University of Oslo
Real Analysis - MAT2400
Spring 2015

Ivar Stangeby

April 4, 2015

Abstract

This document is going to be a way for me as a student of MAT2400 at the University of Oslo to gather my thoughts around the course Real Analysis. I've struggled with my intuition for this subject, and this is a last ditch effort to build it all up from scratch.

For this task, I've decided to use the text books written by Terence Tao, namely Analysis I and II. There is absolutely nothing wrong with the text book offered at my university, it is brilliantly written, but I have been exposed to the writings of Terence Tao before, and therefore I wish to give his books a try.

The first part of this document related to the book Analysis I, is going to be mostly involved in building a solid foundation for the concepts discussed in Analysis II. The material included from Analysis I is very similar to the curriculum of the subject MAT1140 at the University of Oslo.

The structure of this document is going to be me writing down the results encountered throughout the text books along the proofs I find extra intriguing. I'm going to attempt to prove the theorems myself, and if I find it reasonable I'm going to write down my own proof. Included will also be my attempted solutions to selected exercises.

This document is mainly for my own good and well being, but if anyone can find any use from them, then that is great.

Contents

Chapter 1

Introduction

Chapter 2

Starting at the beginning: the natural numbers.

In order for us to start exploring the various properties of the real numbers, which is what real analysis is concerned with, we are going to have to start from the very beginning. That is the natural numbers, denoted $\mathbb{N}$. From these natural numbers, we can construct the integers, $\mathbb{Z}$, the rationals $\mathbb{Q}$, the real numbers $\mathbb{R}$, and finally; the complex numbers $\mathbb{C}$. The latter being the main focus of the subject Complex Analysis.

2.1 The Peano axioms

One of the most standard ways of defining the natural numbers, is in terms of the *Peano axioms.* One can also define natural numbers through the notion of cardinality.

Definition 2.1.1 (Informal)**.** A *natural number* is any element of the set

$$\mathbb{N} = \{0, 1, 2, 3, 4, \cdots\},$$

which is the set of all the numbers created by starting with 0 and then counting forward indefinitely. We call $\mathbb{N}$ the *set of all natural numbers.*

In order for us to rigorously define the set of natural numbers, we're going to use the two fundamental concepts of *the number 0* and the *increment operation.* These will be covered in the Peano Axioms. We will use n++ to denote the *successor* of n.[1]

Starting with the first two:

Axiom 2.1. *0 is a natural number.*

Axiom 2.2. *If n is a natural number, then n++ is also a natural number.*

Now, in order to avoid having to deal with incredibly long strings of +'es. We're going to use an auxilliary definition.

Definition 2.1.3. We define 1 to be the number 0++, 2 to be the number (0++)++, etc.

We can based off of this, propse the following:

Proposition 2.1.4. *3 is a natural number.*

Proof. By Axiom 1, 0 is a natural number. It then follows by Axiom 2 that both 1, 2, and 3 are natural numbers. □

In order for us to avoid the problem of having the successive numbers wrap around to previous numbers, we impose a new axiom, namely:

Axiom 2.3. *0 is not the successor of any natural number: i.e., we have $n{+}{+} \neq 0$ for every natural number n.*

We can, equipped with this new axiom, show for example the following:

Proposition 2.1.6. 4 *is not equal to* 0*.*

Proof. By definition, $4 = 3{+}{+}$. By the first two axioms, 3 is a natural number. Thus, since 0 is not the successor of any natural number, $3{+}{+} \neq 0$, i.e., $4 \neq 0$. □

[1] When I've previously encountered the successor of a natural number, it has been described in terms of a successor function S, where $S(n)$ denotes the successor of n.

Assuming the following axiom allows us to rule out any behaviour where the successors wrap around, but not to 0, i.e., $5{+}{+} = 1$.

Axiom 2.4. *Different natural numbers must have different successors; i.e., if n, m are natural numbers and $n \neq m$, then $n{+}{+} \neq m{+}{+}$. Equivalently, if $n{+}{+} = m{+}{+}$, then we must have $n = m$.*

We can now prove extensions of the previous proposition where we do not have zeroes on the right hand side of the equation.

Proposition 2.1.8. 6 *is not equal to* 2.

Proof. Assume for contradiction that $6 = 2$. By the previous axiom we must have $5{+}{+} = 1{+}{+}$. Applying the same axiom again, we have $5 = 1$ so that $4{+}{+} = 0{+}{+}$. But, this leads to a contradiction, because by the same axiom, $4 = 0$. This contradicts our previously proven proposition. □

Assume now that we are presented with a weird number system

$$\mathbb{N} = \{0, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, \dots\}.$$

Even though this set contains real numbers, which we haven't defined or talked about yet, it satisfies all the previous axioms. But this is not the number system we're interested in. We want our set of natural numbers to only be containing all the numbers that can be directly derived from 0 just using the successor operation.

We want to introduce some axiom that does not allow other forms of successors to occur. Therefore we introduce the following:

Axiom 2.5 (Principle of mathematical induction)**.** *Let $P(n)$ be any property pertaining to a natural number n. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(n{+}{+})$ is also true. Then $P(n)$ is true for every natural number n.*

We're now equipped with the tools required to deal with propositions of the following form:

Proposition 2.1.11. *A certain property $P(n)$ is true for every natural number n.*

Proof. Using induction, we show the base case of $P(0)$. Assume, for the sake of induction, that $P(n)$ is true. We now want to show that it has to follow that $P(n{+}{+})$ also must be true. If this is the case, we have shown, using mathematical induction that $P(n)$ is true for every natural number n. □

The previous five axioms are known as the *Peano Axioms* for the natural numbers. We now want to more rigorously define the kind of number system we are to refer to as the *natural numbers.*

Assumption 2.6 (Informal)**.** *There exists a number system $\mathbb{N}$, whose elements we will call natural numbers, for which Axioms 1-5, are true.*

This number system is what we refer to as *the* natural number system. But one should not rule out the possibility that there are more than one natural number system. But as long as these are *isomorphic* one can consider them as equal.

With only this, rather simplistic definition of natural numbers, the five axioms, and some axioms from set theory we can build all other number systems, create functions and do the algebra and calculus that we are used to.

A very common question now arises, and this is about the finiteness or infiniteness of the natural number system. How can something infinite come from something strictly finite? One can easily show that all the natural numbers are finite. It is clear that 0 is finite. If n is finite, then clearly $n{+}{+}$ is finite. Therefore all natural numbers are finite. It then follows that infinity is not a natural number. There are other number systems that admit the infinite numbers.

It is an interesting fact that the definition of $\mathbb{N}$ is *axiomatic* rather than *constructive.* This means, that so far we're only conserned with what the natural numbers are, not what they do, what they measure or what they can be used for.

As long as a mathematical model obeys the previous axioms, it is of no concern whether which mathematical model is "true". It is this form of *abstractness* that makes mathematics so useful. One does not neccesarily need a concrete model, because the numbers can be understood abstractly through the use of axioms.

As a consequence of the axioms previously discussed, we can now define sequences *recursively.* That is, start with some base value and then building the next value in the sequence by means of a function. This leads to the following:

Proposition 2.1.16 (Recursive definitions)**.** *Suppose for each natural number n, we have some function $f_n : \mathbb{N} \to \mathbb{N}$ from the natural numbers to the natural numbers. Let c be a natural number.*

Then we can assign a unique natural number a_n to each natural number n, such that $a_0 = c$ and $a_{n++} = f_n(a_n)$ for each natural number n.

Proof. Using induction, we verify the base case. We clearly see that this procedure gives a single value to a_0, namely c. (We know from axiom 3 that a_0 won't be redefined.) Suppose now inductively that the procedure gives a single value to a_n. Then it gives a single value to a_{n++}, namely $a_{n++} = f_n(a_n)$. (We know from axiom 4 that a_{n++} won't be redefined.) This completes the induction, since a_n is defined for every natural number n, with a single value assigned to each a_n. □

Equipped with the tools that are recursive definitions we can now define multiple operations on the set of natural numbers. Up until now, we've only dealt with one, being the increment operation.

2.2 Addition

Currently our number system does not support any more advanced operations than incrementing a number. We now turn our heads to addition. The operation is simple. To add 3 to 5, we simply increment 5 three times. This is one increment more than adding 2 to 5, which is one increment more than adding 1 to 5, which is one increment more than adding 0 to 5. We can therefore easily give a recursive definition of addition.

Definition 2.2.1 (Addition of natural numbers)**.** Let m be a natural number. To add zero to m, we define $0+m = m$. Now suppose inductively that we have defined how to add n to m. Then we can add $n{+}{+}$ to m by defining $(n{+}{+}) + m = (n+m){+}{+}$.

For example, $2 + 3 = (3{+}{+}){+}{+} = 4{+}{+} = 5$. By using the priciple of mathematical induction, we see that we now have defined $n + m$ for every natural number n. We are specializing the previous general discussion about recursive definitions to the setting where $a_n = n + m$, and $f_n(a_n) = a_n{+}{+}$.

It's worth noting that this definition is actually *asymmetric*. That is, while yielding the same result, $3 + 5$ is incrementing 5 three times, where as $5 + 3$ is incrementing 3 five times. We shall soon see, that it is a general fact that $a + b = b + a$ for all natural numbers a, b.

One can easily prove, using the first two axioms and the principle of mathematical induction to show that the sum of two natural numbers is again a natural number.

At the present moment, we have only two facts about addition. However, this is perfectly sufficient to deduce everything else we know about addition. Starting with some basic lemmas.

Lemma 2.2.2. *For any natural number n, $n+0 = n$.*

This lemma is not obvious from our previous definition, since we still do not know that $a+b = b+a$.

Proof. Using induction. The base case $0 + 0 = 0$ follows from the definition of addition of natural numbers. $0 + m = m$ for all natural numbers, and 0 is known to be a natural number. Suppose inductively that $n + 0 = n$. We now wish to show that $(n{+}{+}) + 0 = n{+}{+}$. By definition of addition yields that $(n{+}{+}) + 0$ is equal to $(n + 0){+}{+}$, which is equal to $n{+}{+}$ since $n + 0 = n$. This closes the induction. □

Lemma 2.2.3. *For any natural numbers n and m, $n + (m{+}{+}) = (n + m){+}{+}$.*

Again, this is not obvious.

Proof. We induct on n, keeping m fixed. Considering the base case $n = 0$. We therefore have to prove $0 + (m{+}{+}) = (0 + m){+}{+}$. By definition of addition, we have $0 + (m{+}{+}) = m{+}{+}$ and $0 + m = m$. So, both sides are equal to $m{+}{+}$ and are thus equal. Assuming now, that we have shown $n + (m{+}{+}) = (n + m){+}{+}$, we want to show that $(n{+}{+}) + (m{+}{+}) = ((n{+}{+}) + m){+}{+}$. Looking at the left hand side. By definition of addition it is equal to $(n + (m{+}{+})){+}{+}$, which in turn, by the inductive hypothesis, is equal to $((n + m){+}{+}){+}{+}$. Now, examining the right hand side. By the definition of addition, it is equal to $((n + m){+}{+}){+}{+}$. The two sides are equal, and this closes the induction. □

We can now easily show the following result:

Corollary. *For all natural numbers n, $n{+}{+} = n + 1$.*

Proof. This is a special case of the previous lemma, where $m = 0$. We have $n + (m{+}{+}) = (n + m){+}{+}$. Setting $m = 0$, we get $n + (0{+}{+}) = (n + 0){+}{+}$. Evaluating the left hand side we get $n+1$ and evaluating the right hand side, we get $(n){+}{+} = n{+}{+}$, which is what we wanted to show. □

Now for one of the first major results. We can now prove that $a + b = b + a$.

Proposition 2.2.4 (Addition is commutative)**.** *For any natural numbers n and m, $n+m = m+n$.*

Proof. Using induction on n keeping m fixed. First showing the base case, where $n = 0$. We want to show that $0 + m = m + 0$. By the definition of addition, the left hand side is equal to m. By lemma 2.2.2, the right hand side is equal to m. Therefore, the base case is true. Now, assuming that it is shown that $n+m = m+n$. We now want to show that $(n{+}{+}) + m = m + (n{+}{+})$. Looking at the left hand side, we see that it is equal to $(n+m){+}{+}$, by definition of addition. The right hand side, by lemma 2.2.3 must be equal to $(m + n){+}{+}$. Since we assumed $n+m = m+n$, the left and right hand side is equal and therefore the induction is closed. □

Proposition 2.2.5 (Addition is associative)**.** *For any natural numbers a, b, c, we have $(a + b) + c = a + (b + c)$.*

Proof. See Exercise 2.2.1. □

Proposition 2.2.6 (Cancellation law)**.** *Let a, b, c be natural numbers such that $a + b = a + c$.*

Since we haven't explored the concept of subtraction or negative numbers yet we cannot use these properties to prove this law. This law is actually crucial in defining subtraction rigorously.

Proof. We prove this with induction on a, keeping b and c fixed. Showing the base case with $a = 0$. We have $0 + b = 0 + c$. Using the definition of addition, $b = c$. Now, for the inductive hypothesis. Assuming that it is shown that $a + b = a + c$, we want to show that $(a{+}{+}) + b = (a{+}{+}) + c$ implies $b = c$. Left hand side evaluates to $(a + b){+}{+}$ and the right hand side evaluates to $(a + c){+}{+}$ by the definition of addition. By Axiom 2.4 we see that $(a + b) = (a + c)$, and therefore by our assumption $b = c$. This closes the induction. □

We now want to look at how natural numbers interacts with positivity. First, a definition:

Definition 2.2.7 (Positive natural numbers)**.** A natural number n is said to be *positive* if and only if it is not equal to 0.

This leads to the following proposition.

Proposition 2.2.8. *If a is positive and b is a natural number, then $a+b$ is positive (and hence $b+a$ is also, by Proposition 2.2.4).*

Proof. Using induction on b. Showing the base case where $b = 0$. Assuming a a positive number and b a natural number. We then have $a + b = a + 0 = a$, and by assumption a is a positive number. Now for the inductive step. We assume shown that $a+b$ is a positive number. We want to show that $a + (b{+}{+})$ must also be a positive number. Using the commutativity of natural numbers and the definition of addition we can show that this must be equal to $(a + b){+}{+}$. Since we know that 0 is not the successor to any number, and that $(a + b)$ is positive, we must have $(a + b){+}{+} \neq 0$. This closes the induction. □

Corollary 2.2.9. *If a and b are natural numbers such that $a + b = 0$, then $a = 0$ and $b = 0$.*

Proof. Assume for contradiction that $a \neq 0$ and $b \neq 0$. Since $a \neq 0$ then it is positive by definition, and then it follows by 2.2.8 that $a + b$ is positive. The same argument for $b \neq 0$. Therefore, our assumptionds leads to contradictions. In other words, $a = 0, b = 0$. □

Lemma 2.2.10. *Let a be a positive number. Then there exists exactly one natural number b such that $b{+}{+} = a$.*

Proof. See Exercise 2.2.2. □

We can now, since we have a notion of addition, proceed with defining a notion of order on the natural numbers.

Definition 2.2.11 (Ordering of the natural numbers)**.** Let n and m be natural numbers. We say that n is *greater than or equal to* m, and write $n \geq m$ or $m \leq n$, if and only if we have $n = m + a$ for some natural number a. We say that n is *strictly greater than* m and write $n > m$ or $m < n$, if and only if $n \geq m$ or $m \leq n$ and $n \neq m$.

An example would be $8 > 5$ because $8 = 5 + 3$ and $8 \neq 5$. Another important thing to note is that $n{+}{+} > n$ for all natural numbers n. This means that there are no largest natural number n, because the next number $n{+}{+}$ is always larger.

Proposition 2.2.12 (Basic properties of order for natural numbers)**.** *Let a, b, c be natural numbers. Then*

(a) (Order is reflexive) $a \geq a$.

(b) (Order is transitive) If $a \geq b$ and $b \geq c$, then $a \geq c$.

(c) (Order is anti-symmetric) If $a \geq b$ and $b \geq a$, then $a = b$.

(d) (Addition preserves order) $a \geq b$ if and only if $a + c \geq b + c$.

(e) $a < b$ if and only if $a{+}{+} \leq b$.

(f) $a < b$ if and only if $b = a + d$ for some positive number d.

Proof. See Exercise 2.2.3. □

Proposition 2.2.13 (Trichotomy of order for natural numbers)**.** *Let a and b be natural numbers. Then exactly one of the following statements is true: $a < b, a = b$ or $a > b$.*

Proof. The gaps of this proof will be filled in Exercise 2.2.4.

The first step is going to be showing that no more than one of the statements can hold at any given time. That is, assuming $a < b$, then $a \neq b$ by definition. If $a > b$, then $a \neq b$ by definition. Assuming $a < b$ and $b > a$, we have $a = b + m$ and $b = a + n$. Substituting we get $a = a + n + m$, and using the cancellation law for addition we get $0 = n + m$. By 2.2.9 we get $n = 0$ and $m = 0$, thus $a = b$ which is a contradiction. Therefore only one of the statements may apply at any given time.

We must now show that at least one of the statemements must apply. Keeping b fixed we induct on a. Considering the base case where $a = 0$ yields $0 \leq b$ for all b. In other words, either $0 = b$ or $0 < b$. For the inductive hypothesis we assume shown that at least one of the three holds for two natural numbers a and b. We now want to show that it must neccesarily hold at least one for $a{+}{+}$ and b.

If $a < b$ then $a{+}{+} \leq b$, thus $a{+}{+} = b$ or $a{+}{+} < b$ by 2.2.12 If $a = b$ then $a{+}{+} = a{+}1 = b{+}1$ and thus by definition of the ordering of natural numbers, we have $a{+}{+} > b$. If $a > b$ then $a = b + n$ for some number n. It then follows that $a{+}{+} = (b + n){+}{+}$ which in turn is equal to $b + (n{+}{+}) = b + (n + 1)$. In other words, by definition $a{+}{+} > b$. This closes the induction. □

Armed with the previous proposition, we can now obtain a stronger version of the principle of induction.

Proposition 2.2.14 (Strong principle of induction)**.** *Let m_0 be a natural number, and let $P(m)$ be a property pertaining to an arbitrary natural number m. Suppose that for each $m \geq m_0$, we have the following implication: if $P(m')$ is true for all natural numbers $m_0 \leq m' < m$, then $P(m)$ is also true. (In particular, this means that $P(m_0)$ is true, since in this case the hypothesis is vacuous.) Then we can conclude that $P(m)$ is true for all natural numbers $m \geq m_0$.*

Proof. See Exercise 2.2.5. □

Exercise 2.2.1. Prove 2.2.5. (Hint: fix two of the variables and induct on the third).

Solution: Fixing b and c we induct on a. Examining the base case where $a = 0$ yields $(0 + b) + c = 0 + (b + c)$. Evaluating both sides using the definition of addition of natural numbers yields $b + c$ on both sides. Therefore the base case holds.

For the inductive hypothesis we assume that we have shown that $(a + b) + c = a + (b + c)$ holds. We want to show that it also holds for $a{+}{+}$. We get $((a{+}{+}) + b) + c = (a{+}{+}) + (b + c)$. Evaluating the left hand side by applying the definition of addition twice, we get

$$\begin{aligned} ((a{+}{+}) + b) + c &= ((a + b){+}{+}) + c \\ &= ((a + b) + c){+}{+}. \end{aligned}$$

Similarily, evaluating the right hand side yields

$$(a{+}{+}) + (b + c) = (a + (b + c)){+}{+}.$$

By our assumption we know $a + (b + c) = (a + b) + c$, and therefore this closes the induction. □

Exercise 2.2.2. Prove 2.2.10. (Hint: use induction.)

SOLUTION: Let a be a positive number. We want to show that there exists exactly one natural number b such that $b{+}{+} = a$. Fixing b we induct on a. We first want to show the base case where $a = 1$. It then follows that if we set $b = 0$, then we have $b{+}{+} = 0{+}{+} = 1 = a$.

For the inductive hypothesis we assume that we have shown that there exists exactly one natural number b such that $b{+}{+} = a$. We want to show that it then follows that there exists exactly one natural number c such that $c{+}{+} = a{+}{+}$. Substituting this for a we get $c{+}{+} = (b{+}{+}){+}{+}$. From axiom 4 we know that $c = b{+}{+}$. This closes the induction.

□

Exercise 2.2.3. Prove 2.2.12. (Hint: You will need many of the preceding propositions, corollaries and lemmas.)

SOLUTION: Proving basic properties of order for natural numbers.

(a) $a \geq a$.

From the assumption, we have $a = a$ or $a > a$. For $a > a$ there must exist a positive number b such that $a = a + b$. Using the law of cancellation, we get $b = 0$, which contradicts the fact that b is positive. Therefore $a = a$, which always holds. In any case, we're done.

(b) If $a \geq b$ and $b \geq c$, then $a \geq c$.

From the assumption, there exists natural numbers m and n such that $a = b + m$ and $b = c + n$. Substituting we get $a = (c + n) + m$. Using the associativity of addition of we get $a = c + (n + m)$. Since $(n + m)$ is a natural number, by definition $a \geq c$.

(c) If $a \geq b$ and $b \geq a$ then $a = b$.

If $a \geq b$, then there exist a natural number c such that $a = b + c$. Also, if $b \geq a$ then there exists a natural number d such that $b = a + d$. Substituting we get $a = (a + d) + c$. Using the associativity of the natural numbers, we have $a = a + (d + c)$. The law of cancellation gives $0 = (d + c)$. From 2.2.9 we have $d = 0$, $c = 0$. Again, substituting yields $a = 0 + b = b$ and $b = 0 + a = a$.

(d) $a \geq b$ if and only if $a + c \geq b + c$.

We argue contrapositively. Assume that $a+c < b+c$. By definition, then there exists a natural number d such that $b + c = (a + c) + d$. Using associativity and the law of cancellation, this simplifies to $b = a + d$, which in turn means that $a < b$. We have now shown the contrapositive of the right implication. Thus the right implication holds.

Now to show the left implication. Assume that $a + c \geq b + c$. We see that there exist a natural number d such that $a + c = (b + c) + d$ (equality when $d = 0$). Using associativity and the law of cancellation, we get $a = b + d$. This is the definition of *greater than*, therefore we can conclude that $a \geq b$.

We have now shown both implications and the statement holds.

(e) $a < b$ if and only if $a{+}{+} \leq b$.

Assume $a < b$, then by definition there exists a positive number c such that $b = a + c$. Substituting this into the right hand side we achieve $a{+}{+} \leq a + c$. Rephrased, $a + 1 \leq a + c$. This clearly holds true for any positive number c. (Can be shown rigorously by mathematical induction).

Now, assume that $a{+}{+} \leq b$. In other words, there exists a natural number d such that $b = (a{+}{+}) + d$. (d is allowed to be zero). Using the law of associativity we can deduce that $b = a + (1 + d)$. In other words, the definition of $a < b$.

The two implications have been shown and the statement holds.

(f) $a < b$ if and only if $b = a + d$ for some positive number d.

Assume $a < b$. From the definition, we get $a \leq b$ and $a \neq b$. $a \leq b$ means that there must exist a natural number n such that $a + n = b$. In the case where $n = 0$, $a = b$ which is a contradiction of our assumption, therefore n must be positive by definition of positive since it is not equal to 0. Let $d = n$, and we have shown that $a < b$ if $b = a + d$ for some positive number d.

Now, assume that $b = a + d$ for some positive number d. Since d is not 0 by definition, we know that $b \neq a$. Therefore, we have both $a \leq b$ as well as $a \neq b$. This is the definition of $a < b$, and we are done.

□

Exercise 2.2.4. Justify the three statements marked (why?) in the proof of 2.2.13

Solution: Filling in the gaps in the proof of 2.2.13.

(a) When $a = 0$ we have $0 \leq b$ for all b

$a = 0$ means that in the definition of $\leq$ there exist some natural number c such that we have $b = 0 + c$. Using 2.2.2 gives $b = c$. Thus, just chosing c to be equal to b satisfies the definition of $a \leq b$ for all b in the cases where $a = 0$. Therefore the base case of the mathematical induction holds.

(b) If $a > b$, then $a{+}{+} > b$

Assuming $a > b$. From the definition we know we have $a \geq b$ and $a \neq b$. This again means there exists some natural number, c, different from zero that satisfy $a = b + c$. In other words, a positive number c.

Incrementing both sides gives us $a{+}{+} = (b + c){+}{+}$. This gives us $a{+}{+} = b + (c + 1)$, by using the definition of addition and associativity. This is the definition of $a{+}{+} \geq b$, but since c cannot be 0, there is no way of obtaining the equality $a{+}{+} = b{+}{+}$, thus by 2.4 we have $a \neq b$ which gives us the condition we need for setting $a{+}{+} > b$ which is what we wanted to show.

(c) If $a = b$, then $a{+}{+} > b$.

Assuming $a = b$. This means, that in the definition of $a \geq b$, we know that the natural number c that satisfies $a = b + c$ must be zero (this follows from the law of cancellation and 2.2.2). Incrementing both sides yield $a{+}{+} = (b + 0){+}{+}$, which in turn gives us $a{+}{+} = b{+}{+} = b + 1$. This satisfies the definition of $a{+}{+} > b$ because there exist a positive number 1 such that $a{+}{+} = b + 1$.

□

Exercise 2.2.5. **To do** (1) Prove 2.2.14. (Hint: define $Q(n)$ to be the property that $P(m)$ is true for all $m_0 \leq m < n$; note that $Q(n)$ is vacuously true when $n < m_0$.)

Exercise 2.2.6. Let n be a natural number, and let $P(m)$ be a property pertaining to the natural numbers such that whenever $P(m{+}{+})$ is true, then $P(m)$ is true. Suppose that $P(n)$ is also true. Prove that $P(m)$ is true for all natural numbers $m \leq n$; this is known as the *principle of backwards induction.* (Hint: apply induction to the variable n.)

Solution: Inducting on n and examining the base case where $n = 1$ yields $P(1) = P(0{+}{+})$ being true. By the properties of $P(m{+}{+})$ it follows that $P(0)$ is true.

Now, assume that we have shown this to be true up to $n = d{+}{+}$, we now want to show that it holds for $(d{+}{+}){+}{+}$. $P((d{+}{+}){+}{+})$ true tells us that $P(d{+}{+})$ must be true. Since $P(d{+}{+})$ is true $P(d)$ is true, and so on and so forth.

Thus by *backwards induction* we have shown $P(m)$ is true for all natural numbers $m \leq n$. □

2.3 Multiplication

We have now shown all the basic facts known to be true for the addition and ordering of natural numbers. We now introduce multiplication. Just as addition is iterated incrementation, we can define multiplication to be iterated addition.

Definition 2.3.1 (Multiplication of natural numbers)**.** Let m be a natural number number. To multiply zero to m, we define $0 \times m = 0$. Now suppose inductively that we have defined how to multiply n to m. Then we can multiply $n{+}{+}$ to m by defining $(n{+}{+}) \times m = (n \times m) + m$.

An example would be $2 \times m = 0 + m + m$. By induction, it is easily verified that the product of two natural numbers is also a natural number.

Lemma 2.3.2 (Multiplication is commutative)**.** *Let n, m be natural numbers. Then $n \times m = m \times n$.*

Proof. See Exercise 2.3.1. □

We now, in order to ease writing, start abbreviating $n \times m$ as nm. Using the usual rules of precedence there is no ambiguitiy. Therefore $ab + c$ is equal to $(a \times b)+c$. We will also use the usual precedence rules for the other arithmetic operations as they are defined later.

Lemma 2.3.3 (Natural numbers have no zero divisors)**.** *Let n, m be natural numbers. Then $n \times m = 0$ if and only if at least one of n, m is equal to zero. In particular, if n and m are both positive, then nm is also positive.*

Proof. See Exercise 2.3.2. □

Proposition 2.3.4 (Distributive law)**.** *For any natural numbers a, b, c, we have $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.*

Proof. Assume a, b, c to be natural numbers. Using the commutativity of multiplication, we see that $a(b+c) = (b+c)a$. Therefore we only have to show the first case.

Inducting on a keeping b and c fixed. The base case, with $a = 0$ gives us for the left hand side: $0(b+c)$ which is equal to 0 by definition of multiplication. Right hand side equates to $0a + 0b$, which is equal to 0. Therefore the two sides are equal and the statement holds.

Now, assume for the sake of induction that we have shown $a(b+c) = ab+ac$. We now want to show that it must also hold for $(a{+}{+})(b+c) = (a{+}{+})b+(a{+}{+})c$. By definition of mutlitplication, we have that the left side equates to $a(b+c)+(b+c)$. Using our assumption this evaluates to $ab + ac + (b + c)$. Using the laws of commutativity we can rearrange this to $(ab + b) + (ac + c)$. From the definition of multiplication this is equal to $(a{+}{+})b + (a{+}{+})c$ which is what we wanted to show. The induction is closed. □

Proposition 2.3.5 (Multiplication is associative)**.** *For any natural numbers a, b, c we have $(a \times b) \times c = a \times (b \times c)$*

Proof. See Exercise 2.3.3. □

Proposition 2.3.6 (Multiplication preserves order)**.** *If a, b are natural numbers such that $a < b$, and c is positive, then $ac < bc$.*

Proof. Assuming $a < b$, then by definition $a \leq b$ and $a \neq b$. Thus, again by definition there must exist some natural number d such that $a + d = b$, but since $a \neq b$, we must have $d \neq 0$. Therefore d is a positive number. Multiplying by a positive number c we get $(a + d)c = bc$, and using the law of commutativity we have $ac + dc = bc$, thus by definition $ac \leq bc$. But since $d \neq 0$ we cant have equality, and therefore $ac < bc$. □

Corollary 2.3.7 (Cancellation law)**.** *Let a, b, c be natural numbers such that $ac = bc$ and c is non-zero. Then $a = b$.*

Proof. Initially assume that $ac = bc$. By the trichotomy of order (2.2.13), exactly one of the following must hold: $a = b$, $a < b$ or $a > b$. Assume first that $a < b$. By 2.3.6 we have $ac < bc$ which is a contradiction. Similarly, assuming $b < a$ we have by the same proposition that $bc < ac$ which also is a contradiction. Therefore, by the trichotomy of order, $a = b$ is the only possibility. □

We can now, since we have all the familiar operations of addition and multiplication discard the increment operation and just use the fact that $n{+}{+} = n+1$ in the cases where we need to describe incrementation. We're getting closer and closer to things being the way they are used to.

We're now proposing one of the fundamental theorems in number theory, namely the Euclidean algorithm

Proposition 2.3.9 (Euclidean algorithm)**.** *Let n be a natural number, and let q be a positive number. Then there exist natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$.*

Proof. See Exercise 2.3.5 □

Just like addition is iterated incrementation and multiplication is iterated addition, we can recursively define *exponentiation* as iterated multiplication.

Definition 2.3.11 (Exponentiation for natural numbers)**.** Let m be a natural number. To raise m to the power 0, we define $m^0 = 1$. Now suppose recursively that m^n has been defined for some natural number n, then we define $m^{n{+}{+}} = m^n \times m$.

Exercise 2.3.1. Prove Lemma 2.3.2. (Hint: Modify the proofs of 2.2.2, 2.2.3 and 2.2.4.)

Solution: In order for us to show this we must first prove some auxilliary results. Firstly, we need to show that multiplication commute with 0. We do this by showing $n \times 0 = 0 \times n$ for all natural numbers

n. Secondly, we need to prove that multiplication commutes with successors. That is, $n \times (m{+}{+}) = (n \times m) + n$.

1. For any natural number $n, n \times 0 = 0 \times n$.

   Inducting on n gives us the base case $0 \times 0 = 0 \times 0$. It is clear, that by definition of multiplication both sides equal 0.

   Now, for the inductive step, assume that it is shown that $n \times 0 = 0 \times n$. We now want to show that this holds for the successor $n{+}{+}$.

   Evaluating the left hand side gives us; $(n{+}{+}) \times 0 = (n \times 0) + 0$ by definition. By assumption this equals $(0 \times n) + 0 = 0 + 0 = 0$. Right hand side gives 0 by definition of multiplication. This closes the induction.

2. For any natural number n and m, $n \times (m{+}{+}) = (n \times m) + n$

   We induct on n keeping m fixed. This yields the base case $0 \times (m{+}{+}) = (0 \times m) + 0$. By definition of multiplication, both the left and right hand side is equal to zero.

   For our inductive step we assume that it is already shown that $n \times (m{+}{+}) = (n \times m) + n$. We now want to show that $(n{+}{+}) \times (m{+}{+}) = (n{+}{+}) \times m) + (n{+}{+})$. Evaluating the left hand side, we see that $(n{+}{+}) \times (m{+}{+})$ is by definition equal to $n \times (m{+}{+}) + (m{+}{+})$. By our assumption, we know this can be rewritten as $(n \times m) + n + (m{+}{+})$. By the definition of addition this is equal to $(n \times m) + (n + m){+}{+}$.

   Right hand side is by definition equal to $(n \times m) + m + (n{+}{+})$. Definition of addition gives ut that this is equal to $(n \times m) + (m + n){+}{+}$. Finally, the commutativity of addition sets this equal to $(n \times m) + (n + m){+}{+}$. The two sides are equal. This closes the induction.

Equipped with these two auxilliary results, we can now show that multiplication is commutative. In order to prove that $m \times n = n \times m$ we induct on n keeping m fixed. The base case is $m \times 0 = 0 \times m$. Left hand side equates to zero by our first auxilliary result. The right hand side equates to zero by definition.

We now assume that $m \times n = n \times m$. We want to show $m \times (n{+}{+}) = n \times (m{+}{+})$. The left hand side, by the second auxilliary result: $m \times (n{+}{+}) = (m \times n) + m$. The right hand side is by definition equal to $(n \times m) + m$ and applying our assumption we have $(m \times n) + m$. The two sides are equal, and this closes the induction. □

Exercise 2.3.2. Prove Lemma 2.3.3. (Hint: Prove the second statement first)

Solution: We first want to prove that if n, m are two positive numbers, then nm is also positive.

We induct on n keeping m fixed. The base case is $n = 0{+}{+}$. By definition of multiplication we have $n \times m = (0{+}{+}) \times m = (0 \times m) + m = m$. Since m is a positive number the base case holds.

Now assume that nm is positive. We now want to show $(n{+}{+})m$ is positive. By definition of multiplication, we have $(n{+}{+})m = (n \times m) + m$. By our assumption, we know that $n \times m$ is a positive number. Proposition 2.2.8 tells us that the sum of two positive numbers is also positive. Therefore nm is positive.

We now want to show that $n \times m = 0$ if and only if either one or both of n, m is 0. We show the right implication first.

Assume $n \times m = 0$. If we let be n and m are both positive numbers, our previous result tells us that $n \times m$ is positive. By the definition of positive, $n \times m \neq 0$ which is a contradiction. Therefore either n, m or both are zero.

From the definition of multiplication, if we have either m, n or both zero then $n \times m$ is zero. Our previous result tells us that if both m and n are positive, i.e., non-zero. Then the product mn is positive. Therefore, both implications hold.

□

Exercise 2.3.3. Prove Proposition 2.3.5. (Hint: modify the proof of Proposition 2.2.5 and use the distributive law.)

Solution: We want to prove that multiplication is associative. That is for any natural numbers a, b, c we have $(a \times b) \times c = a \times (b \times c)$. We induct on c keeping a and b fixed.

The base case where $c = 0$ gives us 0 on both the left and right hand side because of commutativity and the definition of multiplication.

Assume now that we have shown $(a \times b) \times c = a \times (b \times c)$. We now want to show $(a \times b) \times (c{+}{+}) = a \times (b \times (c{+}{+}))$

The left hand, due to commutativity and definition of multiplication is equal to $c(ab) + ab$. This equals $(ab)c + ab$. The right hand side equals, by definition and the distributive law, $a(cb + b) = a(cb) + ab = a(bc) + ab = (ab)c + ab$. The two sides are equal and this closes the induction.

□

Exercise 2.3.4. Prove the identity $(a + b)^2 = a^2 + 2ab + b^2$ for all natural numbers a, b.

Solution: We induct on a keeping b fixed. The base case where $a = 0$ gives for the left hand side $(0 + b)^2 = b^2$. The right hand side equates to, by definition of exponentiation $0 \times 0^1 + 0 \times (2b) + b^2 = b^2$.

Now assume that the above identity holds for a, b. We want to show that it holds for $a{+}{+}, b$. That is $((a{+}{+}) + b)^2 = (a{+}{+})^2 + 2(a{+}{+})b + b^2$.

Equating the left side yields $a^2 + 2ab + b^2 + 2b + (2a){+}{+}$. Equating the right side yields the same $a^2 + 2ab + b^2 + 2b + (2a){+}{+}$.

The calculations involved are quite long, so they are left as an exercise to the reader. (First time I'm not on the recieving end of this statement.) □

Exercise 2.3.5. Prove Proposition 2.3.9. (Hint: fix q and induct on n.)

Solution: We want to show that there exists natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$, where n is a natural number and q a positive number. We induct on n keeping q fixed.

This yields the base case $n = mq + r = 0$. Chosing $m = r = 0$ this clearly holds, even though q is still a positive number. $0 \leq 0 < q$

We now assume that the statement holds for the natural number n. We now want to show it must hold for $n{+}{+}$.

We have two cases, where $r{+}{+} < q$ and where $r{+}{+} = q$. In the first case, where $r{+}{+} < q$ we can just set $n{+}{+} = (mq + r){+}{+} = (mq + (r{+}{+}))$.

We now just have to show the second case.**To do** (2) □

Chapter 3

Set theory

In this chapter the more elementary aspects of axiomatic set theory is presented. Some of the more advanced concepts will be left for later chapters, but the finer subtetlies of set theory will be left out.

3.1 Fundamentals

We start with an informal definition of what a set *should* be.

Definition 3.1.1 (Informal)**.** We define a *set* A to be any unordered collection of objects, e.g., $\{3, 8, 5, 2\}$ is a set. If x is an object, we say that x *is an element of* A or $x \in A$ if x lies in the collection; otherwise we say that $x \notin A$. For instance, $3 \in \{1, 2, 3, 4, 5\}$ but $7 \notin \{1, 2, 3, 4, 5\}$.

We first want to clarify the fact that sets themselves are considered objects. Therefore, we impose the following axiom:

Axiom 3.1 (Sets are objects)**.** *If A is a set, then A is also an object. In particular, given two sets A and B, it is meaningful to ask whether A is also an element of B.*

An example of sets being elements of other sets would be the set $\{3, \{3, 4\}, 4\}$. It consists of three distinct objects, one which happens to also be a set. Not all objects are sets. A natural number is not typically considered a set.[1]

More specifically, if x is an object and A is a set, then either $x \in A$ is true, or $x \in A$ is false. If A is not a set, then the statement $x \in A$ is neither true nor false but meaningless.

We now define the notion of equality between sets.

Definition 3.1.4 (Equality of sets)**.** Two sets A and B are *equal*, $A = B$ if and only if for every element of A is an element of B and vice versa. To put it another way, $A = B$ if and only if every element x of A belongs also to B, and every element y of B belongs also to A.

A neat little observation is that if $x \in A$ and $A = B$, then $x \in B$ by Definition 3.1.4. Therefore, the “is an element of” relation $\in$ obeys the axiom of substitution. That is, you can substitute B for A in the statement $x \in A$. This will, as we shall see, be the case for the remaining defintions in this section.

Now that we have defined the notion of a set, we want do discern which objects can be considered sets and which objects cannot. Starting with a single set, the *empty set.*

Axiom 3.2 (Empty set)**.** *There exists a set $\emptyset$, known as the empty set, which contains no elements, i.e., for every object x we have $x \notin \emptyset$.*

One can easily prove the uniqueness of the empty set by assuming that there are two empty sets and showing that they must be equal by Definition 3.1.4. We now examine what it means for a set to be *non-empty.*

Lemma 3.1.6 (Single choice)**.** *Let A be a nonempty set. Then there exists an object x such that $x \in A$.*

Proof. Assume for contradiction that A is nonempty, and there exist no objects x such that

[1] A natural number can be the *cardinality* of a set however.

$x \in A$. We see that our assumption about no objects $x \in A$ coincides with Axiom 3.2. By definition 3.1.4, we must have $A = \emptyset$. However, this contradicts our assumption about A being non-empty. Therefore there must exist an object x such that $x \in A$. □

If Axiom 3.2 was the only axiom set theory had, then there might be just a single set in existence, namely the empty set. The following axioms are here to enrich the number of sets we will have available to us.

Axiom 3.3 (Singleton sets and pair sets)**.** *If a is an object, then there exists a set $\{a\}$ whose only element is a, i.e., for every object y, we have $y \in \{a\}$ if and only if $y = a$; we refer to $\{a\}$ as the singleton set whose element is a. Furthermore, if a and b are objects, then there exists a set $\{a, b\}$ whose only elements are a and b; i.e., for every object y, we have $y \in \{a, b\}$ if and only if $y = a$ or $y = b$; we refer to this set as the pair set formed by a and b.*

It is important to note that there is only one singleton set for each object a. This follows from definition 3.1.4. Similarly, there is only one pair set formed by two objects a and b. Definition 3.1.4 actually ensures that $\{a, b\} = \{b, a\}$ and that $\{a, a\} = \{a\}$. One could keep assuming new axioms for larger and larger sets, with more and more elements, but it is shown that it suffices with the previous two once we assume the next axiom, namely;

Axiom 3.4 (Pairwise union)**.** *Given any two sets A, B, there exists a set $A \cup B$, called the union $A \cup B$ of A and B, whose elements consists of all the elements which belong to A or B or both. In other words, for any object x,*

$$x \in A \cup B \iff (x \in A \text{ or } x \in B) .$$

We now show some basic properties of unions.

Lemma 3.1.13. *If a and b are objects, then $\{a, b\} = \{a\} \cup \{b\}$. If A, B, C are sets, then the union operation is commutative (i.e., $A \cup B = B \cup A$) and associative (i.e., $(A \cup B) \cup C = A \cup (B \cup C)$). Also, we have $A \cup A = A \cup \emptyset = \emptyset \cup A = A$.*

Proof. We prove the associativity identity here and leave the rest for Exercise 3.1.3.

We want to show that $(A \cup B) \cup C = A \cup (B \cup C)$ By definition 3.1.4 we need to show that every element of $(A \cup B) \cup C$ is also an element of $A \cup (B \cup C)$, and vice versa.

Suppose first that x is an element of $(A \cup B) \cup C$. By Axiom 3.4 we have that either $x \in (A \cup B)$ or $x \in C$. In other words, at least one of the two statements must be true. We now divide the proof into two cases:

1. $x \in C$

   Applying Axiom 3.4 several times tells us that if $x \in C$, then $x \in (B \cup C)$, and finally $x \in A \cup (B \cup C)$.

2. $x \in (A \cup B)$

   Again applying Axiom 3.4 several times gives that if $x \in (A \cup B)$ then $x \in A$ or $x \in B$. If $x \in A$, then $x \in A \cup (B \cup C)$, and if $x \in B$ then $x \in (B \cup C)$, which in turn means that $x \in A \cup (B \cup C)$.

A very similar argument shows that if $x \in A \cup (B \cup C)$, then $x \in (A \cup B) \cup C$. Therefore $(A \cup B) \cup C = A \cup (B \cup C)$. □

We kan now define sets with arbitrarily many elements, however we are still not able to define a set with n elements for any natural number n, because we haven't defined n-fold iteration.

We now examine the concept of sets being larger than others. We do this through the notion of a *subset.*

Definition 3.1.15 (Subsets)**.** Let A, B be sets. We say that A is a *subset* of B, denoted $A \subseteq B$, if and only if every element of A is also an element of B, i.e.,

$$\text{For any object } x, \quad x \in A \Longrightarrow x \in B.$$

We say that A is a *proper subset* of B, denoted $A \subset B$[2], if $A \subset B$ and $A \neq B$.

Again, it is easily verified that this definition obey the axiom of substitution. The notion of a *subset* for sets is similiar in many ways to the notion of ordering on the natural numbers. We shall see however that they are not strictly analogous. We therefore propose:

[2] Tao uses the symbol $\subsetneq$ to mean the same thing as the symbol $\subset$

Proposition 3.1.18 (Sets are partially ordered by set inclusion)**.** *Let A, B, C be sets. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$. If $A \subseteq B$ and $B \subseteq A$, then $A = B$. Finally, if $A \subset B$ and $B \subset C$, then $A \subset C$*

Proof. We prove just the first claim. We want to show that $A \subseteq B$ and $B \subseteq C$ implies $A \subseteq C$. Let x be an element in A. That is $x \in A$. By Definition 3.1.15, we must have $x \in B$, and again, by the same definition $x \in C$. Therefore, $A \subseteq C$. □

We say that sets are *partially ordered* by set inclusion because given any two distinct set it is not in general true that one of them is a subset of the other. An example would be the two sets $\{2n \mid n \in \mathbb{N}\}$ and $\{2n+1 \mid n \in \mathbb{N}\}$. The less than relation on natural numbers however is totally ordered.[3]

The axiom now presented makes us able to create subsets out of larger subsets.

Axiom 3.5 (Axiom of specification)**.** *Let A be a set, and for each $x \in A$ let $P(x)$ be a property pertaining to x (i.e., $P(x)$ is either a true statement, or a false statement). Then there exists a set, called $\{x \in A : P(x)$ is true.$\}$ (or simply $\{x \in A : P(x)\}$ for short), whose elements are precicely the elements x in A for which $Px)$ is true. In other words, for any object y,*

$$y \in \{x \in A : P(x)\} \iff (y \in A \text{ and } P(y) \text{ is true}) .$$

This axiom is also known as the *axiom of separation.* Note that $\{x \in A : P(x)\}$ is always a subset of A. This easily follows from the definition of subset.

We sometimes write $\{x \in A \mid P(x)\}$ instead of $\{x \in A : P(x)\}$. I am going to use this bar-notation for the rest of this document.

From the axiom of specification, we can now define some more operations on sets.

Definition 3.1.23 (Intersections)**.** The *intersection* $S_1 \cap S_2$ of two sets is defined to be the set

$$S_1 \cap S_2 = \{x \in S_1 \mid x \in S_2\} .$$

In other words, $S_1 \cap S_2$ consists of all the elements which belong to both S_1 and S_2. Thus, for all objects x,

$$x \in S_1 \cap S_2 \iff x \in S_1 \text{ and } x \in S_2.$$

Definition 3.1.27 (Difference sets)**.** Given any two sets A and B, we define the set $A \setminus B$ to be the set A with any elements of B removed:

$$A \setminus B = \{x \in A \mid x \notin B\} ;$$

for instance, $\{1, 2, 3, 4\} \setminus \{2, 4, 6\} = \{1, 3\}$. In many cases, B will be a subset of A, but not necessarily.

Now for some basic properties of unions, intersections and difference sets.

Proposition 3.1.28 (Sets form a boolean algebra)**.** *Let A, B, C be sets and let X be a set containing A, B, C as subsets.*

(a) (Minimal element) We have $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

(b) (Maximal element) We have $A \cup X = X$ and $A \cap X = A$.

(c) (Identity) We have $A \cap A = A$ and $A \cup A = A$.

(d) (Commutativity) We have $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

(e) (Associativity) We have $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.

(f) (Distributivity) We have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(g) (Partition) We have $A \cup (X \setminus A) = X$ and $A \cap (X \setminus A) = \emptyset$.

(h) (De Morgan laws) We have $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ and $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

Proof. See Exercise 3.1.6. □

In order for us to take each element of a set and transform them in some way or another we need a new axiom, namely the axiom of replacement.

[3] See Axiom 3.5 for notation

Axiom 3.6 (Replacement)**.** *Let A be a set. For any object $x \in A$, and any object y, suppose we have a statement $P(x, y)$ pertaining to x and y, such that for each $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $\{y \mid P(x, y)$ is true for some $x \in A\}$, such that for any object z,*

$$z \in \{y \mid P(x,y) \textit{ is true for some } x \in A\} \iff P(x,z) \textit{ is true for some } x \in A.$$

An example of this axiom in use would be transforming the set $\{3, 5, 9\}$ to the set $\{4, 6, 10\}$. Define $P(x, y)$ to be the statement $y = x{+}{+}$. We know from Axiom 2.4 that at most one y will satisfy $P(x, y)$. It then, by Axiom 3.6, exists a set $\{3{+}{+}, 5{+}{+}, 9{+}{+}\} = \{4, 6, 10\}$.

We often abbreviate a set on the form

$$\{y \mid y = f(x) \text{ for some } x \in A\}$$

as $\{f(x) \mid x \in A\}$. Our previous example would then be the set $\{x{+}{+} \mid x \in A\}$. We can now also combine the axiom of replacement with the axiom of specification to create sets like $f(x) \mid x \in A; P(x)$ is true.

We now formalize the notion that natural numbers are to be treated as objects.

Axiom 3.7 (Infinity)**.** *There exist a set $\mathbb{N}$, whose elements are called natural numbers, as well as an object 0 in $\mathbb{N}$, and an object $n{+}{+}$ assigned to every natural number $n \in \mathbb{N}$ such that the Peano axioms (Axioms 2.1 - 2.5) hold.*

This is a more formal version of Assumption 2.6. This axiom is called the axiom of infinity because it introduces the most basic example of an infinite set. We now know, from Axiom 3.7 see that numbers such as $3, 5$ and 9 are infact objects, and we can therefore legitimately create sets with these as elements, because the elements of a set are required to be objects.

Exercise 3.1.1. Show that the definition of equality (3.1.4) is reflexive, symmetric and transitive.

Solution: We need to show the three properties reflexiveness, symmetry, and transistivity.

(a) Reflexive

We want to show that for a set A, we have $A = A$. By definition of equality, we have $A = A$ if all elements in A are also in A. They are, by definition, therefore equality is reflexive.

(b) Symmetric

We want to show that for two sets A, B, $A = B \implies B = A$. Assume that $A = B$. This means, that for all elements $x \in A \implies x \in B$, and for all elements $y \in B \implies y \in A$. But this is the definition of $B = A$.

(c) Transitive

We need to show that given three sets A, B, C, $A = B$ and $B = C$ implies $A = C$. Assume that $A = B$ and $B = C$. Let $x \in A$. By definition of equality, we have $x \in B$, and since $x \in B$ we must have $x \in C$. Therefore $A = C$.

This concludes the proofs. □

Exercise 3.1.2. Using only Definition 3.1.4, Axiom 3.2 and Axiom 3.3 prove that the sets $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}$ and $\{\emptyset, \{\emptyset\}\}$ are all distinct (i.e., no two of them are equal to each other).

Solution: By Axiom 3.2 there exists a set, namely the empty set, that contains no objects. By Axiom 3.3 there exists a singleton set that consists only of the object $\emptyset$, namely the set $\{\emptyset\}$. By definition of the empty set, $\emptyset \neq \{\emptyset\}$.

Again, by 3.3 there exists a singleton set that consists only of the object $\{\emptyset\}$. This is by Axiom 3.2 not equal to the empty set. By the transistive property of equality it is not equal to the set $\{\emptyset\}$ either.

Finally, by 3.3 there exists a pair set formed by the objects $\emptyset$ and $\{\emptyset\}$. This set is the set $\{\emptyset, \{\emptyset\}\}$. Again, by 3.2, these two are not equal, and therefore not equal to any of the other sets.

□

Exercise 3.1.3. Prove the remaining claims in Lemma 3.1.13.

Solution: (a) If a and b are objects, then $\{a, b\} = \{a\} \cup \{b\}$.

By Axiom 3.3 we know the sets $\{a\}, \{b\}, \{a, b\}$ exist. By definition of set union, we know that $\{a\} \cup \{b\}$ is the set consisting of those elements that are either in $\{a\}$, or in $\{b\}$. These two objects are a and b, and they form the pair set $\{a, b\}$.

(b) If A, B, C are sets, then the union operation is commutative.

We want to show that $A \cup B = B \cup A$. Assume that $A \cup B$. If $x \in A \cup B$, then $x \in A$ or $x \in B$, by definition. But then, also by definition, we have $x \in B \cup A$.

A similar argument goes for the other inclusion. We therefore have $A \cup B = B \cup A$.

(c) $A \cup A = A \cup \emptyset = \emptyset \cup A = A$

Assume $A \cup A$, by definition we know if $x \in A \cup A$, then $x \in A$ and $x \notin \emptyset$ by definition of the empty set. But then we have $x \in A \cup \emptyset$. Since pairwise union is commutative we have $x \in \emptyset \cup A$. We have then shown everything we need to conclude that $A \cup A = A \cup \emptyset = \emptyset \cup A = A$.

□

Exercise 3.1.4. Prove the remaining claims in Proposition 3.1.18.

Solution: Let A, B, C be sets.

(a) If $A \subseteq B$ and $B \subseteq A$ then $A = B$.

By definition of subsets, we have $x \in A \Rightarrow x \in B$, but since we also have $y \in B \Rightarrow y \in A$, we see that we satisfy the definiton for equality (3.1.4) between sets. Therefore $A = B$.

(b) If $A \subset B$ and $B \subset C$ then $A \subset C$.
By definition of subsets we have $A \neq B$ and $B \neq C$. By the transitive property of equality we must also have $A \neq C$.

We have $x \in A \Rightarrow x \in B$, and $x \in B \Rightarrow x \in C$. Therefore $x \in A \Rightarrow x \in C$. We have now shown the two requirements for a set to be a proper subset. Therefore $A \subset C$.

□

Exercise 3.1.5. Let A, B be sets. Show that the three statements $A \subseteq B$, $A \cup B = B$ and $A \cap B = A$ are logically equivalent. That is, any one of them implies the other two.

Solution: By definition, we have from $A \subseteq B$ that $x \in A \Rightarrow x \in B$. From $A \cup B = B$ we have that $x \in A \cup B \Rightarrow x \in B$, and $x \in B \Rightarrow x \in A \cup B$. $A \cap B = A$ tells us that $x \in A \cap B \Rightarrow x \in A$.

If we first assume that $A \subseteq B$. Thus, if $x \in A$ then $x \in B$. We need to show that This means that for the union $A \cup B$, all the elements that are in A are also in B, therefore we have $A \cup B = B$. For the intersection, we have since $x \in A$ $x \in A \cap B$. But since there only the elements that are in both A and B are included, we must have $A \cap B = A$.

A similar argument is used for the two other cases. □

Exercise 3.1.6. Prove Proposition 3.1.28. (Hint: one can use some of these claims to prove others. Some of the claims have also appeared previously in Lemma 3.1.13.)

Solution: (a) We want to show that $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$. By definition of pairwise union, we know that $A \cup \emptyset$ set consists only of the elements that are in either A or the $\emptyset$. By Axiom 3.2, the empty set contains no elements, therefore the union must simply be A.

By definition of set intersection we know that $A \cap \emptyset$ consists of the elements that are in both A and $\emptyset$, but since the empty set contains no elements the intersection is also empty. Therefore the intersection is simply $\emptyset$.

(b) We assumed that $A \subseteq X$. From the previous exercise, we know that $A \cup X = X$ and that $A \cap X = A$.

(c) Since we have $A \subseteq A$, we can use the previous result to directly show that this holds. Just substitute X for A and the previous result turns into $A \cap A = A$ and $A \cup A = A$.

(d) Follows from Lemma 3.1.13

(e) Follows from Lemma 3.1.13

To do (3)

□

Exercise 3.1.7. Let A, B, C be sets. Show that $A \cap B \subseteq A$ and $A \cap B \subseteq B$. Furthermore, show that $C \subseteq A$ and $C \subseteq B$ if and only if $C \subseteq A \cap B$. In a similar spirit, show that $A \subseteq A \cup B$ and $B \subseteq A \cup B$, and furthermore that $A \subseteq C$ and $B \subseteq C$ if and only if $A \cup B \subseteq C$.

Solution: Showing one claim at the time.

1. $A \cap B \subseteq A$

   We need to show that $x \in A \cap B \Rightarrow x \in A$. Let $x \in A \cap B$, by definition of set intersection we have $x \in A$ and $x \in B$. Therefore $x \in A \cap B \Rightarrow x \in A$.

2. $A \cap B \subseteq B$

   Similar proof to the one above. Just use the definition of set intersection.

3. $C \subseteq A$ and $C \subseteq B \Longleftrightarrow C \subseteq A \cap B$.

   Showing right implication first. Assume $C \subseteq A$ and $C \subseteq B$. Let $x \in C$. From our assumption we must have $x \in A$ and $x \in B$. Therefore, we have $x \in A \cap B$. We can then conclude with $C \subseteq A \cap B$.

   Now, the left implication. Assume $C \subseteq A \cap B$. Let $x \in C$. By definition, we have $x \in A \cap B$. From the definition of set intersection, we must have $x \in A$ and $x \in B$, therefore, $C \subseteq A$ and $C \subseteq B$.

4. $A \subseteq A \cup B$

   We need to show that $x \in A \Rightarrow x \in A \cup B$. Let $x \in A$. But then, by definition of pairwise union, we must have $x \in A \cup B$. Therefore, $A \subseteq A \cup B$.

5. $B \subseteq A \cup B$

   Same as above, use the definition of pairwise union.

6. $A \subseteq C$ and $B \subseteq C \Longleftrightarrow A \cup B \subseteq C$.

   We show the right implication first. Assume that $A \subseteq C$ and $B \subseteq C$. $x \in A \Rightarrow x \in C$ and $x \in B \Rightarrow x \in C$. Let $y \in A \cup B$. By definition we must have $y \in A$ or $y \in B$, but in either case we also have $y \in C$. Therefore $A \cup B \subseteq C$.

   Now for the left implication. Assume that $A \cup B \subseteq C$. By definition, we must have $x \in A \cup B \Rightarrow x \in C$. If $x \in A \cup B$, then $x \in A$ or $x \in B$, but in either case, we also have $x \in C$, so therefore we have $A \subseteq C$ and $B \subseteq C$.

□

Exercise 3.1.8. Let A, B be sets. Prove the *absorbtion laws* $A \cap (A \cup B) = A$ and $A \cup (A \cap B) = A$.

Solution: For these we have to prove both left and right inclusion in order for them to be equal.

1. $A \cap (A \cup B) = A$.

   We start with the right inclusion. Assume that $x \in A \cap (A \cup B)$. By definition, we must have $x \in A$ and $x \in (A \cup B)$. Therefore we have $A \cap (A \cup B) \subseteq A$.

   For the left inclusion, we assume $x \in A$. By definition of pairwise union we must also have $x \in A \cup B$, but then it follows that we have $x \in A \cap (A \cup B)$. Therefore $A \subseteq A \cap (A \cup B)$.

   Since we have both inclusions, we must have equality. $A \cap (A \cup B) = A$.

2. $A \cup (A \cap B) = A$.

   We start with the right inclusion. Assume that $x \in A \cup (A \cap B)$. By definition of pairwise union we have $x \in A$. Thus $A \cup (A \cap B) \subseteq A$.

   For the left inclusion, assume $x \in A$. By definition of pairwise union we have either $x \in A$, in which case we are done, or $x \in A \cap B$, in which case we are also done, since $x \in A$ and $x \in B$.

   We have shown both inclusions, therefore we must have $A \cup (A \cap B) = A$.

□

Exercise 3.1.9. Let A, B, X be sets such that $A \cup B = X$ and $A \cap B = \emptyset$. Show that $A = X \setminus B$ and $B = X \setminus A$.

Solution: By assumption we have that A and B are disjoint sets, that is, they have no elements in common. We only show $A = X \setminus B$, the proof for $B = X \setminus A$ is completely analogous. We need to show both left and right inclusion in order to have equality.

For the right inclusion, assume that $x \in A$. Since $x \in A$ we must have $x \in X$. From our assumption, we also have $x \notin B$. For $x \in X \setminus B$ we must have $x \in X$ and $x \notin B$, which we have. We have therefore shown $A \subseteq X \setminus B$.

For the left inclusion, assume $x \in X \setminus B$. We must therefore have $x \in X$ and $x \notin B$. By definition of $X = A \cup B$, we must have $x \in A$. We have therefore shown $X \setminus B \subseteq A$.

Since we have both inclusions, we must have equality. The proof for $B = X \setminus A$ is symmetric. □

Exercise 3.1.10. Let A, B be sets. Show that the three sets $A \setminus B$, $A \cap B$ and $B \setminus A$ are disjoint, and that their union is $A \cup B$.

SOLUTION: To show that the three sets are disjoint we must show that they have no common elements. We do this by showing that if an object is a memeber of one of them, it can't be in any of the other two.

1. Assume $x \in A \setminus B$.

   By definition of set difference we have $x \in A$ and $x \notin B$. Since $x \notin B$ we have $x \notin B \setminus A$, and similarly we have $x \notin A \cap B$.

2. Assume $x \in A \cap B$.

   We have $x \in A$ and $x \in B$, but then we must have $x \notin A \setminus B$ and $x \notin B \setminus A$.

3. Assume $x \in B \setminus A$.

   We have $x \in B$ and $x \notin A$. Since $x \notin A$ we have $x \notin A \setminus B$, and $x \notin A \cap B$.

Since the three sets have no elements in common, they are disjoint. That is $(A \setminus B) \cap (A \cap B) \cap (B \setminus A) = \emptyset$.

We now need to show that the union of the three sets is $A \cup B$. We do this by showing both left and right inclusion.

1. Assume $x \in (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$.

   We therefore have three cases, $x \in A, x \notin B$, or $x \in A, x \in B$ or $x \notin A, x \in B$. In any case we have $x \in A \cup B$.

2. Assume $x \in A \cup B$. We have the same three cases as before. In either case, we have x an element of exactly one of the three sets.

We therefore have that the union between the three sets is $A \cup B$. □

Exercise 3.1.11. Prove that the axiom of replacement implies the axiom of specification. **To do** (4)

3.2 Russell's paradox

Many of the axioms in the previous section makes us able to form sets based on objects with a certain property. One would think that these axioms could be unified into one single axiom. For instance, with the following.

Axiom 3.8 (Universal specification. Dangerous!)**.** *Suppose for every object x we have a property $P(x)$ pertaining to x (so that for every x, $P(x)$ is either a true or a false statement). Then there exists a set $\{x \mid P(x) \text{ is true}\}$ such that for every object y,*

$$y \in \{x \mid P(x) \textit{ is true}\} \iff P(y) \textit{ is true.}$$

This axiom asserts that every property corresponds to a set. In other words, it would make sense to talk about the set of all blue objects. Or the set of all objects that are sets. However, this axiom is the origin of what we call *Russell's paradox.* It cannot be introduced into set theory for this very reason, even though it implies most of the other axioms.

The paradox runs as follows. Let $P(x)$ be the statement

$$P(x) \iff x \text{ is a set, and } x \notin x;$$

i.e., $P(x)$ is only true when x is a set and it does not contain itself. However, if we now let S be the set of all sets, which exists by the axiom of universal specification, then since S is a set, it must also be an element of itself. Therefore $P(S)$ is false. If we now use the axiom of universal specification to construct the set

$$\Omega = \{x \mid P(x) \text{ is true}\} = \{x \mid x \text{ is a set and } x \notin x\}, \tag{3.1}$$

i.e., the set of all sets that does not contain itself. We now ask the question, does Ω contain itself? Is $\Omega \in \Omega$? Assume it does, then by definition $P(\Omega)$ is true and $\Omega \notin \Omega$. Now assume that it doesn't. By definition $P(\Omega)$ is false, therefore $\Omega \in \Omega$. In either case we have both $\Omega \in \Omega$ and $\Omega \notin \Omega$ which is absurd.

The main problem with the above axiom is that is creates sets that are far too large. One can rememedy this by thinking of sets in a hierarchical way. At the bottom of the hierarchy are the *primitive objects*, the objects that are not sets. At the next level we have the sets that only consist of primitive objects (call these *primitive sets*). At the next level, we have the sets that only consists of primitive objects and primitive sets. And so on and so forth. This can be formalized but it is rather complicated to do so, so we instead postulate the following axiom in order to make sure the Russell's paradox does not occur.

Axiom 3.9 (Regularity)**.** *If A is a non-empty set, then there is at least one element x of A which is either not a set, or is disjoint from A.*

One particular consequence of this axiom is that sets are no longer allowed to contain themselves. For the purpose of doing analysis, it turns out that the axiom of regularity is not actually needed, because we are dealing with well-behaved sets. However, this axiom must be included in order to do more advanced set theory.

Exercise 3.2.1. Show that the universal spexification axiom, Axiom 3.8, if assumed to be true, would imply Axioms 3.2, 3.3, 3.4, 3.5 and 3.6. (If we assume all natural numbers to be objects, we also obtain 3.7.) Thus, this axiom, if permitted would simplify the foundations of set theory tremendously (and can be viewed as a basis for an intuitive model of set theory known as "naive set theory"). Unfortunately, as we have seen, Axiom 3.8 is "too good to be true"!

Solution: Assume we for all objects x have a property $P(x)$ pertaining to x. Then there exists a set $\{x \mid P(x)\}$ such that for every object y,

$$y \in \{x \mid P(x)\} \iff P(y).$$

(a) Axiom 3.2

We want to show that Axiom 3.8 implies the existence of the empty set. If we let $P(x)$ be a property pertaining to all objects x such that $P(x)$ is false for all x. Pick any object y. We know from our choice of P that $P(y)$ is false. Since $P(y)$ is false, we have $y \notin \{x \mid P(x)\}$. Since y was arbitrary, this must hold for all objects y, therefore the set $\{x \mid P(x)\}$ contains no elements and is thusly empty. We have now shown the existence of the empty set using only the axiom of universal specification.

(b) Axiom 3.3

We want to show that Axiom 3.8 implies the existence of the singleton sets and the pair sets. Let a be an object, and let $P(x)$ be a property pertaining to x such that $P(x)$ is true if and only if $x = a$. By the axiom of universal specification, there exists a set $\{x \mid P(x)\}$ that only contain the elements x such that $x = a$. However, the only element that can satisfy this is a itself, therefore we have the set $\{a\}$. We can show this is the case by assuming the object a' also has the property that $a' = a$. But we then have the set $\{a, a'\} = \{a', a\} = \{a, a\} = \{a\}$.

We can now apply the same strategy for showing the existence of pair sets. Let a and b be two objects, and let $P(x)$ be the property pertaining to x such that $P(x)$ is true if and only if $x = a$ or $x = b$. By the same token as above, we have the existence of the set $\{a, b\} = \{b, a\}$.

(c) Axiom 3.4

We want to show that Axiom 3.8 implies the existence of the pairwise union.

Let A and B be sets, and let x be an object. Also, let $P(x)$ be the property pertaining to x such that $P(x)$ is true if and only if $x \in A$ or $x \in B$. By the axiom of universal specification, there exists a set $\{x \mid x \in A \text{ or } x \in B\}$ which we will call the *pairwise union* of A and B denoted $A \cup B$.

(d) Axiom 3.5

We want to show that Axiom 3.8 implies the axiom of specification. Let A be a set, and for all x let $P(x)$ be a property pertaining to x such that $P(x)$ is either a true or a false statement. By the axiom of universal specfcation there exists a set $\{x \mid P(x)\}$ which is exactly what the axiom of specification tells us.

(e) Axiom 3.6

We want to show that Axiom 3.8 implies the axiom of replacement. Let A be a set, and for any object $x \in A$, let $P(x)$ be a property pertaining to x such that $P(x)$ is either true or false. By the universal **To do** (5)

(f) Axiom 3.7

Assuming that all natural numbers are object, we want to show that Axiom 3.8 implies 3.7. **To do** (6)

□

Exercise 3.2.2. Use the axiom of regularity (and the singleton set axiom) to show that if A is a set, then $A \notin A$. Furthermore, show that if A and B are two sets, then either $A \notin B$, or $B \notin A$ (or both).

Solution: The axiom of regularity states that if A is a non-empty set, then there is at least one element $x \in A$ which is either not a set, or is disjoint from A.

Assume for contradiction that there exists an object $x = A$ and that $x \in A$. By the axiom of regularity, we must either have x a set or x disjoint from A. Since $x = A$ and A was given to be a set, we must have x disjoint from A. This means that x and A have no common elements, in other words that their intersection is empty. $x \cap A = \emptyset$. However, by proposition 3.1.28, we have $A \cap A = A \neq \emptyset$, therefore $A \notin A$.

Assume further that A and B are two sets. We want to show that at least one of the following must hold: $A \notin B$ or $B \notin A$.

Let us argue by contradiction by showing that not both $A \in B$ and $B \in A$ can be true at the same time.

By the axiom of singleton sets we can form two sets $\{A\}, \{B\}$. Let us assume that $\{A\} \in \{B\}$ and $\{B\} \in \{A\}$. This implies that $B = \{A\}$ and that $A = \{B\}$. We have from the axiom of singularity that $\{A\} \cap B = \emptyset = \{B\} \cap A$. That means, if $x \in \{A\} \cap B$ then $x = A$ and $x \in B$. Similarly, $x = B$ and $x \in A$. We now have $A = B$ as well as $A \in A$ and $B \in B$. Therefore our assumption must be wrong. We can then conclude that at least one of the assumptions must be wrong.[4] **To do** (7)

□

Exercise 3.2.3. Show (assuming the other axioms of set theory) that the universal specification axiom, Axiom 3.8 is equivalent to an axiom postulating the existence of a "universal set" Ω consisting of all objects (i.e., for all objects x we have $x \in \Omega$). In other words, if Axiom 3.8 is true, then a universal set eists, and conversly, if a universal set exists, then Axiom 3.8 is true. (This may explain why Axiom 3.8 is called the axiom of *universal* specification). Note that if a universal set Ω existed, then we would have $\Omega \in \Omega$ by Axiom 3.1, contradicting exercise 3.2.2. Thus the axiom of foundation specifically rules out the axiom of universal specification.

Solution: Assume first that Axiom 3.8 is true. Let $P(x)$ be the property that is true for all objects x. Then there exists a set $\{x \mid P(x)\}$ such that for every object y,

$$y \in \{x \mid P(x)\} \Longleftrightarrow P(y).$$

By definition, we now have a universal set Ω that contains all objects.

Assume now the existence of a universal set $\Omega = \{x\}$ for all objects x. By the axiom of specification, we can select only those objects $y \in \Omega$ for which a certain property $Q(y)$ is true. Based on this, we can create all the other thinkable sets. Certainly, this implies the validity of axiom 3.8. **To do** (8) □

3.3 Functions

In this section we develop the notion of a *function* frome one set to another. This was briefly touched upon during the discussion on natural numbers. Informally, a function $f : X \to Y$ from one set X to another set Y is an operation which assigns each element $x \in X$ to a single element $f(x) \in Y$.

Formally we have:

Definition 3.3.1 (Functions)**.** Let X, Y be sets, and let $P(x, y)$ be a property pertaining to an object $x \in X$ and an object $y \in Y$ such that for every $x \in X$ there is exactly one y for which $P(x, y)$ is true (this is sometimes known as the *vertical line test*). Then we define the *function* $f : X \to Y$ *defined by* P *on the domain* X *and range* Y to be the object which, given any input $x \in X$, assigns an output $f(x) \in Y$, defined to be the unique object $f(x)$ for which $P(x, f(x))$ is true. Thus for any $x \in X$ and $y \in Y$,

$$y = f(x) \Leftrightarrow P(x, y) \text{ is true.}$$

An example of a function could be the following: Let $X = \mathbb{N}$ and $Y = \mathbb{N}$ and let $P(x, y)$ be the property that $y = x{+}{+}$. Then for each $x \in \mathbb{N}$ there is exactly one y for which $P(x, y)$ is true. We can then define the function $f : \mathbb{N} \to \mathbb{N}$ associated to this property, so that $f(x) = x + +$ for all x. We would then have for instance $f(4) = 5$, $f(2n+3) = 2n + 4$ etc.

By the same token, one would think that one could define a *decrement* function $g : \mathbb{N} \to \mathbb{N}$ associated with the property $P(x, y)$ defined by $y{+}{+} = x$. However, this does not define a function, because when $x = 0$ there is no natural number y whose

[4] I have a strong feeling that I have shown something other than requested. Since I never used that assumption $A \in B$ and $B \in A$. I am going to mark this exercise as incomplete.

increment is equal to x. If we however were to redefine g to the domain $\mathbb{N} \setminus \{0\}$. In this case, there is exactly one y for each x such that $y++ = x$.

There are several ways of defining functions. By specifying a functions domain, its range and how one generates the output form each input one has defined a function *explicitly*. In other cases we define a function f by specifying what property $P(x, y)$ links the input x with the output $f(x)$. This is called an *implicit* definition. We also note that functions obey the axiom of substitution: if $x = x'$ then $f(x) = f(x')$.

We also note, that while each input can be assigned to exactly one output, there is nothing stopping us from having unequal inputs giving equal outputs. Consider for instance the property $P(x, y)$ that $y = 7$. The function defined in terms of this property is then $f : \mathbb{N} \to \mathbb{N}$ such that $f(x) = 7$. No matter what input we give this function, we will always get the same output.

We now define some basic concepts and notions for functions. First of them being equality:

Definition 3.3.7 (Equality of functions)**.** Two functions $f : X \to Y, g : X \to Y$ with the same domain and range are said to be *equal*, $f = g$, if and only if $f(x) = g(x)$ for *all* $x \in X$. (If $f(x)$ an $g(x)$ agree for some values of x, but not others, then we do not consider f and g to be equal[5].)

Take for example the functions $x \mapsto x^2 + 2x + 1$ and $x \mapsto (x + 1)^2$ are equal on the domain $\mathbb{R}$ (we haven't defined $\mathbb{R}$ yet, but for the sake of example.)

The functions $x \mapsto x$ and $x \mapsto |x|$ are equal on the positive real axis, but not on $\mathbb{R}$. Therefore, we see that the notion of equality is dependent on the domain the functions are defined on.

We now define the operation of *composition*.

Definition 3.3.10 (Composition)**.** Let $f : X \to Y$ and $g : Y \to Z$ be two functions, such that the range of f is the same set as the domain of g. We then define the *composition* $g \circ f : X \to Z$ of the two functions g and f to be the function defined explicitly by the formula

$$(g \circ f)(x) = g(f(x)).$$

It can easily be shown that $f \circ g$ and $g \circ f$ are not necessarily the same function, however composition is still associative:

Lemma 3.3.12 (Composition is associative)**.** *Let $f : Z \to W, g : Y \to Z$ and $h : X \to Y$ be functions. Then $f \circ (g \circ h) = (f \circ g) \circ h$.*

Proof. Assume that the functions f, g and h are defined as above. We need, by the definition of equality of functions, to show that $(f \circ (g \circ h))(x) = ((f \circ g) \circ h)(x)$ for all $x \in X$.

We first evaluate the left side using the definition of composition:

$$\begin{aligned}(f \circ (g \circ h))(x) &= f(g \circ h(x)) \\ &= f(g(h(x))).\end{aligned}$$

The right hand evaluates to

$$\begin{aligned}((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) \\ &= f(g(h(x))).\end{aligned}$$

Since the left and right hand side agrees, we can conclude with the fact that composition of functions is associative. □

We now describe certain types of functions, namely *one-to-one* functions, *onto* functions, and *invertible* functions.

Definition 3.3.14 (One-to-one functions)**.** A function f is *one-to-one* (or *injecive*) if different elements map to different elements:

$$x \neq x' \implies f(x) \neq f(x').$$

Equivalently, a function is one-to-one if

$$f(x) = f(x') \implies x = x'$$

As we see in the following example, the notion of one-to-one-ness is dependent on the domain. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = n^2$. This function is not one-to-one, because the distinct elements $-1, 1$ map to the same element 1. However, if we restrict the domain to $\mathbb{N}$ the function is one-to-one. $g : \mathbb{N} \to \mathbb{Z}$ defined by $g(n) = n^2$ is one-to-one.

It's important to not what it means for a function not to be one-to-one. In that case one can find distinct elements x and x' in the domain of the function that map to the same element y in the range of the function.

[5] We will later introduce a weaker notion of equality, where two functions are said to be *equal almost everywhere*

Definition 3.3.17 (Onto functions)**.** A function f is *onto* (or *surjective*) if $f(X) = Y$, i.e., every element in Y comes from applying f to some element in X:[6]

For every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

For example, take the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2$ is not onto because the negative numbers are not in the image of f. If we however restrict the range of f to $\mathbb{N}$ then the function becomes onto. We can therefore see that the notion of a function being onto is dependent on the range of the function.

Definition 3.3.20 (Bijective functions)**.** Functions $f : X \to Y$ which are both one-to-one and onto are also called *bijective* or *invertible*.

If we take the function $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ defined by $f(n) = n{+}{+}$ we can see that this is a bijection. This is simply restating Axiom 2.2, 2.3, 2.4. However, if we expand the range of f to $\mathbb{N}$ the function is no longer a bijection. Therefore the notion of a bijective function depends on both the domain and range of the function.

We often call a function $x \mapsto f(x)$ that is bijective a *one-to-one correspondence*. This is a term that will be commonly used in discussions about set cardinality. If f is bijective, then for every $y \in Y$ there is exactly one $x \in X$ such that $f(x) = y$. There is at least one because of surjectivity, and at most one because of injectivity. This value of x is denoted $f^{-1}(y)$; thus f^{-1} is a function from Y to X. We call f^{-1} the *inverse* of f.

Exercise 3.3.1. Show that the definition of equality in Definition 3.3.7 is reflexive, symmetric and transitive. Also verify the substitution property: if $f, \tilde{f} : X \to Y$ and $g, \tilde{g} : Y \to Z$ are functions such that $f = \tilde{f}$ and $g = \tilde{g}$, then $g \circ f = \tilde{g} \circ \tilde{f}$.

Solution: Let us first show the three properties.

(i) Reflexive

We want to show that $f = f$. We must have $f(x) = f(x)$ for all x in X. Therefore by definition, equality between functions is reflexive.

(ii) Symmetric

We want to show that $f = g \Rightarrow g = f$. If we assume $f = g$, then we have $f(x) = g(x)$ for all $x \in X$. We must therefore have $g(x) = f(x)$, therefore $g = f$.

(iii) Transitive

We want to show that if $f = g$ and $g = h$ then $f = h$. Assuming that $f = g$ and $g = h$ we have $f(x) = g(x)$ and $g(x) = h(x)$ for all x. Therefore we have $f(x) = h(x)$ for all x, and thus $f = h$.

We now want to show the substitution property of composition of functions. We need to show that $g \circ f = \tilde{g} \circ \tilde{f}$. By definition we must have $(g \circ f)(x) = (\tilde{g} \circ \tilde{f})(x)$ for all $x \in X$. Using the definition of composition we get the following equation

$$g(f(x)) = \tilde{g}(\tilde{f}(x)).$$

Since we have $f = \tilde{f}$ we have $f(x) = \tilde{f}(x)$ for all x, we can therefore substitute and we get $\tilde{g}(\tilde{f}(x)) = \tilde{g}(f(x))$. Similarly, we can subsitute $\tilde{g}$ for g, and we get that $\tilde{g} \circ \tilde{f} = g \circ f$. □

Exercise 3.3.2. Let $f : X \to Y$ and $g : Y \to Z$ be functions. Show that if f and g are both injective, then so is $g \circ f$; similarly, show that if f and g are both surjective, then so is $g \circ f$.

Solution: First, assume that f and g are both injective. This means that given $x, x' \in X$ such that $x \neq x'$, and $y, y' \in Y$ such that $y \neq y'$ we must have $f(x) \neq f(x')$ and $g(y) \neq g(y')$.

From the definition of composition we have

$$(g \circ f)(x) = g(f(x)) \text{ and } (g \circ f)(x') = g(f(x'))$$

Since f is injective we must have $f(x) \neq f(x')$, but then since g is injective we must have $g(f(x)) \neq g(f(x'))$. We can therefore conclude with $g \circ f$ being injective.

Now assume that f and g are both surjective. This means that for every $y \in Y$ there is at least one element $x \in X$ such that $f(x) = y$, and for every $z \in Z$ there is at least one element $y \in Y$ such that $g(y) = z$.

Again, from the definition of composition we have

$$(g \circ f)(x) = g(f(x)).$$

[6] Strictly speaking, we have not yet defined what it means for $f(X) = Y$, thats the subject of the next section.

For $g \circ f$ to be injective there must for every $z \in Z$ be at least one $x \in X$ such that $(g \circ f)(x) = z$ Since f is injective, we are guaranteed that every element in Y is mapped to, we are therefore because of g being injective guaranteed the whole of Z is mapped to. We can then conclude with the composition $g \circ f$ being injective. □

Exercise 3.3.3. When is the empty function injective? Surjective? Bijective?

Solution: The empty function is the function with the empty set as domain. It can be shown that this function is unique. Let f be the empty function and A be any set.

$$f : \emptyset \to A,$$

is then the empty function.

For f to be injective, we must have $x \neq x' \Rightarrow f(x) \neq f(x')$. This however is vacously true, since the empty set contains no elements.

For f to be surjective, we must have that for every element a in A, there is at least one element $x \in \emptyset$ such that $f(x) = a$, however, this contradicts the definition of the empty set, therefore f can not be surjective. However, if we let $A = \emptyset$, then again this is vacously true. Under the condition that the range of the empty function is the empty set, then f is surjective.

Based on this, we can conclude with f being bijective if and only if $A = \emptyset$. □

Exercise 3.3.4. In this section we give some cancellation laws for composition. Let $f : X \to Y, \tilde{f} : X \to Y, g : Y \to Z$ and $\tilde{g} : Y \to Z$ be functions. Show that if $g \circ f = g \circ \tilde{f}$ and g is surjective, then $f = \tilde{f}$. Is the same statement true if g is not injective? Show that if $g \circ f = \tilde{g} \circ f$ and f is surjective, then $g = \tilde{g}$. Is the same statement true if f is not surjective?

Solution: Assume that $f \neq \tilde{f}$. By definition, we must then have some $x \in X$ such that $f(x) \neq \tilde{f}(x)$.

We have that $g(f(x)) = g(\tilde{f}(x))$ for all $x \in X$, and since g is injective this implies that $f(x) = \tilde{f}(x)$ for all $x \in X$. This contradicts our assumption, therefore $f = \tilde{f}$.

Had g not been injective, there would be no way for us to get to this contradiction, because there would be no way for us to guarantee that $f(x) \neq \tilde{f}(x) \Rightarrow g(f(x)) \neq g(\tilde{f}(x))$.

Now we assume f surjective, and $g \circ f = \tilde{g} \circ f$. Since the two compositions are equal we must have

$$g(f(x)) = \tilde{g}(f(x)) \text{ for all } x \in X.$$

Since f is surjective, we know that for all $y \in Y$ there exist some $x \in X$ such that $f(x) = y$. What this tells us is that the whole domain of g is mapped to by f. In other words, we have

$$g(y) = \tilde{g}(y), \text{ for all } y \in Y,$$

and therefore $g = \tilde{g}$ by definition. □

Exercise 3.3.5. Let $f : X \to Y$ and $g : Y \to Z$ be functions. Show that if $g \circ f$ is injective, then f must be injective. Is it true that g must also be injective? Show that if $g \circ f$ is surjective, then g must be surjective. Is it true that f must also be surjective?

Solution: We know from Exercise 3.2.2 that if the two functions f and g are injective, then so is the composition. We now want to show the other implication. **To do** (9)

□

3.4 Images and inverse images

To do (10)

3.5 Cartesian Products

To do (11)

3.6 Cardinality of sets

To do (12)

Chapter 4

Integers and rationals

4.1 The integers

We would now like to introduce a new operation, namely subtraction. In order for us to do that we have to pass from the natural number system, to a larger nuber system, that of the *integers*. Informally, the integers are what you get when you "subtract" two natural numbers.

We will temporarily write integers not as a difference $a - b$, but instead use a new notation $a — b$ to define integers. The — is a meaningless placeholder.

Definition 4.1.1 (Integers). An *integer* is an expression of the form $a — b$ where a and b are natural numbers. Two integers are considered to be equal $a — b = c — d$, if and only if $a + d = c + b$. We let $\mathbb{Z}$ denote the set of all integers.

For instance $3 — 5$ is an integer, and equal to $2 — 4$ because $3 + 4 = 5 + 2$. The number 3 is not an integer (yet!) since it is not on the form $a — b$.

We need to verify that this is a well defined notion of equality by checking that it is reflexive, transitive and symmetric. We verify transitivity here and leave the two others for the exercises.

Let us assume that $a — b = c — d$ and that $c — d = e — f$. We therefore have $a + d = c + b$ and $c + f = e + d$. We need to show that it then follows that $a + f = e + b$. Adding the two equations we get

$$a + d + c + f = c + b + e + d.$$

By the cancellation law for addition we get

$$a + f = e + b,$$

thus $a — b = e — f$.

We will later, once we define operations on the integers, verify the substitution axiom. We now define addition and multiplication on the integers.

Definition 4.1.2. The sum of two integers, $(a — b) + (c — d)$, is defined by the formula

$$(a — b) + (c — d) = (a + c) — (b + d)$$

The product of two integers, $(a — b) \times (c — d)$, is defined by

$$(a — b) \times (c — b) = (ac + bd) — (ad + bc).$$

For instance, $(3 — 5) + (1 — 4)$ is equal to $(4 — 9)$. Before we truly can accept these definitions, we must verify that if we replace one of the integers by an equal integer, the sum or product does not change.

Lemma 4.1.3 (Addition and multiplication are well-defined). *Let a, b, a', b', c, d be natural numbers. If $(a — b) = (a' — b')$, then $(a — b) + (c — b) = (a' — b') + (c — b)$ and $(a — b) \times (c — d) = (a' — b') \times (c — d)$, and also $(c — d) + (a — b) = (c — d) + (a' — b')$ and $(c — d) \times (a — b) = (c — d) \times (a' — b')$. Thus addition and multiplication are well-defined operations (equal inputs give equal outputs).*

Proof. We evaluate both sides of each equality. $(a — b) + (c — d) = (a + c) — (b + d), (a' — b') + (c — d) = (a' + c) — (b' + d)$. □

To do. . .

□ 1 (p. 10): Finish this exercise

□ 2 (p. 13): Show the second case

□ 3 (p. 18): Finish the rest of the claims

□ 4 (p. 20): Do this exercise

□ 5 (p. 21): Finish this exercise

□ 6 (p. 21): Finish this exercise

□ 7 (p. 22): Finish this exercise

□ 8 (p. 22): Show this rigorously properly using the axioms. Don't be lazy!

□ 9 (p. 25): Finish this exercise

□ 10 (p. 25): Finish this section

□ 11 (p. 25): Finish this section

□ 12 (p. 25): Finish this section