UW W17 PMATH333 - Definitions and Theorems

Johnson Ng

April 12, 2017

Preface

PMATH333 is offered as a course that attempts to bridge the gap for students who have taken the regular math courses instead of the advanced math courses, in particular for MATH147, MATH148 and MATH247 in UW. This set of notes is taken from the W2017 term.

Contents

List of Definitions

List of Theorems

Chapter 1

The Real Number System

1.1 Ordered Field Axioms

Please review Appendix A. We shall use all of the set notations that are introduced in Appendix A. We will also introduce one more notation.

Definition 1.1.1 (Removal)
Let A and B be sets. The set A remove B, denoted as $A \setminus B$, is the set

$$A \setminus B = \{x | x \in A \wedge x \notin B\}$$

Definition 1.1.2 (Disjoint)
Let A and B be sets. We say that A and B are disjoint when $A \cap B = \emptyset$

Theorem 1.1.1 (Properties of Sets)
Let $A, B, C \subseteq X$. Then

1. *(Idempotence)* $A \cup A = A, A \cap A = A$
2. *(Identity)* $A \cup \emptyset = A, A \cap \emptyset = \emptyset, A \cup X = X, A \cap X = A$
3. *(Associativity)* $(A \cup B) \cup C = A \cup (B \cup C)$ *and* $(A \cap B) \cap C = A \cap (B \cap C)$
4. *(Commutativity)* $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$
5. *(Distributivity)* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *and* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. *(De Morgan's Laws)* $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ *and* $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

Definition 1.1.3 (Intervals)
For $a, b \in \mathbb{R}$ with $a \leq b$ we write

$$\begin{gathered}(a,b)=\{x\in\mathbb{R}|a<x<b\},\quad [a,b]=\{x\in\mathbb{R}|a\leq x\leq b\},\\ (a,b]=\{x\in\mathbb{R}|a<x\leq b\},\quad [a,b)=\{x\in\mathbb{R}|a\leq x<b\},\\ (a,\infty)=\{x\in\mathbb{R}|a<x\},\qquad [a,\infty)=\{x\in\mathbb{R}|a\leq x\},\\ (-\infty,b)=\{x\in\mathbb{R}|x\leq b\},\qquad (-\infty,b]=\{x\in\mathbb{R}|x<b\},\\ (-\infty,\infty)=\mathbb{R}\end{gathered}$$

An interval in $\mathbb{R}$ is any set of one of the above forms. In the case that $a = b$, we have $(a, b) = [a, b) = (a, b] = \emptyset$ and $[a, b] = \{a\}$, and these intervals are called ***denegerate*** *intervals. The intervals $\emptyset, (a, b), (a, \infty), (-\infty, b)$ and (∞, ∞) are called open intervals. The intervals $\emptyset, [a, b], [a, \infty), (-\infty, b]$ and $(-\infty, \infty)$ are called closed intervals.*

Remark
Note on how the intervals $\emptyset$ and $(-\infty, \infty)$ are both open and closed intervals.

Definition 1.1.4 (Ring)
A ring is a set F with two distinct elements $0, 1 \in F$ and two binary operations $+$ and $\cdot$ such that

1. *(Additive Associativity) For all $x, y, z \in F$ we have $(x + y) = z = x + (y + z)$,*
2. *(Additive Commutativity) For all $x, y \in F$ we have $x + y = y + x$,*
3. *(Additive Identity) For all $x \in F$ we have $0 + x = x$.*
4. *(Additive Inverse) $\forall x \in F\ \exists! y \in F\ x + y = 0$*
5. *(Multiplicative Associativity) $\forall x, y, z \in F$ we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,*
6. *(Multiplicative Identity) $\forall x \in F$ we have $1 \cdot x = x = x \cdot 1$,*
7. *(Distributivity) $\forall x, y, z \in F$ we have $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$*

Definition 1.1.5 (Commutative Ring)
A ring F is a commutative ring if it has the following (additional) property:
(Multiplicative Commutativity) $\forall x, y \in F$ we have $x \cdot y = y \cdot x$.

Definition 1.1.6 (Field)
A commutative ring F is a field if it has the following (additional) property:
(Multiplicative Inverse) $\forall x \neq 0 \in F\ \exists! y \in F$ such that $x \cdot y = 1$.

Remark
For the sake of simplicity, we will write $x \cdot y = xy$ for any x and y.

Theorem 1.1.2 ($\mathbb{Q}$ and $\mathbb{R}$ as Fields)
$\mathbb{Q}$ and $\mathbb{R}$ are fields.

Remark
Note that $\mathbb{Z}$ and $\mathbb{N}$ are not fields since their elements do have have a multiplicative inverse. They are, however, commutative rings.

Remark (Some shorthand notations)
Let F be a friend and let $a, b \in F$. We denote the unique additive inverse of a by -a and we write a - b = a + (-b). When $a \neq -$, we denote the unique multiplicatie inverse of a by a^{-1} and we write $b \div a = \frac{b}{a} = ba^{-1}$.

Theorem 1.1.3 (Cancellations & Identities)
Lt F be a field. Then $\forall x, yz \in F$ we have

1. *(Additive Cancellation)* $x + y = x + z \implies x = z$
2. *(Uniqueness of Additive Identity)* $x + y = x \implies y = 0$
3. *(Multiplicative Cancellation)* $xy = xz \implies (x = 0 \vee y = z)$
4. *(Uniqueness of Multiplicative Identity)* $xy = x \implies y = 1$
5. *(No Zero Divisors)* $xy = 0 \implies (x = 0 \vee y = 0)$

Theorem 1.1.4 (Properties of Fields)
Let F be a field. Then for all $x, y \in F$ we have

$$\begin{array}{cccc} 0 \cdot x = 0 & \text{-(-}x\text{)} = x & \text{-(}x + y\text{)} = \text{-}x \text{ - } y & \text{(-1)}x = x \\ \text{(-}x\text{)}y = \text{-(}xy\text{)} & \text{(-}x\text{)(-}y\text{)} = xy & (a^{-1})^{-1} = a & (ab)^{-1} = a^{-1}b^{-1} \\ & & (-a)^{-1} = -a^{-1} & \end{array}$$

Definition 1.1.7 (Order)
An order on a set X is a binary relation $\leq$ on X such that

1. *(Totality)* $\forall x, y \in X (x \leq y \vee y \leq x)$
2. *(Antisymmetry)* $\forall x, y \in X\ (x \leq y \wedge y \leq x) \implies x = y$
3. *(Transitivity)* $\forall x, y, z \in X\ (x \leq y \wedge y \leq z) \implies x \leq z$

Remark (Order defined using the < operator)
Note that we may also make a definition of the above using ¡ instead of $\leq$. Then the properties that will define an order will be:

1. *(Trichotomy Property)* $\forall x, y \in X (x < y \vee y < x \vee x = y)$
2. *(Transitive Property)* $\forall x, y, z \in X (x < y \wedge y < z) \implies x < z$
3. *(Additive Property)* $\forall x, y, z \in X\ x < y \implies x + z < y + z$

4. *(Multiplicative Property)* $\forall a, b, c \in X$ *we have*
   (a) $a < b \wedge c > 0 \implies ac < bc$
   (b) $a < b \wedge c < 0 \implies bc < ac$

Remark (Non-negative and Non-positive)
Let $a \in \mathbb{R}$*. We say that* a *is non-negative when* $0 \leq a$ *and that* a *is non-positive* $a \leq 0$*.*

Remark
Some ways of writing the order symbol. Let $a, b, c \in \mathbb{R}$

- *b ¿ a is equivalent to b ¡ a*
- $b \leq a$ *is equivalent to* $b < a \vee b = a$
- *If a ¡ b and b ¡ c, we can write a ¡ b ¡ c.*

Theorem 1.1.5 ($\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ are ordered)
Each of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ *and* $\mathbb{R}$ *is an ordered set using the standard order* $\leq$*. Under the inclusions* $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ *the orders coincide (e.g. when* $a, b \in \mathbb{N}$ *we have* $a \leq b$ *in* $\mathbb{N}$ *if and only if* $a \leq b$ *in* $\mathbb{R}$*)*

Definition 1.1.8 (Ordered Field)
An ordered field is a field F *with an order* $\leq$ *such that for all* $x, y, z \in F$

1. $x \leq y \implies x + z \leq y + z$*, and*
2. $0 \leq x \wedge 0 \leq y \implies 0 \leq xy$*.*

Theorem 1.1.6 ($\mathbb{Q}$ and $\mathbb{R}$ as Ordered Fields)
$\mathbb{Q}$ *and* $\mathbb{R}$ *are ordered fields.*

Theorem 1.1.7 (Properties of Ordered Fields)
Let F *be an ordered field. Then* $\forall x, y, z \in F$ *we have*

1. $x > 0 \implies -x < 0$ *and* $x < 0 \implies -x > 0$
2. $x \neq 0 \implies x^2 > 0$ *and in particular 1 ¿ 0*
3. $0 < x < y \implies 0 < \frac{1}{y} < \frac{1}{x}$

Definition 1.1.9 (Absolute Value)
Let F be an ordered field. For $a \in F$ we define the absolute value of a to be

$$|a| = \begin{cases} a & \text{if } a \geq 0, \\ -a & \text{if } a \leq 0. \end{cases}$$

Theorem 1.1.8 (Properties of Absolute Values)
Let F be an ordered field. Then for all $x, y, z \in F$ we have

1. *(Positive Definiteness)* $|x| \geq 0$ *and* $|x| = 0 \iff x = 0$
2. *(Symmetry)* $|x - y| = |y - x|$
3. *(Multiplicativeness)* $|xy| = |x||y|$
4. *(Triangle Inequality)* $|x + y| \leq |x| + |y|$
5. *(Approximation)* $|x - y| \leq z \implies y - z \leq x \leq y + z$

Theorem 1.1.9 (Basic Order Properties in $\mathbb{Z}$)

1. $\forall n \in \mathbb{Z}(n \in \mathbb{N} \iff n \geq 0)$
2. $\forall k, n \in \mathbb{Z}(k \leq n \iff k < n + 1)$

1.2 Completeness Axiom

Definition 1.2.1 (Upper and Lower Bounds)
Let X be an ordered set and let $A \subseteq X$

1. *We say that A is bounded above (in X) when $\exists b \in X \, \forall a \in A \; a \leq b$, in which case we call b the upper bound of A.*
2. *We say that A is bounded below (in X) when $\exists c \in X \, \forall a \in A \; c \leq a$, in which case we call c the lower bound of A.*

We say that A is bounded when it is bounded above and below.

Definition 1.2.2 (Supremum and Infimum)
Let X be an ordered set and let $A \subseteq X$.

1. *We say that A has a supremum (or the least upper bound) when*

$$\exists b \in X (\forall a \in A \; a \leq b) \quad \forall c \in X (\forall a \in A \; a \leq c) \quad b < c.$$

We write b = sup A.
Now if b = sup A and $b \in A$, we call b the maximum of A, and denote it as b = max A.

2. *We say that A has an infimum (or the greatest lower bound) when*

$$\exists d \in X(\forall a \in A\, d \leq a) \quad \forall c \in X(\forall a \in A\, c \leq a) \quad c < d.$$

We write d = inf A.
Now if d = inf A and $d \in A$, we call d the minimum of A, and denote it as d = min A.

Theorem 1.2.1 (Approximation Property of Supremum and Infimum)
Let $\emptyset \neq A \subseteq \mathbb{R}$.

1. $b = \sup A \implies \forall 0 < \epsilon \in \mathbb{R}\, \exists x \in A\, (b - \epsilon < x \leq b)$
2. $c = \inf A \implies \forall 0 < \epsilon \in \mathbb{R}\, \exists x \in A\, (c \leq x < c + \epsilon)$

Theorem 1.2.2 (Completeness Properties of $\mathbb{R}$)

1. $\forall \emptyset \neq A \subseteq \mathbb{R}$, *if A is bounded above, then A has a supremum in $\mathbb{R}$*
2. $\forall \emptyset \neq A \subseteq \mathbb{R}$, *if A is bounded below, then A has an infimum in $\mathbb{R}$*

Theorem 1.2.3 (Well-Ordering Properties of $\mathbb{Z}$ in $\mathbb{R}$)

1. *Every nonempty subset of $\mathbb{Z}$ which is bounded above in $\mathbb{R}$ has a maximum.*
2. *Every nonempty subset of $\mathbb{Z}$ which is bounded below in $\mathbb{R}$ has a minimum. In particular, every nonempty subset of $\mathbb{N}$ has a minimum.*

Theorem 1.2.4 (Floor and Ceiling Properties of $\mathbb{Z}$ in $\mathbb{R}$)

1. *(Floor Properties)* $\forall x \in \mathbb{R}\, \exists! n \in \mathbb{Z}\, (x - 1 < n \leq x)$
2. *(Ceiling Properties)* $\forall x \in \mathbb{R}\, \exists! n \in \mathbb{Z}\, (x \leq n < x + 1)$

Definition 1.2.3 (Floor and Ceiling Functions)
Given $x \in \mathbb{R}$ we define the floor of x to be the unique $n \in \mathbb{Z}$ with $x - 1 < n \leq x$ and denote the floor of x by $\lfloor x \rfloor$. The function $f : \mathbb{R} \to \mathbb{Z}$ given by $f(x) = \lfloor x \rfloor$ is called the floor function.

Similarly, we define the ceiling of x to be the unique $n \in \mathbb{Z}$ with $x \leq n < x + 1$ and denote the ceiling of x by $\lceil x \rceil$. The function $f : \mathbb{R} \to \mathbb{Z}$ given by $f(x) = \lceil x \rceil$ is called the ceiling function.

Theorem 1.2.5 (Archimedean Properties of $\mathbb{Z}$ in $\mathbb{R}$)

1. $\forall x \in \mathbb{R}\, \exists n \in \mathbb{Z}\, (n > x)$

2. $\forall x \in \mathbb{R}\, \exists m \in \mathbb{Z}\, (m < x)$

Theorem 1.2.6 (Density of $\mathbb{Q}$)

$$\forall a, b \in \mathbb{R}(a < b) \quad \exists q \in \mathbb{Q}(a < q < b)$$

Chapter 2

Sequences

2.1 Limits of Sequences

Definition 2.1.1 (Sequence)
For $p \in \mathbb{Z}$, let $\mathbb{Z}_{\geq p} = \{k \in \mathbb{Z} | k \geq p\}$. A sequence in a set A is a function of the form $x : \mathbb{Z}_{\geq p} \to A$ for some $p \in \mathbb{Z}$. Given a sequence $x : \mathbb{Z}_{\geq p} \to A$, the k-th term of the sequence is the element $x_k = x(k) \in A$, and we denote the sequence x by

$$\langle x_k \rangle_{k \geq p} = \{x_k | k \geq p\} = \{x_p, x_{p+1}, x_{p+2}, ...\}$$

Note that the range of the sequence $\langle x_k \rangle_{k \geq p}$ is the set $\{x_k\}_{k \geq p} = \{x_k | k \geq p\}$.

Remark
While the notation $\{x_k\}_{k \geq p}$ is more commonly used, since this set of notes works a lot between sequences and sets, we shall use the notation $\langle x_k \rangle_{k \geq p}$ to denote a sequence instead to make a clear distinction between the two.

Definition 2.1.2 (Subsequence)
Let $\langle x_k \rangle_{k \geq p}$ be a sequence. A subsequence of $\langle x_k \rangle_{k \geq p}$ is a sequence of the form $\langle x_{k_n} \rangle_{n \in \mathbb{N}}$ such that $k_1 < k_2 < k_3 < \dots$ and $x_{k_1} < x_{k_2} < x_{k_3} < \dots$, where $x_{k_l} = x_m$ for all $n \geq l \in \mathbb{N}$ and a unique $k \geq m \in \mathbb{Z}_{\geq p}$.

Remark
In other words, a subsequence $\langle x_{k_n} \rangle_{n \in \mathbb{N}}$ is constructed from $\langle x_k \rangle_{k \geq p}$ by "removing" from $x_p, x_{p+1}, x_{p+2}, ...$ all the x_m's except for those such that $m = k_l$ for some l.

Definition 2.1.3 (Extended Ordered Field)
Let F be an ordered field. We can define the extended ordered field $\hat{F}$ to be the set $\hat{F} =$

$F \cup \{-\infty, \infty\}$, such that $\forall a \in F, -\infty < a < \infty$.

We also define, $\forall a \in F$:

- *$a + \infty = \infty$,*
- *$a - \infty = -\infty$,*
- *if $a > 0$, then $a \cdot \infty = \infty$, and*
- *if $a < 0$, then $a \cdot \infty = -\infty$.*

We define some indeterminant forms:

$$\infty - \infty,\ \infty \cdot 0,\ \frac{\infty}{\infty},\ \frac{\infty}{0},\ \frac{0}{\infty}$$

We extend the order relation ¡ on F such that $-\infty < \infty$.

Definition 2.1.4 (Convergence, Divergence and Limits of a Sequence)
Let F be an extended ordered field. and $\langle x_k \rangle_{k \geq p}$ be a sequence in F. For $a \in F$, we say that the sequence $\langle x_k \rangle_{k \geq p}$ converseges to a (or that the limit of $\langle x_k \rangle_{k \geq p}$ is equal to a), and we write $x_k \to a$(as $k \to \infty$), or we write $\lim_{k\to\infty} = a$, when

$$\forall 0 < \epsilon \in F\ \exists m \in \mathbb{Z}\ \forall k \in \mathbb{Z}_{\geq p}\ (k \geq m \implies |x_k - a| \leq \epsilon).$$

We say that the sequence $\langle x_k \rangle_{k \geq p}$ diverges (in F) when it does not converge (to any $a \in F$). We say that $\langle x_k \rangle_{k \geq p}$ diverges to infinity, or that the limit of $\langle x_k \rangle_{k \geq p}$ is equal to infinity, and we write $x_k \to \infty$(as $k \to \infty$, or we write $\lim_{k\to\infty} x_k = \infty$, when

$$\forall r \in F\ \exists m \in \mathbb{Z}\ \forall k \in \mathbb{Z}_{\geq p}\ (k \geq m \implies x_k \geq r)$$

Similarly, we say that $\langle x_k \rangle_{k \geq p}$ diverges to $-\infty$, or that the limit of $\langle x_k \rangle_{k \geq p}$ is equal to negative infinity, and we write $x_k \to -\infty$(as $k \to \infty$), or we write $\lim_{k\to\infty} x_k = -\infty$, when

$$\forall r \in F\ \exists m \in \mathbb{Z}\ \forall k \in \mathbb{Z}_{\geq p}\ (k \geq m \implies x_k \leq r)$$

Theorem 2.1.1 (Independence of Limit from Initial Terms)
Let $\langle x_k \rangle_{k \geq p}$ be a sequence in a subfield F of $\mathbb{R}$.

1. *If $q \geq p$ and $y_k = x_k$ for all $k \geq q$, then $\langle x_k \rangle_{k \geq p}$ converges iff $\langle y_k \rangle_{k \geq q}$ converges, and in this case $\lim_{k\to\infty} x_k = \lim_{k\to\infty} y_k$.*

   (Note that in this statement, $\langle y_k \rangle_{k \geq q}$ is a subsequence of $\langle x_k \rangle_{k \geq p}$, such that it takes on all the elements of the sequence after some $q \geq p$.)

2. *If* $l \geq 0$ *and* $y_k = x_{k+l}$ *for all* $k \geq p$*, then* $\langle x_k \rangle_{k \geq p}$ *converges iff* $\langle y_k \rangle_{k \geq p}$ *converges, and in this case* $\lim_{k\to\infty} x_k = \lim_{k\to\infty} y_k$.

   (Note that in this statement, $\langle x_k \rangle_{k \geq p}$ *is a subsequence of* $\langle y_k \rangle_{k \geq p}$ *instead, such that* $\langle x_k \rangle_{k \geq p}$ *takes on all the values of* $\langle y_k \rangle_{k \geq p}$ *from* $k + l$*.)*

Theorem 2.1.2 (Uniqueness of Limit)

2.2 Limit Theorems

Appendix A

ZF Set Theory and the Axiom of Choice

A.1 Introduction

Example A.1.1 (Russel's Paradox)
Let X be the set of all sets, and let $S = \{A \in X | A \notin A\}$.
Note for example that $Z \notin Z \implies Z \in S$, and $X \in X \implies X \notin S$.
Thus we have $S \in S \iff S \notin S$.

To ensure that mathematical paradoxes (like the above) can no longer arise, mathematicians considered the following questions, and with these questions, rough answers are provided:

1. What exactly is an allowable mathematical object?
   A: Every mathematical object is a mathematical set, and a mathematical set can be constructed using certain rules, for e.g. the now widely accepted Zermelo-Fraenkel Set Theory and the Axiom of Choice. While the Axiom of Choice is still highly criticized even today (e.g. the highly controversial Banach-Tarski Paradox), the Zermelo-Fraenkel Set Theory is widely welcomed, but not without critics. We shall call the Zermelo-Fraenkel Set Theory and the Axiom of Choice as the ZFC Axioms of Set Theory.

2. What exactly is an allowable mathematical statement?
   A: Every mathematical statement can be expressed in a formal symbolic language, which uses symbols rather than words from any spoken language.

3. What exactly is allowable in a mathematical proof?
   A: Every mathematical proof is a finite list of ordered pairs $(\mathscr{S}_n, \mathscr{F}_n)$ (which we can think of as proven theorems), where each $\mathscr{S}_n$ is a finite set of formulas (called the *premises*) and each $\mathscr{F}_n$ is a single formula (called the *conclusion*), which that each pair $(\mathscr{S}_n, \mathscr{F}_n)$ can be obtained from previous pairs $(\mathscr{S}_i, \mathscr{F}_i)$ with $i < n$, using certain proof rules.

In the remainder of this appendix, we shall look more into the first 2 questions.

A.2 ZFC Axioms of Set Theory

Definition A.2.1 (Mathematical Symbols)
We allow ourselves to use only the following symbols from the following symbol set:

$\neg$	*not*
$\wedge$	*and*
$\vee$	*or*
$\implies$	*implies*
$\iff$	*if and only if*
$=$	*equals*
$\in$	*is an element of*
$\forall$	*for all*
$\exists$	*there exists*
$()$ $\{\}$ $[]$	*parenthesis*

along with some variable symbols such as $x, y, z, u, v, w, ...$ *or* $x_1, x_2, x_3, ...$

Definition A.2.2 (Formula)
A formula (in the formal symbolic language of first order set theory) is a non-empty finite string of symbols, from the above list, which can be obtained using finitely many applications following the three rules below:

1. *If x and y are variable symbols, then each of the following strings are formulas.*
$$x = y, \quad x \in y$$
2. *If F and G are formulas then each of the following strings are formulas.*
$$\neg F, \quad (F \wedge G), \quad (F \vee G), \quad (F \implies G), \quad (F \iff G)$$
3. *If x is a variable symbol and F is a formula then each of the following is a formula.*
$$\forall x \in F, \quad \exists x \in F$$

Definition A.2.3 (Free or Bounded Variable)
Let x be a variable symbol and let F be a formula. For each occurrence of the symbol x, which does not immediately follow a quantifier, in the formula F, we define whether the occurrence of x is free or bound inductively as follows:

1. *If F is a formula of one of the forms $y = z$ or $y \in z$, where y and z are variable symbols (possibly equal to x), then every occurence of x in F is free, and no occurrence is bound.*
2. *If F is a formula of one of the forms $\neg H, (H \wedge G), (H \vee G), (H \implies G), (H \iff G)$, where G and H are formulas, then each occurence of the symbol x is either an occurrence in the formula G or an occurrence in the formula H, and each free (respectively, bound) occurence of x in G remains free (respectively, bound) in F, and similarly for each free (or bound) occurrence of x in G. In other words, wlog, if x is bounded in G, then it is bounded in F, and vice versa.*
3. *If F is a formula of one of the forms $\forall y \in G$ or $\exists y \in G$, where G is a formula and y is a variable symbol. If y is different from x, then each free (or bound) occurrence of x in G remains free (or bound) in the formula G, and if $y = x$ then every free occurrence of x in G becomes bound in F, and every bound occurrence of x in G remains bound in F.*

Definition A.2.4 (Is Bound By and Binds)
When a quantifier symbol occurs in a given formula F, and is followed by the variable symbol x and then by the formula G, any free occurence of x in G will become bound in the given formula F (by the 3rd definition above). We shall say that the occurrence of x is bound by (that occurrence of) the quantifier symbol, or that (the occurrence of) the quantifier symbol binds the occurence of x.

Definition A.2.5 (Free Variable, Statement, Statement About)
A ***free variable*** *in a formula F is any variable symbol that has at least one free occurence in F. A formula F with no free variables is called a* ***statement****. When the free variables in F all lie in the set $\{x_1, x_2, ..., x_n\}$, we shall write F as $F(x_1, x_2, ..., x_n)$ and we shall say that F is a* ***statement about*** *the variables $x_1, x_2, ..., x_n$.*

Definition A.2.6 (Unique Existence)
When F(x) is a statement about x, we sometimes write F(y) as a short form for the formula $\forall x(x = y \implies F(x))$, and we sometimes write

$$\exists! y \quad F(y)$$

which we read as "there exists a unique y such that F(y)", as a short form for the formula

$$(\exists y \quad F(y) \wedge \forall z \quad F(z)) \implies z = y))$$

which is, in turn, for the formula

$$\exists y\Big(\forall x\Big(x = y \implies F(x)\Big) \wedge \forall z\Big(\forall x(x = z \implies F(x)) \implies z = y\Big)\Big)$$

Remark (The ZFC Axioms of Set Theory (informal))
Every mathematical set can be constructed using specific rules, which we shall use the ZFC Axioms of Set Theory. Below is a list of the ZFC Axioms, stated informally.

- *Empty Set Axiom: There exists an empty set* $\emptyset$ *with no elements.*
- *Extension Axiom: 2 sets are equal if and only if they have the same elements.*
- *Separation Axiom: If u is a set and F(x) is a statement about x,* $\{x \in u : F(x)\}$ *is a set.*
- *Pair Axiom: If u and v are sets then u, v is a set.*
- *Union Axiom: If u is a set then* $\cup u = \bigcup\limits_{v \in u} v$ *is a set.*
- *Power Set Axiom: If u is a set then* $\mathcal{P}(u) = \{v : v \in u\}$ *is a set.*
- *Axiom of Infinity: If we define the natural numbers to be the sets* $0 = \emptyset, 1 = \{0\}, 2 = \{0, 1\}, 3 = \{0, 1, 2\}$ *and so on, then* $\mathbb{N} = \{0, 1, 2, 3, ...\}$ *is a set.*
- *Replacement Axiom: If u is a ste and F(x, y) is a statement about x and y with the property that* $\forall x\, \exists! y\, F(x, y)$ *then* $\{y : \exists x \in u\, F(x, y)\}$ *is a set.*
- *Axiom of Choice: Given a set u of non-empty pairwise disjoint sets, there exists a set which contains exactly one element from each of the sets in u.*

Definition A.2.7 (Empty Set Axiom)
The Empty Set Axiom is the formula

$$\exists u\, \forall x \quad \neg x \in u$$

Definition A.2.8 (Extension Axiom)
The Extension Axiom is the formula

$$\forall u\, \forall v\, \Big(u = v \iff \forall x\, (x \in u \iff x \in v)\Big)$$

Theorem A.2.1 (Uniqueness of the Empty Set)
The empty set is unique.

Definition A.2.9 ($\emptyset$)
We denote the unique empty set by $\emptyset$*.*

Definition A.2.10 (Subset)
*Given sets u and v, we say that u is a **subset** of v, and write $u \subseteq v$, when $\forall x(x \in u \implies x \in v)$*

Definition A.2.11 (Separation Axiom)
For any statement $F(x)$ about x, the following formula is an axiom.

$$\forall u\, \exists v\, \forall x\Big(x \in v \iff (x \in u \wedge F(x))\Big)$$

More generally, for any statement $F(x, u_1, u_2, ..., u_n)$ about $x, u_1, u_2, ..., u_n$ where $n \geq 0$, the following formula is an axiom.

$$\forall u\, \forall u_1 \ldots \forall u_n\, \exists v\, \forall x\Big(x \in v \iff (x \in i \wedge F(x, u_1, ..., u_n))\Big)$$

Any axiom of this form is called the Separation Axiom.

Note
It is important to realize that a Separation Axiom only allows us to construct a subset of a given set u. So, e.g., we cannot use the Separation Axiom to show that the collection $S = \{x : \neg x \in x\}$, which is used to formulate Russel's Paradox, is a set.

Definition A.2.12 (Pair Axiom)
The Pair Axiom is the formula

$$\forall u\, \forall v\, \exists w\, \forall x\Big(x \in w \iff (x = u \vee x = v)\Big)$$

Definition A.2.13 (Union Axiom)
The Union Axiom is the formula

$$\forall u\, \exists w\, \forall x\Big(x \in w \iff \exists v(v \in u \wedge x \in v)\Big)$$

Definition A.2.14 (Union)
*Given a set u, by the Union Axiom there exists a set w with the property that $\forall x\Big(x \in w \iff \exists v(v \in u \wedge x \in v)\Big)$, and by the Extension Axiom, this set w is unique. We call the set w the **union** of the elements in u, and denote it by*

$$\cup u = \bigcup_{v \in u} v.$$

Given two sets u and v, we define the union of u and v to be the set

$$u \cup v := \bigcup \{u, v\}.$$

Given three sets u, v, and w, note that $\{z\} = \{z, z\}$ *is a set and so* $\{x, y, z\} = \{x, y\} \cup \{z\}$ *is also a set. More generally, if* $u_1, u_2, ..., u_n$ *are sets then* $\{u_1, u_2, ..., u_n\}$ *is a set and we define the union of the sets* $u_1, u_2, ..., u_n$ *to be*

$$u_1 \cup u_2 \cup \ldots \cup u_n = \bigcup_{k=1}^{n} u_k = \bigcup \{u_1, u_2, ..., u_n\}$$

Definition A.2.15 (Intersection)
Given a st u, we define the intersection of the elements in u to be the set

$$\bigcap u = \left\{ x \in \bigcup u \,\middle|\, \forall v (v \in u \implies x \in v) \right\}$$

Given two sets u and v, we define the intersection of u and v to be the set

$$u \cap v = \bigcap \{u, v\}$$

and more generally, given sets $u_1, u_2, ..., u_n$*, we define the intersection of* $u_1, u_2, ..., u_n$ *to be the set*

$$u_1 \cap u_2 \cap \ldots \cap u_n = \bigcap_{k=1}^{n} u_k = \bigcap \{u_1, u_2, ..., u_n\}$$

Definition A.2.16 (Power Set Axiom)
The Power Set Axiom is the formula

$$\forall u\, \exists w\, \forall v (v \in w \iff v \subseteq u)$$

Definition A.2.17 (Power Set)
Given a set u, the set w is with the property that $\forall v (v \in w \iff v \subseteq u)$ *(which exists by the Power Set Axiom and is unique by the Extension Axiom) is called the power set of u and is denoted by* $\mathcal{P}(u)$*, so we have*

$$\mathcal{P}(u) = \{v | v \subseteq u\}$$

Definition A.2.18 (Ordered Pair)
Given two sets x and y, we define the ordered pair (x, y) to be the set

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Given two sets u and v, note that if $x \in u$ *and* $y \in v$ *then we have* $\{x\} \in \mathcal{P}(u \cup v)$ *and* $\{x, y\} \in \mathcal{P}(u \cup v)$ *and so* $(x, y) = \{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(u \cup v))$*. We define the product* $u \times v$ *to be the set*

$$u \times v = \{(x, y) | x \in u \wedge y \in v\},$$

i.e.

$$u \times v = \Big\{ z \in \mathcal{P}(\mathcal{P}(u \cup v)) | \exists x \exists y \big((x \in u \wedge y \in v) \wedge z = (x, y) \big) \Big\}$$

Definition A.2.19 (Successor, Inductive)
We define

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\} = 1 \cup \{1\}, \quad 3 = \{0, 1, 2\} = 2 \cup \{2\},$$

and so on. For a set x, we define the successor of x to be the set

$$x + 1 = x \cup \{x\}.$$

A set u is called inductive when it has the property that

$$(0 \in u \wedge \forall x(x \in u \implies x + 1 \in u))$$

Definition A.2.20 (Axiom of Infinity)
The Axiom of Infinity is the formula

$$\exists u(0 \in u \wedge \forall x(x \in u \implies x + 1 \in u))$$

so the Axiom of Infinity states that there exists an inductive set.

Theorem A.2.2 (Existence & Uniqueness of an Inductive Set)
$\exists w := \{x | x \in v$ *for every inductive set* $v\}$
Moreover, this set w is an inductive set.

Definition A.2.21 (Natural Numbers)
The unique set w in the above theorem is called the set of natural numbers, and we denote it by $\mathbb{N}$. We write

$$\begin{aligned} \mathbb{N} &= \{x | x \in v \textit{ for every inductive set } v\} \\ &= \{0, 1, 2, 3, ...\} \end{aligned}$$

For $x, y \in \mathbb{N}$, we write x ¡ y when $x \in y$ and write $x \leq y$ when $x < y \vee x = y$.

Remark
For a formula F, we write $\forall x \in u\, F$ as a shorthand notation for the formula $\forall x(x \in u \implies F)$. Similarly, we write $\exists x \in u\, F$ as a shorthand notation for $\exists x(x \in u \wedge F)$

Theorem A.2.3 (Principle of Induction)
Let F(x) be a statement about x. SPS that

1. *F(0), and*
2. $\forall x \in \mathbb{N}(F(x) \implies F(x + 1))$.

Then $\forall x \in \mathbb{N}\, F(x)$

Remark
The expression F(0) is short for $\forall x(x = 0 \implies F(x))$*, which in turn is short for* $\forall x(\forall y \neg y \in x \implies F(x))$*.Similarly, F(x + 1) is short for the formula* $\forall y(y = x + 1 \implies F(y))$*, where F(y) is short for* $\forall x(x = y \implies F(x))$*.*

Definition A.2.22 (Replacement Axiom)
Given a statement F(x, y) about x and y, the following formula is an axiom:

$$\forall u\Big(\forall x \exists! y\, F(x, y) \implies \exists w \forall y\big(y \in w \iff \exists x \in u\, F(x, y)\big)\Big)$$

where $\exists! y\, F(x, y)$ *is short for* $\exists y\Big(F(x, y) \wedge \forall z\big(F(x, z) \implies z = y\big)\Big)$ *with F(x ,z) short for the formula* $\forall y(y = z \implies F(x, y))$*. More generally, given a statement* $F(x, y, u_1, ..., u_n)$ *about* $x, y, u_1, ..., u_n$ *with* $n \geq 0$*, the following formula is an axiom:*

$$\forall u \forall u_1 \ldots \forall u_n\Big(\forall x \exists! y\, F(x, y, u_1, ..., u_n) \implies \exists w \forall y\big(y \in w \iff \exists x \in u\, F(x, y, u_1, ..., u_n)\big)\Big)$$

An axiom of this form is called a Replacement Axiom.

Definition A.2.23 (Axiom of Choice)
The Axiom of Choice is the formula given by

$$\forall u\Big(\big(\neg \phi \in u \wedge \forall x \in u\, \forall y \in u(\neg x = y \implies x \cap y = \emptyset)\big) \implies \exists w \forall v \in u\, \exists! x \in v\, x \in w\Big)$$

From this point on, we will be using upper-case letters to denote sets, instead of lower-case as per the statements above.

A.3 Relations, Equivalence Relations, Functions and Recursion

Definition A.3.1 (Binary Relation)
A binary relation R on a set X is a subset $R \subseteq X \times X$*. More generally, a binary relation is any set R whose elements are ordered pairs. For a binary relation R, we usually write xRy instead of* $(x, y) \in R$*.*

Definition A.3.2 (Domain, Range, Image, Inverse Image, Inverse, Composition)
Let R and S be binary relations.
The domain of R is

$$Domain(R) = \{x | \exists y\, xRy\}$$

and the range of R is

$$Range(R) = \{x|\exists y\, xRy\}.$$

For any set A, the image of A under R is

$$R(A) = \{y|\exists x \in A\, xRy\}$$

and the inverse image of A under R is

$$R^{-1}(A) = \{x|\exists y \in A\, xRy\}.$$

The inverse of R is

$$R^{-1} = \{(y,x)|(x,y) \in R\}$$

and the composition S composed with R is

$$S \circ R = \{(x,z)|\exists y\, xRy \wedge ySz\}$$

Theorem A.3.1 (Domain, Range, Image and Inverse Image as Sets)
Let A be a set and let R be a binary relation. Then Domain(R), Range(R), R(A) and $R^{-1}(A)$ are sets.

Theorem A.3.2 (Inverse and Composition as Binary Relations)
Let A be a set and let R and S be binary relations. Then R^{-1} and $S \circ R$ are binary relations.

Definition A.3.3 (Equivalence Relation)
An equivalence relation on a set X is a binary relation R on X such that

1. *R is **reflexive**, i.e. $\forall x \in X\, xRx$*
2. *R is **symmetric**, i.e. $\forall x, y \in X\, (xRy \implies yRx)$, and*
3. *R is **transitive**, i.e. $\forall x, y, z \in R\, \big((xRy \wedge yRz) \implies xRz\big)$.*

Definition A.3.4 (Equivalence Class)
Let R be an equivalence relation on the set X. For $a \in X$, the equivalence class of a modulo R is the set

$$[a]_R = \{x \in X|xRa\}$$

Definition A.3.5 (Partition)
A partition of a set X is a set S of non-empty pairwise disjoint sets whose union is X, that is a set S such that

1. *$\forall X, Y \in S\, (X \neq Y \implies X \cap Y = \emptyset)$*
2. *$\bigcup S = X$.*

Theorem A.3.3 (Correspondence of Equivalence Relations and Partitions)
Given a set X, we have the following correspondence between equivalence relations on X and partitions of X.

1. *Given an equivalence relation R on X, the set of all equivalence classes*

   $$S_R = \{[a]_R | a \in X\}$$

   is a partition of X.

2. *Given a partition S of X, the relation R_S on X is defined by*

   $$R_S = \{(x, y) \in X \times X | \exists A \in S(x \in A \wedge y \in A)\}$$

   is an equivalence relation on X.

3. *Given an equivalence relation R on X we have $R_{S_R} = R$, and a given partition S of X, we have $S_{R_S} = S$.*

Note (Set of All Equivalence Classes)
Given an equivalence relation R on X, the set of all equivalence classes, which we denote by S_R in the above theorem, is usually denoted by X/R, so

$$X/R = \{[a]_R | a \in X\}$$

Definition A.3.6 (Set of Representatives)
Let R be an equivalence relation. A set of representatives for R is a subset of X which contains exactly one element from each equivalence class in X/R.

Remark
Notice that the AC is equivalent to the statement that every equivalence relation has a set of representatives.

Definition A.3.7 (Function)
Get sets X and Y, a function from X to Y is a binary relation $f \subseteq X \times Y$ with the property that

$$\forall x \in X\ \exists! y \in Y\ (x, y) \in f$$

More generally, a function is a binary relation with the property that

$$\forall x \in Domain(f)\ \exists! y\ (x, y) \in f.$$

For a function f, we usually write y = f(x) instead of xfy. It is customary to use the notation $f : X \to Y$ when X = Domain(f) and Y is any set with $Range(f) \subseteq Y$.

Definition A.3.8 (One-to-one & Onto)
Let $f : X \to Y$. THe function f is called one-to-one (or injective) when

$$\forall y \in Y \; \exists \text{ at most one } x \in X \; y = f(x)$$

and f is called onto (or surjective) when

$$\forall y \in Y \; \exists \text{ at least one } x \in X \; y = f(x)$$

Definition A.3.9 (Left and Right Inverses)
Let $f : X \to Y$. Let I_X and I_Y denote the identity function on X and Y respectively. A left inverse of f is a function $g : Y \to X$ such that $g \circ f = I_X$. A right inverse of f is a function $H : X \to Y$ such that $f \circ H = I_Y$. Note that if f has a left inverse g and a right inverse H, then we have $g = g \circ I_Y = g \circ f \circ H = I_X \circ H = H$. In this case, we say that g is the (unique two-sided) inverse of f.

Theorem A.3.4 (Surjective and Injective VS Inverses)
Let $f : X \to Y$. Then

1. *f is one-to-one if and only if f has a left inverse.*
2. *f is onto if and only if f has a right inverse.*
3. *f is one-to-one and onto if and only if f has a (two-sided) inverse.*

Definition A.3.10 (Invertible)
A function $f : X \to Y$ is called invertible (or bijective) when it is one-to-one and onto, or equivalently, when it has a (unique two-sided) inverse.

Theorem A.3.5 (The Recursion Theorem)

1. *Let A be a set, let $a \in A$, and let $g : A \times \mathbb{N} \to A$. Then there exists a unique function $f : \mathbb{N} \to A$ such that*

$$f(0) = a \text{ and } f(n+1) = g(f(n), n) \text{ for all } n \in \mathbb{N}$$

2. *Let A and B be sets, let $g : A \to B$, and let $h : A \times B \times \mathbb{N} \to B$. Then there exists a unique function $f : A \times \mathbb{N} \to B$ such that for all $a \in A$ we have*

$$f(a, 0) = g(a) \text{ and } f(a, n+1) = h(a, f(a, n), n) \text{ for all } n \in \mathbb{N}$$

A.4 Construction of Integers, Rational, Real and Complex Numbers

Definition A.4.1 (Sum and Product)
By Part(2) of the Recursion Theorem, there is a unique function $s : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *such that for all* $a, b \in \mathbb{N}$ *we have*

$$s(a, 0) = a, \quad s(1, b + 1) = s(a, b) + 1.$$

We call s(a, b) the sum of a and $b \in \mathbb{N}$ *and write it as*

$$a + b = s(a, b).$$

Also, there is a unique function $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *such that for all a,* $b \in \mathbb{N}$ *we have*

$$p(a, 0) = 0, \quad p(a, b + 1) = p(a, b) + a$$

We call p(a, b) the product of a and b in $\mathbb{N}$*, and we write it as*

$$a \cdot b = p(a, b)$$

Definition A.4.2 (Integers)
We define the set of integers to be the set

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R$$

where R is the equivalence relation given by

$$(a, b)R(c, d) \iff a + d = b + c$$

For [(a, b)] and [(c,d)] in $\mathbb{Z}$*, we define*

$$\begin{aligned}
[(a, b)] \leq [(c, d)] &\iff b + c \leq a + d \\
[(a, b)] + [(c, d)] &\iff [(a + c, b + d)] \\
[(a, b)] \cdot [(c, d)] &= [(ac + bd, ad + bc)]
\end{aligned}$$

For $n \in \mathbb{N}$ *we write n = [(n, 0)] and -n = [(0, n)], so that every element of* $\mathbb{Z}$ *can be written as* $\pm n$ *for some* $n \in \mathbb{N}$*, and we can identity* $\mathbb{N}$ *with a subset of* $\mathbb{Z}$

Definition A.4.3 (Rational Numbers)
We define the set of reational numbers to be the set

$$\mathbb{Q} = (\mathbb{N} \times \mathbb{Z}^{+})/R$$

where $\mathbb{Z}^+ = \{x \in \mathbb{N} | x \neq 0\}$ *and* R *is the equivalence relation given by*

$$(a, b)R(c, d) \iff ad = bc$$

For [(a, b)] and [(c, d)] in $\mathbb{Q}$ *we define*

$$[(a, b)] \leq [(c, d)] \iff a \cdot d \leq b \cdot c$$
$$[(a, b)] + [(c, d)] \iff [(a \cdot d + b \cdot c, b \cdot d)]$$
$$[(a, b)] \cdot [(c, d)] = [(ac, bd)]$$

For $a \in \mathbb{N}$ *and* $b \in \mathbb{Z}^+$*, it is customary to write* $\frac{a}{b} = [(a, b)]$*. Also for* $a \in \mathbb{Z}$ *we write a = [(a, 1)], and we identify* $\mathbb{Z}$ *with a subset of* $\mathbb{Q}$

Definition A.4.4 (Real Numbers)
We define the set of real numbers of the the set

$$\mathbb{R} = \{x \subseteq \mathbb{Q} | x \neq \emptyset, x \neq \mathbb{Q}, \forall a \in x \, \forall b \in \mathbb{Q}(b \leq a \implies b \in x), \forall a \in x \, \exists b \in x \; a < b\}$$

For $x, y \in \mathbb{R}$ *we define*

$$x \leq y \iff x \subseteq y$$
$$x + y = \{a + b | a, b \in \mathbb{Q}, a \in x, b \in y\}$$

For $0 \leq x, y \in \mathbb{R}$ *we define*

$$x \cdot y = \{a \cdot b | 0 \leq a, b \in \mathbb{Q}, a \in x, b \in y\} \cup \{c \in \mathbb{Q} | c < 0\},$$

and YOU can try to, similarly, define $x \cdot y$ *in the case that x ¡ 0 and y ¡ 0.*

Definition A.4.5 (Complex Numbers)
We define the set of complex numbers to be the set

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}.$$

We define addition and multiplication in $\mathbb{C}$ *by*

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

We write $i = (0, 1)$*. For* $x \in \mathbb{R}$ *we write x = (x, 0) and identify* $\mathbb{R}$ *with a subset of* $\mathbb{C}$*.*

Appendix B

Functions and Cardinality

B.1 Functions

Definition B.1.1 (Range, Image, and Inverse Image)
Let X and Y be sets and let $f : X \to Y$. Recall (see Function in Appendix A) that the domain of f and the range of f are the sets

$$Domain(f) = X, \quad Range(f) = f(X) = \{f(x) | x \in X\}$$

For $A \subseteq X$, the image of A under f is the set

$$f(A) = \{f(x) | x \in A\}$$

For $B \subseteq Y$, the inverse image of B under f is the set

$$f^{-1}(B) = \{x \in X | f(x) \in B\}$$

Definition B.1.2 (Composite Function)
Let X, Y and Z be sets. Let $f : X \to Y$ and let $g : Y \to Z$. We define the composite function $g \circ f : X \to Z$ by $(g \circ f)(x) = g\big(f(x)\big)$ for all $x \in X$

Definition B.1.3 (Bijection)
Let X and Y be sets. Let $f : X \to Y$. We say that f is a bijection, or that f is bijective, if f is both one-to-one and onto (or that f is both injective and surjective).

Theorem B.1.1 (Bijectiveness and Inverse of the Composite Function)
Let X, Y and Z be sets. Let $f : X \to Y$ and $g : Y \to Z$. Then

1. *if f and g are both injective then so is $g \circ f$,*

2. *if f and g are both surjective then so is $g \circ f$, and*

3. *if f and g are both invertible then so is $g \circ f$, and in this case $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$*

Definition B.1.4 (Identity Function)
For a set X, we define the identity function on X to be the function $I_X : X \to X$ given by $I_X(x) = x$ for all $x \in X$. Note that for $f : X \to Y$ we have $f \circ I_X = f$ and $I_Y \circ f = f$.

Theorem B.1.2 (Bijectiveness and Invertability of Functions)
Let X and Y be nonempty sets and let $f : X \to Y$. Then

1. *f is injective if and only if f has a left inverse,*

2. *f is surjective if and only if f has a right inverse, and*

3. *f is bijective if and only if f has a left inverse g and a right inverse h, and in this case we have $g = h = f^{-1}$.*

Corollary B.1.2.1 (Relationship between Injection and Surjection)
Let X and Y be sets. Then there exists an injective map $f : X \to Y$ if and only if there exists a surjective map $g : Y \to X$.

B.2 Cardinality

Definition B.2.1 (Equal Cardinality)
Let A and B be sets. We say that A and B have the same cardinality, and wrtie —A— = —B—, when there exists a bijective map $f : A \to B$.

We say that the cardinality of A is less than or equal to the cardinality of B, and write $|A| \leq |B|$, when there exists an injective map $f : A \to B$.

We say that the cardinality of A is less than the cardinality of B, and write $|A| < |B|$, when $|A| \leq |B| \wedge |A| \neq |B|$ (i.e. there exists an injective map from A to B but no surjective map from A to B).

We also write $|A| \geq |B|$ when $|B| \leq |A|$ and $|A| > |B|$ when $|B| < |A|$.

Definition B.2.2 (Properties for Cardinality of Sets)
For all sets A, B, and C,

1. *—A— = —A—,*

2. *if —A— = —B—, then —B— = —A—,*

3. *if —A— = —B— and —B— = —C—, then —A— = —C—,*

4. $|A| \leq |B| \iff (|A| = |B| \vee |A| < |B|)$, *and*
5. $|A| \leq |B| \wedge |B| \leq |C| \implies |A| \leq |C|$.

Definition B.2.3 (Finiteness and Countability of Sets)
Let A be a set. For each $n \in \mathbb{N}$, let $S_n = \{0, 1, 2, ..., n-1\}$. For $n \in \mathbb{N}$, we say that the cardinality of A is equal to n, or that A has n elements, and write —A— = n, when $|A| = |S_n|$. We say that A is finite when —A— = n for some $n \in \mathbb{N}$. We say that A is infinite when A is not finite. We say that A is countable when $|A| = |\mathbb{N}|$.

Remark
Note that a set A is said to be countable when A is of the form $A = \{a_0, a_1, a_2, ...\}$ where all its element are distinct.

Theorem B.2.1
Let A be a set. Then the following are equivalent.

1. *A is infinite.*
2. *A contains a countable subset.*
3. $|\mathbb{N}| \leq |A|$
4. *There exists a map $f : A \to A$ which is injective but not surjective.*

Corollary B.2.1.1
Let A and B be sets.

1. *If A is countable then A is infinite.*
2. *When $|A| \leq |B|$, if B is finite then so is A, and if A is infinite, so is B.*
3. *If —A— = n and —B— = m, then —A— = —B— iff $n = m$.*
4. *If —A— = n and —B— = m, then $|A| \leq |B| \iff n \leq m$.*
5. *When one of the two sets A or B is finite. If $|A| \leq |B| \wedge |B| \leq |A| \implies |A| = |B|$.*

Theorem B.2.2 ($|\mathbb{N}|$ as a Threshold for Finiteness and Countability)
Let A be a set. $|A| \leq |\mathbb{N}| \iff A$ is finite or countable.

Theorem B.2.3
Let A be a set. Then

1. $|A| < |\mathbb{N}| \iff A$ *is finite,*
2. $|\mathbb{N}| < |A| \iff A$ *is neither finite nor countable, and*

3. $|A| \leq |\mathbb{N}| \wedge |\mathbb{N}| \leq |A| \implies |A| = |\mathbb{N}|$.

Definition B.2.4 (Countability and $\aleph_0$)
Let A be a set. When A is countable we write $|A| = \aleph_0$.

When A is finite we write $|A| < \aleph_0$.

When A is infinite we write $|A| \geq \aleph_0$.

When A is either finite or countable we write $|A| \leq \aleph_0$, and say that A is at most countable.

When A is neither finite nor countable we write $|A| > \aleph_0$, and say that A is uncountable.

Theorem B.2.4 (Set Cartesian Product and Union, and $\mathbb{Q}$ are Countable)

1. *If A and B are countable sets, then so is $A \times B$.*
2. *If A and B are countable sets, then so is $A \cup B$.*
3. *If $A_0, A_1, A_2, \dots$ are countable sets, then so is $\bigcup_{k=0}^{\infty} A_k$.*
4. *$\mathbb{Q}$ is countable.*

Remark
For a set A, we let 2^A denote the set of all functions from A to $S_2 = \{0, 1\}$, i.e.

$$2^A = \{f | f : A \to S_2\}$$

Theorem B.2.5 ($\mathbb{R}$ as an Uncountable Set)

1. *For every set A, $|\mathcal{P}(A| = |2^A|$.*
2. *For every set A, $|A| < |\mathcal{P}(A)|$.*
3. *$\mathbb{R}$ is uncountable.*

Theorem B.2.6 (Cantor-Schröder-Bernstein Theorem)
Let A and B be sets.

$$|A| \leq |B| \wedge |B| \leq |A| \implies |A| = |B|.$$