. Let S be a nonempty set. The following three conditions are equivalent.

1. S is countable.
2. There exists an injection $f : S \to \mathbb{N}$.
3. There exists a surjection $g : \mathbb{N} \to S$.

Proof. Suppose that S is countable. Then there exists some bijection $h : J \to S$ where $J = I_n$ for some $n \in \mathbb{N}$ if S is finite, or $J = \mathbb{N}$ if S is infinite. In either case, $h^{-1} : S \to \mathbb{N}$ is at least injective. Thus (1) implies (2).

Now suppose that there exists an injection $f : S \to \mathbb{N}$. Then f is a bijection from S to $f(S)$, so f^{-1} is a bijection from $f(S)$ to S. Let $g : \mathbb{N} \to S$ be defined by

$$g(n) = \begin{cases} f^{-1}(n), & \text{if } n \in f(S) \\ p, & \text{if } n \notin f(S) \end{cases}$$

where $p \in S$. Then $g[f(S)] = f^{-1}[f(S)] = S$ and $g[\mathbb{N} \backslash f(S)] = \{p\}$, so that g is a surjection from $\mathbb{N}$ onto S. Thus, (2) implies (3).

Finally, suppose that there exists a surjection $g : \mathbb{N} \to S$. Define $h : S \to \mathbb{N}$ by

$$h(s) \text{ is the smallest } n \in \mathbb{N} \text{ such that } g(n) = s.$$

Then h is an injection from S to $\mathbb{N}$, and hence a bijection from S onto the subset $h(S)$ of $\mathbb{N}$. Since $\mathbb{N}$ is countable, theorem 2.26 implies that $h(S)$ is countable. Since S and $h(S)$ are set equivalent, because there exists a bijection between the two sets, S is also countable. □

Theorem 2.28. The set $\mathbb{R}$ of real numbers is uncountable.

Proof. Since any subset of a countable set is countable (theorem 2.26), it suffices to show that the interval $J = (0, 1)$ is uncountable. If J were countable, we could list its members and have

$$J = \{x_1, x_2, x_3, \ldots\} = \{x_n : n \in \mathbb{N}\}.$$

Each element of J has an infinite decimal expansion, so we can write

$$\begin{aligned} x_1 &= 0.a_{11}a_{12}a_{13}\dots, \\ x_2 &= 0.a_{21}a_{22}a_{23}\dots, \\ x_3 &= 0.a_{31}a_{32}a_{33}\dots, \\ &\vdots \end{aligned}$$

where each $a_{ij} \in \{0, 1, \dots, 9\}$. We now construct a real number $y = b_1b_2b_3\dots$ by defining

$$b_n = \begin{cases} 2, & \text{if } a_{nn} \neq 2 \\ 3, & \text{if } a_{nn} = 2 \end{cases}$$

Since each digit in the decimal expansion of y is either 2 or 3, $y \in J$. But y is not one of the numbers x_n, since it differs from x_n in the nth decimal place. This contradicts our assumption that J is countable, so J must be uncountable. $\square$

Definition 2.29 (Cardinal Number of a Set)**.** We denote the cardinal number of a set S by $|S|$, so that we have $|S| = |T|$ iff S and T are set equivalent, which implies that there exists a bijection $f : S \to T$. We define $|S| \leq |T|$ to mean that there exists an injection $f : S \to T$, and $|S| < |T|$ means that $|S| \leq |T|$ and $|S| \neq |T|$.

Theorem 2.30. If $S \subseteq T$, then $|S| \leq |T|$.

Proof. (1) If $S \subseteq T$, then for each $s \in S$ there exists one $t \in T$ with the relation $s = t$. If we let a function $f : S \to T$ be defined by $f(s) = s$, it is injective, and since there exists an injection that maps S into T, we say that $|S| \leq |T|$ by definition. $\square$

Remark. $|\mathbb{R}|$ is usually written as c, for continuum. Since $\mathbb{N} \subseteq \mathbb{R}$, we have $\aleph_0 \leq c$ by the theorem above. In fact, since $\mathbb{N}$ is countable and $\mathbb{R}$ is uncountable, we have $\aleph_0 < c$. Therefore, there exists more than one transfinite cardinal number.

Definition 2.31 (Power Set)**.** For any set S, $\mathscr{P}(S)$ is the collection of all subsets of S. This collection is called the **power set** of S.

Theorem 2.32. For any set S, we have $|S| < |\mathscr{P}(S)|$

Proof. The function $g : S \to \mathscr{P}(S)$ given by $g(s) = \{s\}$ is injective, so we have $|S| \leq |\mathscr{P}(S)|$. To prove that $|S| \neq |\mathscr{P}(S)|$, we show that no function from S to $\mathscr{P}(S)$ can be surjective[a]. Suppose that $f : S \to \mathscr{P}(S)$. Then for each $x \in S$, $f(x) \subseteq S$. For some x in S it may be that $x \in f(x)$, or $x \notin f(x)$. Let

$$T = \{x \in S : x \notin f(x)\}.$$

Then $T \subseteq S$, so $T \in \mathscr{P}(S)$. If f were surjective, then $T = f(y)$ for some $y \in S$. Now either $y \in T$ or $y \notin T$. If $y \in T$, then by the definiton of T, $y \notin T$. If $y \notin T$, then by the definition of T, $y \in T$. Therefore, $y \in T$ iff $y \notin T$, which is a contradiction, so it must be that $|S| < |\mathscr{P}(S)|$. $\square$

[a]This ensures that no function can be bijective from S to $\mathscr{P}(S)$, so that $|S| \neq |P(S)|$

Chapter 3

The Real Numbers $\mathbb{R}$

This will be an axiomatic approach, not constructive.

Axiom 3.1. ($\mathbb{R}$ is an Ordered Field).

We assume the existence of a set $\mathbb{R}$, called the set of real numbers, and two operations "+" and "$\cdot$", called addition and multiplication, such that the following properties apply:

1. For all $x, y \in \mathbb{R}$, $x + y \in \mathbb{R}$ and if $x = w$ and $y = z$, then $x + y = w + z$.
2. For all $x, y \in \mathbb{R}$, $x + y = y + x$.
3. For all $x, y, z \in \mathbb{R}$, $x + (y + z) = (x + y) + z$.
4. There is a unique real number 0 such that $x + 0 = x$, for all $x \in \mathbb{R}$.
5. For each $x \in \mathbb{R}$ there is a unique real number $-x$ such that $x + (-x) = 0$.
6. For all $x, y \in \mathbb{R}$, $x \cdot y \in \mathbb{R}$ and if $x = w$ and $y = z$, then $x \cdot y = w \cdot z$.
7. For all $x, y \in \mathbb{R}$, $x \cdot y = y \cdot x$.
8. For all $x, y \in \mathbb{R}$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
9. There is a unique real number 1 such that $1 \neq 0$ and $x \cdot 1 = x$ for all $x \in \mathbb{R}$.
10. For each $x \in \mathbb{R}$ with $x \neq 0$, there is a unique real number $1/x$ such that $x(1/x) = 1$. We also write x^{-1} or $\frac{1}{x}$ in place of $1/x$.
11. For all $x, y, z \in \mathbb{R}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.[a]

Also, $\mathbb{R}$ satisfies four order axioms, which identify the properties of the relation "$<$". We may write $y > x$ instead of $x < y$, and $x \leq y$ is equivalent to "$x < y$ or $x = y$".

1. For all $x, y \in \mathbb{R}$, exactly one of the relations $x = y$, $x > y$, or $x < y$ holds.[b]
2. For all $x, y, z \in \mathbb{R}$, if $x < y$ and $y < z$, then $x < z$.
3. For all $x, y, z \in \mathbb{R}$, if $x < y$ then $x + z < y + z$.
4. For all $x, y, z \in \mathbb{R}$, if $x < y$ and $z > 0$, then $xz > yz$.

[a]These first eleven axioms are called field axioms because they describe a system known as a **field** in abstract algebra.

[b]This is the **trichotomy law**.

Note. The set of complex numbers, $\mathbb{C}$, is not an ordered field and does not satisfy the order axioms.

These fifteen axioms are not unique to $\mathbb{R}$, but also hold for $\mathbb{Q}$, as an example. What makes $\mathbb{R}$ unique is its completeness axiom. To define this axiom, we must first develop some tools for it.

Definition 3.2 (Upper and Lower Bounds). Let $S \subseteq \mathbb{R}$. If there exists a real number m such that $m \geq s$ for all $s \in S$, then m is called an **upper bound** of S, and we say that S is bounded above. If $m \leq s$ for all $s \in S$, then m is a **lower bound** of S and S is bounded below.

If an upper bound m of S is a member of S, then m is called the **maximum** of S, denoted by $\max S$.

Similarly, if a lower bound of S is a member of S, then it is called the **minimum** of S, denoted by $\min S$.

Chapter 4

Exercises and My Solutions

4.1 Analysis with an Introduction to Proof - Steven R. Lay

4.1.1 Sets and Functions

4.1.1.1 Exercises 3

(21) *Suppose that $f : A \to B$ and let C be a subset of A.*

1. *Prove or give a counterexample: $f(A\backslash C) \subseteq f(A)\backslash f(C)$.*

2. *Prove or give a counterexample: $f(A)\backslash f(C) \subseteq f(A\backslash C)$.*

3. *What condition on f will ensure that $f(A\backslash C) = f(A)\backslash f(C)$? Prove your answer.*

4. *What condition of f will ensure that $f(A\backslash C) = B\backslash f(C)$? Prove your answer.*

Proof. (**1**) Suppose that $f(A\backslash C) \subseteq f(A)\backslash f(C)$.

Let $x \in A\backslash C$, $x' \in C$ and $f(x) = f(x')$. Then, $f(x) \in f(A\backslash C)$, and therefore $f(x') \in f(A\backslash C)$. But since $f(x') \in f(C)$ and therefore $f(x) \in f(C)$, neither $f(x)$ or $f(x')$ is in $f(A)\backslash f(C)$. This contradicts our original statement because there exists a member in $f(A\backslash C)$ which is not in $f(A)\backslash f(C)$, so $f(A\backslash C) \nsubseteq f(A)\backslash f(C)$. □

Proof. (**2**) For any $y \in f(A)\backslash f(C)$, there exists an $x \in A$ such that $f(x) = y$. If $x \in C$, then $f(x) \in f(C)$ which means that $f(x) \neq y$, so by contradiction it must be that $x \notin C$. This implies that $x \in A\backslash C$, and therefore that $f(x) \in f(A\backslash C)$ and $y \in f(A\backslash C)$. Since $y \in f(A)\backslash f(C)$ implies that $y \in f(A\backslash C)$, the statement $f(A)\backslash f(C) \subseteq f(A\backslash C)$ must be true. □

Proof. (**3**) Proof 2 have already shown that $f(A)\backslash f(C) \subseteq f(A\backslash C)$, so to prove that $f(A)\backslash f(C) = f(A\backslash C)$ I must only prove the reverse of the first statement.

Let f be injective[a]. For any $y \in f(A\backslash C)$, there exists one and only one $x \in A\backslash C$ such that $f(x) = y$. Since $x \in A\backslash C$, $x \in A$ and $f(x) \in f(A)$. Also, since $x \in A\backslash C$, $x \notin C$ and $f(x) \notin f(C)$. This implies that $f(x) \in f(A)\backslash f(C)$ and thus $y \in f(A)\backslash f(C)$. Since $y \in f(A\backslash C)$ implies $y \in f(A)\backslash f(C)$, and $y \in f(A)\backslash f(C)$ implies $y \in f(A\backslash C)$ from proof 2, it must be that $f(A\backslash C) = f(A)\backslash f(C)$. □

[a]this is the necessary condition such that $f(A\backslash C) = f(A)\backslash f(C)$.

Proof. (**4**) Proof 3 in combination with that f is surjective[a] means that $f(A\backslash C) = f(A)\backslash f(C) = B\backslash f(C)$ since $B = \text{rng } f = f(A)$. □

[a]Proof 3 needed the condition that f was injective, and since proof 4 needs f to be surjective and is based on proof 3, f is now bijective.

(32) *Suppose that $f : A \to B$ is any function. Then a function $g : B \to A$ is called a*

- ***left inverse*** *for f if $g(f(x)) = x$ for all $x \in A$,*
- ***right inverse*** *for f if $f(g(y)) = y$ for all $y \in B$.*

1. *Prove that f has a left inverse iff f is injective.*
2. *Prove that f has a right inverse iff f is surjective.*

Proof. (**1**) Suppose that f is injective. Let $g = \{(b, a) \in B \times A : (a, b) \in f\} \cup \{(b, a) \in B \times A : b \notin f(A)\}^a$. By definition, each $a \in A$ corresponds to one and only one $b \in B$ such that $f(a) = b$, and because of the definition of g, for each $b \in B$ such that $f(a) = b$, $g(b) = a$, which implies that $g(f(a)) = a$ for all $a \in A$.

Conversely, suppose that $f(x) \in B$ and $f(x') \in B$, and that $f(x) = f(x')$. If $g(f(a)) = a$ for all $a \in A$, $g(f(x)) = g(f(x'))$ implies that $x = x'$. Therefore, f is injective. □

[a] I added the part $\cup\{(b, a) \in B \times A : b \notin f(A)\}$ to g to show that f must not be surjective.

Proof. (**2**) Suppose that f has a right inverse and therefore $f(g(y)) = y$ for all $y \in B$. This implies that f is surjective, since for all $y \in B$ there exists some $x \in A$, which may be $g(y)$, such that $f(x) = y$. □

(33) *Let S be a nonempty set and let F be the set of all functions that map S into S. Suppose that for every f and g in F we have*

$$(f \circ g)(x) = (g \circ f)(x), \forall x \in S$$

Prove that S has only one element.

Proof. If S contains more than one element, then there exists some functions f and g in F that are neither surjective nor injective. Suppose that $x, x' \in S$ and that $x \neq x'$, and that $f(x) = x'$ and $f(x') = x'$, and that $g(x) = x$ and $g(x') = x$. Then $f(g(x)) = f(x) = x'$, and $g(f(x)) = g(x') = x$, which contradicts the statement that $(f \circ g)(x) = (g \circ f)(x), \forall x \in S$, so S must contain less than two elements. Since S is nonempty, it must therefore contain one element. $\square$

4.1.2 The Real Numbers

4.1.2.1 Exercises 1

(3) *Prove that* $1^2 + 2^2 + \ldots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ *for all* $n \in \mathbb{N}$.

First, we must know if this is true for $n = 1$.

$$1^2 = \frac{1}{6}(1)(2)(3)$$

$$1 = 1$$

Now, suppose that the statement is true for some $k \in \mathbb{N}$,

$$1^2 + 2^2 + \ldots + k^2 = \frac{1}{6}k(k+1)(2k+1).$$

$$\begin{aligned}
1^2 + 2^2 + \ldots + k^2 + (k+1)^2 = \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 &= \\
= \frac{1}{6}k(k+1)(2k+1) + (k^2 + 2k + 1) &= \\
= \frac{1}{6}(2k^3 + k^2 + 2k^2 + k) + (k^2 + 2k + 1) &= \\
= \frac{1}{6}(2k^3 + k^2 + 2k^2 + k) + \frac{1}{6}(6k^2 + 12k + 6) &= \\
= \frac{1}{6}(2k^3 + 9k^2 + 13k + 6) &= \\
= \frac{1}{6}(k+1)(2k^2 + 7k + 6) &= \\
= \frac{1}{6}(k+1)(k+2)(2k+3) &= \\
= \frac{1}{6}[k+1]([k+1]+1)(2[k+1]+1)&
\end{aligned}$$

Since the statement is true for $n = 1$, and if it is true for some $k \in \mathbb{N}$ then it it also true for $(k+1) \in \mathbb{N}$, it must be that the statement is true for all $n \in \mathbb{N}$ by induction.

(16) *If a, b and $c \in \mathbb{N}$ such that $a-b$ is a multiple of c, prove that $a^n - b^n$ is a multiple of c for all $n \in \mathbb{N}$.*

$$a^n - b^n = (a-b)(a+b)(a^2+b^2)(a^4+b^4)(a^8+b^8)\dots(a^{n/2}+b^{n/2}) =$$
$$= \prod_{k=0}^{\frac{n}{2}-1}(a-b)(a^{2^k}+b^{2^k})$$

for all $n = 2^k$ such that $k \in \mathbb{N}$.

—Not Finished—

I can only prove it for $n = 2^k$ such that $k \in \mathbb{N}$, not for all $n \in \mathbb{N}$:(