Numbers, Counting, and Infinities

version 7

Brian B. Tenneson

Abstract We introduce concepts from set theory as necessary to build the foundation for various sorts of numbers such as real numbers and integers. We rely heavily on the notion of an equivalence class and associated equivalence relations. Some important background material is included in the appendices which should be consulted by readers not already acquainted with concepts such as equivalence classes.

Keywords: Foundations of Number Theory, Set Theory, Construction of Integers, Rationals, Reals, and Complex Numbers. Arithmetic defined in terms of operations on sets.

Contents

1 Introduction

Mathematical concepts will be introduced as they are needed. One thing we will do is run through various number sets such as the set of real numbers and the set of complex numbers and show how they are "built" from sets alone. To do this, one thing we will need is the notion of equivalence relations which will be introduced in appendix A.

This is an informal presentation. The full strength version of this text will treat, among other things, axiomatic number theory as well as complete proofs of some of the more challenging theorems. It will be written in a manner suitable for consideration as scholarship as though things like integers and division by zero were new. For the moment, we will provide a framework for transitioning from the way numbers are normally described to, say, children, to the way a mathematician could define and manipulate numbers. This carries over into the infinite which will be examined to some extent. You'll note a distinct absence of pictures in reference to counting. This is because we take an abstract approach to counting. Finally, I would like to say that these notes are not enclosing original research; these notes serve as a collection of like-minded results into one more or less self-contained document. In the full strength version, there will be frequent mention of axioms and first-order theories (a.k.a. formal systems).

When we prove a theorem or other statement, the end of the proof will be denoted $\diamondsuit$

2 Sets

A concept fundamental to most of mathematics is that of a set. Typically, the word set is not given a mathematical definition since the set concept is, in a sense, primary relative to other concepts in mathematics. Consequently, most authors will define the word set “intuitively” or “naively.” Just as fundamental as the concept of set is the concept of membership.

Definition 2.1 Intuitively, the word **set** has many synonyms, including collection, container, group, aggregate, amalgam, and conglomerate.

According to [1*], Georg Cantor, one of the pioneers of modern set theory, defined sets as follows: *A **set** is a collection into a whole of definite, distinct objects of our intuition or our thought. The objects are called elements (members) of the set.*

A natural question is “what sort of things are sets collections of?” This question is important because the answer might point to some other fundamental mathematical objects besides sets. There are two answers: one in theory and one in practice. In set theory, sets are collections of sets. The elements of a set, in other words the contents of a container, are also *all* sets. In practice, by contrast, a set might contain objects (i.e., elements or members) that are *not* sets such as the set of all past and present presidents of the U.S.A. or the set of all potatoes in a heap of potatoes. In this document we will take a set theoretical approach; so, all objects which are contained in a set are also sets.

Definition 2.2 A set x is a **member** of a set y if x is amongst the collection that is y. One also says that x is an **element** of y. Membership is denoted by $\in$ so we write $x \in y$ if the set x is an element of the set y.

Examples. Here are some examples of sets. The set a of all whole numbers, the set b of all fractions, the set c of all fractions between 0 and the square root of 2, the set d of all prime numbers, the set e of vertices of a triangle, the set f of points on a circle, and the set g of all counting numbers that do not exceed 10. To illustrate the concept of membership, we would say that every whole number is a member of a, $1/2$ is not a member of a but is a member of b and c, 5 is a member of d while 100 is not a member of d, and 11 is a member of a, b (because 10 can be viewed as the fraction $10/1$), and d, but not g because 11 exceeds 10. Note that all instances of "is a member of" can be thought of as "is an element of" or "belongs to," and the way we will write these statements using the notation provided will be as follows: $1/2 \notin a$ (the slash through the $\in$ denotes negation), $1/2 \in b$, $1/2 \in c$, $5 \in d$, $100 \notin d$, $11 \in a$, $11 \in b$, $11 \in d$, and $11 \notin g$.

Definition 2.3 The set x is called a **subset** of the set y if every element of x is also an element of y. This is usually written as $x \subseteq y$. Another way this can be phrased is that $x \subseteq y$ if, and only if, for all sets z, if $z \in x$ then $z \in y$.

Examples. Keeping the sets as defined in the previous examples, $a \subseteq b$ because every whole number n can be viewed as the fraction $n/1$. $c \subseteq b$ since all fractions between 0 and the square root of 2 are all fractions, $d \subseteq a$ because all prime numbers are whole numbers, and $g \subseteq a$ because all counting numbers that do not exceed 10 are also whole numbers.

The set x is not a subset of y if, and only if, there is an element of x that is not an element of y. When x is not a subset of y, we write $x \nsubseteq y$.

Definition 2.4 Two sets x and y are considered **equal** if both $x \subseteq y$ and $y \subseteq x$. In other words, $x = y$ if every element of x is an element of y and every element of y is an element of x. That is to say that x and y have the same elements. If $x \subseteq y$ and x and y are *un*equal, then x is called a **proper subset** of y; this is denoted $x \subset y$.

Example. Consider the set h of all counting numbers less than or equal to 10. This is just a rephrasing of "all counting numbers that do not exceed 10," so $g = h$. The elements of g can be listed:

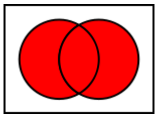
$$g = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}\,.$$

And notice that $h = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, demonstrating that they have the same elements.

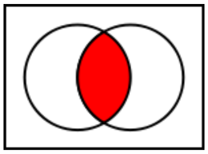
The **braces** $\{$ and $\}$ are quite often used to denote a set.

Definition 2.5 Given two sets x and y, their **union** is the set of all elements that are members of x or members of y, or both. The union of x and y is denoted $x \cup y$.

Definition 2.6 Given two sets x and y, their **intersection** is the set of all elements that are members of x and y. The intersection of x and y is denoted $x \cap y$.



This is called a Venn diagram. The two circles represent the two sets x and y. The red region represents $x \cup y$.



In this Venn diagram, the red region represents $x \cap y$.

Often enough, two sets have nothing in common. In that case their intersection is what is known as the empty set.

Definition 2.7 The **empty set** is the set that has no elements. More precisely, it is the set with the property that for all sets z, z is not an element of the empty set. The notation for this set is $\emptyset$.

Examples. Let $a = \{0\}$, $b = \{1\}$, and $c = \{0, 1\}$. Then

- $a \cup b = \{0, 1\}$
- $a \cap b = \emptyset$ because a and b have no elements in common
- $a \cup c = \{0, 1\}$, illustrating the property that if $x \subseteq y$ then $x \cup y = y$
- $a \cap c = \{0\}$ because 0 is the only element common to both a and c
- $b \cup c = \{0, 1\}$
- $b \cap c = \{1\}$, illustrating the property that if $x \subseteq y$ then $x \cap y = x$.

Theorem 2.8 For every set y, $\emptyset \subseteq y$ and $y \subseteq y$.

Proof Recall that $x \nsubseteq y$ means that there is an element of x that is not an element of y. Therefore, $\emptyset \nsubseteq y$ if and only if there is an element of $\emptyset$ that is not an element of y. Given the definition of the empty set, "there is an element of $\emptyset$ that is not an element of y" is false. In other words, $\emptyset \nsubseteq y$ is false; consequently, $\emptyset \subseteq y$. To prove the second statement, note that for all sets z, if $z \in y$ then $z \in y$. This satisfies the definition of subset.$\diamondsuit$

Definition 2.9 Given a set x, the **power set** of x is the set of all sets which are subsets of x. This set is denoted $\mathcal{P}(x)$.

Examples. To calculate something like $\mathcal{P}(\{0, 1\})$, we must list all sets which are subsets of $\{0, 1\}$. Keeping in mind theorem 2.8, the following are all subsets of $\{0, 1\}$: $\emptyset$, $\{0\}$, $\{1\}$, and $\{0, 1\}$. Therefore, $\mathcal{P}(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$. Notice that $\mathcal{P}(\{0, 1\})$ has four elements.

Theorem 2.10 If x has n elements, then $\mathcal{P}(x)$ has 2^n elements. For example, $\{0,1\}$ has two elements and $\mathcal{P}(\{0,1\})$ has 2^2 elements. Another example is $\mathcal{P}(\{0,1,2\})$ which should have, according to this theorem, $2^3 = 8$ elements. In fact, $\mathcal{P}(\{0,1,2\})$ is the following eight-element set:

$$\{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}.$$

Sketch of proof There is an identity (an equation which is "always true") whose proof is a bit beyond the scope of this document which states that for all counting numbers n,

$$C(n,0) + C(n,1) + ... + C(n,n) = 2^n.$$

The notation $C(n,k)$, read out loud as "n choose k," is the number of ways one can select k elements from a set with n elements. For example, $C(3,2) = 3$ because there are three ways of selecting two elements from a set with three elements (namely, if the set with three elements is $\{0,1,2\}$ then there are three ways to select two-element sets: $\{0,1\}$, $\{0,2\}$, and $\{1,2\}$). Another example is $C(4,2) = 6$ because if we start with a set of four elements such as $\{0,1,2,3\}$, there are six ways of selecting two elements at a time: $\{0,1\}$, $\{0,2\}$, $\{0,3\}$, $\{1,2\}$, $\{1,3\}$, and $\{2,3\}$.

Now if we consider the number of elements in $\mathcal{P}(x)$, i.e. the number of subsets of x, then we could arrange the count as follows:

the number of elements in $\mathcal{P}(x)$ is equal to the sum of the number of subsets of x that have 0 elements and the number of subsets of x that have 1 element and ... the number of subsets of x that have n elements. This means that the number of elements of $\mathcal{P}(x)$ is equal to $C(n,0) + C(n,1) + ... + C(n,n)$ which is, by the above identity, equal to 2^n.$\diamondsuit$

Incidentally, there is a formula for $C(n,k)$ which isn't directly helpful but is included for the sake of completeness:

$$C(n,k) = \frac{n!}{k!\,(n-k)!},$$

where the exclamation point represents what's called **factorial**. 0! is defined to be 1, $1! = 1$, $2! = 2 \times 1 = 2$, $3! = 3 \times 2 \times 1 = 6$, $4! = 4 \times 3 \times 2 \times 1 = 24$, and in general, $(n+1)! = (n+1) \times n!$. For further reading, look up "binomial coefficient."

2.1 Ordered Pairs and Cartesian Products

Ordered pairs and Cartesian Products play a central role in what is to come.

Definition 2.1.1 (a,b) is an **ordered pair** by which we mean that a and b are sets and (b,a) is not necessarily equal to (a,b). This is in contrast to an "unordered pair" $\{a,b\}$ which equals $\{b,a\}$. In set theory, (a,b) is defined to be the set $\{a,\{a,b\}\}$. Observe that $(a,b) = (c,d)$ if and only if both $a = c$ and $b = d$.

Definition 2.1.2 Let A and B be sets. Then the **Cartesian product** of A and B, written $A \times B$, is the set of all possible ordered pairs whose first coordinates are taken from A and whose second coordinates are taken from B. Symbolically, $A \times B = \{(a,b) : a \in A \wedge b \in B\}$. The symbol $\wedge$ denotes "and."

Examples Let $A = \{x,y\}$ and $B = \{1,2,3\}$. Then $A \times B = \{(x,1),(x,2),(x,3),(y,1),(y,2),(y,3)\}$. $A \times A = \{(x,x),(x,y),(y,x),(y,x)\}$ and

$$B \times B = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}.$$

We may, on occasion, write A^2 in place of $A \times A$.

3 Numbers

In this section I will state how various kinds of numbers can be defined in terms of sets. The natural numbers, also known as the counting numbers, are constructed from sets directly. I will mention the principle of induction which is one technique for proving statements about natural numbers (such as the identity mentioned in the proof of theorem 2.10). Next, I will introduce the notion of equivalence relation in order to show how more complicated number sets are certain equivalence classes of less complicated number sets. After we introduce a formal definition of natural number, we will use equivalence relations to mathematically construct the integers, rational numbers, real numbers, and, lastly, complex numbers. **With this progression in mind, this proves that all of the number types mentioned can be defined strictly with set theory alone.** All numbers of the varieties mentioned are sets.

3.1 Natural Numbers

The following formulation of the natural numbers, also known as the counting numbers, is attributed to Von Neumann (at least in spirit). We will define zero and the notion of successor and then define a natural number to be a set which is either zero or the successor of a natural number.

Definition 3.1 **Zero** is defined to be the empty set $\emptyset$. The first **natural number** is defined to be zero.

Definition 3.2 Given a natural number n, the **successor** of n is defined to be the set $n \cup \{n\}$. In general, a set is a **natural number** if it is either zero or the successor of a natural number. The notation we will use for the successor of n is $n + 1$.

Examples. I will list the first six natural numbers; this will also illustrate an important trait of natural numbers which is that the number of elements in a natural number is equal to that natural number.

- 0 is $\emptyset$ and, therefore, 0 has zero elements;
- 1 is the successor of 0 so it equals $0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$;
- 2 is the successor of 1 so it equals $1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$;
- 3 is the successor of 2 so it equals $2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$;
- 4 is the successor of 3 so it equals $3 \cup \{3\} = \{0, 1, 2\} \cup \{3\} = \{0, 1, 2, 3\}$;
- 5 is the successor of 4 so it equals $4 \cup \{4\} = \{0, 1, 2, 3\} \cup \{4\} = \{0, 1, 2, 3, 4\}$.

Notice that 1 is a set with one element, 2 is a set with two elements, and so on for all the natural numbers. For instance, 5 is a set with five elements (namely 0, 1, 2, 3, and 4).

Definition 3.3 Given two natural numbers n_1 and n_2, then $n_1 < n_2$ (i.e., n_1 is less than n_2) if and only if $n_1 \in n_2$. Also, $n_1 \leq n_2$ if and only if $n_1 \subseteq n_2$.

Definition 3.4 The set consisting of all natural numbers and only natural numbers is denoted $\mathbb{N}$.

Something to keep in mind is that formal set theory deals with axioms, statements assumed true for the sake of argument, and the consequences of those axioms. From the simpler axioms of set theory, it is impossible to prove that there is a such a set $\mathbb{N}$. What is known as the axiom of infinity must be assumed in order to "show" that $\mathbb{N}$ exists. The axioms of set theory have already been involved in what we have done so far; for example, it is unclear from simpler axioms that every set has a power set, so, there is an axiom of the power set. Also, the existence of the empty set is an axiom.

3.1.1 The Induction Principle

The induction principle is a method by which statements about natural numbers can be proved. At first glance, it doesn't appear to deliver such a method but, with examples, we will see how to apply the induction principle.

Theorem 3.5 (The Induction Principle) Let $X \subseteq \mathbb{N}$. If the following two conditions hold, then $X = \mathbb{N}$:

1. $0 \in X$

2. for all $n \in \mathbb{N}$, if $n \in X$ then $n + 1 \in X$, i.e., $n \in X$ *implies* $n + 1 \in X$

Proof. We will take a little detour and return to the proof in a moment.

We will invoke a property of natural numbers: every nonempty subset of $\mathbb{N}$ has a least element. That is to say that we are assuming that the set $\mathbb{N}$ is well-ordered (see http://en.wikipedia.org/wiki/Well-ordering_principle). Roughly speaking, when working in this area one can assume that the induction principle is true and prove that $\mathbb{N}$ is well-ordered or one can assume, as I am choosing to do here, that $\mathbb{N}$ is well ordered and prove the principle of induction from that. Therefore, the induction principle is equivalent to the statement "$\mathbb{N}$ is well ordered" and *both of these statements are axioms.*

I feel that the statement "$\mathbb{N}$ is well ordered" is highly credible because if we are given a nonempty subset of $\mathbb{N}$, we can devise an effective procedure to not only prove that nonempty subset of $\mathbb{N}$ has a least element but also find out what it is. That procedure would consist of the following instructions:

1. input x a nonempty subset of $\mathbb{N}$

2. let $k = 0$

3. if $k \in x$ then print "k is the least element of x" and HALT

4. if $k \notin x$ then let $k = k + 1$ (in other words, increase k by one) and GOTO (3).

This procedure is a search algorithm whose goal is to find the least element of x. First, if 0 is an element of x, then that is its least element. Then continue to test if k is an element of x until we find a value for k such that it is an element of x. Step 3 implies we halt as soon as we have found a value of k that is in x.

The statement "$\mathbb{N}$ is well-ordered" is then equivalent to the statement, "the above procedure will succeed and terminate for all nonempty subsets x of $\mathbb{N}$." (One fly in that ointment is that it is often very difficult to determine if $k \in x$.

With some background in the well-ordering of $\mathbb{N}$, we will return to the proof of the principle of induction.

We will prove $X = \mathbb{N}$ by contradiction. A **proof by contradiction** proceeds by showing that the negation of the conclusion implies the negation at least one of the hypotheses (i.e., premises or assumptions) of the theorem. In this case, the hypotheses of the theorem are that $X \subseteq \mathbb{N}$, $0 \in X$, and that for all $n \in \mathbb{N}$, if $n \in X$ then $n+1 \in X$. The conclusion of the theorem is $X = \mathbb{N}$. The **negation** of a statement is its logical opposite; for example the negation of the statement "$z = 3$" is the statement "z is not equal to 3."

For further reading on proofs by contradiction, see the Wikipedia article: link

To arrive at a contradiction, assume that $X \neq \mathbb{N}$. Let D be the set of all elements of $\mathbb{N}$ which are **not** elements of X. Since $X \neq \mathbb{N}$, D is not empty. Therefore, D has a least element d. d can't be 0 because $0 \in X$; so $0 < d$. That means d is the successor of some natural number c. As d is the least element of D, $c \in X$. But the 2nd condition

$$\text{for all } n \in \mathbb{N}, \text{ if } n \in X \text{ then } n + 1 \in X$$

implies that for c in particular the successor of c is an element of X. The successor of c is d; so $d \in X$. This contradicts the definition of D: elements of D are not elements of X.$\diamondsuit$

3.1.2 Addition of Natural Numbers

I will give one definition of addition of two natural numbers and then prove that addition is commutative and associative.

Definition 3.6 Given a natural number n, let $S(n)$ denote the successor of n. Given a natural number m, let $S_0(n) = n$, and for natural numbers k, let $S_{k+1}(n) = S(S_k(n))$. Define $n + m$ to be $S_m(n)$.

Example. Let's use this definition to find the sum $2 + 3$ (so $n = 2$ and $m = 3$). $S_0(2) = 2$, $S_1(2) = S(S_0(2)) = S(2) = 3$. $S_2(2) = S(S_1(2)) = S(3) = 4$. Finally, $2 + 3 = S_3(2) = S(S_2(2)) = S(4) = 5$. Notice that $S_3(2) = S(S(S(2)))$. In general, $S_m(n) = S(\ldots S(n)\ldots)$ where there are m S's on the right hand side. Now let's compute $3 + 2$ (so $n = 3$ and $m = 2$). $S_0(3) = 3$. $S_1(3) = S(S_0(3)) = S(3) = 4$. Finally, $3 + 2 = S_2(3) = S(S_1(3)) = S(4) = 5$.

In the language of functions, explored in appendix B, S_m is the mth iterate of the successor function.

Theorem 3.7 Addition is commutative. For all natural numbers n and m, $n + m = m + n$.

In order to prove this theorem, we must first mention two other facts about addition.

Lemma 3.8 For all natural numbers m, $S_m(0) = m$. **Proof.** We will proceed by using the principle of mathematical induction. Let $G = \{m \in \mathbb{N} : S_m(0) = m\}$. The statement, "for all natural numbers m, $S_m(0) = m$," is equivalent to the statement "$G = \mathbb{N}$". First, note that $S_0(0) = 0$ by the definition of S_0.

Therefore, $0 \in G$. For the induction step, let m be a given natural number and suppose that $m \in G$; we wish to prove that $m+1 \in G$. Since $m \in G$, $S_m(0) = m$. By definition, $S_{m+1}(0) = S(S_m(0))$. Since $S_m(0) = m$, $S_{m+1}(0) = S(m) = m+1$. Since $S_{m+1}(0) = m+1$, $m+1 \in G$. The two conditions in the principle of induction are satisfied; so $G = \mathbb{N}$, implying that for all natural numbers m, $S_m(0) = m$.$\diamondsuit$

Lemma 3.9 For all natural numbers n and m, $S(S_m(n)) = S_m(S(n))$. In other words, $(n+m)+1 = (n+1)+m$. **Proof.** Let n be a given natural number and let $G_n = \{m \in \mathbb{N} : S(S_m(n)) = S_m(S(n))\}$. The statement, "for all natural numbers n and m, $S(S_m(n)) = S_m(S(n))$," is equivalent to the statement, "for all natural numbers n, $G_n = \mathbb{N}$." Hence the principle of induction will be applied in this situation. In the case $m = 0$, we have $S(S_0(n)) = S(n)$ and $S_0(S(n)) = S(n)$, by the previous lemma. Therefore, $0 \in G_n$ since $S(S_0(n)) = S_0(S(n))$. $S(S_{m+1}(n)) = S(S(S_m(n)))$ by definition. $S(S(S_m(n))) = S(S_m(S(n)))$ by the induction hypothesis (note the reversal in order among the subscripts). $S(S_m(S(n))) = S_{m+1}(S(n))$ by definition. Putting this all together, we have shown that $S(S_{m+1}(n)) = S_{m+1}(S(n))$, implying that $m+1 \in G_n$. By the induction principle, $G_n = \mathbb{N}$. As n was arbitrary, we have shown that for all natural numbers n, $G_n = \mathbb{N}$; hence, for all natural numbers n and m, $S(S_m(n)) = S_m(S(n))$.$\diamondsuit$

Proof of theorem 3.7 The proof will resemble the proof of lemma 3.9 and will make use of both lemmas. Let $H_m = \{n \in \mathbb{N} : S_m(n) = S_n(m)\}$. Recalling the definition of $n+m$, the following two statements are equivalent:

$$\text{for all } m \in \mathbb{N},\ H_m = \mathbb{N}$$

$$\text{for all natural numbers } n \text{ and } m,\ n+m = m+n.$$

To show that $H_m = \mathbb{N}$, we will use the principle of induction. Let m be a given natural number. In the case $n = 0$, we wish to prove that $S_m(0) = S_0(m)$. $S_m(0) = m$ by lemma 3.8 and $S_0(m) = m$ by definition; so $S_m(0) = S_0(m)$. For the induction step, assume $n \in H_m$. $n \in H_m$ implies that $S_m(n) = S_n(m)$. We want to show that $n+1 \in H_m$, i.e., that $S_m(n+1) = S_{n+1}(m)$. $S_{n+1}(m) = S(S_n(m))$ by definition. $S(S_n(m)) = S(S_m(n))$ by the induction hypothesis. $S(S_m(n)) = S_m(S(n))$ by lemma 3.9. Putting all these equations together, $S_{n+1}(m) = S_m(S(n))$. Recall that $S(n) = n+1$; so we have, in fact, shown that $n+1 \in H_m$. By the induction principle, $H_m = \mathbb{N}$. As m was arbitrary, we have shown that for all natural numbers m, $H_m = \mathbb{N}$; so for all natural numbers n and m, $n + m = m + n$.$\diamondsuit$

Theorem 3.10 Addition is associative. For all l, m, $n \in \mathbb{N}$, $(l+m)+n = l+(m+n)$. The parentheses dictate which order the addition is occurring in. The left hand side says to first add l to m and then n to that sum while the right hand side says to add l to the sum of m and n. This theorem states that both ways will always yield the same sum. In the expression $(l+m)+n$, l and m are called **associates**; in $l+(m+n)$, m and n are **associates**.

In order to prove theorem 3.10, we will make use of the lemma 3.9 which states that for all l and $m \in \mathbb{N}$, $S_m(S(l)) = S(S_m(l))$, i.e., $(l+1)+m = (l+m)+1$. Also note that lemma 3.9 implies that for a natural number x, $S_k(S(x)) = S(S_k(x))$, i.e., $S_k(x+1) = S_k(x)+1$. To establish associativity, given two natural numbers m and n, let $I_{m,n} = \{l \in \mathbb{N} : S_n(l+m) = S_{m+n}(l)\}$. We wish to prove that for all m and n, $I_{m,n} = \mathbb{N}$ because $S_n(l+m) = S_{m+n}(l)$ is equivalent to $(l+m)+n = l+(m+n)$. First, we wish to show that $0 \in I_{m,n}$ so assume $l = 0$. $S_n(0+m) = S_n(m) = m+n$. By lemma 3.8, $S_{m+n}(0) = m+n$; so $S_n(l+m) = S_{m+n}(l)$ in the case where $l = 0$. Now we wish to demonstrate that for all $l \in \mathbb{N}$, $l \in I_{m,n}$ implies $l+1 \in I_{m,n}$; so assume $l \in I_{m,n}$.

$S_n\left((l+1)+m\right) = S_n\left((l+m)+1\right)$ by lemma 3.9

$= S_n\left(l+m\right)+1$ by lemma 3.9

$= S_{m+n}\left(l\right)+1$ by the induction hypothesis

$= S_{m+n}\left(l+1\right)$ by lemma 3.9.

Since $S_n\left((l+1)+m\right) = S_{m+n}\left(l+1\right)$, $l+1 \in I_{m,n}$. By the principle of induction, $I_{m,n} = \mathbb{N}$, implying the associativity of addition.$\diamondsuit$

3.1.3 Multiplication of Natural Numbers

The definition of multiplication will resemble the definition of addition. However, in contrast, will define a function that adds n to its input. When that function is iterated m times, then the result will be $n \times m$.

Definition 3.10 Multiplication of natural numbers. Define $M_0\left(n\right) = 0$ and for $k \in \mathbb{N}$, $M_{k+1}\left(n\right) = M_k\left(n\right) + n = S_n\left(M_k\left(n\right)\right)$. $n \times m$ is defined to be $M_m\left(n\right)$.

Example. We will use this definition to calculate 2×3. We will calculate $M_0\left(2\right)$, $M_1\left(2\right)$, $M_2\left(2\right)$, and $M_3\left(2\right)$. $M_0\left(2\right) = 0$. $M_1\left(2\right) = M_0\left(2\right)+2 = 0+2 = 2$. $M_2\left(2\right) = M_1\left(2\right)+2 = 2+2 = 4$. $2 \times 3 = M_3\left(2\right) = M_2\left(2\right)+2 = 4+2 = 6$. Now let's calculate 3×2. To do so, we need to find $M_0\left(3\right)$, $M_1\left(3\right)$, and $M_2\left(3\right)$. $M_0\left(3\right) = 0$. $M_1\left(3\right) = M_0\left(3\right)+3 = 0+3 = 3$. $M_2\left(3\right) = M_1\left(3\right)+3 = 3+3 = 6$.

Theorem 3.11 Multiplication is commutative. For all n and m in $\mathbb{N}$, $n \times m = m \times n$.

Proof Let $H_m = \{n \in \mathbb{N} : M_m\left(n\right) = M_n\left(m\right)\}$. Recalling the definition of $n \times m$, the following two statements are equivalent:

$$\text{for all } m \in \mathbb{N},\ H_m = \mathbb{N}$$

$$\text{for all natural numbers } n \text{ and } m,\ n \times m = m \times n.$$

Lemma 3.12 For all natural numbers n and m, $M_m(n+1) = M_m(n) + m$.

Proof. Given a natural number n, let $K_n = \{m \in \mathbb{N} : M_m(n+1) = M_m(n) + m\}$. To perform the base case for induction, let $m = 0$. If $m = 0$ then we have $M_0(n+1) = 0 = 0 + 0 = M_0(n) + 0$. Now we wish to show that for all natural numbers m, $m \in K_n$ implies $m + 1 \in K_n$; so assume $M_m(n+1) = M_m(n) + m$. We will show that

$$\text{(A) } M_{m+1}(n+1) = M_{m+1}(n) + (m+1).$$

The left hand side of (A) equals $M_m(n+1)+(n+1)$ by definition. $M_m(n+1)+(n+1) = (M_m(n)+m) + (n+1)$ by the induction hypothesis. The right hand side of (A) equals $(M_m(n)+n) + (m+1)$ by definition. One can show that$(M_m(n)+n) + (m+1)$ equals $(M_m(n)+m) + (n+1)$ by using the commutativity and associativity of addition. This concludes the proof of lemma 3.13. (Note that lemma 3.13 says $(n+1) \times m = n \times m + m$, thus it is a specific instance of the distributive property which will be mentioned shortly.)

To prove theorem 3.12, let m be a given natural number. We will use induction to prove $H_m = \mathbb{N}$. In the case $n = 0$, we have $M_0(0) = M_0(0)$. To prove that $n \in H_m$ implies $n+1 \in H_m$, assume $n \in H_m$, i.e., that $M_m(n) = M_n(m)$. $M_{n+1}(m) = M_n(m) + m$ by definition. $M_n(m) + m = M_m(n) + m$ by the induction hypothesis. $M_m(n) + m = M_m(n+1)$ by lemma 3.13; so $M_{n+1}(m) = M_m(n+1)$, implying that $n + 1 \in H_m$.$\diamondsuit$

Theorem 3.13 Multiplication is associative. For all l, n, and m in $\mathbb{N}$, $l \times (m \times n) = (l \times m) \times n$.

Proof.

Theorem 3.14 Multiplication distributes over addition. For all l, n, and m in $\mathbb{N}$, $l \times (m+n) = (l \times m) + (l \times n)$.

Proof. Given arbitrary natural numbers l and n, define $D_{l,n} = \{m \in \mathbb{N} : M_{m+n}(l) = M_m(l) + M_n(l)\}$. (Observe that $l \times (m+n) = (l \times m) + (l \times n)$ is equivalent to $M_{m+n}(l) = M_m(l) + M_n(l)$.) To show that $D_{l,n} = \mathbb{N}$, we will use the principle of induction. Consider the case $m = 0$. $M_{0+n}(l) = M_n(l) = 0 + M_n(l) = M_0(l) + M_n(l)$. Now to prove that for all natural numbers m, $m \in D_{l,n}$ implies $m+1 \in D_{l,n}$, assume that $m \in D_{l,n}$. Our goal is to show that $m+1 \in D_{l,n}$, i.e., that $M_{(m+1)+n}(l) = M_{m+1}(l) + M_n(l)$. We will start with the right hand side of that equation:

$M_{m+1}(l) + M_n(l) = (M_m(l) + l) + M_n(l)$ by the definition of M_{m+1}

$= M_m(l) + (l + M_n(l))$ by the associativity of addition

$= M_m(l) + (M_n(l) + l)$ by the commutativity of addition

$= (M_m(l) + M_n(l)) + l$ by the associativity of addition

$= M_{m+n}(l) + l$ by the induction hypothesis

$= M_{(m+n)+1}(l)$ by the definition of M_k

$= M_{(m+1)+n}(l)$ by lemma 3.9.$\diamondsuit$

3.1.4 Exponentiation of Natural Numbers

Exponentiation (for natural numbers) is repeated multiplication of a natural number with itself.

Definition 3.15 Exponentiation of natural numbers. Define $E_0(n) = 1$ for all natural numbers n. For $k \in \mathbb{N}$, $E_{k+1}(n) = E_k(n) \times n$. Then n^m is defined to be $E_m(n)$. n is called the **base** and m is called the **exponent**.

We will now prove two laws of exponents. Also, observe that in this definition, $0^0 = 1$.

Theorem 3.16 Let n, p, and q be natural numbers. Then

A $n^p \times n^q = n^{p+q}$ and

B $(n^p)^q = n^{p \times q}$.

Proof.

3.2 Integers

The integers, informally positive or negative whole numbers, can be defined in terms of natural numbers. Since natural numbers are all sets, all integers are sets as well. Again this underscores the importance of sets. We will define the integers and define addition and subtraction among integers. We will also mention the definition of multiplication. Appendix A contains many useful facts about equivalence relations which will be relied upon in order to define the integers. Much of the material for this section can be found in this wikipedia article.

The integers will be defined to be a certain set of equivalence classes (see appendix A) for the following equivalence relation:

Definition Let a, b, c, and d be natural numbers. Then the ordered pair (a, b) is **equivalent** to (c, d), written $(a, b) \cong (c, d)$, if and only if $a + d = b + c$.

This definition might seem out of the blue so let me explain the rationale behind it. (a, b) is to be thought of as $a - b$. Note that we have not defined subtraction for natural numbers but this is what we imagine (a, b) to mean. Note that the defining condition for $(a, b) \cong (c, d)$, namely that $a+d = b+c$, can be thought of as $a - b = b - d$ (via algebraic rearrangement). Since we think of (a, b) as $a - b$, $(a, b) \cong (c, d)$ if and only if $a - b = c - d$. For example, we expect that $3 - 4$ is the same integer as $10-11$. Notice that $(3, 4) \cong (10, 11)$ because $3+11 = 4+10$.

Lemma $\cong$ as defined above is an equivalence relation. **Proof.** We must show that $\cong$ is (a) reflexive, (b) symmetric, and (c) transitive.$\diamondsuit$

Definition The set of **integers**, denoted $\mathbb{Z}$, is defined to be $(\mathbb{N} \times \mathbb{N})/\cong$. (Recall the definition of Cartesian product from section 2.1 and see the definition of equivalence classes in appendix A.)

In English, $\mathbb{Z}$ is the set of $\cong$-equivalence classes of ordered pairs of natural numbers. The equivalence class that (a, b) belongs to will be denoted with brackets, $[(a, b)]$. To reiterate, we are thinking of (a, b) as representing $a - b$.

Definition -1 is, by definition, equal to $[(0, 1)]$ which is the set of all ordered pairs of natural numbers that are $\cong$-equivalent to $(0, 1)$. (There is an endless supply of representatives of that equivalence class; -1 can be written as $[(1, 2)]$ or, in general, by $[(k, k + 1)]$ for any natural number k.) -2 is, by definition, equal to $[(0, 2)]$. For a natural number n, $-n$ is defined to be $[(0, n)]$.

Definition less than

3.2.1 Addition and Subtraction of Integers

commutative and associative

3.2.2 Multiplication of Integers

commutative and associative

distributive property

3.2.3 The Embedding of $\mathbb{N}$ in $\mathbb{Z}$

Lemma $\mathbb{N}$ can be embedded within $\mathbb{Z}$ with the function f that maps n to $[(n, 0)]$.

Proof. An embedding is a special type of injection (see appendix B for a definition of injection) that preserves structure. An injection that preserves structure in this case means the following:

1. f is an injection;
2. for all natural numbers n and m, $f(n+m) = f(n) + f(m)$;
3. for all natural numbers n and m, $f(n \times m) = f(n) \times f(m)$; and
4. for all natural numbers n and m, $n < m$ if and only if $f(n) < f(m)$.

$f(n) = [(n, 0)]$, by definition. We will think of $f(n)$ to be the representative of the natural number n in "integer land." n and $f(n)$ are essentially identical where the word essentially precisely means that structure is preserved.

The notation is being abused here in the sense that in equations like $f(n+m) = f(n) + f(m)$, the + used in the left hand side is not the same as the + used in the right hand side. The + used in the left hand side is in "natural number land" while the + used in the right hand side is in "integer land." What + means will be entirely based on context, i.e., its meaning will be determined by the type of the two things are being added.

Proof of (1).

Proof of (2).

Proof of (3).

Proof of (4).$\diamondsuit$

Technically, in this development, $\mathbb{N}$ is not a subset of $\mathbb{Z}$ as one might think. But the embedded copy of $\mathbb{N}$ within $\mathbb{Z}$ is a subset of $\mathbb{Z}$. So when we write $\mathbb{N} \subseteq \mathbb{Z}$, what we really mean is that $f[\mathbb{N}] \subseteq \mathbb{Z}$ and $f[\mathbb{N}]$ is structurally identical to $\mathbb{N}$. This phenomena occurs at all steps of the progression from naturals to integers to rationals to reals to complex.

3.2.4 Exponentiation of Integers

basic exponent laws, negative exponents (rational numbers)

3.3 Rational Numbers

The rational numbers, informally ratios of integers, can be defined in terms of integers. Since integers are all sets, all rational numbers are sets as well. Again this underscores the importance of sets. We will define the rational numbers and define addition and subtraction among rational numbers. We will also mention the definition of multiplication and division. Appendix A contains many useful facts about equivalence relations which will be relied upon in order to define the rational numbers.

The rational numbers will be defined to be a certain set of equivalence classes (see appendix A) for the following equivalence relation:

Definition Let a, b, c, and d be integers. Then the ordered pair (a, b) is **equivalent** to (c, d), written $(a, b) \equiv (c, d)$, if and only if $a \times d = b \times c$.

Let me explain the rationale behind this definition. (a, b) is to be thought of as a/b. Note that we have not defined division for integers but this is what we imagine (a, b) to mean. Note that the defining condition for $(a, b) \equiv (c, d)$, namely that $a \times d = b \times c$, can be thought of as $a/b = c/d$ (via algebraic rearrangement). Since we think of (a, b) as a/b, $(a, b) \equiv (c, d)$ if and only if $a/b = c/d$. For example, we expect that 3/4 is the same rational number as 6/8. Notice that $(3, 4) \equiv (6, 8)$ because $3 \times 8 = 4 \times 6$.

Lemma $\equiv$ as defined above is an equivalence relation. **Proof.** We must show that $\equiv$ is (a) reflexive, (b) symmetric, and (c) transitive.$\diamondsuit$

Definition The set of **rational numbers**, denoted $\mathbb{Q}$, is defined to be $(\mathbb{Z} \times \mathbb{Z})/\equiv$. (Recall the definition of Cartesian product from section 2.1 and see the definition of equivalence classes in appendix A.)

In English, $\mathbb{Q}$ is the set of $\equiv$-equivalence classes of ordered pairs of integers. The equivalence class that (a, b) belongs to will be denoted with brackets, $[(a, b)]$. To reiterate, we are thinking of (a, b) as representing a/b.

Definition less than

3.3.1 Addition and Subtraction of Rational Numbers

commutative and associative

3.3.2 Multiplication and Division of Rational Numbers

commutative and associative

distributive property

3.3.3 The Embedding of $\mathbb{Z}$ in $\mathbb{Q}$

Lemma $\mathbb{Z}$ can be embedded within $\mathbb{Q}$ with the function g that maps x to $[(x, 1)]$.

Proof. An embedding is a special type of injection (see appendix B for a definition of injection) that preserves structure. An injection that preserves structure in this case means the following:

1. g is an injection;
2. for all integers x and y, $g(x + y) = g(x) + g(y)$;
3. for all integers x and y, $g(x \times y) = g(x) \times g(y)$; and
4. for all integers x and y, $x < y$ if and only if $g(x) < g(y)$.

$g(x) = [(x, 1)]$, by definition. We will think of $g(x)$ to be the representative of the integer x in "rational number land." x and $g(x)$ are essentially identical where the word essentially precisely means that structure is preserved.

Proof of (1).

Proof of (2).

Proof of (3).

Proof of (4).$\diamondsuit$

3.3.4 Exponentiation of Rational Numbers

basic exponent laws, rational exponents

3.3.5 Division By Zero

To be expanded..

3.4 Real Numbers

The real numbers, informally numbers representable with a decimal expansion, can be defined in terms of rational numbers. We will define the real numbers and define addition and subtraction among real numbers. We will also mention the definition of multiplication and division. Appendix A contains many useful facts about equivalence relations which will be relied upon in order to define the real numbers. First, we will introduce sequences to help us define real numbers. Then we will define an equivalence relation among sequences of rational numbers; the set of real numbers will be the set of equivalence classes of sequences of rational numbers.

Definition A **sequence** is a function whose domain is $\mathbb{N}$ or $\mathbb{N}^+$, the set of positive natural numbers, and range is a set Y of numbers. The set of all sequences in a number set Y is denoted ${}^{\mathbb{N}}Y$.

Definition absolute value

Definition Given two rational numbers, the **distance** between

Definition A sequence a of numbers selected from the number set Y is said to be a **Cauchy sequence** if and only if for all $r \in \mathbb{Q}^{+}$ (i.e., for all positive rationals r) there is an $N \in \mathbb{N}$ such that if $m \geq N$ and $n \geq N$, then $|a(m) - a(n)| < r$. Let the set of all Cauchy sequences be denoted Y_C. (So, for example, the set of Cauchy rational number sequences is denoted $\mathbb{Q}_C$.)

explanation . Convergence. Not all Cauchy sequences of rational numbers converge to a rational number.

Definition Let a and b be Cauchy sequences of rational numbers. Then the sequence a is **equivalent** to the sequence b, written $a \doteq b$, if and only if for all $r \in \mathbb{Q}^{+}$ there is an $N \in \mathbb{N}$ such that if $n \geq N$ then $|a(n) - b(n)| < r$.

Let me explain the rationale behind this definition.

Lemma $\doteq$ as defined above is an equivalence relation. **Proof.** We must show that $\doteq$ is (a) reflexive, (b) symmetric, and (c) transitive.$\diamondsuit$

Definition The set of **real numbers**, denoted $\mathbb{R}$, is defined to be $(\mathbb{Q}_C) / \doteq$. (Recall the definition equivalence classes in appendix A.)

In English, $\mathbb{R}$ is the set of $\doteq$-equivalence classes of Cauchy sequences of rational numbers. The equivalence class that a belongs to will be denoted with brackets, $[a]$. We are thinking of a as representing the real number a converges to.

Definition less than

3.4.1 Addition and Subtraction of Real Numbers

commutative and associative

3.4.2 Multiplication and Division of Real Numbers

commutative and associative

distributive property

3.4.3 The Embedding of $\mathbb{Q}$ in $\mathbb{R}$

Lemma $\mathbb{Q}$ can be embedded within $\mathbb{R}$ with the function h that maps x to $[\{(n, x) : n \in \mathbb{N}\}]$.

Proof. An embedding is a special type of injection (see appendix B for a definition of injection) that preserves structure. An injection that preserves structure in this case means the following:

1. h is an injection;
2. for all rationals x and y, $h(x + y) = h(x) + h(y)$;
3. for all rationals x and y, $h(x \times y) = h(x) \times h(y)$; and
4. for all rationals x and y, $x < y$ if and only if $h(x) < h(y)$.

$h(x) = [\{(n, x) : n \in \mathbb{N}\}]$, by definition. We will think of $g(x)$ to be the representative of the rational number x in "real number land." x and $h(x)$ are essentially identical where the word essentially precisely means that structure is preserved.

Proof of (1).

Proof of (2).

Proof of (3).

Proof of (4).◊

3.4.4 Exponentiation of Reals

basic exponent laws, real exponents

3.4.5 Further Properties of Real Numbers

Decimal expansions. .999...=1. Density of Q in R. Lub property

3.5 Complex Numbers

Euler's Identity

4 Counting and Infinities

In this section, I will describe a method by which finite sets can be counted which is extremely convenient to generalize to infinite sets. We first will take a look at what it means to be finite and infinite. The reader is encouraged to be familiar with the results mentioned in Appendix B on functions and equipollence prior to reading this section.

The highlight of this section is the result that states there is more than one "type" of infinity; moreover, there are infinitely many "types" of infinity.

Definition 4.1 Let $F_0 = \emptyset$ and for $n \in \mathbb{N}^+$, let $F_n = \{k \in \mathbb{N} : 1 \leq k \leq n\}$, i.e., $F_n = \{1, \ldots, n\}$. Let x be a set. We say that x is **finite** if and only if there is a natural number n for which x is equipollent to F_n. If x is finite and equipollent to F_n we say the **size** (or **cardinality**) of x is n.

For finite sets, their size is precisely the count of how many elements they have. As a simple example, if $x = \{a, b, c\}$ then note a correspondence given by $\{(a, 1), (b, 2), (c, 3)\}$ that shows that $\{a, b, c\}$ is equipollent to F_3.

Definition 4.2 We say that x is **infinite** precisely when it is not finite. This means that for all $n \in \mathbb{N}$, $x \not\approx F_n$.

Theorem 4.3 $\mathbb{N}$ is infinite.

Proof. We will show that every function $g \in [F_n \to \mathbb{N}]$ is not onto. That will imply that $\mathbb{N} \not\approx F_n$ for any $n \in \mathbb{N}$. To arrive at a contradiction, suppose that for a given n, $g \in [F_n \to \mathbb{N}]$ is onto. Then $\{g(1), ..., g(n)\} = \mathbb{N}$. Let $M = \mathsf{max}\{g(1), ..., g(n)\}$. Note that $\{g(1), ..., g(n)\} = g[F_n] \subseteq F_M$ but $F_M \subset \mathbb{N}$; so $g[F_n] \subset \mathbb{N}$, meaning that g is not onto.$\diamondsuit$

Something to keep in mind is that in formal set theory, one cannot prove that the collection of natural numbers is even a set without assuming what's known as the axiom of infinity. The axiom of infinity entails that the set of all natural numbers $\mathbb{N}$ exists.

Theorem 4.3 The following conditions are equivalent:

(A) x is infinite

(B) there is a proper subset y of x such that $x \sim y$ (when this happens, we say x is **Dedekind-infinite**)

(C) $\mathbb{N} \precsim x$ (This entails that there is no infinity smaller than $\mathbb{N}$.)

Proof. The order we will prove this equivalence is (B) implies (A) implies (C) implies (B); so there are three proofs in total.

(B) implies (A) In this step of the proof, we will assume (B) is true and use that assumption to prove (A). To arrive at a contradiction, suppose (A) is false, i.e., that $x \sim F_n$ for some $n \in \mathbb{N}$. (x can't be empty as the empty set has no proper subsets.) Let $g \in [F_n \to x]$ be a bijection. Then $x = \{g(1), ..., g(n)\}$. (B) implies there is a y a proper subset of x such that $x \sim y$. Without loss of generality, suppose y is one element less than x, and assume it is does not contain $g(1)$; i.e., suppose $y = \{g(2), ..., g(n)\}$. Note that $y \sim F_{n-1}$ and $x \sim F_n$ which implies $n-1 = n$, a contradiction. This contradiction shows that our assumption that (A) was false is incorrect, thus proving that (A) follows from (B).

(A) implies (C) In this step of the proof, we will assume (A) is true and use that assumption to prove (C).

(C) implies (B) In this step of the proof, we will assume (C) is true and use that assumption to prove (B). Let g be an injection in $[\mathbb{N} \to x]$. Define y to be the set of all elements of x minus the element $g(0)$. This is denoted

$x-\{g\left(0\right)\}$. Note that y is a proper subset of x; now we wish to show that $x\sim y$. Define a function $h\in[x\rightarrow y]$ as follows: given $u\in x$, let

$$h\left(u\right)=\begin{cases} g\left(n+1\right) \text{ if } u=g\left(n\right) \text{ for some } n\in\mathbb{N} \\ u \text{ otherwise} \end{cases}.$$

We will show that h is a bijection.$\diamondsuit$

Theorem 4.4 For every set X, $X\precnsim\mathcal{P}\left(X\right)$, meaning that X is not equipollent to $\mathcal{P}\left(X\right)$.

Proof We will show that no matter what function one has mapping X to $\mathcal{P}\left(X\right)$, that function cannot be onto. Let X be an arbitrary set and let $f\in[X\rightarrow\mathcal{P}\left(X\right)]$ be given. I claim that $D_f:=\{x\in X:x\notin f\left(x\right)\}$ is an element of $\mathcal{P}\left(X\right)$ not in the range of f, thus establishing that f is not onto. First note that D_f is a subset of X, so $D_f\in\mathcal{P}\left(X\right)$. To prove that D_f is not in the range of f, suppose for the moment that $f\left(x\right)=D_f$ where x is the element in X mapped to D_f by f. Notice that if, hypothetically speaking, $x\in f\left(x\right)$, then $x\in D_f$ as the two sets are equal. If $x\in D_f$ then by the definition of D_f, $x\notin f\left(x\right)$. Consequently, $x\in f\left(x\right)$ implies $x\notin f\left(x\right)$. Similarly, suppose that $x\notin f\left(x\right)$. Then since $f\left(x\right)=D_f$, $x\notin D_f$. x not being an element of D_f means that $x\in f\left(x\right)$, by the definition of D_f. Hence, $x\notin f\left(x\right)$ implies $x\in f\left(x\right)$. We now have that $x\in f\left(x\right)$ if and only if $x\notin f\left(x\right)$, a contradiction. The assumption that there is an element x mapped to D_f by f is wrong. Therefore, f is not a surjection. As f was arbitrary, there are no functions in $[X\rightarrow\mathcal{P}\left(X\right)]$ which are onto.$\diamondsuit$

Corollary 4.5 There are infinitely many types of infinity. **Proof.** Consider $\mathbb{N}$ which is infinite. $\mathcal{P}\left(\mathbb{N}\right)$ is not equipollent to $\mathbb{N}$, implying that $\mathcal{P}\left(\mathbb{N}\right)$ is a larger infinity than $\mathbb{N}$. Moreover, iteration of the power set operation leads to larger infinities. If we define $\mathcal{P}^n(\mathbb{N})$ recursively by saying$\mathcal{P}^{n+1}(\mathbb{N}) = \mathcal{P}(\mathcal{P}^n(\mathbb{N}))$, then the sequence $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}^2(\mathbb{N})$, $\mathcal{P}^3(\mathbb{N})$, etc., demonstrates a list of sets each with a larger type of infinity than the previous set in the list.$\diamondsuit$

Definition 4.6 We say a set X is **countably infinite** if X is equipollent to $\mathbb{N}$. We say X is **at most countable** if $X \precsim \mathbb{N}$. X is called **uncountable** if $\mathbb{N} \precnsim X$, meaning that $[\mathbb{N} \to X]$ contains at least one injection and contains no bijections.

Observe that every finite set is at most countable. Also, by theorem 4.4, $\mathcal{P}(\mathbb{N})$ is uncountable. By theorem 4.3 (C), every uncountable set is automatically infinite while at most countable sets need not be infinite.

Lemma 4.7 If $X \precsim Y$ and $Y \precsim Z$, then $X \precsim Z$. **Proof.** Compose the two injections to get an injection from X to Z.$\diamondsuit$

Theorem 4.8 An equivalence relation (see appendix A) on a countable set has at most countably many equivalence classes.

Proof. Let A be countable and E an equivalence relation on A. Consider the function f that maps $a \in A$ to the equivalence class $[a]_E$. f is a surjection, so the quotient set $A/E \precsim A$. Since $A \precsim \mathbb{N}$, it follows from lemma 4.7 that $A/E \precsim \mathbb{N}$; i.e., A/E is at most countable.$\diamondsuit$

Theorem 4.9 If A and B are at most countable then $A \times B$, the Cartesian product of A and B, is also at most countable.

Proof. If we can show that $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$, the result will follow. This is because $A \times B \precsim \mathbb{N} \times \mathbb{N} \precsim \mathbb{N}$ implies $A \times B \precsim \mathbb{N}$. We know that $\mathbb{N} \precsim \mathbb{N} \times \mathbb{N}$ by noting the function that maps n to $(n, 0)$ is 1-1. It remains to be seen that $\mathbb{N} \times \mathbb{N} \precsim \mathbb{N}$. In conjunction with $\mathbb{N} \precsim \mathbb{N} \times \mathbb{N}$, $\mathbb{N} \times \mathbb{N} \precsim \mathbb{N}$ would imply $\mathbb{N} \times \mathbb{N} \sim$

$\mathbb{N}$ by the Cantor–Bernstein–Schröder theorem (B.7). The following is, we claim, a 1-1 function in $[\mathbb{N} \times \mathbb{N} \to \mathbb{N}]$: $f(k,n) = 2^k \times (2n+1) - 1$.$\Diamond$

Theorem 4.10 $\mathbb{N} \sim \mathbb{Z} \sim \mathbb{Q} \precnsim \mathcal{P}(\mathbb{N}) \sim \mathbb{R} \sim \mathbb{C}$.

Proof.

5 Appendix A: Relations, Equivalence Relations, and Equivalence Classes

In this appendix, we will cover relations, equivalence relations, equivalence classes, and the quotient set (set of all equivalence classes). We will also mention partitions of sets which give rise to equivalence relations.

Definition A.1 A (binary) **relation** is any set of ordered pairs. See section 2.1 for a definition of "ordered pair."

I will now give two examples of relations. The first is a binary relation involving the first three letters of the alphabet. Let $R = \{(a,b), (a,c), (b,c)\}$, a set of three ordered pairs. Verbally, this relation can be phrased as "comes before (alphabetically)". $(a,b) \in R$ because a comes before b. $(a,c) \in R$ because a comes before c. $(b,c) \in R$ because b comes before c.

The second example is what is symbolized as $\leq$. An ordered pair consisting of two natural numbers is an element of the $\leq$ relation precisely if the first coordinate is less than or equal to the second coordinate. Symbolized formally, $\leq = \{(n,m) : n \textsf{ is less than or equal to } m\}$. Consequently, $(0,n) \in \leq$ for all natural numbers n because $0 \leq n$ for all natural numbers n.

Definition A.x Let R be a binary relation (i.e., any set of ordered pairs). Then the **domain** of R is the set of first coordinates of ordered pairs in R: $\mathsf{dom}(R) = \{x : \exists y\,(x,y) \in R\}$. The symbol $\exists$ means there exists, so $\{x : \exists y\,(x,y) \in R\}$ is the set of all x for which there exists a y such that $(x,y) \in R$. The **range** of R is the set of second coordinates of ordered pairs in R: $\mathsf{range}(R) = \{y : \exists x\,(x,y) \in R\}$.

If R is a relation, then the following two notations mean the same thing: $(x,y) \in R$ and xRy.

To be considered a relation, there are no restrictions on the ordered pairs themselves. Any set of ordered pairs is a (binary) relation. For example,

$$R' = \{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), (c,a), (c,b), (c,c)\}$$

is a relation as well. As the first few examples demonstrate, relations can be finite or infinite.

A basic but important relation is that of *equality*. For example, equality on $\mathbb{N}$ is the relation $=$ which is the set $\{(0,0), (1,1), (2,2), ...\}$. An ordered pair is an element of equality if and only if the first coordinate equals the second coordinate. Equality on $\{a,b,c\}$ is the following relation: $\{(a,a), (b,b), (c,c)\}$. This is so because $a = a$, $b = b$, and $c = c$.

Often in mathematics, such as several times in this document when concerning "building" new number sets from old ones, there are relations which capture the essence of equality yet are not the equality relation. The essence of equality involves the following three properties of equality:

A equality is *reflexive*, meaning that everything equals itself

B equality is *symmetric*, meaning that if $x = y$, then $y = x$

C equality is *transitive*, meaning that if $x = y$ and $y = z$, then $x = z$.

Definition A.2 A relation R is called an **equivalence relation** on the set X if all of the following three statements are true of all ordered pairs in R:

A R is **reflexive**, meaning that xRx for all $x \in X$

B R is **symmetric**, meaning that for all $x \in X$ and all $y \in X$, if xRy then yRx

C R is **transitive**, meaning that for all $x \in X$ and all $y \in X$ and all $z \in X$, if xRy and yRz, then xRz.

To illustrate this concept, let's look at the relations mentioned previously (plus some extras) and see which of them are equivalence relations.

$R = \{(a,b),(a,c),(b,c)\}$. This **is not** an equivalence relation because it is not reflexive. It is also not symmetric though it is transitive.

$\leq = \{(n,m) : n \text{ is less than or equal to } m\}$. This **is not** an equivalence relation. This relation is reflexive and transitive (check this) but not symmetric since $0 \leq 1$ but $1 \nleq 0$.

$< = \{(n,m) : n \text{ is less } m\}$. This **is not** an equivalence relation because it is not reflexive. It is also not symmetric.

$\mathbb{N} \times \mathbb{N} = \{(n,m) : n \in \mathbb{N} \text{ and } m \in \mathbb{N}\}$. This **is** an equivalence relation, somewhat trivially since all possible ordered pairs are elements of $\mathbb{N} \times \mathbb{N}$.

$R' = \{a,b,c\} \times \{a,b,c\} = \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\}$. This **is** an equivalence relation, somewhat trivially since all possible possible ordered pairs are elements of R'.

$R'' = \{(a,a),(a,b),(a,c),(b,b),(b,c),(c,c)\}$ ("does not come after [alphabetically]"). This **is not** an equivalence relation because a does not come after c but c does come after a.

$E_{\mathbb{N}} = \{(0,0),(1,1),(2,2),...\}$ (equality on $\mathbb{N}$). This **is** an equivalence relation. Essentially this is because equality amongst natural numbers is reflexive, symmetric, and transitive.

$E_{\{a,b,c\}} = \{(a,a),(b,b),(c,c)\}$ (equality on $\{a,b,c\}$). This **is** an equivalence relation for the same reason.

A perhaps more interesting example is a relation on $\mathbb{N}$ that is not equality. Let T_0 denote the set of all multiples of 3, T_1 is the set of all natural numbers that leave a remainder of 1 when divided by 3, and T_2 is the set of all natural numbers that leave a remainder of 2 when divided by 3. The the following is, we claim, an equivalence relation:

$$M = \{(n,m) : \text{there is a } k \text{ such that } n \in T_k \text{ and } m \in T_k\} .$$

In plain English, nMm if and only if they give they same remainder when divided by 3. For example, $(3,6) \in M$ because 3 and 6 have remainder 0 when divided by 3 but $(0,1) \notin M$ because 0 has remainder 0 when divided by 3 and 1 has remainder 1 when divided by 3. Note that M is reflexive since $(n,n) \in M$ for all natural numbers n, n and n both have the same remainder when divided by 3. If n and m have remainder k when divided by 3, then m and n have remainder k when divided by 3; so M is symmetric. M is transitive since if we assume nMm and mMo, that means n and m have the same remainder when divided by 3 and m and o have the same remainder when divided by 3. n and o therefore have the same remainder when divided by 3 because both of their remainders equals the remainder of m when divided by 3. Another way to look at M is that $(n,m) \in M$ if and only if $n - m$ is divisible by 3 (no remainder), which is equivalent to $m - n$ being divisible by 3.

Definition A.3 Given a set x and a natural number $n \geq 2$, then x is called an **n-ary relation** if it is a set of ordered n-tuples. Ordered n-tuples look like this: $(x_1, x_2, \ldots x_n)$. Sets of ordered n-tuples are called n-ary relations. There can also be unary relations ($n = 1$) which are "ordered 1-tuples" which are naturally in correspondence with the elements of the set.

We will now move on to what are known as equivalence classes. Equivalence classes play a critical role in our treatment of ascending number sets.

Definition A.4 Let X be a given set and R an equivalence relation where $R \subseteq X \times X$. (For a definition of the Cartesian product of a set, see section 2.1.) Then each element $x \in X$ gives rise to an **equivalence**

class, denoted $[x]$, which is defined to be the set of elements in X which are R-equivalent to x. Symbolically, $[x] = \{y \in X : xRy\}$.

A set J is an equivalence class if there is an equivalence relation R and some some set X, with $R \subseteq X \times X$, and all elements of J are R-equivalent to each other. In other words, for all u and v elements of J, we have uRv. Note that $J \subseteq X$. The definition of equivalence class is predicated on R not just being any old relation but an *equivalence* relation.

I should mention that there are many different notations seen in practice for equivalence classes, such as $\overline{x}$, $\langle x \rangle$, and when we need to be specific, then we will write $[x]_R$.

Examples. Let's examine the equivalence relations above and look at the related equivalence classes. Five equivalence relations were given.

$\mathbb{N} \times \mathbb{N}$ is an equivalence relation in which every element of $\mathbb{N}$ is equivalent to every other element of $\mathbb{N}$. Instead of $\mathbb{N} \times \mathbb{N}$, let's call this equivalence relation R_0. Note that for all natural numbers n and m, $(n, m) \in R_0$. Thus, in particular, for all natural numbers m, $(0, m) \in R_0$. The equivalence class that 0 belongs to is $[0]_{R_0} = \{m \in \mathbb{N} : (0, m) \in R_0\}$. Consequently, $[0]_{R_0} = \mathbb{N}$ and, moreover, for all $n \in \mathbb{N}$, $[n]_{R_0} = \mathbb{N}$ by the same argument. Thus, there is only one equivalence class given rise to by the equivalence relation R_0, the entire set of natural numbers.

Now let's consider $R' = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$. This situation is similar to the previous one involving $\mathbb{N} \times \mathbb{N}$. Let's call the *abc* set A. Note that for all ordered pairs of elements of A are elements of R'. Thus, in particular, for a, b, and c, we have $(a, a) \in R'$, $(a, b) \in R'$, and $(a, c) \in R'$. The equivalence class that a belongs to is $[a]_{R'} = \{a, b, c\}$. Consequently, $[a]_{R'} = A$ and, moreover, $[b]_{R'} = A$ and $[c]_{R'} = A$ by the same argument. Thus, there is only one equivalence class given rise to by the equivalence relation R', the entire set $\{a, b, c\}$.

Equality on a set goes to the opposite extreme where the equivalence classes are as small as they possibly could be, in contrast to the above two situations where the equivalence classes are as large as they possibly could be. Consider $E_{\mathbb{N}} = \{(0,0), (1,1), (2,2), ...\}$ (equality on $\mathbb{N}$). Then the only thing $E_{\mathbb{N}}$-equivalent to 0 is 0. Thus, $[0]_{E_{\mathbb{N}}} = \{0\}$ and, moreover, for all natural numbers n, $[n]_{E_{\mathbb{N}}} = \{n\}$ as the only natural number equal to n is n. Here, each equivalence class has only *one* element of $\mathbb{N}$, in contrast to the previous two examples in which there was only one equivalence class, having *all* elements of the ground set. A similar situation holds for E_A where A is again $\{a, b, c\}$. Then the only thing E_A-equivalent to a is a. Thus, $[a]_{E_A} = \{a\}$ and, moreover, $[b]_{E_A} = \{b\}$ and $[c]_{E_A} = \{c\}$. In this situation, there are three equivalence classes, each with one element.

There are many interesting situations between these two extremes; these situations are when an equivalence relation is neither the set of all ordered pairs nor equality. A typical example of this is our relation M defined above, having to do with division by 3. Let's examine $[0]_M$. By definition, $[0]_M = \{n \in \mathbb{N} : (0, n) \in M\}$. That is, $[0]_M = \{n \in \mathbb{N} : n - 0 \text{ is divisible by } 3\}$ which reduces to $[0]_M = \{n \in \mathbb{N} : n \text{ is divisible by } 3\}$ which is the set of all multiples of 3, namely $[0]_M = \{0, 3, 6, 9, 12, ...\}$. By definition, $[1]_M = \{n \in \mathbb{N} : (1, n) \in M\}$. That is, $[1]_M = \{n \in \mathbb{N} : n - 1 \text{ is divisible by } 3\}$ which is the set of all natural numbers that give remainder 1 when divided by 3, namely $[1]_M = \{1, 4, 7, 10, 13, ...\}$. Similarly, $[2]_M = \{2, 5, 8, 11, 14, ...\}$. At this point, it is crucial to observe what happens when we examine $[3]_M$. Since $3 \in [0]_M$, $[3]_M = [0]_M$. Similarly, $[4]_M = [1]_M$ and $[5]_M = [2]_M$. So we have already found all of the equivalence classes generated by M. There are three distinct equivalence classes, each containing infinitely many elements.

Now we proceed to the definition of quotient sets. A quotient set is the set of all equivalence classes for a given equivalence relation. Quotient sets play a critical role in our development of number sets. After the natural numbers, every more complicated number set (except for the complex numbers) is a certain quotient set with respect to a particular equivalence relation. See in particular sections 3.2, 3.3, 3.4, and 3.6.

Definition A.4 Let X be a set and R and equivalence relation on X (so $R \subseteq X \times X$). The **quotient set** denoted X/R is defined to be the set of all R-equivalence classes, namely $X/R = \{[x]_R : x \in X\}$.

Note that for all $x \in X$, $[x]_R \subseteq X$, so X/R is a set of elements each of whom are subsets of X.

Examples. Sections 3.2, 3.3, 3.4, and 3.6 all contain interesting examples of quotient sets when the equivalence relations in question are neither the full set of ordered pairs nor are equality. Let's look at the quotient sets of the equivalence relations mentioned in this appendix. Our first example is the equivalence relation R_0 on $\mathbb{N}$. We established that there is only one equivalence class, the entire set of natural numbers $\mathbb{N}$. Therefore, $\mathbb{N}/R_0 = \{\mathbb{N}\}$. Our second, similar example is the equivalence relation R' on $A = \{a, b, c\}$. Again there is only one equivalence class, so $A/R' = \{A\}$. The third example involves an equivalence relation M that is neither the entire set of ordered pairs $\mathbb{N}\times\mathbb{N}$ nor is equality. We found earlier that there are three equivalence classes: $[0]_M$, $[1]_M$, and $[2]_M$. Therefore, $\mathbb{N}/M = \{[0]_M, [1]_M, [2]_M\}$, a three-element set. (Note that each element in $\mathbb{N}/M$ is an infinite set.)

Instead of starting with an equivalence relation and from it derive a set of equivalence classes, one can first partition a set and from that derive an equivalence relation.

Definition A.5 Let X be a set. Then P is called a **partition** of X if $P \subseteq \mathcal{P}(X)$ and P is pairwise disjoint, meaning that for all elements A and B of P, $A \neq B$ implies $A \cap B = \emptyset$, X is equal to the set of elements of elements of P (called the union of P, denoted $\bigcup P$), and, finally, no set in the partition P is allowed to be empty.

Let me give two concrete examples of partitions to illustrate the concept. First, consider the set $X = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Then the following set is a partition of X:

$$P = \{\{0, 2, 4, 6\}, \{1, 3, 5\}, \{7\}\}.$$

Note that P is a set of sets, each of which is a subset of X, so $P \subseteq \mathcal{P}(X)$. Note that among the elements of P, all of them have no overlap so P is pairwise disjoint. And all elements of X are "used" in P so we have $\bigcup P = X$. There are many different ways to partition X.

The second example involves our relation M having to do with division by 3. Recall that $[0]_M = \{0, 3, 6, ...\}$, $[1]_M = \{1, 4, 7, ...\}$, and $[2]_M = \{2, 5, 8, ...\}$. Notice that all natural numbers are in exactly one of these three sets. Then $P = \{[0]_M, [1]_M, [2]_M\}$ is a partition of $\mathbb{N}$. In other words, $\mathbb{N}/M$ is a partition of $\mathbb{N}$. This happens in general as the next theorem states.

Theorem A.6 (Fundamental Theorem Of Equivalence Relations) If R is an equivalence relation on X then X/R is a partition of X.

Proof. Our proof is an adaptation of the following proof:http://www.proofwiki.org/wiki/Fundamental_Theore

As the next theorem will state, we can also go backwards: start with a partition and define an equivalence relation in which two elements are equivalent if they are in the same partition.

Theorem A.7 Let X be a set and P a partition of X. Then the relation

$$R_P = \{(x_1, x_2) \in X \times X : \exists p \in P\,(x_1 \in p \wedge x_2 \in p)\}$$

is an equivalence relation on X such that $X/R_P = P$.

Let me explain the notation used to define R_P. R_P is the set of ordered pairs in $X \times X$ such that there is a partition that both coordinates of the ordered pair are in. The symbol $\exists$ means "there exists" and the symbol $\wedge$ denotes "and." Consequently, the ordered pair (x_1, x_2) is an element of R_P if and only if there exists some set p in the partition P such that both $x_1 \in p$ and $x_2 \in p$. That means that $x_1 R_P x_2$ if and only if x_1 and x_2 are in the same partition.

Proof of Theorem A.7 Our proof is an adaptation of the following proof:

http://www.proofwiki.org/wiki/Relation_Induced_by_Partition_is_Equivalence

It is sometimes useful to start with a relation that isn't an equivalence relation and extend it to an equivalence relation by adding ordered pairs to the original relation.

Theorem A.8 Let X be a set and $R \subseteq X \times X$ a relation. Then there is a smallest equivalence relation R^+ on X containing R. Symbolically, this can be stated as follows: There exists a set R^+ such that

- $R^+ \subseteq X \times X$, $R \subseteq R^+$, and R^+ is an equivalence relation
- If there is an S such that $S \subseteq X \times X$, $R \subseteq S$, and S is an equivalence relation, then $R^+ \subseteq S$.

Proof http://www.proofwiki.org/wiki/Transitive_Closure_Always_Exists_%28Relation_Theory%29

Call the transitive closure of R R^t. Let n be a natural number. Define $R^0 = R$ and for $n > 0$, R^n is defined to be

$$R^{n-1} \cup \left\{(x_1, x_3) : \exists x_2 \left((x_1, x_2) \in R^{n-1} \wedge (x_2, x_3) \in R^{n-1}\right)\right\}.$$

Finally, R^t is defined to be the union of the R^n's: $R^t = \bigcup_{n \in \mathbb{N}} R^n$. This is proved to be a closure in the link.

Now will will look at the reflexive closure and symmetric closure of R. The reflexive closure will just start with R and add to it all ordered pairs of the form (x, x). Symbolically, the reflexive closure of R, which I will denote by R^r. $R^r = R \cup \{(x, x) : x \in \mathsf{dom}\,(R) \cup \mathsf{range}\,(R)\}$. Need to show that this really is a closure.

Next, we will look for a symmetric closure R^s of R. Let $R^s = R \cup \{(y, x) : (x, y) \in R\}$. Need to show that this is really a closure.

Finally, we will prove that $\left((R^t)^r\right)^s$ is the desired equivalence relation R^+. Need to show that $R^+ = \left((R^t)^r\right)^s$ satisfied conditions of the theorem. Explain.$\diamondsuit$

Let's look at some specific examples of the principle summarized in theorem A.8 that arbitrary sets of ordered pairs can be "fleshed out" into a smallest set of ordered pairs that is an equivalence relation and contains the arbitrary set. We mentioned some examples of relations that are not equivalence relations. For instance, consider the relation $R = \{(a, b), (a, c), (b, c)\}$. This **is not** an equivalence relation because it is not reflexive. It is also not symmetric though it is transitive. Let $A = \{a, b, c\}$. What is the smallest equivalence relation on A that extends R? First we will calculate R^t, the transitive closure of R. $R^0 = R = \{(a, b), (a, c), (b, c)\}$. $R^1 = R^0 \cup \left\{(x_1, x_3) : \exists x_2 : (x_1, x_2) \in R^0 \wedge (x_2, x_3) \in R^0\right\}$ which is $\{(a, b), (a, c), (b, c)\} \cup \{(a, c)\}$. But this last set equals R; so the transitive closure of R is R. This is because R is transitive already. So $R^t = R = \{(a, b), (a, c), (b, c)\}$. Now let's look at the reflexive closure. The domain of R is $\{a, b\}$ and the range of R is $\{b, c\}$. Then we will add the following ordered pairs to R to form the reflexive closure: (a, a), (b, b), and (c, c). So $(R^t)^r = R \cup \{(a, a), (b, b), (c, c)\} = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)\}$.

Finally, the symmetric closure $\left((R^t)^r\right)^s$ is $(R^t)^r \cup \left\{(y,x) : (x,y) \in (R^t)^r\right\} =$

$\{(a,a),(a,b),(a,c),(b,b),(b,c),(c,c)\} \cup \{(a,a),(b,a),(c,a),(b,b),(c,b),(c,c)\}.$

Thus,

$$R^+ = \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\} = A \times A$$

$A \times A$ is a rather simple equivalence relation but it is one nonetheless.

6 Appendix B: Functions

The reader is encouraged to be familiar with section 1 on sets and familiar with the definition of relation in appendix A prior to reading this section.

Definition B.1 A **function** is a relation such that no two distinct ordered pairs in the relation share the same first coordinate. (There are a few synonyms for the word function, including "map" and "mapping".)

Notation Given the defining trait of functions, for each first coordinate in the function, there is only one second coordinate associated with it. So if f is a function, we can say $f(x)$ (read "f **of** x") means the second coordinate whose first coordinate is x.

Examples. Let $f_1 = \{(0,1), (1,2), (2,3), (3,4), ...\}$. Notice that f_1 is a relation such that no two distinct ordered pairs in the relation share the same first coordinate; so f_1 is a function. In algebraic terms, here we have a function for which there is a simple formula: $f_1(x) = x + 1$. When we write something like $g(x) = 2x$, that is code for defining g to be $g = \{(x, 2x) : x \in X\}$. Another example of a function is this: T=\{(green, go), (yellow, go), (red, stop)\}. Observe that T(green) = go, T(yellow) = go, and T(red) = stop.

In light of the examples, one can view a function as a rule that assigns a 2nd coordinate to every 1st coordinate. Moreover, one can also view functions as machines that have inputs and outputs. The inputs of a function are its 1st coordinates and the outputs of a function are its 2nd coordinates. The function f_1 can be viewed as "the successor machine" that assigns the output natural number $x + 1$ to the input natural number x.

Given that every function is a relation, the definitions for domain and range are carried over from relation theory.

The set of all functions from X to Y is denoted $[X \to Y]$ and we will sometimes write $f : X \to Y$ if we mean that $f \in [X \to Y]$.

There are several types of functions which are important with respect to infinite sets, among other things.

Definition B.2 Let X and Y be sets and suppose $f \in [X \to Y]$. Then f is called **one-to-one** if different inputs lead to different outputs. This can be restated as f is one-to-one if for all x_1 and x_2, if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Observe that f is one-to-one if and only if $\{(y, x) : (x, y) \in f\}$ (called the **inverse** of f) is a function. We also use the word **injection** to describe a one-to-one function and we also write **1-1** instead of one-to-one.

Examples Our functions f_1 and g are injections because their inverses are functions. However, T is not an injection because the inverse of T is the relation {(go, green), (go, yellow), (stop, red)} and the first two ordered pairs are distinct and share the same first coordinate. Since the inverse of T is not a function, T is not an injection.

Definition B.3 Let X and Y be sets and suppose $f \in [X \to Y]$. Then f is called **onto** if the range of f equals Y. This means every element in Y has a corresponding input in X that is mapped to by f. This can be restated as follows: f is onto if and only if it is the case that $\forall y \in Y \exists x \in X\, (f(x) = y)$. In English, that statement reads, "for all y in Y there is an x in X such that $f(x) = y$." We also use the word **surjection** to describe an onto function.

Definition B.4 Let X and Y be sets and suppose $f \in [X \to Y]$. Then f is called a **one-to-one correspondence** (or 1-1 correspondence) if and only if it is both 1-1 and onto. We will also say that f is a **bijection**.

Example. Let $F_0 = \emptyset$ and for $n \in \mathbb{N}^+$ (the positive natural numbers), let

$F_n = \{k \in \mathbb{N} : 1 \leq k \leq n\}$, i.e., $F_n = \{1, \ldots, n\}$. Let's examine the sets $F_2 = \{1, 2\}$ and $F_3 = \{1, 2, 3\}$. A relation R is any subset of $F_2 \times F_3 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$. As $F_2 \times F_3$ has six elements, there are $2^6 - 1 = 63$ different nonempty relations. In order for a function to be an element of $[F_2 \to F_3]$, it must have precisely two ordered pairs, one for each element in the domain. Each of those two ordered pairs can have any value in F_3; so there are nine functions in $[F_2 \to F_3]$ given below:

1. $\{(1,1), (2,1)\}$. This function is not an injection and not a surjection. It is not an injection because two distinct ordered pairs share the same first coordinate. It is not a surjection because 2 is not in the range of this function. (Nor is 3 in the range.)

2. $\{(1,1), (2,2)\}$. This function is 1-1 because the inverse of this, which happens to equal itself, is a function. This function is not onto because 3 is not the second coordinate of any ordered pair in this function.

3. $\{(1,1), (2,3)\}$. This function is also 1-1 but not onto as 2 is not the second coordinate of any ordered pair in this function.

4. $\{(1,2), (2,1)\}$. This function is also 1-1 but not onto as 3 is not the second coordinate of any ordered pair in this function.

5. $\{(1,2), (2,2)\}$. This function is not 1-1 because the inverse table $\{(2,1), (2,2)\}$ is not a function (it's just a relation). It is also not onto because 1 is not the second coordinate of any ordered pair in this function. (Neither is 3 but all we need to prove not onto is one example.)

6. $\{(1,2), (2,3)\}$. This function is 1-1 but not onto since 1 is not the second coordinate of any pair in the function.

7. $\{(1,3),(2,1)\}$. This function is 1-1 but not onto since 2 is not the second coordinate of any pair in the function.

8. $\{(1,3),(2,2)\}$. This function is 1-1 but not onto since 1 is not the second coordinate of any pair in the function.

9. $\{(1,3),(2,3)\}$. This function is not 1-1 because 3 is the output of two different inputs and it's not onto since 1 is not the second coordinate of any pair in the function.

There are a few observations here. The first is that some functions in $[F_2 \to F_3]$ are 1-1 but not every function in $[F_2 \to F_3]$ is 1-1. Also, and perhaps more importantly, $[F_2 \to F_3]$ **contains no onto functions.** That entails that **no** function in $[F_2 \to F_3]$ is a bijection. It certainly seems reasonable to surmise that there aren't any surjections because F_3 has more elements than F_2.

We will do two more examples, one in which we examine $[F_3 \to F_2]$ and another in which we examine $[F_2 \to F_2]$.

A function in $[F_3 \to F_2]$ must consist of three ordered pairs where the 2nd coordinate is chosen among $\{1,2\}$ and 1st coordinate is chosen among a three-element set. Therefore, there are $2 \times 2 \times 2 = 8$ functions in $[F_3 \to F_2]$. As we did before, we will investigate all of these eight functions and see what we come up with. Elements of $[F_3 \to F_2]$ can be listed:

1. $\{(1,1),(2,1),(3,1)\}$. This function is not 1-1 nor onto.

2. $\{(1,1),(2,1),(3,2)\}$. This function is not 1-1 but it is onto since both elements of F_2 are outputs.

3. $\{(1,1),(2,2),(3,1)\}$. This function is not 1-1 because the inverse is not a function. This function is onto.

4. $\{(1,2),(2,1),(3,1)\}$. This function is not 1-1 but it is onto.

5. $\{(1,1),(2,2),(3,2)\}$. This function is not 1-1 but it is onto.

6. $\{(1,2),(2,1),(3,2)\}$. This function is not 1-1 but it is onto.

7. $\{(1,2),(2,2),(3,1)\}$. This function is not 1-1 but it is onto.

8. $\{(1,2),(2,2),(3,2)\}$. This function is not 1-1 but it is onto.

Observe that some functions in $[F_3 \to F_2]$ are onto but not every function in $[F_3 \to F_2]$ is onto. Also, and perhaps more importantly, $[F_3 \to F_2]$ **contains no 1-1 functions.** That entails that **no** function in $[F_3 \to F_2]$ is a bijection. It certainly seems reasonable to surmise that there aren't any injections because F_3 has more elements than F_2.

We will do this one more time with the function set $[F_2 \to F_2]$ and find a markedly different outcome compared to the previous two examples. This time, $[F_2 \to F_2]$ has four elements:

1. $\{(1,1),(2,1)\}$. This function is neither 1-1 nor onto.

2. $\{(1,1),(2,2)\}$. This function is both 1-1 and onto. Hence this function is a bijection.

3. $\{(1,2),(2,1)\}$. This is also a bijection.

4. $\{(1,2),(2,2)\}$. This function is neither 1-1 nor onto.

Observe that some functions in $[F_2 \to F_2]$ are bijections and some are neither injections nor surjections. In the previous two examples, there were no bijections and one can reasonably surmise that there aren't going to be any bijections if the two sets have a different number of elements.

Definition B.5 Let X and Y be sets. We say X is **equipollent** to Y and write $X \sim Y$ if there is a bijection $f \in [X \to Y]$.

The intuition with equipollence is that if there is a one-to-one correspondence between the elements of X and Y, then they have the same number of elements.

Theorem B.6 Let X and Y be sets. Then the following two statements are equivalent:

(A) $[X \to Y]$ contains an injection

(B) $[Y \to X]$ contains a surjection.

Proof (A) implies (B) Let $f \in [X \to Y]$ be an injection. Then f^{-1} the inverse of f (given by $\{(y,x) : (x,y) \in f\}$) is a function. Let $f[X] = \{y \in Y : \exists x \in X\, ((x,y) \in f)\}$, the set of elements of Y which are outputs for some element x in X. Note that $f[X] \subseteq Y$. Define a function $g \in [Y \to X]$ as follows: if $y \in f[X]$ let $g(y) = f^{-1}(y)$ and if $y \notin f[X]$ then define $g(y)$ to be any fixed element x^* of X. To show that g is onto, let x be any element of X. $f(x)$ is the element in Y that g maps to x.

Proof (B) implies (A) Let $g \in [Y \to X]$ be a surjection. Let $x \in X$ be given; we wish to define $f(x)$ and prove that f is 1-1. Let $g^{-1}[\{x\}] = \{y \in Y : g(y) = x\}$. Define $f(x)$ to be any arbitrarily chosen element of $g^{-1}[\{x\}]$. The axiom of choice tells us that since $\left\{g^{-1}[\{x\}] : x \in X\right\}$ is a collection of nonempty sets (nonempty because g is onto), there is a set C such that for all $x \in X$, $C \cap g^{-1}[\{x\}]$ is a single element in $g^{-1}[\{x\}]$. So we will define $f(x)$ to be the element in $C \cap g^{-1}[\{x\}]$. Need to show that f is 1-1.$\diamondsuit$

A **corollary** to theorem B.6 is that the following are also equivalent:

(A) $[X \to Y]$ contains no injections

(B) $[Y \to X]$ contains no surjections.

Notation When $[X \to Y]$ contains an injection or, equivalently when $[Y \to X]$ contains a surjection , we write $X \precsim Y$. Given our examples above, we would say that $F_2 \precsim F_3$ because $[F_2 \to F_3]$ contains at least one injection. An alternative reason why we would say that $F_2 \precsim F_3$ is because $[F_3 \to F_2]$ contains at least one surjection.

Theorem B.7 (Cantor–Bernstein–Schröder) Let X and Y be sets. If $X \precsim Y$ and $Y \precsim X$ then $X \sim Y$. This theorem states that if $[X \to Y]$ and $[Y \to X]$ both contain at least one injection, then $[X \to Y]$ contains at least one bijection.

A proof of this theorem can be found here.

iteration of functions (to help reinforce the definition of n+m)

sequences as functions

7 References

author, title, publisher, year

1. Karel Hrbacek and Thomas Jech, *Introduction to Set Theory* (3rd ed), Marcel Dekker, Inc., 1999.

2. Wikipedia http://en.wikipedia.org/wiki/Venn_diagram

3. http://en.wikipedia.org/wiki/Axiom_of_choice

4. http://www.proofwiki.org