Proofs and Mathematical Writing

Ebrahim Ebrahim

This document was compiled on May 7, 2021 at 14:17.

Contents

Layout Section 2 will develop mathematical logic and show you how logical arguments factor into writing. We will not yet have anything to argue *about*, so our "proofs" in section 2 will be about nothing in particular. Section 3 will then give some mathematical objects to talk about, and we will then put content into the empty skeleton arguments of section 2. Section 3 will take you from the axioms of set theory up through a construction of the natural numbers and more. We start in section 1 with an introduction to formal axiomatic systems and informal proofs.

1 Mathematical Language

1.1 Parts of Speech

In a language, a *part of speech* is a collection of words that share grammatical properties. For example here are some common English parts of speech: pronouns, nouns, verbs, adjectives, and adverbs. Different languages can have different parts of speech that are useful for describing their grammar. To build up the grammar of a language, one can specify how parts of speech fit together to form larger *constituents*, such as noun phrases and clauses. One can further describe how constituents fit together to form even more complex constituents, eventually grammatical sentences.

Mathematics is a language, and so it makes sense to build up its grammar (its *syntax*) using this same strategy. Instead of pronouns, nouns, verbs, noun phrases, sentences, and so on, there are just four constituents in mathematics. Two are basic parts of speech and two are more complex constituents:

- *Variables* are a basic part of speech.
- *Constants* are a basic part of speech.
- *Terms* can be built out of variables, constants, other terms, and propositions.
- *Propositions* can be built out of variables, constants, terms, and other propositions.

Let's go through each of these in detail.

Variables Variables serve as placeholders, waiting to be replaced by other symbols. They are most like pronouns in English. For example the pronoun "it" is a placeholder referring to something in a discussion, but what it refers to depends on the context of the discussion. Variables are like that. Here are some variables:

$$a \quad b \quad A \quad f \quad q \quad x \quad \alpha \quad \beta$$

Variables are copies of letters coming from an alphabet (usually Latin or Greek) and written in ink/chalk/pixels.

Constants Constants are used as fixed names for specific mathematical objects. They are most like *proper* nouns in English. Here are some constants:

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad \mathbb{N} \quad \mathbb{R} \quad \{\}$$

The difference between constants and variables is that constants are not meant to be substituted for. The constant "2" refers to a specific thing, rather than being a placeholder for something.

Note that when we discuss parts of speech here, we are mainly talking about *elements of language* and not about what those elements *refer* to. Germany is not a noun, it's a country. "Germany" is, however, a noun. Similarly, we can say that 2 is not a constant, but rather "2" is. And x is not a variable, but rather "x" is. Quotation marks help us make the distinction between a symbol and what the symbol refers to (though I will often be lazy and drop the quotation marks).

Terms Terms are strings of marks (expressions) that refer to *mathematical objects*. Since variables and constants refer to mathematical objects, they are special cases of terms. But you can also have more complicated terms that are built out of simpler ones. Terms are most like *noun phrases* in English. For example the phrase "the cup that you drank from" is a noun phrase– it doesn't make any assertion but rather it just refers to a *thing*. Here are some terms:

x

7

$\{2, 3, a, 7\}$

$f(x)$

$\{(z, w)\} \circ g$

$S \times Q$

the square of the seventh prime number

a triangle

twelve dimensional euclidean space

the collection of even integers

$\{\, n \mid n \in \mathbb{Z} \text{ and } n \text{ is even} \,\}$

$$\{\, n \mid (n \in \mathbb{Z}) \wedge (\exists k \,|\, (k \in \mathbb{Z}) \wedge (2k = n)) \,\}$$

The last three terms actually refer to the same mathematical object; this will soon become clear when we get into *how* the symbols refer to objects (semantics). For now we are only looking at *which* strings of symbols *can* refer to objects (syntax). You can see that some terms are more "symbolic," while others are more "Englishy." The formal language of mathematics is purely symbolic, but we almost never use the language in its purest form. Typically, we communicate by some combination of English and mathematics.

Propositions Propositions are strings of marks (expressions) that *make assertions*. They are most like *sentences* in English (*declarative* sentences, to be precise). Propositions can be true or false. Here are some propositions:

$x \in S$.

$5 \notin x$.

$0 = 2$.

$(x \neq y) \wedge (x \neq z) \wedge (y \neq z)$.

x, y, and z are distinct.

Either $A \subseteq P$ or $x \in S$, but not both.

$f : X \to Y$.

If $x \in S$, then we either have $x \notin W$ or we have $x \in \mathbb{Z}$.

$\neg(X \times Y \subseteq Z)$.

Every integer is even.

$(\, \forall n \mid (n \in \mathbb{Z}) \Rightarrow (\, \exists k \mid (k \in \mathbb{Z}) \wedge (2k = n)\,)\,)$.

The last two propositions are actually saying the same thing, as we will see when we get into semantics. Again, you can see that some propositions are more "symbolic," while others are more "Englishy." Typically, we make mathematical assertions by using some combination of English and mathematics. The English that we use is a crude, but human-friendly, stand-in for formal mathematical statements.

Exercise 1: Determine whether each of the following is a term or a proposition.

1. n

2. $1 + 1 = 0$
3. n is an odd integer
4. an odd integer
5. f is a function with domain S
6. $1 + (2 + 3)$
7. the empty set
8. the sum of two vectors is another vector
9. the zero vector
10. the evenness of 2

1.2 Theorems and Proofs

Mathematics is ultimately about propositions. Propositions *say* things, sometimes true things and sometimes false things. We want to know: Which propositions are true? What does "true" even mean? We will not exactly define "true," but we will define "provable," and provability will be our notion of truth.

The rules of logic allow us to make deductions and *prove* new propositions from already proven propositions. Those already proven propositions themselves had to be proven via a sequence of logical deductions that was applied to other previously proven propositions. And so on... but where does it all start?

Axioms Some propositions are declared to be *axioms*, which makes them serve as starting points in our mathematical system. The next paragraph will clarify this.

Proofs A *proof* is a sequence of propositions such that each proposition is either (1) an axiom, (2) an already proven proposition, or, (3) the result of applying the rules of logic to *previous* propositions in the sequence. A proposition that appears in a proof is said to be *proven*.

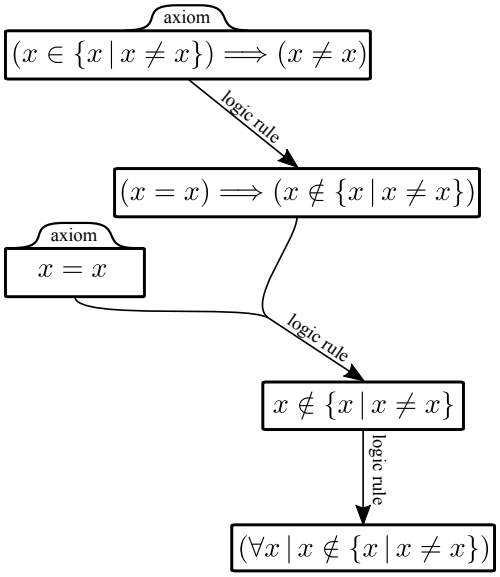
Theorems A *theorem* is a proposition which is asserted to have a proof.

Example Here is an example of a proof of the proposition "$(\forall x \mid x \notin \{\, x \mid x \neq x \,\})$":

$(x \in \{\, x \mid x \neq x \,\}) \implies (x \neq x)$
$(x = x) \implies (x \notin \{\, x \mid x \neq x \,\})$

$x = x$
$x \notin \{\, x \mid x \neq x \,\}$
$(\forall x \,|\, x \notin \{\, x \mid x \neq x \,\})$

Do not worry about interpreting what the propositions are trying to *say*– I just want to make a point about formal proofs. What you see above is a sequence of five propositions, ending with the one I claimed to be proving, namely "$(\forall x \,|\, x \notin \{\, x \mid x \neq x \,\})$". To really be convinced that we are looking at a proof, we would need a *justification* for each of the five propositions– for each proposition we need to either point out that it is an axiom, or we need to verify that it follows logically from the previous propositions. In this example, two of the propositions are axioms, and the other three are logical deductions; here is a schematic depiction of these relationships:



Again, don't worry yet about understanding why this works. What I want you to take away from this is the general structure: we have axioms serving as starting propositions, and we use logic to "flow" out from the starting points and prove other propositions.

Given a bunch of axioms to start with, what theorems can we deduce? To answer this question is to do math.

Remark about Axioms Axioms often serve to *give meaning* to symbols. For example, the axiom $x = x$ (along with some other axioms related to equality) gives meaning to the symbol "=". Without the axiom, we would still be able to form propositions like $a = b$ but we would never be able to prove anything about them. Suppose you "disagree" with the axiom $x = x$ and instead use some other propositions related to "=" as axioms. That's perfectly fine– you would just be giving a different meaning to the symbol "=" and it would serve a different purpose in your language.

Math is for Humans The five-line proof given above is a *formal proof*– it is written in pure mathematical language with absolutely no English. This is great if you want absolute rigor, but it is not friendly to read if you are not a computer. The main purpose of a mathematical proof is for it to convince a *human* that a theorem is true. But formal proofs make for really inefficient communication between humans. Thus we are faced with a trade-off: we can sacrifice some rigor to gain efficiency of communication.

Informal proofs use a mixture of English and mathematics to make arguments. For an example, look ahead a few paragraphs for an informal version of the five-line proof above.

We need to find a good balance between rigor and efficient communication. Finding that balance is one of the great challenges when you first learn how to write proofs. If we sacrifice too much rigor in an argument, then we can lose confidence in its correctness. Or worse, we can start to prove false things! When developing a new mathematical theory, it's generally good to err on the side of being more rigorous. Then, as the theory develops and common patterns of arguments become routine, one can slowly relax the rigor in favor of efficiency.

That's what this text is all about. While it is partly giving you some specific mathematical content like set theory, this text is mainly about how to communicate proofs in that balanced way– rigorous, yet informal and efficient.

Here is an informal version of the five-line proof from above.

Theorem: The set $\{ x \mid x \neq x \}$ has no elements.

Proof: If $\{ x \mid x \neq x \}$ did have an element, say x, then we would have $x \neq x$. But in fact it is an axiom that $x = x$. Thus $\{ x \mid x \neq x \}$ cannot have any elements. ■

The arguments are essentially the same ones that appeared in the five-line formal proof. But, compared to the formal proof, it's much easier to process the arguments in the informal proof (though I'm still not expecting you to do so just yet).

Exercise 2: In this exercise we will work with a made-up deductive language which works as follows:

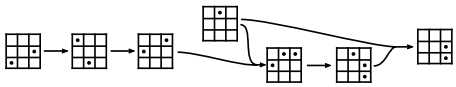
- Propositions are the only part of speech. The propositions are 3×3 grids in which each square is either blank or contains a dot. Here are three random example propositions:

- There are two logical rules in this language. The first rule is that if a particular proposition holds, then its clockwise rotation by ninety degrees follows. So if  holds, then you can deduce that  . The second rule is that if two propositions Φ and Ψ hold, then you can deduce a third proposition which contains a dot in any square that has a dot in either Φ or Ψ, but not both. So for example if you have the two propositions  and  , then you can deduce from them that  .

- There are only two axioms in this language, and they are as follows:

As a demonstration of this deductive language, here is a proof that  :

Can you see how this proof is correct? These annotations may help:



Now...

1. How many propositions are there in this language? How many propositions do you think there are in mathematics? How many sentences are there in English?

2. Give a completely formal proof that  . To help out your reader, annotate the proof with arrows like in the example above.

3. (Open-ended) Can you think of a way to write an *informal* version of your proof? It would be an English description of your proof that does not explain every detail but still captures the essence of your formal proof.

4. (Irrelevant but fun) Can you figure out how many propositions in this language are provable and how many are not?

2 Logic and Writing Mathematical Arguments

The rest of this course will introduce logic and set theory, starting with logic in this section. Our goal with logic is not only to understand the rules of deduction, but also to gain the ability to *write* paragraph-style deductive arguments– informal proofs.

Logic is all about manipulating *propositions*, so you will not see many *terms* showing up in this section. In fact, we will find ourselves having to discuss proofs while having nothing in particular to prove anything about. Mathematical propositions are supposed to say things about mathematical objects; without any mathematical objects in hand, we cannot form any actual mathematical propositions. We will proceed with the discussion anyway, using two strategies:

First, we will use the following capital Greek letters as placeholders for mathematical propositions:

$$\Phi, \Psi, \Omega, \Sigma, \Gamma, \Delta.$$

When you see these capital Greek letters, remember that they are *not variables*, at least not in the sense of mathematical variables. They are not to be replaced by mathematical *objects*. Rather, they are meant to be replaced by *propositions*. When they appear in English sentences, they will take the grammatical role of independent clauses. So, for example, we accept the following as grammatically correct English sentences:

> I believe that Φ.
> They thought that Φ, but in fact Ψ.
> Φ.

Our second strategy is to apply the rules of logic to English sentences. Even though Φ, Ψ, etc. are supposed to stand for *mathematical* propositions, we will allow ourselves to replace them by declarative sentences in *English*. For example, replacing Φ by "Jim stole the car" and Ψ by "Jim is an upstanding guy" in the above examples, we get the sentences

> I believe that Jim stole the car.
> They thought that Jim stole the car, but in fact Jim is an upstanding guy.
> Jim stole the car.

Later when we reach section 3, we will start to work with actual mathematical propositions.

Section 2.8 contains a reference table summarizing the logical constructions that are about to show up; you can look there to get a sense for what is to come.

Exercise 3: Which of the following are grammatically correct? Hint: replace Greek letters with English sentences and see what makes sense.

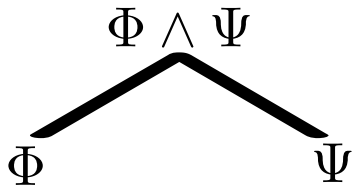
1. She said that Ω, and I think she's onto something.
2. Take that, you accursed Φ!
3. Why don't we just Ψ?
4. To Φ, or not to Φ, that is the question.
5. Whether Ω or Σ, it will always be the case that Φ.
6. Σ and Δ, but not Ψ.
7. Despite all the Γ, they still wanted to Δ.
8. Whenever Ω, it turns out that Γ.
9. It is not true that Φ.

2.1 And, Or, and Not

Conjunction Given propositions Φ and Ψ, we can form their *conjunction*

$$\Phi \wedge \Psi,$$

which is expressed in English as "Φ and Ψ." From the conjunction $\Phi \wedge \Psi$, you can deduce Φ and you can deduce Ψ. In order to prove that $\Phi \wedge \Psi$, you must prove both that Φ and that Ψ. The following diagram, showing what you can deduce from $\Phi \wedge \Psi$, kind of looks like the "$\wedge$" symbol:

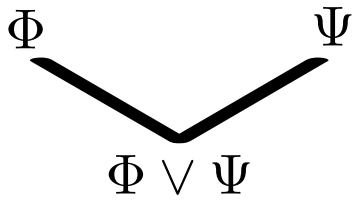


Order does not matter for $\wedge$; we consider $\Phi \wedge \Psi$ and $\Psi \wedge \Phi$ to be the same.

Disjunction Given propositions Φ and Ψ, we can form their *disjunction*

$$\Phi \vee \Psi,$$

which is expressed in English as "Φ or Ψ." In order to prove that $\Phi \vee \Psi$, you can either prove that Φ or you can prove that Ψ. So if Φ and Ψ happen to both hold, then you can still deduce that $\Phi \vee \Psi$ (unlike the way "or" is sometimes used in English). The following diagram, showing what you can use to deduce $\Phi \vee \Psi$, kind of looks like the "$\vee$" symbol:



Order does not matter for $\vee$; we consider $\Phi \vee \Psi$ and $\Psi \vee \Phi$ to be the same.

If you know that $\Phi \vee \Psi$, then how can you use this fact in your arguments? You cannot deduce Φ and you cannot deduce Ψ, so how do you proceed if you want to prove some other proposition Ω? The rule that lets you proceed is called *proof by cases*:

Rule 1: Proof by cases
Suppose that you can prove Ω by assuming Φ, and you can also prove Ω by assuming Ψ. Then you can deduce Ω from $\Phi \vee \Psi$.

In a written proof, the format of a proof by cases ends up like this:

Theorem: Assuming that either Φ or Ψ holds, we have Ω.

Proof: Assume that either Φ or Ψ holds.
Case 1: Suppose that Φ holds.

[insert argument here convincing the reader that Ω holds]

Case 2: Suppose that Ψ holds.

[insert argument here convincing the reader that Ω holds]

Since Ω holds in both cases, we can conclude that Ω holds. ■

Let's do an example using English sentences. Say you are hiking with your friend, and you see your friend brush past a plant with three-leaf bunches. You're not sure if it's poison ivy or poison oak, but you know that it is one of them, and you know that both plants will cause a rash when touched. So you argue to your friend: "Suppose that plant was poison ivy. Then you would get a rash. Now suppose the plant was poison oak. Then you would also get a rash. I'm sure that the plant was either poison ivy or it was poison oak, so you can expect a rash my friend." That's a proof by cases. To make the proof structure apparent in the formatting given above, replace Φ by "the plant is poison ivy," replace Ψ by "the plant is poison oak," and replace Ω by "you will get a rash."

Negation Given a proposition Φ, we can form its *negation*

$$\neg\Phi,$$

which is expressed in English as "it is not the case that Φ." To prove $\neg\Phi$ is to disprove Φ, and in fact this is what "disprove" means. When Φ holds we say that Φ is *true*, and when $\neg\Phi$ holds we say that Φ is *false*. We consider $\neg\neg\Phi$ to be the same as Φ.

A proposition of the form $\Phi \wedge \neg\Phi$ is called a *contradiction*. If something can both be and not be the case, then our entire deductive system is certainly broken. We hope that no contradiction is provable in our language. This leads us to accept the following as a way of proving a negation $\neg\Phi$:

Rule 2: Proof by contradiction
If assuming Φ allows you to deduce a contradiction, then it must be that $\neg\Phi$.

In a written proof, the format of a proof by contradiction ends up like this:

Theorem: $\neg\Phi$.

Proof: Suppose, for the sake of obtaining a contradiction, that Φ holds.

> [insert argument convincing reader that a contradiction, something of the form $\Psi \wedge \neg\Psi$, now follows]

Since this is a contradiction, we conclude that $\neg\Phi$. ■

Let's do an example using English sentences. Say you're investigating a crime and you are considering a particular suspect. Assuming the suspect did commit the crime, you can deduce that the suspect must have been at the crime scene on that day. Upon questioning witnesses, you discover that the suspect was at work and could not have been at the crime scene that day. This contradiction leads you to reject the original assumption; the suspect must not have committed the crime. Making an assumption so that you can reject it after deducing an impossible situation– that is a proof by contradiction. To make the proof structure apparent in the formatting given above, replace Φ by "the suspect committed the crime" and replace Ψ by "the suspect was at the crime scene that day".

The proof by contradiction rule rejects that a mathematical proposition can be both true and false. There's another rule involving negation which enforces that mathematical propositions must be either true or false:

Rule 3: Excluded middle
$\Phi \vee \neg\Phi$

There is no "middle ground" in which a proposition is neither true nor false.

Exercise 4: The "or" of mathematical logic sometimes behaves differently from the English "or." Describe a situation in which

"The cake is flavored with either vanilla or chocolate."

would pretty much be considered false, while

"The cake is flavored with vanilla" $\vee$ "The cake is flavored with chocolate".

would be true.

Exercise 5: Suppose we know the following three facts:

- Whenever it rains over night, the grass gets wet.
- On a night that it doesn't rain, the sprinklers are run.
- Whenever sprinklers are run, the grass gets wet.

Now write a proof of the following statement: "The grass got wet last night." To make your argument, apply excluded middle to the statement "It rained last night," and then do a proof by cases. Follow the formatting given in this section for proof by cases.

Exercise 6: Suppose we know the following four facts:

- Whenever it rains over night, the grass gets wet.
- On a night that it doesn't rain, the sprinklers are run.
- Whenever sprinklers are run, *as long as they are not broken*, the grass gets wet.
- The grass was dry last night.

Now write a proof of the following statement: "It did not rain last night and the sprinklers are broken." To make your argument, do a proof by contradiction to establish "it did not rain last night," and do another proof by contradiction to establish "the sprinklers are broken." Once both are established you can conclude the conjunction. Follow the formatting given in this section for proof by contradiction.

Exercise 7: Thanks to the law of excluded middle, there are only two possibilities for a

single proposition Φ: it is either true or false. For *two* propositions Φ and Ψ, there are *four* possibilities, which we can list in a nice table:

Φ	Ψ
F	F
F	T
T	F
T	T

For three propositions there are eight possibilities, and so on. This suggests a useful way to think about the logical operators $\wedge$, $\vee$, and $\neg$:

Φ	Ψ	$\Phi \wedge \Psi$
F	F	F
F	T	F
T	F	F
T	T	T

Φ	Ψ	$\Phi \vee \Psi$
F	F	F
F	T	T
T	F	T
T	T	T

Φ	$\neg\Phi$
F	T
T	F

Here we are simply listing all the possibilities for the component propositions Φ, Ψ, etc., and then we are indicating whether the complex proposition is true or false in each case. These are called *truth tables*.

1. Write out a truth table for $\neg(\Phi \wedge \Psi)$. It should have four rows.

2. Write out a truth table for $(\Phi \wedge \Psi) \vee \Omega$, and also for $\Phi \wedge (\Psi \vee \Omega)$. The table should have eight rows, and you can feel free to make just one table in which there is a column for $(\Phi \wedge \Psi) \vee \Omega$ and a column for $\Phi \wedge (\Psi \vee \Omega)$.

3. Your answer to the above should convince you that it's a terrible idea to write something like "$\Phi \wedge \Psi \vee \Omega$." Replace Φ, Ψ, and Ω by English sentences in $\Phi \wedge \Psi \vee \Omega$ such that you get an ambiguous English sentence. Explain the ambiguity in your sentence.

4. Write out a truth table for $(\Phi \wedge \Psi) \wedge \Omega$, and also for $\Phi \wedge (\Psi \wedge \Omega)$. The answer should convince you that there is no trouble at all with writing $\Phi \wedge \Psi \wedge \Omega$, though you were probably convinced anyway since $\Phi \wedge \Psi \wedge \Omega$ can obviously only mean: "Φ, Ψ, and Ω are all true."

5. Write out a truth table for $(\Phi \wedge \Psi) \vee \Phi$. This one should just have four rows. Looking at the table, do you see a way to "simplify" the complex proposition $(\Phi \wedge \Psi) \vee \Phi$?

6. Write out a truth table for $(\Phi \wedge \Psi) \vee \Omega$, and also for $(\Phi \vee \Omega) \wedge (\Psi \vee \Omega)$. This should show you that $\vee$ can "distribute" over $\wedge$.

7. Write out a truth table for $(\Phi \vee \Psi) \wedge \Omega$, and also for $(\Phi \wedge \Omega) \vee (\Psi \wedge \Omega)$. This should

show you that $\wedge$ can "distribute" over $\vee$.

8. Write out a truth table for $\neg(\Phi \wedge \Psi)$, and also for $(\neg\Phi) \vee (\neg\Psi)$.

In parts 4 through 8, you see that certain propositions are "equivalent" in some sense. The formal meaning of "equivalent" will be discussed in the next section.

2.2 If and Iff

Implication Given propositions Φ and Ψ, we can form the *implication*

$$\Phi \Rightarrow \Psi,$$

which is expressed in English as "Φ implies Ψ" or "if Φ, then Ψ." The "Φ" part of an implication $\Phi \Rightarrow \Psi$ is called the *hypothesis*, and the "Ψ" part is called the *conclusion*. To prove $\Phi \Rightarrow \Psi$, start by assuming Φ and then give an argument that Ψ follows. That is, assume the hypotheses and then argue that the conclusion follows. Such a proof ends up structured like this:

Theorem: If Φ, then Ψ.

Proof: Assume that Φ.

[insert argument convincing reader that Ψ holds]

Thus, $\Phi \Rightarrow \Psi$. ■

The rule that allows us to use $\Phi \Rightarrow \Psi$ is modus ponens:

Rule 4: Modus Ponens
Given $\Phi \Rightarrow \Psi$ and Φ, you can deduce Ψ.

Here is also another great rule for using an implication (this one can be derived from modus ponens via a proof by contradiction):

Derived Rule 5: Modus Tollens
Given $\Phi \Rightarrow \Psi$ and $\neg\Psi$, you can deduce $\neg\Phi$.

Logical Equivalence Given propositions Φ and Ψ, we can form the *logical equivalence*

$$\Phi \Leftrightarrow \Psi,$$

which is expressed in English as "Φ if and only if Ψ," often shortened to "Φ iff Ψ."

An equivalence holds when two propositions are forced to be true or false *together*– that is, when they are either both true or both false.

To prove an equivalence $\Phi \Leftrightarrow \Psi$, simply prove both of the implications $\Phi \Rightarrow \Psi$ and $\Psi \Rightarrow \Phi$. The proof will be structured like this:

Theorem: $\Phi \Leftrightarrow \Psi$.

Proof: Assume that Φ.

[insert argument convincing reader that Ψ holds]

Now assume that Ψ.

[insert argument convincing reader that Φ holds]

■

Using an equivalence works a lot like modus ponens, except it goes in both directions. If you know that $\Phi \Leftrightarrow \Psi$, then you can deduce Φ from Ψ, $\neg\Phi$ from $\neg\Psi$, Ψ from Φ, and $\neg\Psi$ from $\neg\Phi$.

Here are the truth tables for $\Rightarrow$ and $\Leftrightarrow$:

Φ	Ψ	$\Phi \Rightarrow \Psi$
F	F	???
F	T	???
T	F	F
T	T	T

Φ	Ψ	$\Phi \Leftrightarrow \Psi$
F	F	T
F	T	F
T	F	F
T	T	T

There should be nothing surprising there, except that I've left some question marks in position where I think you might be surprised. If Φ is false, then what of the proposition $\Phi \Rightarrow \Psi$? It has to be either true or false (due to excluded middle), so which is it? Put another way: Suppose you say "If 3 is even, then 3 is divisible by 2." Knowing that 3 is not even, are you a liar? Is your statement true or false? The answer is that it's *true*! Here is the completed truth table for $\Rightarrow$:

Φ	Ψ	$\Phi \Rightarrow \Psi$
F	F	T
F	T	T
T	F	F
T	T	T

Putting T there is not an arbitrary choice– if you agreed with all the previous logical rules then you *must* agree that $\Phi \Rightarrow \Psi$ is *true* when Φ is false. Let me try and convince you. First we need to revisit contradictions.

Recall how *proof by contradiction* works: If an assumption leads to a contradiction, then the assumption is rejected as false. If you assume Ψ, and then after some argumentation you deduce $\Phi \wedge \neg\Phi$, then you can back out of your original assumption and conclude without a doubt that $\neg\Psi$. Now let's think, hypothetically, what would happen if a contradiction $\Phi \wedge \neg\Phi$ were actually *true*? If $\Phi \wedge \neg\Phi$ holds, then we can prove Ψ by contradiction as follows:

> Suppose, for the sake of contradiction, that $\neg\Psi$ holds.
>
> Since $\Phi \wedge \neg\Phi$ has already been assumed to hold, we've already reached a contradiction.
>
> We conclude that $\neg\neg\Psi$, and therefore Ψ, must hold.

Let's be clear about what just happened: from the assumption $\Phi \wedge \neg\Phi$, we were able to prove an *arbitrary proposition*! This mechanism was always present in the proof by contradiction rule, but it is worth highlighting:

Derived Rule 6: Contradictions are powerful!
From $\Phi \wedge \neg\Phi$ you can deduce *any* proposition Ψ.

Now back to the question of how to treat $\Phi \Rightarrow \Psi$ when Φ is false. Recall that in order to prove $\Phi \Rightarrow \Psi$, one can assume Φ and then deduce Ψ. If we know that Φ is false to start with, then here is a proof that $\Phi \Rightarrow \Psi$:

> Assume Φ.
>
> Since Φ is known to be false, we now have a contradiction $\Phi \wedge \neg\Phi$.
>
> Using "contradictions are powerful," we can now deduce anything we want! In particular, we can deduce Ψ.

Thus if you accept proofs by contradiction as valid, then you must accept that $\Phi \Rightarrow \Psi$ is true when Φ is false. An implication that is true because its hypothesis is false is sometimes said to be *vacuously true*.

Exercise 8: Assume that we know the following facts:

- Alice is an accountant and holds no other profession.
- Bob has brown hair.
- Charles loves chocolate and despises all other foods.

Determine whether each of the following is true or false.

1. If Bob's hair is purple then Charles loves chocolate.
2. If Alice is an accountant then Charles likes green beans.
3. Alice is an accountant if and only if Alice is a doctor.
4. If Bob has brown hair then Charles loves chocolate.
5. Charles likes baked salmon if and only if Bob has brown hair.
6. Charles likes clam chowder if and only if Alice is a professional underwater welder.
7. If Bob's hair is green then Bob's hair is white.
8. Bob's hair is brown if and only if Charles loves chocolate.

Notice how the implication of mathematical logic has nothing to do with causality. Some of the sentences above sound weird in English because we often use "if... then..." to indicate that one state of affairs *causes* another, as in the sentence

"If you don't brush your teeth, then you will get cavities."

In mathematical logic, that sentence is simply true if you either brush your teeth, or if you don't brush your teeth and end up getting cavities. Interestingly, that sentence is true even in a situation where you brush your teeth and still get cavities. That's quite different from the "if... then..." of conversational English! In conversation, we would expect there to be an implicit

"(And if you do brush your teeth then you will not get cavities.)"

Be aware that this implicit additional statement is not there in mathematical logic; an implication $\Phi \Rightarrow \Psi$ doesn't give you any information in the case where you know that $\neg\Phi$.

Exercise 9: Write a truth table for $(\Phi \Rightarrow \Omega) \wedge (\Psi \Rightarrow \Omega)$. It should have eight rows. In the same truth table, add a column for $(\Phi \vee \Psi) \Rightarrow \Omega$. Finally, in the same truth table, add a column for

$$((\Phi \Rightarrow \Omega) \wedge (\Psi \Rightarrow \Omega)) \Rightarrow ((\Phi \vee \Psi) \Rightarrow \Omega).$$

The latter proposition could be called "proof by cases," and so your truth table result should not be too surprising.

2.3 Some Derived Logical Rules

In this section we will derive some logical rules from the basic ones given in previous sections. We still have no specific mathematical propositions to talk about and so we still use the placeholders Φ, Ψ, etc. The arguments given in this section are useful logical patterns that can help us build other arguments later on.

The following derived rule could be written as "$((\Phi \Rightarrow \Psi) \wedge (\Psi \Rightarrow \Omega)) \Rightarrow (\Phi \Rightarrow \Omega)$", but we instead mix in some English to cut down on the number of parentheses and to make things more pleasant to read.

Derived Rule 7: Transitivity of Implication

If $\Phi \Rightarrow \Psi$ and $\Psi \Rightarrow \Omega$, then $\Phi \Rightarrow \Omega$.

Proof: Assume that $\Phi \Rightarrow \Psi$ and $\Psi \Rightarrow \Omega$. In order to prove that $\Phi \Rightarrow \Omega$, let us assume Φ. (Our goal is now to prove Ω.) From Φ and $\Phi \Rightarrow \Psi$, it follows that Ψ. From Ψ and $\Psi \Rightarrow \Omega$, it follows that Ω.

In the above argument you can see two applications of modus ponens– this is how implications can be put to use. And you can also see how an implication is proven, by assuming the hypotheses and arguing for the conclusion.

Derived Rule 8: Conjunction and Implication

$(\Phi \wedge \Psi) \Rightarrow \Omega$ if and only if $(\Phi \Rightarrow (\Psi \Rightarrow \Omega))$

Proof: Assume that $(\Phi \wedge \Psi) \Rightarrow \Omega$. In order to prove $(\Phi \Rightarrow (\Psi \Rightarrow \Omega))$, assume Φ. Now in order to prove $\Psi \Rightarrow \Omega$, assume Ψ. Since we have both Φ and Ψ, we have $\Phi \wedge \Psi$. Since $(\Phi \wedge \Psi) \Rightarrow \Omega$, we can now conclude Ω.

Now assume that $(\Phi \Rightarrow (\Psi \Rightarrow \Omega))$. In order to prove that $(\Phi \wedge \Psi) \Rightarrow \Omega$, assume $\Phi \wedge \Psi$. That is, we have assumed Φ and we have assumed Ψ. From Φ and $\Phi \Rightarrow (\Psi \Rightarrow \Omega)$, it follows that $\Psi \Rightarrow \Omega$. From Ψ and $\Psi \Rightarrow \Omega$, it follows that Ω.

The first thing to notice about the above argument is the way in which an "if and only if" statement gets proven. There are two parts to the proof, one for each of the two implications. The first half of the proof establishes

$$((\Phi \wedge \Psi) \Rightarrow \Omega) \Rightarrow ((\Phi \Rightarrow (\Psi \Rightarrow \Omega))),$$

while the second half establishes

$$((\Phi \Rightarrow (\Psi \Rightarrow \Omega))) \Rightarrow ((\Phi \wedge \Psi) \Rightarrow \Omega).$$

Together, they allow us to conclude the "if and only if" statement

$$((\Phi \wedge \Psi) \Rightarrow \Omega) \Leftrightarrow ((\Phi \Rightarrow (\Psi \Rightarrow \Omega))).$$

Another thing to notice is the way in which $\wedge$ is handled. In the first half of the argument, we establish that $\Phi \wedge \Psi$ holds by establishing each of Φ and Ψ– this is the way to prove a conjunction. In the second half, we get to assume that $\Phi \wedge \Psi$ holds and this allows us to deduce both Φ and Ψ– this is the way conjunctions get used. In typical proofs this handling of conjunctions happens very quickly; the distinction between

"Assume that $\Phi \wedge \Psi$"

and

"Assume that Φ and assume that Ψ"

will be blurred completely.

Derived Rule 9:

If $\Phi \Rightarrow \Psi$ and $\Omega \Rightarrow \Sigma$, then $(\Phi \wedge \Omega) \Rightarrow (\Psi \wedge \Sigma)$.

Proof: Exercise 10.

Derived Rule 10: Disjunction and Implication

$(\Phi \vee \Psi) \Rightarrow \Omega$ if and only if $(\Phi \Rightarrow \Omega) \wedge (\Psi \Rightarrow \Omega)$

Proof: $\Rightarrow$: Assume that $(\Phi \vee \Psi) \Rightarrow \Omega$.

In order to prove that $(\Phi \Rightarrow \Omega)$, assume Φ. From Φ it follows that $\Phi \vee \Psi$. From $\Phi \vee \Psi$ and $(\Phi \vee \Psi) \Rightarrow \Omega$, we can conclude that Ω. Thus we have proven that $\Phi \Rightarrow \Omega$.

We also need to prove that $\Psi \Rightarrow \Omega$. To this end, assume Ψ. From Ψ it follows that $\Phi \vee \Psi$. From $\Phi \vee \Psi$ and $(\Phi \vee \Psi) \Rightarrow \Omega$, we can conclude that Ω. Thus we have proven that $\Psi \Rightarrow \Omega$.

Since we proved $\Phi \Rightarrow \Omega$ and $\Psi \Rightarrow \Omega$, we can conclude that $(\Phi \Rightarrow \Omega) \wedge (\Psi \Rightarrow \Omega)$.

$\Leftarrow$: Assume that $(\Phi \Rightarrow \Omega) \wedge (\Psi \Rightarrow \Omega)$. That is, assume $\Phi \Rightarrow \Omega$ and assume $\Psi \Rightarrow \Omega$. For the sake of proving $(\Phi \vee \Psi) \Rightarrow \Omega$, assume that $\Phi \vee \Psi$.

Case 1: In the case that Φ holds, it follows from $\Phi \Rightarrow \Omega$ that Ω holds.

Case 2: In the case that Ψ holds, it follows from $\Psi \Rightarrow \Omega$ that Ω holds.

Since Ω holds in both cases, we conclude that Ω holds.

Here the two halves of the "if and only if" proof are difficult to separate by paragraphs alone, since each half needed multiple paragraphs. So the two halves of the proof are headed by "$\Rightarrow$" and "$\Leftarrow$". You should always feel free to use headings to separate different components of your argument.

Another thing to notice in the above argument is the way in which $\vee$ is handled. In the first half of the argument, we establish $\Phi \vee \Psi$ by deducing it from Φ, and we also establish it by deducing it from Ψ. In the second half, we use an $\vee$ statement in pretty much the only way we can– a proof by cases.

Derived Rule 11:

If $\Phi \Rightarrow \Psi$ and $\Omega \Rightarrow \Sigma$, then $(\Phi \vee \Omega) \Rightarrow (\Psi \vee \Sigma)$.

Proof: Exercise 11.

Derived Rule 12: Alternative Eliminated

If $\Phi \vee \Psi$ holds but Φ does not hold, then Ψ must hold. In other words,

$$((\Phi \vee \Psi) \wedge (\neg\Phi)) \Rightarrow \Psi.$$

Proof: Assume that $\Phi \vee \Psi$ holds and $\neg\Phi$ holds.

Case 1: Suppose that Φ holds. Then we have $\Phi \wedge \neg\Phi$! From a contradiction we can conclude anything, in particular we can conclude that Ψ holds.

Case 2: Suppose that Ψ holds... that's it for case 2.

In both cases we conclude Ψ, so we can conclude Ψ.

In the above argument we've made use of rule 6.

Derived Rule 13: Or Distributes over And

$(\Phi \vee (\Psi \wedge \Omega)) \Leftrightarrow ((\Phi \vee \Psi) \wedge (\Phi \vee \Omega))$.

Proof: $\Rightarrow$: Assume $\Phi \vee (\Psi \wedge \Omega)$.

Case 1: Suppose Φ holds. Then we can immediately conclude $\Phi \vee \Psi$ and $\Phi \vee \Omega$, and from these we can conclude $(\Phi \vee \Psi) \wedge (\Phi \vee \Omega)$.

Case 2: Suppose $\Psi \wedge \Omega$ holds. Then Ψ holds, and $\Phi \vee \Psi$ then follows from that. Also Ω holds, and $\Phi \vee \Omega$ follows from that. Finally we conclude $(\Phi \vee \Psi) \wedge (\Phi \vee \Omega)$.

Since both cases lead to $(\Phi \vee \Psi) \wedge (\Phi \vee \Omega)$, we conclude $(\Phi \vee \Psi) \wedge (\Phi \vee \Omega)$.

$\Leftarrow$: Assume $((\Phi \vee \Psi) \wedge (\Phi \vee \Omega))$. That is, assume $\Phi \vee \Psi$ and assume $\Phi \vee \Omega$. Due to excluded middle, we know that either Φ or $\neg\Phi$ holds.

Case 1: Suppose that Φ holds. It immediately follows that $\Phi \vee (\Psi \wedge \Omega)$.

Case 2: Suppose that $\neg\Phi$ holds. Using the rule "alternative eliminated," it then follows from $\Phi \vee \Psi$ that Ψ holds. Similarly, it follows from $\Phi \vee \Omega$ that Ω holds. Thus $\Psi \wedge \Omega$ holds. Finally, we conclude that $\Phi \vee (\Psi \wedge \Omega)$.

Since both cases lead to $\Phi \vee (\Psi \wedge \Omega)$, we conclude $\Phi \vee (\Psi \wedge \Omega)$.

Observe that a proof by cases need not proceed from the exact $\vee$-proposition one has assumed; sometimes it is useful to do a proof by cases based on excluded middle.

Given an implication $\Phi \Rightarrow \Psi$, there are a few "flipped" implications one can write down:

The *converse* of $\Phi \Rightarrow \Psi$ is $\Psi \Rightarrow \Phi$.
The *inverse* of $\Phi \Rightarrow \Psi$ is $\neg\Phi \Rightarrow \neg\Psi$.
The *contrapositive* of $\Phi \Rightarrow \Psi$ is $\neg\Psi \Rightarrow \neg\Phi$.

It is a common mistake to think that the converse or the inverse of an implication follows from the implication. The confusion stems from the inconsistent ways in which "if... then..." can work in conversation. When a bank robber says

"If you don't hand over the money, I'll shoot!",

they implicitly also mean to say the inverse

"If you do hand over the money, then I won't shoot!",

and the converse

"I'll shoot only if you don't hand over the money!"

If the bank robber were using strict mathematical logic (that is, if their original threat took the form "you don't hand over the money"⇒"I will shoot"), then they could, without lying, shoot even after the money is handed over.

The *contrapositive* of an implication, on the other hand, *does* follow from the implication. This rule is derived below. An implication is always equivalent to its contrapositive. Since the converse of an implication is the contrapositive of its inverse, the converse and inverse of an implication are equivalent.

Derived Rule 14: Contraposition

$(\Phi \Rightarrow \Psi) \Leftrightarrow (\neg\Psi \Rightarrow \neg\Phi)$

Proof: Assume that $\Phi \Rightarrow \Psi$. To prove that $\neg\Psi \Rightarrow \neg\Phi$, assume that $\neg\Psi$. Now assume Φ, for the sake of obtaining a contradiction. Since $\Phi \Rightarrow \Psi$, we see that Ψ follows. We end up with the contradiction $\Psi \wedge \neg\Psi$. Thus we reject the original assumption and conclude that $\neg\Phi$.

Now to prove the other direction, assume that $\neg\Psi \Rightarrow \neg\Phi$. To prove that $\Phi \Rightarrow \Psi$, assume Φ. For the sake of obtaining a contradiction, assume $\neg\Psi$. From $\neg\Psi \Rightarrow \neg\Phi$, it then follows that $\neg\Phi$. But we've now reached the contradiction $\Phi \wedge \neg\Phi$. Thus we reject the original assumption and conclude that $\neg\neg\Psi$. In other words, Ψ.

The above argument is a great demonstration of how proofs by contradiction work. Sometimes, in order to proceed with your argument, you need something *more* to work with. Assuming that your desired conclusion doesn't hold can sometimes give you something more

and help push your argument forward.

The above argument should make you feel that "proof by contradiction" and "contraposition" are very closely related. One can prove $\Phi \Rightarrow \Psi$ by assuming Φ, then assuming $\neg\Psi$ and trying to obtain a contradiction. Or, one can prove $\Phi \Rightarrow \Psi$ by instead proving its contrapositive $\neg\Psi \Rightarrow \neg\Phi$, which we now see is equivalent to the original implication. Both approaches amount to pretty much the same argument.

Derived Rule 15: Inverting an Equivalence

If $\Phi \Leftrightarrow \Psi$, then $\neg\Phi \Leftrightarrow \neg\Psi$.

Proof: Assume that $\Phi \Leftrightarrow \Psi$. Then $\Phi \Rightarrow \Psi$ and $\Psi \Rightarrow \Phi$. By contraposition, it follows that $\neg\Psi \Rightarrow \neg\Phi$ and $\neg\Phi \Rightarrow \neg\Psi$. Thus we have $\neg\Phi \Leftrightarrow \neg\Psi$.

Derived Rule 16: De Morgan's Law 1

$\neg(\Phi \wedge \Psi) \Leftrightarrow (\neg\Phi \vee \neg\Psi)$

Proof: $\Rightarrow$: Assume $\neg(\Phi \wedge \Psi)$. Due to excluded middle, either Φ or $\neg\Phi$.

Case 1: Suppose that Φ holds. Now if Ψ held we would obtain $\Phi \wedge \Psi$, which leads to the contradiction $(\Phi \wedge \Psi) \wedge \neg(\Phi \wedge \Psi)$. Therefore it must be that $\neg\Psi$. From this it follows that $\neg\Phi \vee \neg\Psi$.

Case 2: Suppose that $\neg\Phi$ holds. Then it immediately follows that $\neg\Phi \vee \neg\Psi$.

Since we ended up with $\neg\Phi \vee \neg\Psi$ in both cases, we can conclude that $\neg\Phi \vee \neg\Psi$.

$\Leftarrow$: Assume $(\neg\Phi) \vee (\neg\Psi)$. Suppose, for the sake of contradiction, that $\Phi \wedge \Psi$ holds. Then Φ holds, and Ψ holds. Since we know that $(\neg\Phi) \vee (\neg\Psi)$ holds, there are two cases to consider:

Case 1: Suppose that $\neg\Phi$ holds. Then, since we already said that Φ holds, we obtain the contradiction $\Phi \wedge \neg\Phi$.

Case 2: Suppose that $\neg\Psi$ holds. Then, since we already said that Ψ holds, we obtain the contradiction $\Psi \wedge \neg\Psi$.

We obtain a contradiction either way, and so we are forced to reject that $\Phi \wedge \Psi$. That is, we have $\neg(\Phi \wedge \Psi)$.

Derived Rule 17: De Morgan's Law 2

$\neg(\Phi \vee \Psi) \Leftrightarrow (\neg\Phi \wedge \neg\Psi)$

Proof: **Exercise 12**.

Derived Rule 18: Implication in Terms of Disjunction

$(\Phi \Rightarrow \Psi) \Leftrightarrow (\neg\Phi \vee \Psi)$

Proof: $\Rightarrow$: **Exercise 13**: Prove that $(\Phi \Rightarrow \Psi) \Rightarrow (\neg\Phi \vee \Psi)$. Hint: Use excluded middle.

$\Leftarrow$: Assume that $\neg\Phi \vee \Psi$. With the goal of proving that $\Phi \Rightarrow \Psi$, assume that Φ. Applying the previous rule "alternative eliminated," we can conclude Ψ from $\neg\Phi \vee \Psi$ and Φ.

The fact that $\Phi \Rightarrow \Psi$ can be rewritten as $\neg\Phi \vee \Psi$ suggests that we never needed to formally introduce $\Rightarrow$ into our language. Every time we want to say "if Φ, then Ψ," we could instead say "either Ψ, or it's not the case that Φ." But life is better when we can phrase things in terms of $\Rightarrow$, and that is why we choose to have it.

Derived Rule 19: Negating an Implication

$\neg(\Phi \Rightarrow \Psi) \Leftrightarrow (\Phi \wedge \neg\Psi)$

Proof: **Exercise 14**.

The rule above and De Morgan's laws give you a way "push" a negation $\neg$ into complicated propositions. This will really come in handy later on! For example, negating $\Phi \Rightarrow (\Psi \vee \Omega)$ initially yields $\neg(\Phi \Rightarrow (\Psi \vee \Omega))$, but after pushing the negation in it becomes $\Phi \wedge \neg(\Psi \vee \Omega)$. After pushing the negation in further this becomes $\Phi \wedge \neg\Psi \wedge \neg\Omega$.

Exercise 15: Negate each of the following propositions, and push the negation into the innermost component propositions.

1. $\Phi \Rightarrow (\Psi \vee \Omega)$
2. $((\Phi \vee \Psi) \Rightarrow \Omega) \wedge \Sigma$
3. If you eat right and you sleep well, then you are healthy and you will live long.

The main purpose of the derived rules in this section is to make us familiar with common

patterns of proofs. Typically we do not reference these rules directly, but rather we rely on our intuitive sense for mathematical logic to enable us to read mathematical arguments and to construct our own arguments. A second purpose of this section is to help strengthen that intuitive sense for mathematical logic, which really must be sufficiently developed in order for us to write correct proofs. It is especially important to be aware of the ways in which mathematical logic differs from the sometimes ambiguous logic of everyday conversation.

2.4 Substitution

Our entire discussion has so far been restricted to propositions, but for the next part *variables* will have a role to play. Before moving on, review section 1.1 as needed to remind yourself about variables, constants, terms, and propositions.

Given a proposition Φ, the notation

$$\Phi_{[\boxed{\text{variable}}\to\boxed{\text{term}}]}$$

stands for the proposition that is obtained by replacing each copy of the indicated variable in Φ with a copy of the indicated term. In this notation, any variable can go in place of the box marked "variable," and any term can go in place of the box marked "term." Some examples:

If Φ is "$x \in A \cup B$" then $\Phi_{[x\to y]}$ is "$y \in A \cup B$".

If Φ is "$x \in A \cup B$" then $\Phi_{[A\to x]}$ is "$x \in x \cup B$".

If Φ is "$z^2 = z + y$" then $\Phi_{[z\to a+y]}$ is "$(a+y)^2 = (a+y) + y$".

If Φ is "$a + b \in B$" then $\Phi_{[c\to 3]}$ is "$a + b \in B$".

If Φ is "the product of a and b is even" then $\Phi_{[b\to c^2]}$ is "the product of a and c^2 is even".

Observe that parentheses are added as needed to avoid ambiguity.

A Clarification (If you find this remark to be more confusing than clarifying, then please feel free to skip this paragraph for now.) What *is* the string of symbols "$\Phi_{[x\to y]}$"? What part of speech are we looking at here? It's almost a proposition, in that you get a proposition once you carry out the substitution that involves replacing x by y. But the string of symbols "$\Phi_{[x\to y]}$" is not itself a proposition. It's more like a set of *instructions* telling you how to obtain a certain proposition. The string of symbols "$\Phi_{[x\to y]}$" has no part of speech because it is in fact not a part of the mathematical language at all! Instead, it is part of the language we are currently using to communicate. That is, it is a part of the English language in which this document is written, and it will help us in our mission to *specify* the language of mathematics. You can think of "$\Phi_{[x\to y]}$" as simply a shorthand for the instruction

Take the proposition "Φ" and replace each copy of the variable "x" with the symbol "y", and then write the resulting proposition.

More on substitution is coming later. There is a little more to substitution than simple mechanical replacement of symbols. I've left out some important details in this section. Take a look at these examples:

If Φ is "$(\,\forall x \,\mathbb{!}\, x = 2\,)$" then $\Phi_{[x\to y]}$ is "$(\,\forall x \,\mathbb{!}\, x = 2\,)$".

If Φ is "$(x \in A) \wedge (\,\exists x \,\mathbb{!}\, x = 2\,)$" then $\Phi_{[x\to y]}$ is "$(y \in A) \wedge (\,\exists x \,\mathbb{!}\, x = 2\,)$".

If Φ is "$a \in \{\, a \,\mathbb{!}\, a^2 = z\,\}$" then $\Phi_{[a\to 3]}$ is "$3 \in \{\, a \,\mathbb{!}\, a^2 = z\,\}$".

In these examples, substitution does not work as you might expect. You might guess from the examples that the barbell symbol "$\mathbb{!}$" has a hand in the strange substitution rules. We are not ready to dig into these details just yet. Later in section 2.7, there will be more on "$\mathbb{!}$" and its effect on substitution. For now, rest assured that the substitutions in the upcoming exercise are all straightforward ones– there will be no funny business with barbells.

Exercise 16: For each of the following, write the proposition that results from the substitution.

1. " $\frac{a+b}{x+y} > x^2$ "$_{[x\to A+B]}$
2. " $B \neq B$ "$_{[B\to y]}$
3. " $z \in \{\alpha, \beta, \gamma\}$ "$_{[\beta\to\gamma^{-1}]}$
4. " $f \subseteq A \times B$ "$_{[f\to g\circ f]}$
5. " $x \in y \Rightarrow x \in z$ "$_{[x\to 3]}$
6. " $a = 2 \vee a = 3$ "$_{[b\to 5]}$
7. $\Psi_{[b\to 5]}$, where Ψ is the proposition "$b \times b \subseteq J$"
8. " n^2 is even "$_{[n\to 1]}$
9. " n^2 is even "$_{[n\to n+1]}$
10. " $n^2 \sim k$ "$_{[n\to j+k][k\to 3]}$

Exercise 17: Is $\Phi_{[x\to y][y\to x]}$ always the same as Φ? Explain.

2.5 Universal and Existential Quantifiers

Universal Quantifiers Given a proposition Φ and a variable x, we can form the *universally quantified* proposition

$$(\,\forall x \mathbin{!} \Phi\,),$$

which is expressed in English as "for all x, Φ." Typically the proposition Φ would somehow involve the variable x. Here are some examples, along with their expressions in English:

$(\,\forall x \mathbin{!} x = x\,)$	For all x, $x = x$.
$(\,\forall n \mathbin{!} n > x\,)$	For all n, $n > x$.
$(\,\forall y \mathbin{!} (y \text{ is green}) \wedge (y \text{ is a flower})\,)$	For all y, y is green and y is a flower.
$(\,\forall y \mathbin{!} (y \text{ is a flower}) \Rightarrow (y \text{ is green})\,)$	For all y, if y is a flower then y is green.

In each proposition, the variable behind the "!" is said to be *quantified*. The quantified variable is special in that it's really just a placeholder. The proposition "$(\,\forall x \mathbin{!} x = x\,)$" is no different from "$(\,\forall y \mathbin{!} y = y\,)$". We might as well write them both as as "$(\,\forall \_ \mathbin{!} \_ = \_\,)$", with the understanding that the blanks all refer to the same thing. It is always possible to express universally quantified propositions in English *without mentioning the quantified variable*, as in the following renderings of the four examples from above:

Everything equals itself.

Everything is greater than x.

Everything is a green flower.

All flowers are green.

Now let's get into how "$\forall$" is used in proofs.

Universal Instantiation If you know that $(\,\forall x \mathbin{!} \Phi\,)$ holds, then you can deduce Φ. In fact, you can deduce *any* proposition that results from the substitution $\Phi_{[x \to \boxed{\text{term}}]}$, where *any* term can be put in the box. For example, if you know that $(\,\forall x \mathbin{!} x \text{ is even}\,)$, then you can deduce "$x$ is even", and you can also deduce things like "3 is even" and "$A + B$ is even".

Universal Generalization To *prove* a universally quantified proposition $(\,\forall x \mathbin{!} \Phi\,)$, prove Φ in a context in which you have made *no assumptions* about the quantified variable x. In such a context, the variable x is said to be *arbitrary*. For example, let's say you are trying to prove that $(\,\forall x \mathbin{!} x \text{ is green}\,)$. Your argument could be formatted something like this:

Consider any x.

[insert argument establishing that x is green]

Since x was arbitrary, we conclude that $(\forall x \mathbin{!} x \text{ is green})$. In other words, everything is green.

Upon reaching that first line, "Consider any x," there are no assumptions about x. If there were previous assumptions about x in the larger context of the proof, then they no longer apply after that line because *this is a new and arbitrary* x that we are now talking about.

Existential Quantifiers Given a proposition Φ and a variable x, we can form the *existentially quantified* proposition

$$(\exists x \mathbin{!} \Phi),$$

which is expressed in English as "there exists an x such that Φ." Here are some examples, along with their expressions in English:

$(\exists x \mathbin{!} x = x)$	There exists an x such that $x = x$.
$(\exists n \mathbin{!} n > x)$	There exists an n such that $n > x$.
$(\exists y \mathbin{!} (y \text{ is green}) \wedge (y \text{ is a flower}))$	There exists a y such that y is green and y is a flower.
$(\exists y \mathbin{!} (y \text{ is a flower}) \Rightarrow (y \text{ is green}))$	There exists a y such that if y is a flower then y is green.

Again, the variable behind the "!" is said to be *quantified*, and it serves as a mere placeholder in the proposition. It is always possible to express existentially quantified propositions in English *without mentioning the quantified variable*, as in the following renderings of the four examples from above:

Something equals itself.

Something is greater than x.

There exists a green flower.

There exists something with the property that if it is a flower, then it is green.

Now let's get into how "$\exists$" is used in proofs.

Existential Generalization To prove that $(\exists x \mathbin{!} \Phi)$, all you need to do is prove Φ or some variant of Φ such as $\Phi_{[x \to \boxed{\text{term}}]}$, in which a particular term sits in place of x. In other words, to prove that "there exists an x such that Φ," you must *find* an x, such that Φ.

Suppose someone tells you that there's no such thing as a spotted hamster. Disagreeing, you reach into your pocket and pull out a spotted hamster, proving that in fact there *exists* a spotted hamster. That is existential generalization.

Existential Instantiation If you know that $(\exists x \mathbin{!} \Phi)$ holds, then *as long the variable* x *was not previously used in your proof*, you may bring Φ into your argument. That is, it is

valid to assume Φ for the rest of your argument. If the variable x was already in use in your proof, then to avoid a conflict of variables you would have to introduce a brand new variable, say "y", and then from $(\,\exists x \restriction \Phi\,)$ you may bring $\Phi_{[x\to y]}$ into your argument.

This is one of the trickiest manipulations with quantifiers, and it will take some getting used to. As an example, suppose you knew for a fact that $(\,\exists x \restriction x$ is green$\,)$, and you want to use this fact to argue that Ω. Then your argument could be formatted like this:

> Since we know that $(\,\exists x \restriction x$ is green$\,)$, it is possible to *get* an x such that x is green.
>
> > [insert argument using the fact that x is green to deduce Ω]

You can think of it like this: If you and the person you are trying to convince both agree that there exists a green thing, then you can work with a *hypothetical* green thing, without needing to specify it, in order to draw some conclusions to which you would both agree. The key word in the example formatting above is "get." It's almost like you're instructing the reader of your proof to "go get a green thing, and then come back so we can continue the argument using that green thing." Except, no one ever really has to get an actual green thing; working with a hypothetical one called "x" is sufficient to run the argument.

Quantifying over Fewer Things Sometimes you don't want to say that *everything* is green, but you want to say that everything of a certain *type* is green. Maybe you want to say that all *flowers* are green, rather than all *things*. The way to express this with $\forall$ is to use $\Rightarrow$, like this:

$$(\,\forall x \restriction (x \text{ is a flower}) \Rightarrow (x \text{ is green})\,)\,.$$

It is still the case that the quantified variable x can be replaced by *anything*. The quantified proposition still says "for all *things*, if that thing is a flower then it is green." However, the implication "$(x$ is a flower$) \Rightarrow (x$ is green$)$" only says something interesting when x is a flower; otherwise it is *vacuously* true. For this reason, "$(\,\forall x \restriction (x$ is a flower$) \Rightarrow (x$ is green$)\,)$." is typically expressed in English as

"All flowers are green."

What if we wanted to say that *some* flower is green? Would "$(\,\exists x \restriction (x$ is a flower$) \Rightarrow (x$ is green$)\,)$" work? Not at all! In fact, the latter proposition would be true as long as there is at least one non-flower. Instead of $\Rightarrow$, to say "some flower is green" we should use $\wedge$, like this:

$$(\,\exists x \restriction (x \text{ is a flower}) \wedge (x \text{ is green})\,)\,.$$

In summary: If you want to restrict the class of things you are quantifying over, then use $\Rightarrow$ with $\forall$, and use $\wedge$ with $\exists$.

Exercise 18: Express each of the following propositions in English without ever mentioning the quantified variable. Insisting that the quantified variable not be mentioned can make the phrasing awkward for some of the more complicated propositions, but so be it.

1. $(\forall x \mid x \text{ is good })$
2. $(\exists x \mid x \text{ is good })$
3. $(\forall x \mid (x \text{ is a human }) \wedge (x \text{ is mortal }))$
4. $(\forall x \mid (x \text{ is a human }) \vee (x \text{ is mortal }))$
5. $(\forall x \mid (x \text{ is a human }) \Rightarrow (x \text{ is mortal }))$
6. $(\forall x \mid (x \text{ is mortal }) \Rightarrow (x \text{ is a human }))$
7. $(\exists x \mid (x \text{ is a human }) \wedge (x \text{ is mortal }))$
8. $(\exists x \mid (x \text{ is a human }) \vee (x \text{ is mortal }))$
9. $(\exists x \mid (x \text{ is a human }) \Rightarrow (x \text{ is mortal }))$
10. $(\forall x \mid \neg(x \text{ is good }))$
11. $\neg(\forall x \mid x \text{ is good })$
12. $(\exists x \mid \neg(x \text{ is good }))$
13. $\neg(\exists x \mid x \text{ is good })$
14. $(\forall x \mid x \text{ loves } y)$
15. $(\exists x \mid x \text{ loves } y)$
16. $(\forall y \mid x \text{ loves } y)$
17. $(\exists y \mid x \text{ loves } y)$
18. $(\forall x \mid (\exists y \mid x \text{ loves } y))$
    Hint: Work from the inside towards the outside. So start by eliminating the mention of y, for example by writing it as $(\forall x \mid x \text{ loves something})$. Then try to express that in English without mentioning x.
19. $(\exists y \mid (\forall x \mid x \text{ loves } y))$
20. $(\forall x \mid (x \text{ is a flower}) \Rightarrow (\exists y \mid (y \text{ is a petal of } x) \wedge (y \text{ is green})))$
21. $(\exists x \mid (x \text{ is a flower}) \wedge (\forall y \mid (y \text{ is a petal of } x) \Rightarrow (y \text{ is green})))$

Exercise 19: Write each of the following using quantifier notation (i.e. using $\forall$ and

$\exists$).

1. All birds can fly.
2. Some bird can fly.
3. Everything that can fly is a bird.
4. All birds that can fly have wings.

2.6 Derived Logical Rules for Quantifiers

We now continue to derive logical rules, as we were doing in section 2.3. This time, the rules involve quantifiers. Like in section 2.3, we will still not work with actual mathematical propositions, instead favoring more general *placeholders* for propositions, like Φ, Ψ, etc. However, I think that the arguments in this section can become difficult to follow if we adhere strictly to this level of generality. For this reason, we will sometimes also include a version of the arguments that contains generic-sounding English propositions, like "x is green," or "x loves y." These will often appear alongside the strictly general derivations; you are welcome to follow whichever version you find to be more convenient.

Derived Rule 20: Global Existence Implies Local Existence

$(\exists y \restriction (\forall x \restriction \Phi)) \Rightarrow (\forall x \restriction (\exists y \restriction \Phi))$

Proof: Assume that $(\exists y \restriction (\forall x \restriction \Phi))$. Then we can get a y such that $(\forall x \restriction \Phi)$. Now consider any x. Since $(\forall x \restriction \Phi)$, we know that in particular Φ holds. Since we have found y such that Φ holds, we can conclude that $(\exists y \restriction \Phi)$. Since x was arbitrary, we can conclude that $(\forall x \restriction (\exists y \restriction \Phi))$.

A particular instance of the derived rule:
$(\exists y \restriction (\forall x \restriction y \text{ loves } x)) \Rightarrow (\forall x \restriction (\exists y \restriction y \text{ loves } x))$
(In other words: If there is something that loves everything, then everything is loved by something.)

Proof: Assume that $(\exists y \restriction (\forall x \restriction y \text{ loves } x))$. That is, assume that there is something that loves everything. Then we can get something that loves everything; call it y. Now consider any x. Since y loves everything, we know in particular that that y loves x. Thus *something* loves x. That is, $(\exists y \restriction y \text{ loves } x)$. Since x was arbitrary, we can conclude that *everything* is loved by something. That is, $(\forall x \restriction (\exists y \restriction y \text{ loves } x))$.

In the argument above you can see all four of the fundamental rules involving quantifiers:

universal instantiation (UI), universal generalization (UG), existential instantiation (EI), and existential generalization (EG). Here is a repeat of the last argument with those rules pointed out:

> Assume that $(\exists y \,\mathbf{!}\, (\forall x \,\mathbf{!}\, y \text{ loves } x))$. That is, assume that there is something that loves everything. Then we can get (EI) something that loves everything; call it y. Now consider any x. Since y loves everything, we know in particular (UI) that that y loves x. Thus *something* (EG) loves x. That is, $(\exists y \,\mathbf{!}\, y \text{ loves } x)$. Since x was arbitrary, we can conclude (UG) that *everything* is loved by something. That is, $(\forall x \,\mathbf{!}\, (\exists y \,\mathbf{!}\, y \text{ loves } x))$.

As you study the arguments in this section, try to identify exactly where UI, UG, EI, and EG are being used.

Regarding the derived rule above, the converse cannot be proven! It may be useful to look at what goes wrong if we attempt to prove it anyway:

> A failed attempt to prove that $(\forall x \,\mathbf{!}\, (\exists y \,\mathbf{!}\, y \text{ loves } x)) \Rightarrow (\exists y \,\mathbf{!}\, (\forall x \,\mathbf{!}\, y \text{ loves } x))$:
>
> Assume that $(\forall x \,\mathbf{!}\, (\exists y \,\mathbf{!}\, y \text{ loves } x))$. Consider any x. Since $(\forall x \,\mathbf{!}\, (\exists y \,\mathbf{!}\, y \text{ loves } x))$, we know in particular (UI) that $(\exists y \,\mathbf{!}\, y \text{ loves } x)$. Thus we can get (EI) a y such that y loves x. Since x was arbitrary, we have established (UG) that $(\forall x \,\mathbf{!}\, y \text{ loves } x)$. That is, y loves everything. Since we have found a y that loves everything, we can conclude (EG) that $(\exists y \,\mathbf{!}\, (\forall x \,\mathbf{!}\, y \text{ loves } x))$.

The error in the proof is colored in red. Do you see what is wrong with it? It should feel wrong to you– before reading on you might want to take a moment and consider what it is that feels wrong in the argument.

In order to generalize from a statement about x to a statement about *all* x, there must be no prior assumption attached to x. There must be nothing special about x. It must be that x is truly *arbitrary*. Here, however, the variable x stopped being arbitrary as soon as we introduced a specific y into the proof, a y that loves x. The y loves *that* particular x, and it does not make sense to generalize from this fact and deduce that y loves *everything*.

The error in applying UG was really subtle, and it would have been quite difficult to catch in strictly general proof written in terms of "Φ". This is why we will often include specific English propositions like "y loves x" as an aide. It's actually fairly technical to work with quantifiers in a completely general pure logic setting.

Besides the proof, there is also a lesson that we can draw from the derived rule itself: when multiple quantifiers are involved, be careful with the order in which you write them!

We do not need to worry about order when the same type of quantifier is repeated, as we will see in the next two rules.

Derived Rule 21: Irrelevance of order of $\forall$

$(\,\forall x \mathbin{!} (\,\forall y \mathbin{!} \Phi\,)\,) \Rightarrow (\,\forall y \mathbin{!} (\,\forall x \mathbin{!} \Phi\,)\,)$

Proof: Assume that $(\,\forall x \mathbin{!} (\,\forall y \mathbin{!} \Phi\,)\,)$. Consider any y. Consider any x. From $(\,\forall x \mathbin{!} (\,\forall y \mathbin{!} \Phi\,)\,)$ we can conclude $(\,\forall y \mathbin{!} \Phi\,)$, and from that we can conclude Φ. Since we deduced Φ while x is arbitrary, we can conclude that $(\,\forall x \mathbin{!} \Phi\,)$. Since we deduced $(\,\forall x \mathbin{!} \Phi\,)$ while y is arbitrary, we can conclude that $(\,\forall y \mathbin{!} (\,\forall x \mathbin{!} \Phi\,)\,)$.

It should be intuitive that $(\,\forall x \mathbin{!} (\,\forall y \mathbin{!} x \text{ loves } y\,)\,)$ is the same as $(\,\forall y \mathbin{!} (\,\forall x \mathbin{!} x \text{ loves } y\,)\,)$, since they both mean "everything loves everything." The same goes for "something loves something," derived next:

Derived Rule 22: Irrelevance of order of $\exists$

$(\,\exists x \mathbin{!} (\,\exists y \mathbin{!} \Phi\,)\,) \Rightarrow (\,\exists y \mathbin{!} (\,\exists x \mathbin{!} \Phi\,)\,)$

Proof: Assume that $(\,\exists x \mathbin{!} (\,\exists y \mathbin{!} \Phi\,)\,)$. We can get an x such that $(\,\exists y \mathbin{!} \Phi\,)$. Now we can get a y such that Φ. Since we have found an x such that Φ, we can conclude $(\,\exists x \mathbin{!} \Phi\,)$. Since we have found a y such that $(\,\exists x \mathbin{!} \Phi\,)$, we can conclude $(\,\exists y \mathbin{!} (\,\exists x \mathbin{!} \Phi\,)\,)$.

We will often use the following shorthand for repeated quantifiers: $(\,\forall x, y \mathbin{!} \Phi\,)$ will stand for $(\,\forall x \mathbin{!} (\,\forall y \mathbin{!} \Phi\,)\,)$, and similarly $(\,\exists x, y \mathbin{!} \Phi\,)$ will stand for $(\,\exists x \mathbin{!} (\,\exists y \mathbin{!} \Phi\,)\,)$.

Now that we've looked at how quantifiers interact with each other, the rest of this section explores the interaction between quantifiers and our old friends $\wedge$, $\vee$, $\neg$, and $\Rightarrow$.

Derived Rule 23: Quantifiers and Implication 1

If $(\forall x \restriction \Phi \Rightarrow \Psi)$, then $(\forall x \restriction \Phi) \Rightarrow (\forall x \restriction \Psi)$.

Proof: Assume that $(\forall x \restriction \Phi \Rightarrow \Psi)$. Assume that $(\forall x \restriction \Phi)$ (for the sake of proving that $(\forall x \restriction \Psi)$). Consider any x. Since $(\forall x \restriction \Phi)$, we have in particular that Φ. Since $(\forall x \restriction \Phi \Rightarrow \Psi)$, we have in particular that $\Phi \Rightarrow \Psi$. From Φ and $\Phi \Rightarrow \Psi$, we conclude that Ψ. Since x remains arbitrary, we may generalize to conclude that $(\forall x \restriction \Psi)$.

A particular instance of the derived rule:
If $(\forall x \restriction x$ is a bird $\Rightarrow x$ can fly$)$, then $(\forall x \restriction x$ is a bird$) \Rightarrow (\forall x \restriction x$ can fly$)$.
In other words:
If all birds can fly, then it must be that if everything is a bird then everything can fly.

Proof: Assume that all birds can fly. Assume that everything is a bird– our goal is now to establish that everything can fly. Consider any x. Since everything is a bird, we have in particular that x is a bird. Since all birds can fly, we have in particular that if x is a bird then x can fly. Therefore x can fly. Since x remains arbitrary, we may generalize to conclude that *everything* can fly.

The above argument contains two uses of UI and one use of UG.

Exercise 20: The converse of the rule above cannot be established. In fact, in the real world in which we live, (1) it is true that if everything is a bird then everything can fly, but (2) it is false that all birds can fly. Explain how the assertions (1) and (2) hold for our reality.

Derived Rule 24: Quantifiers and Implication 2

If $(\forall x \restriction \Phi \Rightarrow \Psi)$, then $(\exists x \restriction \Phi) \Rightarrow (\exists x \restriction \Psi)$.

Proof: Assume that $(\forall x \restriction \Phi \Rightarrow \Psi)$. Assume that $(\exists x \restriction \Phi)$ (for the sake of proving that $(\exists x \restriction \Psi)$). Then we can get an x such that Φ. Since $(\forall x \restriction \Phi \Rightarrow \Psi)$, we have in particular that $\Phi \Rightarrow \Psi$. From Φ and $\Phi \Rightarrow \Psi$, we conclude that Ψ. Since we have found an x such that Ψ, we conclude that $(\exists x \restriction \Psi)$.

A particular instance of the derived rule:
If $(\forall x \restriction x$ is a bird $\Rightarrow x$ can fly$)$, then $(\exists x \restriction x$ is a bird$) \Rightarrow (\exists x \restriction x$ can fly$)$.
In other words:
If all birds can fly, then it must be that if a bird exists then something can fly.

Proof: Assume that all birds can fly. Assume that there exists a bird– our goal is now to establish that there exists something that can fly. Since a bird exists, let's get one and call it x. Since all birds can fly, we have in particular that if x is a bird then x can fly. Therefore x can fly. Since we have found something x that can fly, we conclude that *something* can fly.

The above argument contains a use of EI, a use of UI, and a use of EG.

Exercise 21: The converse of the rule above cannot be established. In fact, in the real world in which we live, (1) it is true that if there exists a bird then something can fly, but (2) it is false that all birds can fly. Explain how the assertions (1) and (2) hold for our reality.

Exercise 22: There are at least two errors in the following foolish attempt to establish a converse to the rule above. Find at least one of them, and explain why it is an error. If you are stuck, consider reading a bit more of this section and then returning to this exercise.

> Assume that if $(\exists x \restriction x$ is a bird$)$, then $(\exists x \restriction x$ can fly$)$. We shall now attempt to prove that $(\forall x \restriction x$ is a bird $\Rightarrow x$ can fly$)$. Consider any x and assume that x is a bird. Then *something* is a bird, so $(\exists x \restriction x$ is a bird$)$. It follows that $(\exists x \restriction x$ can fly$)$. Since $(\exists x \restriction x$ can fly$)$, we can get something that can fly; call this something x. Since x is a bird and it can fly, we have proven that x is a bird $\Rightarrow x$ can fly. Since x is arbitrary, we can generalize to conclude that $(\forall x \restriction x$ is a bird $\Rightarrow x$ can fly$)$.

Derived Rule 25: Quantifiers and Conjunction 1

If $(\exists x \restriction \Phi \wedge \Psi)$, then $(\exists x \restriction \Phi) \wedge (\exists x \restriction \Psi)$.

Proof: Assume that $(\exists x \restriction \Phi \wedge \Psi)$. Then we can get an x such that $\Phi \wedge \Psi$. Since we have found an x such that Φ, we can conclude that $(\exists x \restriction \Phi)$. Since we have found an x such that Ψ, we can conclude that $(\exists x \restriction \Psi)$. Thus $(\exists x \restriction \Phi)$ and $(\exists x \restriction \Psi)$.

A particular instance of the derived rule:
If $(\exists x \restriction x$ is a flower $\wedge\ x$ is green$)$, then $(\exists x \restriction x$ is a flower$)$ and $(\exists x \restriction x$ is green$)$.
In other words:
If there exists a green flower, then something is a flower and something is green.

Proof: Assume that there exists a green flower. Then we can get a green flower, call it x. Since x is a flower, we have found a flower and we can conclude that there exists a flower. Since x is green, we have found a green thing and we can conclude that there exists a green thing. Thus something is a flower and something is green.

The above argument contains a use of EI and two uses of EG.

It should be intuitive that the converse doesn't work. If a flower exists and a green thing exists, then we cannot necessarily conclude that a green flower exists. It could be that our world is full of non-green flowers and green non-flowers, but contains no green flowers. We can learn something by trying to prove the converse anyway, and looking for the error:

> Assume that $(\exists x \restriction x$ is a flower$)$ and $(\exists x \restriction x$ is green$)$. We shall now attempt to prove that $(\exists x \restriction x$ is a flower $\wedge\ x$ is green$)$. Since $(\exists x \restriction x$ is a flower$)$, we can get (EI) a flower; let's call it x. Since also $(\exists x \restriction x$ is green$)$, we can get (EI) a green thing; let's call that x as well. Since x is a green flower, we have found a green flower and we can conclude (EG) that $(\exists x \restriction x$ is a flower $\wedge\ x$ is green$)$.

Before reading on you might want to take a moment and consider what exact part of the argument feels wrong, and what is wrong with it.

...

The error is in the second use of EI. Recall that when you use EI to go from $(\exists x \restriction \Phi)$ to Φ, the variable x cannot already be in use. If it is in use, then you have to substitute in a new variable such as y, and then you can bring $\Phi_{[x \to y]}$ into the argument. The critical error in the argument given here is in "let's call that x as well," which is where we decided to name the green thing x. We should have used a different name, like y, since we only knew that we could get *some* green thing and we should not allow that to conflict with the name x that we gave to our hypothetical flower. If we had called the flower x and the green thing y, then there would be no way for the argument to proceed, and all's right with the world.

Derived Rule 26: Quantifiers and Conjunction 2

$(\forall x \restriction \Phi \wedge \Psi)$ if and only if $(\forall x \restriction \Phi) \wedge (\forall x \restriction \Psi)$.

Proof: $\Rightarrow$: Assume that $(\forall x \restriction \Phi \wedge \Psi)$. Consider any x. Since $(\forall x \restriction \Phi \wedge \Psi)$, we have in particular that $\Phi \wedge \Psi$ Since x is arbitrary and we have Φ, we conclude that $(\forall x \restriction \Phi)$. Since x is arbitrary and we have Ψ, we conclude that $(\forall x \restriction \Psi)$. Thus $(\forall x \restriction \Phi) \wedge (\forall x \restriction \Psi)$.
$\Leftarrow$: Assume that $(\forall x \restriction \Phi) \wedge (\forall x \restriction \Psi)$. Consider any x. Since $(\forall x \restriction \Phi)$, we have in particular that Φ. Since $(\forall x \restriction \Psi)$, we have in particular that Ψ. Since we now have $\Phi \wedge \Psi$ and since x is arbitrary, we may generalize to conclude that $(\forall x \restriction \Phi \wedge \Psi)$.

A particular instance of the derived rule:
$(\forall x \restriction x \text{ is large} \wedge x \text{ is green})$ if and only if $(\forall x \restriction x \text{ is large})$ and $(\forall x \restriction x \text{ is green})$.
In other words:
Everything is large and green if and only if everything is large and everything is green.

Proof: $\Rightarrow$: Assume that everything is large and green. Consider any x. Since everything is large and green, we know in particular that x is large and green. Since x is arbitrary and we showed that it is large, we may generalize to conclude that everything is large. Similarly, since x is arbitrary and we showed that it is green, we may generalize to conclude that everything is green. Thus everything is large and everything is green.

$\Leftarrow$: **Exercise 23**: Prove that if everything is large and everything is green, then it follows that everything is large and green. Hint: your argument should involve two uses of UI and one use of UG.

Derived Rule 27: Quantifiers and Disjunction 1

If $(\forall x \restriction \Phi) \vee (\forall x \restriction \Psi)$, then $(\forall x \restriction \Phi \vee \Psi)$.

Proof: Assume that $(\forall x \restriction \Phi) \vee (\forall x \restriction \Psi)$.

Case 1: Assume that $(\forall x \restriction \Phi)$. Consider any x. Since $(\forall x \restriction \Phi)$, it follows in particular that Φ. Thus we have $\Phi \vee \Psi$, and since x is arbitrary we may generalize and conclude that $(\forall x \restriction \Phi \vee \Psi)$.

Case 2: Assume that $(\forall x \restriction \Psi)$. Consider any x. Since $(\forall x \restriction \Psi)$, it follows in particular that Ψ. Thus we have $\Phi \vee \Psi$, and since x is arbitrary we may generalize and conclude that $(\forall x \restriction \Phi \vee \Psi)$.

Since we ended up with $(\forall x \restriction \Phi \vee \Psi)$ in both cases, we may conclude that $(\forall x \restriction \Phi \vee \Psi)$.

A particular instance of the derived rule:
If $(\forall x \restriction x \text{ is dry}) \vee (\forall x \restriction x \text{ is hot})$, then $(\forall x \restriction x \text{ is dry} \vee x \text{ is hot})$.
In other words:
If either everything is dry or everything is hot, then everything is either dry or hot.

Proof: Assume that either everything is dry or everything is hot.

Case 1: Suppose that everything is dry. Consider any x. Since everything is dry, x, in particular, is dry. Thus x is dry or it is hot. Since x is arbitrary, we may generalize and conclude that *everything* is either dry or hot.

Case 1: Suppose that everything is hot. Consider any x. Since everything is hot, x, in particular, is hot. Thus x is dry or it is hot. Since x is arbitrary, we may generalize and conclude that *everything* is either dry or hot.

Since both cases lead us to conclude that everything is either dry or hot, we can go ahead and conclude that everything is either dry or hot.

The above argument contains a use of UI and two uses of UG.

It should be intuitive that the converse doesn't work. If everything is either dry or hot, then it does not necessarily follow that either everything is dry or everything is hot. There could still be some dry things that aren't hot as well as some hot things that aren't dry.

Exercise 24: Here is an attempt at arguing for the converse. What is the exact mis-

take?

Assume that everything is either dry or hot. We will attempt to prove that either everything is dry, or everything is hot. Consider any x. Since everything is dry or it is hot, we know that x, in particular, is either dry or hot.

Case 1: Suppose that x is dry. Then, since x is arbitrary, we may generalize and conclude that everything is dry. It follows that either everything is dry or everything is hot.

Case 2: Suppose that x is hot. Then, since x is arbitrary, we may generalize and conclude that everything is hot. It follows that either everything is dry or everything is hot.

Since we concluded in both cases that everything is dry or everything is hot, we can go ahead and conclude that everything is dry or everything is hot.

Derived Rule 28: Quantifiers and Disjunction 2

$(\exists x \restriction \Phi \vee \Psi)$ if and only if $(\exists x \restriction \Phi) \vee (\exists x \restriction \Psi)$.

Proof: $\Rightarrow$: Assume that $(\exists x \restriction \Phi \vee \Psi)$. We may then get an x such that $\Phi \vee \Psi$.

Case 1: Suppose that Φ. Since we have found an x such that Φ, we may conclude that $(\exists x \restriction \Phi)$. It follows that $(\exists x \restriction \Phi) \vee (\exists x \restriction \Psi)$.

Case 2: Suppose that Ψ. Since we have found an x such that Ψ, we may conclude that $(\exists x \restriction \Psi)$. It follows that $(\exists x \restriction \Phi) \vee (\exists x \restriction \Psi)$.

Since both cases led us to conclude that $(\exists x \restriction \Phi) \vee (\exists x \restriction \Psi)$, we may go ahead and conclude that $(\exists x \restriction \Phi) \vee (\exists x \restriction \Psi)$.

$\Leftarrow$: **Exercise 25**.

A particular instance of the derived rule:
$(\exists x \restriction x$ is dry $\vee\ x$ is hot$)$ if and only if $(\exists x \restriction x$ is dry$) \vee (\exists x \restriction x$ is hot$)$.
In other words:
"Something is either dry or hot" is equivalent to "Either something is dry, or something is hot."

Proof: $\Rightarrow$: Assume that something is either dry or hot. We may then get an x which is either dry or hot.

Case 1: Suppose that x is dry. Since we have found an x that is dry, we may conclude that *something* is dry. It follows that either something is dry or something is hot.

Case 2: Suppose that x is hot. Since we have found an x that is hot, we may conclude that *something* is hot. It follows that either something is dry or something is hot.

Since both cases led us to conclude that either something is dry or something is hot, we may go ahead and conclude that either something is dry or something is hot.
$\Leftarrow$: **Exercise 26**.

Derived Rule 29: Quantifiers and Negation 1

$\neg\,(\,\forall x \restriction \Phi\,) \Leftrightarrow (\,\exists x \restriction \neg\Phi\,)$

Proof: $\Leftarrow$: Assume that $(\,\exists x \restriction \neg\Phi\,)$. Suppose, for the sake of obtaining a contradiction, that $(\,\forall x \restriction \Phi\,)$. Since $(\,\exists x \restriction \neg\Phi\,)$, we can get an x such that $\neg\Phi$. Since $(\,\forall x \restriction \Phi\,)$, we have in particular that Φ. Having arrived at the contradiction $\Phi \wedge \neg\Phi$, we find that we must reject $(\,\forall x \restriction \Phi\,)$. That is, $\neg\,(\,\forall x \restriction \Phi\,)$.

$\Rightarrow$: For this direction we will prove the contrapositive $\neg\,(\,\exists x \restriction \neg\Phi\,) \Rightarrow (\,\forall x \restriction \Phi\,)$ (see Derived Rule 14). Assume that $\neg\,(\,\exists x \restriction \neg\Phi\,)$. Consider any x.

Suppose, for the sake of contradiction, that $\neg\Phi$. Then we found an x such that $\neg\Phi$, so we may conclude that $(\,\exists x \restriction \neg\Phi\,)$. We've reached the contradiction $(\,\exists x \restriction \neg\Phi\,) \wedge \neg\,(\,\exists x \restriction \neg\Phi\,)$. Therefore we must reject $\neg\Phi$ and we see that in fact Φ.

Since we've established Φ for an arbitrary x, we can generalize to conclude that $(\,\forall x \restriction \Phi\,)$.

A particular instance of the derived rule:
$\neg\,(\,\forall x \restriction x$ is good$\,) \Leftrightarrow (\,\exists x \restriction x$ is not good$\,)$
In other words: "Not everything is good" is equivalent to "Something is not good."

Proof: $\Leftarrow$: Assume that something is not good. Suppose, for the sake of obtaining a contradiction, that everything is good. Since something is not good, we can get a non-good thing and call it x. Since everything is good, we have in particular that x is good. This is a contradiction– x cannot be both good and not good. Thus we reject the assumption that everything is good. That is, not everything is good.

$\Rightarrow$: We would like to prove that if not everything is good, then something is not good. By contraposition, it suffices to prove that if it's *not* the case that something is not good, then everything must be good. Assume that it's not the case that something is not good. Consider any x.

Suppose, for the sake of contradiction, that x is not good. Then we found an x that is not good, so we may conclude that something is not good. But we now have a contradiction– it both is and isn't the case that something is not good. Therefore we must reject "x is not good" and we see that in fact x must be good.

Since we've established that x is good for arbitrary x, we can generalize to conclude that *everything* is good.

Derived Rule 30: Quantifiers and Negation 2

$\neg\,(\,\exists x \restriction \Phi\,) \Leftrightarrow (\,\forall x \restriction \neg\Phi\,)$

Proof: Apply "Quantifiers and Negation 1" to the proposition $\neg\Phi$ (putting $\neg\Phi$ in place of Φ) to obtain $\neg\,(\,\forall x \restriction \neg\Phi\,) \Leftrightarrow (\,\exists x \restriction \Phi\,)$. Then invert this equivalence (see Derived Rule 15) to obtain the desired equivalence.

A particular instance of the derived rule:
$\neg\,(\,\exists x \restriction x$ is good$\,) \Leftrightarrow (\,\forall x \restriction x$ is not good$\,)$
In other words: "Nothing is good" is equivalent to "Everything is not good."

Proof: **Exercise 27**: Write this proof without relying on "Quantifiers and Negation 1." Your argument could look pretty similar to the argument that "Not everything is good" is equivalent to "Something is not good," which is given in "Quantifiers and Negation 1."

The two rules above, along with Derived Rules 16, 17, and 19 form a complete toolkit for "pushing" $\neg$ into complicated propositions. For example, here are the stages of negating $(\,\forall x \restriction \Phi \Rightarrow (\Psi \vee (\,\exists y \restriction \Omega\,))\,)$ and pushing the negation inward:

$$\begin{array}{ll}
\neg\,(\,\forall x \restriction \Phi \Rightarrow (\Psi \vee (\,\exists y \restriction \Omega\,))\,) & \Leftrightarrow \\
(\,\exists x \restriction \neg(\Phi \Rightarrow (\Psi \vee (\,\exists y \restriction \Omega\,)))\,) & \Leftrightarrow \\
(\,\exists x \restriction \Phi \wedge \neg(\Psi \vee (\,\exists y \restriction \Omega\,))\,) & \Leftrightarrow \\
(\,\exists x \restriction \Phi \wedge \neg\Psi \wedge \neg\,(\,\exists y \restriction \Omega\,)\,) & \Leftrightarrow \\
(\,\exists x \restriction \Phi \wedge \neg\Psi \wedge (\,\forall y \restriction \neg\Omega\,)\,). &
\end{array}$$

Here's the exact same procedure with Φ replaced by "x is a flower", Ψ replaced by "x is purple", and Ω replaced by "y is a green petal of x":

"It is not the case that all flowers are either purple or have a green petal" iff
"There is something for which it is not the case that if it is a flower then it is either purple or it has a green petal " iff
"There is some flower for which it is not the case that it is either purple or it has a green petal" iff
"There is some non-purple flower which does not have a green petal" iff
"There is some non-purple flower all of whose petals are non-green"

Hopefully the overall negation feels intuitive, even if the individual steps in pushing the negation are a little awkward.

Exercise 28: Negate each of the following propositions, and push the negation into the innermost component propositions. Recall from Derived Rule 18 that $\neg\Phi\vee\Psi$ can be rewritten

as $\Phi \Rightarrow \Psi$. When you encounter things like $\neg\Phi \vee \Psi$, you can rewrite them in terms of "$\Rightarrow$" in order to reduce the overall number of "$\neg$" symbols.

1. $(\,\forall x \,\rfloor\, \Phi \Rightarrow \Psi\,)$
2. $(\,\exists x \,\rfloor\, \Phi \vee \Psi\,)$
3. $(\,\forall x \,\rfloor\, \Phi \wedge \Psi\,)$
4. $(\,\forall x \,\rfloor\, \Phi \vee \Psi\,)$
5. $(\,\exists x \,\rfloor\, \Phi \Rightarrow \Psi\,)$
6. $(\,\exists x \,\rfloor\, \Phi \wedge \Psi\,)$
7. $(\,\forall x \,\rfloor\, \Phi \Rightarrow (\,\exists y \,\rfloor\, \Psi \wedge (\Omega \vee \Sigma)\,)\,)$
8. $(\,\exists x \,\rfloor\, \Phi \wedge \Psi \wedge (\,\forall y \,\rfloor\, \Omega \Rightarrow \Sigma\,)\,)$
9. $(\,\forall x \,\rfloor\, \Phi \Rightarrow (\,\exists y \,\rfloor\, \Psi \wedge (\,\forall z \,\rfloor\, \Omega \Rightarrow \Sigma\,)\,)\,)$

Exercise 29: Again negate each of the following propositions, pushing the negation into the innermost component propositions. Whenever you see the English "or" being used, remember that it actually stands for the mathematical "$\vee$" and not whatever sort of "or" would suit a conversational context.

1. Everything is warm and fuzzy.
2. Everything is either good or it is bad.
3. There is something which is either a dog or a wolf.
4. Every person has a friend who is either very skinny or very fat.
5. Some bird can fly.
6. Every company has at least one committee whose members are all loyal to the company.
7. Every bird can fly.
8. There exists something with the property that if it is a bird, then it can fly.
9. Some flower is green and has all of its petals being pointy.

Exercise 30: Each proposition in Exercise 29 is actually modeled on exactly one proposition from Exercise 28– "modeled on" in the sense that Φ, Ψ, etc. have been replaced by some

specific propositions in English. Can you match them up? For each proposition in Exercise 29, figure out which proposition in Exercise 28 it was modeled on.

2.7 Substitution Revisited

Now that we've thoroughly explored quantifiers, we can better understand the anomalous substitution examples from the end of section 2.4. Here is one of those anomalous substitutions:

If Φ is "$(\,\forall x \,!\, x$ is good$\,)$" then $\Phi_{[x\to y]}$ is "$(\,\forall x \,!\, x$ is good$\,)$".

Why didn't the x symbol physically get replaced by y when the substitution was carried out? Well, the proposition $(\,\forall x \,!\, x$ is good$\,)$ simply says that everything is good. If we do physically replace every "x" mark with a "y" then it still says that everything is good. Since the meaning doesn't change anyway, substitution does not need to affect the x. If we *did* allow the substitution to affect the x, this would cause problems in examples like the following:

$$(\,\forall x \,!\, x \text{ loves } y\,).$$

This proposition asserts that everything loves y. If we now replace each physical x mark by a y, then we end up with

$$(\,\forall y \,!\, y \text{ loves } y\,),$$

which asserts something totally different: everything loves *itself*! Formally, we design our substitution rules so that the barbell "$!$" protects the variable preceding it from being replaced in a substitution. A variable that is guarded by a barbell is said to be a *bound* variable of the proposition that it is in. Otherwise it is said to be a *free* variable. Free variables can get affected by substitution; for example making the substitution $[y \to z]$ in "$(\,\forall x \,!\, x$ loves $y\,)$" yields "$(\,\forall x \,!\, x$ loves $z\,)$." This works as intended: if you take "everything loves y" and replace y with a z you should get "everything loves z."

However, there is yet another subtlety involving substitutions which can lead to unintended consequences. Consider the substitution $[y \to x]$ in "$(\,\forall x \,!\, x$ loves $y\,)$". This time y is free variable, and there is no "$!$" to protect it from being replaced, so the substitution yields "$(\,\forall x \,!\, x$ loves $x\,)$". Again we find that a simple variable replacement has drastically changed the meaning of what's being asserted! This is not supposed to happen. In mathematical logic, certain substitutions are considered to be "unacceptable." All substitution troubles can be avoided if, whenever you make a substitution, you *never replace a bound variable* and you *never use a bound variable in a replacement.*

Free and Bound Variables When you read a mathematical proposition, it's a very good thing to be aware of which variables are free and which variables are bound. Free variables are *really there* in the proposition in which they appear, whereas bound variables are more like *dummy* variables. For example, in the proposition "$(\,\exists x \,!\, x$ loves $y\,)$" we have a free

variable y and a bound variable x. The proposition is really saying something about y; it says that there is something that loves y, something that specifically loves y. But it says nothing about x. The proposition doesn't really involve x, even though an "x" symbol is physically present. As you saw in Exercise 18, a proposition with bound variables can be expressed in English without mentioning any of the bound variables– that's because it's just not saying anything about those variables.

The terminology of "free" and "bound" variables also gives us an interesting way to think about how UI, UG, EI, and EG work in written proofs. When you use EI to go from "$(\,\exists x \,\fatsemi\, x \text{ loves } y\,)$" to "$x$ loves y" in a proof, you are in some sense *freeing* the bound variable x. You go from "*something* loves y" to "x loves y". You go from some unspecified unnamed thing that loves y, to a specific thing called x that loves y. In written proofs, EI and UI free up bound variables, while EG and UG *bind* free variables.

Implicit Universal Suppose you prove a theorem with some free variables in it. Say you've proven "If x and y are odd, then $x+y$ is even." This has x and y as free variables, so it looks like it's making a statement specifically about x and y. But they are still *variables*, and they are *arbitrary*; that's because they appear in a standalone theorem statement with no external assumptions. Thus UG applies and you can generalize to deduce

$$(\,\forall x, y \,\fatsemi\, \text{if } x \text{ and } y \text{ are odd, then } x+y \text{ is even}\,). \tag{1}$$

Now there are no free variables, and indeed the theorem can be expressed in an English sentence that has no variables: "The sum of two odd things is even." Mathematicians are actually more likely to state the theorem as

$$\text{if } x \text{ and } y \text{ are odd, then } x+y \text{ is even.} \tag{2}$$

with free x and y, rather than explicitly including the "$\forall x, y$" as in (1). It's just easier to write this way, and everyone understands that since x and y are arbitrary, there's sort of an implicit "$\forall x, y$" that could be included.

Recall that UI allows you to deduce $\Phi_{[x\to\boxed{\text{term}}]}$ from $(\,\forall x \,\fatsemi\, \Phi\,)$, for any term that you'd like to have replace x. For example you can deduce

$$\text{if } 5 \text{ and } z+1 \text{ are odd, then } 5+(z+1) \text{ is even} \tag{3}$$

from (1), which itself was deduced from (2). The bottom line is that if you've proven Φ as a theorem, then you can substitute any terms you like for the free variables in Φ, and you would also have proven the resulting proposition.

Derived Rule 31: Variable Substitution

Given Φ, if x is *arbitrary* then you can deduce $\Phi_{[x \to \boxed{\text{term}}]}$, where any term can sit in the box labeled "term." (For example, all free variables would be arbitrary if Φ is already proven as a standalone theorem, so free variables in a theorem can freely be replaced by terms.)

2.8 Logic Summary

Here is a reference table for each of the logical constructions that we've looked at. Many of the table entries will be clickable references if your pdf reader supports hyperlinks.

name	symbolic	English	to prove	to use
conjunction	$\Phi \wedge \Psi$	Φ and Ψ	prove Φ and prove Ψ	can deduce Φ and can deduce Ψ
disjunction	$\Phi \vee \Psi$	Φ or Ψ	prove Φ or prove Ψ	proof by cases
negation	$\neg\Phi$	it is not the case that Φ	proof by contradiction	push the $\neg$ in before using
implication	$\Phi \Rightarrow \Psi$	Ψ if Φ	assume Φ, then prove Ψ	given Φ, can deduce Ψ
equivalence	$\Phi \Leftrightarrow \Psi$	Φ if and only if Ψ	prove both implications	know whether Φ based on Ψ
universal	$(\forall x \mid \Phi)$	for all x, Φ	universal generalization	universal instantiation
existential	$(\exists x \mid \Phi)$	for some x, Φ	existential generalization	existential instantiation

3 Set Theory

Recall that the game of mathematics consists of starting points, which are the axioms, and ways of generating new results from the starting points, which are the rules of deduction. In the previous section, we established all the rules of deduction. In this section, we will introduce axioms and generate some results from them. Appendex B can be a useful reference throughout.

3.1 Membership, Inclusion, and Equality

Axiom 1 (Reflexiveness for Equality): $x = x$.

Axiom 2 (Equality Used): If $x = y$, then $\Phi_{[a \to x]} \Leftrightarrow \Phi_{[a \to y]}$.

Theorem 3 (Symmetry and Transitivity for Equality):
(1) If $x = y$, then $y = x$.
(2) If $x = y$ and $y = z$, then $x = z$.

Proof of (1): Assume that $x = y$. Applying Axiom 2 to the proposition "$a = x$" shows us that $x = x$ if and only if $y = x$. Since $x = x$ by Axiom 1, it follows that $y = x$. ■

Proof of (2): Assume that $x = y$ and $y = z$. Apply Axiom 2 to the proposition "$a = z$" and the equality $x = y$. This gives us that $x = z$ if and only if $y = z$. Since $y = z$ by hypothesis, it follows that $x = z$. ■

Fewer Axioms is Better Why should "$x = x$" be an axiom while symmetry and transitivity are theorems? Are symmetry and transitivity not just as fundamental to the meaning of equality as reflexiveness? Well, we could have set up Theorem 3 as an axiom instead, and then we wouldn't have needed to bother with a proof. But we prefer to keep the axioms to a minimum. If we *can* derive a result from previous results, then we choose to do so.

Otherwise, why not just make everything an axiom and save some effort? To do so would be terribly boring. The interesting part of mathematics is in seeing what *follows* from one's assumptions. It is somehow satisfying to know that equality *must* be symmetric and transitive if it is to satisfy $x = x$ and allow for substitution. It would not have been possible to set up the rules of the game so as to exclude symmetry and transitivity for equality.

Another motivation for having fewer axioms is *consistency*. If it is possible to prove a contradiction within our mathematical framework, then the entire framework is said to be *inconsistent*. This would be absolutely disastrous; recall Rule 6. We really *hope* that it is impossible to prove a contradiction from our axioms, but the more axioms we introduce the worse our confidence becomes that it is impossible to prove a contradiction.

One can also think about it in strategic terms. When you make an argument to convince someone of your view, it only works if they agree with the premises of your argument. This is more likely when there are fewer premises. If mathematics is one giant argument that is being made, then the axioms are the premises of that argument.

Using Equality on Propositions and Terms Axiom 2 tells us that if we know $x = y$, then we can replace x by y in any proposition to obtain an equivalent proposition. Axiom 2 also allows for variable replacements in *terms* and not just propositions. If $x = y$ then here is how Axiom 2 allows us to argue that $x^2 = y^2$: Assume that $x = y$ and apply Axiom 2 to the proposition "$a^2 = y^2$". We get that $x^2 = y^2$ if and only if $y^2 = y^2$. Since $y^2 = y^2$ due to Axiom 1, it follows that $x^2 = y^2$.

In summary: If $x = y$, then replacing x by y in a *proposition* gives a *logically equivalent* proposition, and replacing x by y in a *term* gives an *equal* term. We will package these ideas into the next theorem, whose proof is just a general application of the idea above.

In the following theorem, we will use "☺" as a placeholder for a *term*, just as we use "Φ" as a placeholder for a *proposition*. We will use the notation "$☺_{[\boxed{\text{variable}}\to\boxed{\text{term}}]}$" to indicate that a substitution is to be made in a term, just as we have been using "$\Phi_{[\boxed{\text{variable}}\to\boxed{\text{term}}]}$" to indicate that a substitution is to be made in a proposition. We can apply parts (2) and (4) of the theorem below to a specific situation by replacing each copy of "☺" by a chosen term, just as we can obtain specific instances of parts (1) and (3) by replacing each "Φ" by a chosen proposition.

Theorem 4 (Equality Used): If $x = y$, then:
(1) $\Phi_{[a\to x]} \Leftrightarrow \Phi_{[a\to y]}$
(2) $☺_{[a\to x]} = ☺_{[a\to y]}$
(3) $\Phi \Leftrightarrow \Phi_{[x\to y]}$
(4) $☺ = ☺_{[x\to y]}$

Proof: Assume that $x = y$. Part (1) is just Axiom 2.

To prove part (2), apply Axiom 2 to the proposition "$☺_{[a\to x]} = ☺$" and to the fact that $x = y$. We get that

$$(☺_{[a\to x]} = ☺)_{[a\to x]} \Leftrightarrow (☺_{[a\to x]} = ☺)_{[a\to y]}.$$

Carrying out a substitution instruction involves applying the substitution to every part of an expression, so here we must apply the substitutions to the individual expressions on both sides of the "=". Thus we have

$$(☺_{[a\to x]_{[a\to x]}} = ☺_{[a\to x]}) \Leftrightarrow (☺_{[a\to x]_{[a\to y]}} = ☺_{[a\to y]}).$$

After carrying out the substitution $☺_{[a\to x]}$, there will be no free "a" left to be further replaced in a substitution, so $☺_{[a\to x]}$, $☺_{[a\to x]_{[a\to x]}}$, and $☺_{[a\to x]_{[a\to y]}}$ all result in the same string of

symbols. We therefore have

$$(☺_{[a\to x]} = ☺_{[a\to x]}) \;\Leftrightarrow\; (☺_{[a\to x]} = ☺_{[a\to y]}).$$

Since the left hand side of this holds by Axiom 1, we conclude that $☺_{[a\to x]} = ☺_{[a\to y]}$.

To prove (3), simply apply (1), with "x" playing the role of "a". We get $\Phi_{[x\to x]} \Leftrightarrow \Phi_{[x\to y]}$. Noting that $\Phi_{[x\to x]}$ is Φ, we have $\Phi \Leftrightarrow \Phi_{[x\to y]}$.

To prove (4), simply apply (2), with "x" playing the role of "a". We get $☺_{[x\to x]} = ☺_{[x\to y]}$. Noting that $☺_{[x\to x]}$ is $☺$, we have $☺ = ☺_{[x\to y]}$. ■

How to Gain Equality? The axioms so far give us a mechanism for using and manipulating equalities. But where can we get some equalities to play with in the first place (other than ones like $x = x$)? How can we *prove* an interesting equality? This will be addressed shortly in Axiom 8; we first need to get membership into the picture.

Notation The proposition "$a \in b$" is read as "a is in b" or "a is an element of b." The term "$\{\, x \mid \Phi \,\}$" is read as "the set of x such that Φ." The appearance of "$\mid$" suggests that "x" is a *bound* variable in the term "$\{\, x \mid \Phi \,\}$", and indeed it is! Terms of this form can be expressed in English without any mention of the bound variable. For example $\{\, x \mid x$ is green $\}$ could be referred to as "the set of green things," with no mention of x. Also, the bound variable can be replaced without any change in meaning: the term "$\{\, y \mid y$ is green $\}$" refers just as much to "the set of green things." The following axiom establishes how $\in$ and $\{\, x \mid \Phi \,\}$ work.

Axiom 5 (Membership): $a \in \{\, x \mid \Phi \,\} \Leftrightarrow \Phi_{[x\to a]}$.
Warning: this axiom is broken.

The notation $\{\, x \mid \Phi \,\}$ serves to "collect" together all the x's for which Φ holds. A set $\{\, x \mid \Phi \,\}$ is like an exclusive club, and Φ is the condition for membership in that club. Various propositions could go in the position of Φ to create collections like the following:

$\{\, x \mid x$ is a person $\wedge\, (\,\exists y \mid y$ is a friend of $x\,)\,\}$ The set of people who have a friend.
$\{\, n \mid 3 < n^2 < 4 + x \,\}$ The set of things whose square is strictly between 3 and $4 + x$.

Axiom 5 says that a is an element of $\{\, x \mid x$ is a person $\wedge\, (\,\exists y \mid y$ is a friend of $x\,)\,\}$ if and only if a is a person and $(\,\exists y \mid y$ is a friend of $a\,)$. Axiom 5 says that $b \in \{\, n \mid 3 < n^2 < 4 + x \,\}$ if and only if $3 < b^2 < 4 + x$.

Broken? We should talk about that warning. Axiom 5 is the way people at one point thought they could set up set theory. But it turns out to be broken in the worst possible way– Axiom 5 allows us to prove a contradiction (see appendix A). Allowing Φ to really be

any proposition does not work; certain choices of Φ seem to cause trouble. So what do we do about this? People have handled the bug in various ways by modifying Axiom 5. Different approaches have led to different types of set theory. We can also choose to *ignore* the bug and move on. Then we would be doing what is called *naive set theory*. This is what we do throughout this text, while just bearing in mind that there are some propositions Φ on which Axiom 5 should not be used. There are comments in appendix A on how to fix the bug; most of our approach is not affected much by the fix.

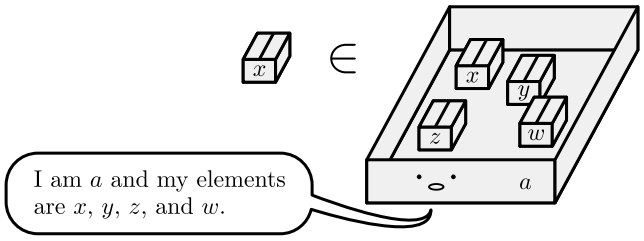
Moving on.

Definition 6 (Inclusion): $a \subseteq b \Leftrightarrow (\forall z \, ! \, z \in a \Rightarrow z \in b)$.

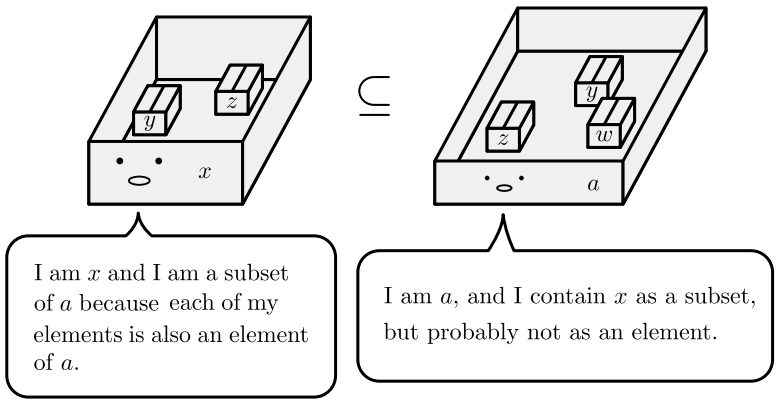
Here are some ways to read "$a \subseteq b$" in English:

- a is a subset of b
- a is contained in b
- a is included in b

For a to be a subset of b, every element of a must be an element of b. Do not confuse this with "a is in b," which is actually a way of saying "$a \in b$"! Explicitly using the symbols "$\in$" and "$\subseteq$", or explicitly saying "element" and "subset" can help to avoid confusion. Here is a way to imagine the situation $x \in a$:



And here is a way to imagine the situation $x \subseteq a$:



On Definitions Definitions are like axioms in that they serve as starting points. But we distinguish them from axioms because all they do is provide a convenient *name* for something by introducing new symbols or terminology. Definitions don't assert anything truly new, so they don't allow us to prove anything truly new. More precisely, the only things a definition allows us to prove are the same things we proved before, but with old names replaced by new names. Definitions could be omitted from our entire framework without changing which theorems can be proven, just changing how we are able to state those theorems. Having too many axioms is undesirable, but there is nothing wrong with having lots of definitions.

Theorem 7 (Reflexivity and Transitivity for Inclusion):
(1) $a \subseteq a$.
(2) If $a \subseteq b$ and $b \subseteq c$, then $a \subseteq c$.

Proof of (1): If $z \in a$ then $z \in a$, so we have $(\forall z \,\mathbin{!}\, z \in a \Rightarrow z \in a)$. In other words, $a \subseteq a$. ■

Proof of (2): Assume that $a \subseteq b$ and $b \subseteq c$. To prove that $a \subseteq c$, consider any $z \in a$. Since $a \subseteq b$, it follows that $z \in b$. Since $b \subseteq c$, it follows further that $z \in c$. Since we showed that $z \in c$ for an arbitrary $z \in a$, we have shown $(\forall z \,\mathbin{!}\, z \in a \Rightarrow z \in c)$. In other words, $a \subseteq c$. ■

In the proof of Theorem 7 part (2), you should be able to spot two uses of UI and one use of UG.

If $a = b$, then by Axiom 2 we have $z \in a \Leftrightarrow z \in b$, for all z. So the equality $a = b$ gives both inclusions $a \subseteq b$ and $b \subseteq a$. In other words, if a and b are equal then they must have exactly the same elements. We will take this to be the full *meaning* of equality, by taking on the converse as an axiom.

Axiom 8 (Equality Gained): If $(\forall z \,\mathbin{!}\, z \in a \Leftrightarrow z \in b)$, then $a = b$.

This makes it so that anything and everything that we can refer to in our mathematical language is nothing more than its elements. In other words, *everything is a set*:

Theorem 9: $y = \{\, z \mid z \in y \,\}$.

Proof: We will show that $(\forall w \mid w \in y \Leftrightarrow w \in \{\, z \mid z \in y \,\})$. Then we will be finished, due to Axiom 8.

Consider any w. Axiom 5 tells us that $w \in \{\, z \mid z \in y \,\}$ holds if and only if "$z \in y$"$_{[z \to w]}$ holds. In other words, $w \in \{\, z \mid z \in y \,\}$ if and only if $w \in y$. Since w was arbitrary, we are done. ■

Theorem 10 (Equality as Double Inclusion): $a = b$ if and only if $a \subseteq b$ and $b \subseteq a$.

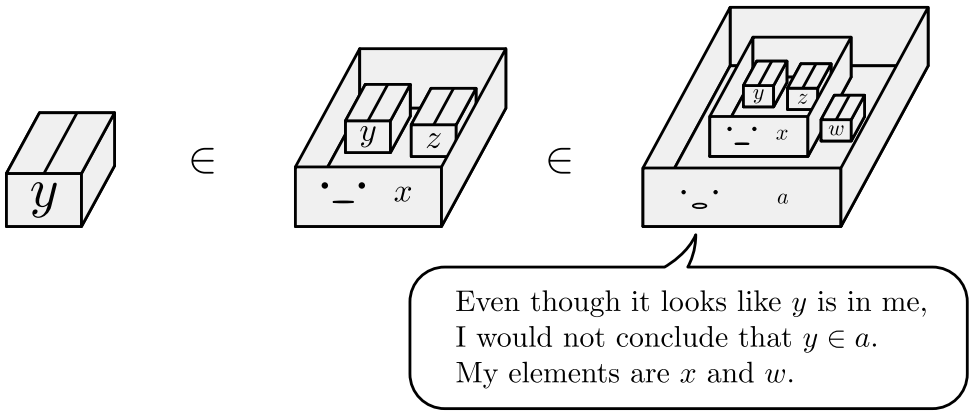
Proof: $\Rightarrow$: Assume that $a = b$. Then by Axiom 2 we have $z \in a \Leftrightarrow z \in b$, for all z. From $z \in a \Rightarrow z \in b$ we can generalize to conclude that $(\forall z \mid z \in a \Rightarrow z \in b)$. In other words, $a \subseteq b$. Similarly, from $z \in b \Rightarrow z \in a$ we can generalize to conclude that $b \subseteq a$.

$\Leftarrow$: Assume that $a \subseteq b$ and $b \subseteq a$. We will show that $(\forall z \mid z \in a \Leftrightarrow z \in b)$. Then we will be finished, due to Axiom 8.

Consider any z. From $a \subseteq b$ we have $z \in a \Rightarrow z \in b$, and from $b \subseteq a$ we have $z \in b \Rightarrow z \in a$. It follows that $z \in a \Leftrightarrow z \in b$. Since z is arbitrary, we are done. ■

Since equality is equivalent to two inclusions, proofs of equality are often split into two parts, with each part dedicated to proving one of the inclusions.

Before ending this section, we take a moment to point out that membership is normally not transitive; having $y \in x$ and $x \in a$ does not allow you to conclude that $y \in a$.



Exercise 31: For each of the following, determine if it is a term, a proposition, or nothing because it is ill-formed.

1. $\{\, a \mid a \in a \,\}$
2. $\{\, x \mid x \,\}$
3. $\{\, y \mid (\forall z \mid z \subseteq y) \,\}$
4. $x + y \in z$
5. $a = (b \in c)$
6. $3 \subseteq P$

Exercise 32: Express each of the following sets in English without mentioning any bound variables.

1. $\{\, x \mid x \text{ is good} \,\}$
2. $\{\, x \mid x \text{ loves } y \,\}$
3. $\{\, y \mid x \text{ loves } y \,\}$
4. $\{\, z \mid z \subseteq p \,\}$
5. $\{\, z \mid (\forall x \mid x \subseteq p \Rightarrow z \in x) \,\}$

Exercise 33: Prove that $a \in \{\, k \mid k = a \,\}$.

Exercise 34: Prove that if $\{\, k \mid k = a \,\} \subseteq m$, then $a \in m$.

Exercise 35: Let $B = \{\, a \mid a \subseteq \{\, k \mid k = b \,\} \,\}$. Prove that if $j \in z$ and $z \in B$, then $j = b$.

Exercise 36: For this exercise, let

$$s = \{\, x \mid (\exists a \mid x \in a \wedge a \in y) \,\}$$

and let

$$t = \{\, a \mid (\exists x \mid x \in a \wedge a \in y) \,\}.$$

1. Which variables are free in the definition of s and which are bound?
2. Describe s in English without mentioning any bound variables.
3. What does it mean for z to be an element of s? (Use Axiom 5.)
4. What does it mean for y to be an element of s? Express your answer in English without mentioning any bound variables.

5. Answer questions 1-4 for t instead of s.

6. Assume that every element of y has an element. That is, assume that

$$(\forall z \mid z \in y \Rightarrow (\exists w \mid w \in z)).$$

Prove that $t = y$.

3.2 Empty Set, Singletons, and Uniqueness

Definition 11 (Empty Set): $\{\} = \{ x \mid x \neq x \}$

Here we have defined the first constant of our language.

The notation $a \notin b$ is a shorthand for $\neg(a \in b)$, and similarly $a \neq b$ is short for $\neg(a = b)$.

Theorem 12 (Empty Set is Empty): $x \notin \{\}$.

Proof: If $x \in \{\}$ then $x \neq x$, but this would contradict Axiom 1. ■

Theorem 13 (Minimality of the Empty Set):
(1) $\{\} \subseteq a$.
(2) If $a \subseteq \{\}$, then $a = \{\}$.

Proof of (1): Consider any z. Since $z \notin \{\}$ (Theorem 12), it is vacuously true that $z \in \{\} \Rightarrow z \in a$. ■

Proof of (2): Assume that $a \subseteq \{\}$. We already have $\{\} \subseteq a$ from part (1). Since we got both inclusions, we have proven the equality $a = \{\}$ (Theorem 10). ■

Theorem 14 (Only the Empty Set is Empty): If $x \notin a$ for all x, then $a = \{\}$.

Proof: Assume that $(\forall x \mid x \notin a)$. Consider any z. Since $z \notin a$ by hypothesis, it is vacuously true that $z \in a \Rightarrow z \in \{\}$. Since z is arbitrary, we may conclude that $a \subseteq \{\}$. It follows that $a = \{\}$ (Theorem 13). ■

In the proof of Theorem 14, you should be able to spot one use of UI and one use of UG.

Theorem 14 is an example of a *uniqueness theorem*. If you know that g is green and you want to assert that g is the only green thing in existence, then the way to assert that is

$$(\forall a \mid a \text{ is green} \Rightarrow a = g).$$

If we read "$(\forall x \mid x \notin a)$" as "$a$ is empty," then Theorem 14 looks like this:

$$(\forall a \mid a \text{ is empty} \Rightarrow a = \{\}).$$

The universal quantifier "$\forall a$" does not show up explicitly in the statement of Theorem 14, but remember that it is sort of implicitly there.

Theorem 14 tells us that "being empty" is the same thing as "being equal to $\{\}$." When a set is described "nonempty," that is the same as saying that the set is not equal to $\{\}$.

Theorem 15 (Nonemptiness): $a \neq \{\} \Leftrightarrow (\exists x \mid x \in a)$.

Proof: $\Rightarrow$: This implication can be established by considering the contraposition

$$\neg(\exists x \mid x \in a) \Rightarrow a = \{\}$$

and pushing the negation in to see that it is equivalent to Theorem 14.

$\Leftarrow$: Assume that $(\exists x \mid x \in a)$. Then we can get some x such that $x \in a$. Now we cannot have $a = \{\}$, for if we did then $x \in a$ would contradict Theorem 12. ■

In the proof of Theorem 15, you should be able to spot one use of EI.

Definition 16 (Singleton): $\{x\} = \{a \mid a = x\}$.

This definition gives us an object $\{x\}$ with the property that any a is an element of $\{x\}$ if and only if $a = x$. In other words, x is an element of $\{x\}$ and it is the *unique* element of $\{x\}$.

Definition 17 (Doubleton): $\{x, y\} = \{a \mid (a = x) \vee (a = y)\}$.

You can probably guess how $\{x, y, z\}$ and longer "lists of elements" are defined:

Definition 18 (More Ways to List Elements):
(1) $\{x, y, z\} = \{a \mid (a = x) \vee (a = y) \vee (a = z)\}$
(2) $\{x, y, z, u\} = \{a \mid (a = x) \vee (a = y) \vee (a = z) \vee (a = u)\}$
(3) $\{x, y, z, u, v\} = \{a \mid (a = x) \vee (a = y) \vee (a = z) \vee (a = u) \vee (a = v)\}$
(4) $\{x, y, z, u, v, w\} = \{a \mid (a = x) \vee (a = y) \vee (a = z) \vee (a = u) \vee (a = v) \vee (a = w)\}$

Of course we are restricted to finite lists, because we can only write finite lists with our finite ink and finite paper.

Theorem 19 (Singleton and Inclusion): $x \in S$ if and only if $\{x\} \subseteq S$.

Proof: $\Rightarrow$: Assume that $x \in S$. Consider any $z \in \{x\}$. Then $z = x$, so we have $z \in S$. Since z was arbitrary, we may conclude that $\{x\} \subseteq S$.

$\Leftarrow$: Assume that $\{x\} \subseteq S$. We have $x \in \{x\}$ (since $x = x$). Therefore we have $x \in S$. ■

Theorem 20 : $\{x, y\} = \{y, x\}$

Proof: This essentially follows from the logical rule $\Phi \vee \Psi \Leftrightarrow \Psi \vee \Phi$. Here are the details.

Consider any z. We have

$$\begin{aligned} z \in \{x, y\} &\Leftrightarrow (z = x) \vee (z = y) \\ &\Leftrightarrow (z = y) \vee (z = x) \\ &\Leftrightarrow z \in \{y, x\}. \end{aligned}$$

From $z \in \{x, y\} \Leftrightarrow z \in \{y, x\}$ we generalize to conclude that $\{x, y\} = \{y, x\}$. ■

Theorem 21 : $\{x\} = \{y\}$ if and only if $x = y$.

Proof: $\Rightarrow$: Assume that $\{x\} = \{y\}$. We have $x \in \{x\}$, since $x = x$. Thus we have $x \in \{y\}$, and from this we get $x = y$.

$\Leftarrow$: Assume that $x = y$. Then $\{x\} = \{y\}$, by Axiom 2. ■

Theorem 22 : $\{x, y\} = \{u\}$ if and only if $x = y = u$.

Proof: **Exercise 37**. ■

Theorem 23 : If $\{x, y\} = \{u, v\}$, then either $x = u$ and $y = v$, or $x = v$ and $y = u$.

Proof: **Exercise 38**. ■

Exercise 39: Prove that $\{x\} \subseteq \{x, y\}$.

Exercise 40: Prove that $\{\{\}\} \neq \{\}$.

Exercise 41: Prove that $\{\{\{\}\}\} \neq \{\{\}\}$.

Exercise 42: Prove that if $y = \{b\}$, then $\{ z \mid (\exists x \mid (z \in x) \wedge (x \in y)) \} = b$.

Exercise 43: Prove that if $a \subseteq \{x\}$, then either $a = \{\}$ or $a = \{x\}$.

Definition 24 (Being a Singleton): A set is said to be a *singleton* iff it has the form $\{x\}$ for some x. That is, we call s a singleton iff $(\exists x \mid s = \{x\})$.

A singleton is characterized by the fact that it contains a unique element:

Theorem 25 (Existence and Uniqueness in Terms of Singleton):
A set s is a singleton if and only if it has a unique element. That is, s is a singleton if and only if

$$(\exists x \mid x \in s \wedge (\forall y \mid y \in s \Rightarrow y = x)).$$

Proof: $\Rightarrow$: Assume that s is a singleton. Then we can get an x such that $s = \{x\}$. We have $x \in s$, by Definition 16, and it remains to prove that $(\forall y \mid y \in s \Rightarrow y = x)$. Consider any $y \in s = \{x\}$. Definition 16 immediately gives $y = x$.

$\Leftarrow$: Now assume that $(\exists x \mid x \in s \wedge (\forall y \mid y \in s \Rightarrow y = x))$. Get an $x \in s$ such that

$$(\forall y \mid y \in s \Rightarrow y = x). \qquad (*)$$

We claim that $s = \{x\}$. Since $x \in s$, we have $\{x\} \subseteq s$ by Theorem 19. Since $y = x \Leftrightarrow y \in \{x\}$, the condition $(*)$ can be rewritten as "$(\forall y \mid y \in s \Rightarrow y \in \{x\})$," which is the definition of "$s \subseteq \{x\}$." Thus, having proven both inclusions, we have $s = \{x\}$. ■

"Getting" Unique Things Often in mathematics we know that there exists a unique thing with certain properties. How can we *refer* to it? For example, let's say we know that there exists a unique green thing. In English, we would refer to it by saying "*the* green thing." Is there a mathematical version of "the" that can allow us to write down a *term* which refers to "the unique such-and-such"?

If we know that $(\exists x \mid x \text{ is green})$, then we can always use EI to "get" a green thing x. But that would just be a *hypothetical* green thing that was can use for the sake of arguments. We can use it to draw conclusions, but "x" would still not refer to any *specific* green thing. It would be "a green thing" and not "the green thing." However, if we knew that there were a *unique* green thing, i.e. if we knew

$$(\exists x \mid x \text{ is green} \wedge (\forall y \mid y \text{ is green} \Rightarrow y = x)),$$

then by Theorem 25 we would know that

$$\{ x \mid x \text{ is green} \}$$

is a *singleton*. This means that $\{ x \mid x \text{ is green} \} = \{g\}$ for some g, and then if we "pluck" g out of $\{g\}$, that's "*the* green thing."

It is therefore useful to have a formal mechanism for "plucking" the single occupant of a singleton out from between the curly braces. The following definition provides this, although this may not be clear until Theorem 27.

Definition 26 (Occupant): Let s be a singleton. The *occupant* of s is denoted by $\mathrm{occ}(s)$ and defined by

$$\mathrm{occ}(s) = \{\, z \mid (\forall x \mid x \in s \Rightarrow z \in x) \,\}.$$

The definition above contains an *assumption*, that s is a singleton. When a definition contains an assumption, the definition is only meant to be used under the conditions of the assumption. If you try to use the definition without first verifying that those conditions hold, then the definition may behave in unintended ways. We can declare the notation to be "undefined" in such cases, and reject any argument that breaches into undefined territory. We just don't talk about $\mathrm{occ}(s)$ unless s is already known to be a singleton.

Theorem 27 (Essence of Occupant): $\mathrm{occ}(\{g\}) = g$.

Proof: $\subseteq$: Assume that $z \in \mathrm{occ}(\{g\})$. Then for every $x \in \{g\}$, we have $z \in x$. In particular $g \in \{g\}$, so we have $z \in g$.

$\supseteq$: Assume that $z \in g$. Now we must prove that z is an element of every $x \in \{g\}$. Consider any $x \in \{g\}$. Then $x = g$, so $z \in g$ gives $z \in x$. ■

Now we have an explicit way to refer to "the green thing," when we know that there is a unique green thing:

$$\text{Let } g = \mathrm{occ}(\{\, x \mid x \text{ is green} \,\}).$$

In practice, this is achieved by writing something like

$$\text{Let } g \text{ denote the unique green thing.}$$

Exercise 44: Determine what is $\mathrm{occ}(\{\, x \mid (\forall y \mid y \notin x) \,\})$, and prove your claim. If it is "undefined," then say so. Hint: Theorem 14.

3.3 Intersection, Union, and Relative Complement

Definition 28 (Intersection and Union):

(1) $a \cap b = \{\, x \mid (x \in a) \wedge (x \in b) \,\}$
(2) $a \cup b = \{\, x \mid (x \in a) \vee (x \in b) \,\}$

Theorem 29 (Algebraic Properties of Intersection and Union):

(1)	$a \cap b = b \cap a$	(commutativity of $\cap$)
(2)	$a \cup b = b \cup a$	(commutativity of $\cup$)
(3)	$(a \cap b) \cap c = a \cap (b \cap c)$	(associativity of $\cap$)
(4)	$(a \cup b) \cup c = a \cup (b \cup c)$	(associativity of $\cup$)
(5)	$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$	($\cup$ distributes over $\cap$)
(6)	$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$	($\cap$ distributes over $\cup$)
(7)	$a \cap a = a$	(idempotence of $\cap$)
(8)	$a \cup a = a$	(idempotence of $\cup$)
(9)	$a \cup \{\} = a$	($\{\}$ is an identity for $\cup$)
(10)	$a \cap \{\} = \{\}$	($\{\}$ is an annihilator for $\cap$)

Proof of (1): For any given z, we have

$$z \in a \cap b \quad \Leftrightarrow \quad (z \in a) \wedge (z \in b) \quad \Leftrightarrow \quad (z \in b) \wedge (z \in a) \quad \Leftrightarrow \quad z \in b \cap a.$$

■

Proof of (5): For any given z, we have

$$\begin{aligned} z \in a \cup (b \cap c) \quad &\Leftrightarrow \quad (z \in a) \vee (z \in b \cap c) \\ &\Leftrightarrow \quad (z \in a) \vee ((z \in b) \wedge (z \in c)) \\ &\Leftrightarrow \quad ((z \in a) \vee (z \in b)) \wedge ((z \in a) \vee (z \in c)) \\ &\Leftrightarrow \quad (z \in a \cup b) \wedge (z \in a \cup c) \\ &\Leftrightarrow \quad z \in (a \cup b) \cap (a \cup c). \end{aligned}$$

■

Proof of (9): $\supseteq$: Consider any $z \in a$. Then we have $(z \in a) \vee (z \in \{\})$, so $z \in a \cup \{\}$.

$\subseteq$: Consider any $z \in a \cup \{\}$. Then we have either $z \in a$ or $z \in \{\}$. Since $z \notin \{\}$, it must be that $z \in a$ (Rule 12). ■

Proving the rest of them is **Exercise 45**.

In the proofs given above, you can see some different ways of proving an equality. In the first two proofs, the pattern is to establish a chain of "$\Leftrightarrow$" and then gain an equality like $A = B$ by having proven $(\forall z \restriction z \in A \Leftrightarrow z \in B)$. This is relying on Axiom 8. In the third proof, the pattern is to gain $A = B$ by establishing $A \subseteq B$ and $B \subseteq A$. This is relying on Theorem 10. The latter pattern, gaining equality via double inclusion, is far more commonly used and it will ultimately be much more useful for you. Chains of "$\Leftrightarrow$" really only show up in the basics of set theory– they become very unwieldy when things get the slightest bit complicated.

Theorem 30 (Maximality of Intersection):

The set $b \cap c$ is a subset of both b and c, and it contains anything that is a subset of both b and c. That is,

(1) $b \cap c \subseteq b$
(2) $b \cap c \subseteq c$
(3) If $a \subseteq b$ and $a \subseteq c$, then $a \subseteq b \cap c$.

Proof: To prove (1), consider any $z \in b \cap c$. Then $z \in b$ and $z \in c$. In particular, $z \in b$.

The proof of (2) is similar.

To prove (3), assume that $a \subseteq b$ and $a \subseteq c$. Consider any $z \in a$. Due to our hypothesis we have $z \in b$ and $z \in c$, so $z \in b \cap c$. Since z is arbitrary, we may conclude that $a \subseteq b \cap c$. ■

Theorem 31 (Minimality of Union):

The set $b \cup c$ contains both b and c, and it is a subset of any set that contains both b and c. That is,

(1) $b \subseteq b \cup c$
(2) $c \subseteq b \cup c$
(3) If $b \subseteq a$ and $c \subseteq a$, then $b \cup c \subseteq a$.

Proof: **Exercise 46**. A proof by cases is needed in (3). ■

Theorem 32 (Inclusion in Terms of $\cap$ and $\cup$):

The following are equivalent:

(1) $a \subseteq b$
(2) $a \cap b = a$
(3) $a \cup b = b$

Proof: (1) $\Rightarrow$ (2): Assume that $a \subseteq b$. We already have $a \cap b \subseteq a$ by Theorem 30, so it remains for us to prove that $a \subseteq a \cap b$. Consider any $z \in a$. Since $a \subseteq b$, we have $z \in b$. Now since $z \in a$ and $z \in b$, it follows that $z \in a \cap b$.

(2) $\Rightarrow$ (3): Assume that $a \cap b = a$. We already have $b \subseteq a \cup b$ by Theorem 31, so it remains for us to prove that $a \cup b \subseteq b$. Consider any $z \in a \cup b$. Now either $z \in a$ or $z \in b$.

Case 1: Suppose that $z \in a$. Then, since $a = a \cap b$, we have $z \in a \cap b$. This gives $z \in a$ and $z \in b$.

Case 2: Suppose that $z \in b$. That's all for case 2.

In both cases we got $z \in b$, so we are done.

(3) $\Rightarrow$ (1): **Exercise 47.** ■

When a theorem gives a list of assertions, be attentive to precisely what the theorem is saying about the list. In Theorem 31, for example, the assertion is a conjunction (1) $\wedge$ (2) $\wedge$ (3). In Theorem 32, on the other hand, the assertion is a chain of equivalences (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3). In the proof above, we see a typical strategy for proving a chain of equivalences: prove a "cycle" of implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). With several applications of the transitivity of implication (Rule 7), the cycle of implications yields the chain of equivalences.

Definition 33 (Relative Complement): $a \setminus b = \{\, x \mid (x \in a) \wedge (x \notin b) \,\}$

Theorem 34 (De Morgan's Law - Set Theory Version):
(1) $a \setminus (b \cap c) = (a \setminus b) \cup (a \setminus c)$
(2) $a \setminus (b \cup c) = (a \setminus b) \cap (a \setminus c)$

Proof of (1): $\subseteq$: Consider any $z \in a \setminus (b \cap c)$. We have $z \in a$ and $z \notin (b \cap c)$. Writing $z \notin (b \cap c)$ as $\neg(z \in b \wedge z \in c)$, we can apply the logical version of De Morgan's law (Rule 16) to see that we have either $z \notin b$ or $z \notin c$.

Case 1: If $z \notin b$, then since $z \in a$ we have $z \in (a \setminus b)$. It follows that $z \in (a \setminus b) \cup (a \setminus c)$ simply because $a \setminus b$ is a subset of $(a \setminus b) \cup (a \setminus c)$ (Theorem 31).

Case 2: If $z \notin c$, then since $z \in a$ we have $z \in (a \setminus c)$. Again it follows that $z \in (a \setminus b) \cup (a \setminus c)$ because $a \setminus c$ is a subset of $(a \setminus b) \cup (a \setminus c)$.

In both cases we have $z \in (a \setminus b) \cup (a \setminus c)$, so we are done proving that $a \setminus (b \cap c) \subseteq (a \setminus b) \cup (a \setminus c)$.

$\supseteq$: Consider any $z \in (a \setminus b) \cup (a \setminus c)$. We have either $z \in (a \setminus b)$ or $z \in (a \setminus c)$.

Case 1: Suppose that $z \in (a \setminus b)$. Then $z \in a$ and $z \notin b$. If we had $z \in b \cap c$, then we would in particular have $z \in b$, which gives a contradiction. So it must be that $z \notin b \cap c$. Therefore, since $z \in a$ and $z \notin b \cap c$, we have $z \in a \setminus (b \cap c)$.

Case 2: Suppose that $z \in (a \setminus c)$. Then $z \in a$ and $z \notin c$. If we had $z \in b \cap c$, then we would in particular have $z \in c$, so it must be that $z \notin b \cap c$. Therefore, since $z \in a$ and $z \notin b \cap c$, we have $z \in a \setminus (b \cap c)$.

In both cases we have $z \in a \setminus (b \cap c)$, so we are done proving that $(a \setminus b) \cup (a \setminus c) \subseteq a \setminus (b \cap c)$. ■

Proof of (2): **Exercise 48** ■

Theorem 35 (Iterated Relative Complement): $a \setminus (a \setminus b) = a \cap b$.

Proof: $\subseteq$: Consider any $z \in a \setminus (a \setminus b)$. Then $z \in a$ and $z \notin a \setminus b$.

Suppose, for the sake of contradiction, that $z \notin b$. Then $z \in a$ and $z \notin b$, so $z \in a \setminus b$. This is a contradiction, so it must be that in fact $z \in b$.

Since $z \in a$ and $z \in b$, we have $z \in a \cap b$.

$\supseteq$: Assume that $z \in a \cap b$. Then $z \in a$ and $z \in b$, so it is not the case that $z \in a$ and $z \notin b$. That is, $z \notin a \setminus b$. Since $z \in a$ and $z \notin a \setminus b$, we have $z \in a \setminus (a \setminus b)$. ■

Alternative proof of Theorem 35: Consider any z. We have

$$\begin{array}{rcll} z \in a \setminus (a \setminus b) & \Leftrightarrow & (z \in a) \wedge (z \notin a \setminus b) & \text{(Definition 33)} \\ & \Leftrightarrow & (z \in a) \wedge \neg((z \in a) \wedge (z \notin b)) & \text{(Definition 33)} \\ & \Leftrightarrow & (z \in a) \wedge ((z \notin a) \vee (z \in b)) & \text{(Rule 16)} \\ & \Leftrightarrow & (z \in a) \wedge ((z \in a) \Rightarrow (z \in b)) & \text{(Rule 18)} \\ & \Rightarrow & z \in b & \text{(Rule 4).} \end{array}$$

$\subseteq$: Assume that $z \in a \setminus (a \setminus b)$. We immediately get $z \in a$ and from the reasoning above we also get $z \in b$. Thus we get $z \in a \cap b$.

$\supseteq$: Assume that $z \in a \cap b$. Then $z \in a$ and $z \in b$. Since $z \in b$, we have $(z \notin a) \vee (z \in b)$. So we have $(z \in a) \wedge ((z \notin a) \vee (z \in b))$. As seen in the reasoning above, this is sufficient to conclude that $z \in a \setminus (a \setminus b)$. ■

It is tempting to define some sort of "absolute" complement like this: $a^c = \{ x \mid x \notin a \}$. However, for reasons related to repairing the bug mentioned earlier, such a definition would not behave in the way that you would expect. So it is best to avoid it altogether. In practice, the sets one works with are almost always subsets of some big common "background set," and complements taken relative to the background set are sufficient.

Exercise 49: Prove that $a \cup b = \{\}$ if and only if $a = \{\}$ and $b = \{\}$.

Exercise 50: Prove that $\{x, y\} = \{x\} \cup \{y\}$.

Exercise 51: Prove these fun facts about relative complements:

1. $a \setminus b \subseteq a$.
2. $a \setminus a = \{\}$.
3. $a \cap b = \{\}$ if and only if $a \setminus b = a$.
4. $a \subseteq b$ if and only if $a \setminus b = \{\}$.

5. $(a \setminus b) \cup b = a \cup b$.

6. $(a \setminus b) \cap b = \{\}$.

7. $a \setminus (b \cup c) = (a \setminus b) \setminus c$.

3.4 Power Sets

The set of all subsets of a given set x is called the *power set* of x, denoted by $\mathcal{P}(x)$.

Definition 36 (Power Set): $\mathcal{P}(x) = \{\, y \mid y \subseteq x \,\}$.

Exercise 52: Prove that the empty set is both an element of and a subset of $\mathcal{P}(x)$.

Exercise 53: Prove that $\{x\} \subseteq \mathcal{P}(x)$.

Exercise 54: Prove that $\mathcal{P}(\{\}) = \{\{\}\}$.

Theorem 37: $\mathcal{P}(\{x\}) = \{\{\}, \{x\}\}$.

Proof: $\supseteq$: Consider any $z \in \{\{\}, \{x\}\}$. Either $z = \{\}$ or $z = \{x\}$.

Case 1: Suppose that $z = \{\}$. Then $z \subseteq \{x\}$ (Theorem 13 part (1)).

Case 2: Suppose that $z = \{x\}$. Then $z \subseteq \{x\}$ (Theorem 7 part (1)).

Since $z \subseteq \{x\}$ in both cases, we have $z \subseteq \{x\}$. It follows that $z \in \mathcal{P}(\{x\})$.

$\subseteq$: Consider any $z \in \mathcal{P}(\{x\})$. Then $z \subseteq \{x\}$. Either z is $\{\}$ or it is not.

Case 1: If $z = \{\}$, then $z \in \{\{\}, \{x\}\}$ and we are done.

Case 2: If $z \neq \{\}$, then z must have an element (Theorem 15). So we can get a y such that $y \in z$. Since $z \subseteq \{x\}$, it follows that $y \in \{x\}$, and so in fact $y = x$. Now we have $x \in z$. It follows that $\{x\} \subseteq z$ (Theorem 19), and combining this with $z \subseteq \{x\}$ gives us $z = \{x\}$. Thus we finally have $z \in \{\{\}, \{x\}\}$ and we are done. ■

Exercise 55: Prove that $\mathcal{P}(\{x, y\}) = \{\{\}, \{x\}, \{y\}, \{x, y\}\}$.

Exercise 56: If a set x has n elements, then how many elements do you think its power set $\mathcal{P}(x)$ has? Make your best guess. No proof or justification is needed here (nor is it possible– we have yet to even define numbers or what it means for a set to have a certain number of

elements).

Exercise 57: Prove that $\mathcal{P}(x) \cap \mathcal{P}(y) = \mathcal{P}(x \cap y)$.

Exercise 58: Prove that if $\neg(x \subseteq y)$ and $\neg(y \subseteq x)$, then $\mathcal{P}(x) \cup \mathcal{P}(y) \neq \mathcal{P}(x \cup y)$.

3.5 Pairs and Cartesian Products

Definition 38 (Ordered Pair): $(x, y) = \{\{x\}, \{x, y\}\}$.

The purpose of this mysterious definition is revealed by the following theorem.

Theorem 39 (Essence of Pairs):

$$(x, y) = (u, v) \text{ if and only if } x = u \text{ and } y = v.$$

Proof: The implication "$\Leftarrow$" is just Axiom 2, so it only remains to prove "$\Rightarrow$". Assume that $(x, y) = (u, v)$. According to Theorem 23, we have $\{x\} = \{u\}$ and $\{x, y\} = \{u, v\}$, or we have $\{x\} = \{u, v\}$ and $\{x, y\} = \{u\}$.

Case 1: Suppose that $\{x\} = \{u\}$ and $\{x, y\} = \{u, v\}$. From $\{x\} = \{u\}$ it follows that $x = u$ (Theorem 21). Since $y \in \{x, y\} = \{u, v\}$, we know that either $y = u$ or $y = v$.

Case 1.1: Suppose that $y = u$. Then since $x = u = y$, we have $\{x, y\} = \{u\}$ (Theorem 22). Since we had assumed $\{x, y\} = \{u, v\}$, we now have $\{u, v\} = \{u\}$. It follows that $u = v$ (again using Theorem 22), and so $y = v$.

Case 1.2: If $y = v$, then the proof is done.

Case 2: Suppose that $\{x\} = \{u, v\}$ and $\{x, y\} = \{u\}$. By Theorem 22 it follows that $u = v = x$ and $x = y = u$. In other words, $x = y = u = v$, so in particular $x = u$ and $y = v$. ■

Compare this result to Theorem 20. Thanks to Theorem 39, pairs have a "first entry" and a "second entry." For this reason they are often called *ordered* pairs.

Definition 40: A set is called a *pair* if and only if it has the form (a, b) for some a and b. That is, we call x a pair if and only if

$$(\, \exists a, b \mid x = (a, b)\,).$$

A set s is called a *set of pairs* or a *relation* if every element of s is a pair.

This definition is an instance of a general pattern: When things are said to have a certain

form, there is an implicit existential assertion being made. For example when an integer is called "a square," what this means is that the integer is the square of *some* integer. Definition 24 was another example of this pattern.

Definition 41 (Cartesian Product):

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

Observe that the cartesian product $A \times B$ of two sets A and B is a *set of pairs*. The product $A \times B$ is the collection of all pairs whose first entry is an element of A and whose second entry is an element of B. There is a shorthand for writing

$$\{\, x \mid (\, \exists a, b \mid x = (a, b) \ \wedge\ \Phi\,)\,\}$$

which is to simply write

$$\{\, (a, b) \mid \Phi\,\}\,.$$

So a cartesian product can be described like this: $A \times B = \{\, (a, b) \mid a \in A \ \wedge\ b \in B\,\}$. That's a new bit of notation for us. Up until now, we had only allowed *variables* to appear behind a "$\mid$". The appearance of a more complex *term* behind the "$\mid$" indicates that we are collecting into a set all things of a particular *form*, in this case the form of a pair. Note the implicit existential quantifier. The following theorem seems obvious, but it's worth looking at how the existential quantifier gets handled.

Theorem 42 (Essence of Cartesian Product):

$(y, z) \in A \times B$ if and only if $y \in A$ and $z \in B$.

Proof: $\Rightarrow$: Assume that $(y, z) \in A \times B$. Then we can get some $a \in A$ and $b \in B$ such that $(y, z) = (a, b)$. By Theorem 39, we have $y = a$ and $z = b$. It follows that $y \in A$ and $z \in B$.

$\Leftarrow$: Assume that $y \in A$ and $z \in B$. Define $x = (y, z)$. We have $x = (y, z)$, $y \in A$, and $z \in B$, so we can conclude that $(\, \exists y, z \mid x = (y, z) \ \wedge\ y \in A \ \wedge\ z \in B\,)$. Therefore $x \in A \times B$. In other words, $(y, z) \in A \times B$. ■

The intermediate label "x" was introduced in that proof just to help clarify how the existential generalization took place– normally this extraneous label would not be introduced. In fact, the standard practice is to start from a definition written in the form "$A \times B = \{\, (a, b) \mid a \in A \ \wedge\ b \in B\,\}$," and then to immediately accept Theorem 42 as the way for membership to work in the set $A \times B$.

Exercise 59: For this exercise we define a useless doubleton-based version of cartesian

product:

$$A \otimes B = \{\{a, b\} \mid a \in A \wedge b \in B\}.$$

1. Expand the shorthand out into its full form, with the existential quantifier included.

2. Mimicking Theorem 42, try to prove that if $\{y, z\} \in A \otimes B$, then $y \in A$ and $z \in B$. Exactly what goes wrong?

Theorem 43 (Cartesian Products and Emptiness):
(1) $A \times B$ is nonempty if and only if A and B are both nonempty.
(2) $A \times B$ is empty if and only if either A is empty or B is empty.

Proof: Since (2) is an inversion of (1), it suffices to just prove (1) (Rule 15).

$\Rightarrow$: Assume that $A \times B$ is nonempty. Then we can get some $x \in A \times B$ (Theorem 15). Using Definition 41, we can now get some $a \in A$ and $b \in B$ such that $x = (a, b)$. Since we have exhibited an element of A and an element of B, we conclude that A and B are nonempty (Theorem 15).

$\Leftarrow$: Assume that A and B are both nonempty. Then we can get some $a \in A$ and $b \in B$. We have $(a, b) \in A \times B$ (Theorem 42), so we conclude that $A \times B$ is nonempty (Theorem 15). ■

Theorem 44: If $A \subseteq B$ and $C \subseteq D$, then $A \times C \subseteq B \times D$.

Proof: Assume that $A \subseteq B$ and $C \subseteq D$. Consider any $z \in A \times C$. Since

$$(\, \exists a, c \mid z = (a, c) \wedge a \in A \wedge c \in C \,),$$

we can get some $a \in A$ and $c \in C$ such that $z = (a, c)$. Since $A \subseteq B$, we have $a \in B$. Similarly, since $C \subseteq D$, we have $c \in D$. Thus $(a, c) \in B \times D$, by Theorem 42. That is, $z \in B \times D$. ■

Shorter way of writing the same proof: Assume that $A \subseteq B$ and $B \subseteq C$. Consider any $(a, c) \in A \times C$. We have $a \in A$ and $c \in C$, by Theorem 42. Since $A \subseteq B$, we have $a \in B$. Similarly, since $C \subseteq D$, we have $c \in D$. Thus $(a, c) \in B \times D$, again by Theorem 42. ■

The "shorter" proof really is the same proof, but it's skipping some repetitive steps that would look the same in any proof that a cartesian product is contained in some other set. Pay special attention to the line "Consider any $(a, c) \in A \times C$." This is sort of like the line "Consider any z..." that sets a proof up for a UG, but a pair (a, c) is introduced instead of a *variable* like z. This step is only valid for the UG because *every* element of $A \times C$ has the form of a pair.

Theorem 45:

$$(A \times C) \cap (B \times D) \subseteq (A \cap B) \times (C \cap D).$$

Proof: Consider any $(x, y) \in (A \times C) \cap (B \times D)$. Then we have $(x, y) \in A \times C$ and $(x, y) \in (B \times D)$. It follows from these that $x \in A$, $y \in C$, $x \in B$, and $y \in D$. Since $x \in A$ and $x \in B$, we have $x \in A \cap B$. Since $y \in C$ and $y \in D$, we have $y \in C \cap D$. Therefore $(x, y) \in (A \cap B) \times (C \cap D)$. ■

Theorem 46: If A is nonempty and $A \times C \subseteq B \times D$, then $C \subseteq D$.

Proof: **Exercise 60**. Make sure it's clear where you use the hypothesis that A is nonempty. ■

Exercise 61: Prove that $\{x\} \times \{y\} = \{(x, y)\}$.

Exercise 62: Assuming that a, b, c, d, e are distinct, list all the elements of $\{a, b, c\} \times \{d, e\}$. You do not need to prove anything.

Exercise 63: If A has n elements and B has m elements, then how many elements do you think $A \times B$ has? (Do not give a proof or justification– we have not even defined numbers, let alone the concept of a set having a certain number of elements.)

Definition 47 (Domain and Range): Let S be a set of pairs. The *domain* and the *range* of S are denoted respectively by $\text{dom}(S)$ and $\text{ran}(S)$, and they are defined as follows:

$$\begin{array}{rcl} \text{dom}(S) & = & \{\, x \mid (\exists y \mid (x, y) \in S\,)\,\} \\ \text{ran}(S) & = & \{\, y \mid (\exists x \mid (x, y) \in S\,)\,\} \end{array}$$

Exercise 64: Let $S = \{(a, a), (b, c), (a, d)\}$. Prove that the domain of S is $\{a, b\}$ and the range of S is $\{a, c, d\}$.

Exercise 65: Assuming that $S \subseteq T \subseteq A \times B$, prove that $\text{dom}(S) \subseteq \text{dom}(T)$.

Exercise 66: Assuming that S and T are both sets of pairs, prove that $\text{dom}(S \cup T) = \text{dom}(S) \cup \text{dom}(T)$.

3.6 Functions

Definition 48 (Function): A set f is said to be a *function* iff f is a set of pairs and

$$(\,\forall x, y, z \mid (x, y), (x, z) \in f \;\Rightarrow\; y = z\,)\,.$$

The notation $(x,y),(x,z) \in f$ is short for $((x,y) \in f) \wedge ((x,z) \in f)$.

The quantified statement in Definition 48 should feel a bit like a uniqueness statement, especially if written in this equivalent way:

$$(\,\forall x, y \,\mathbb{!}\, (x,y) \in f \;\Rightarrow\; (\,\forall z \,\mathbb{!}\, (x,z) \in f \;\Rightarrow\; y = z\,)\,).$$

It says that if a pair shows up as an element of f with its first entry being x, then the second entry of the pair is uniquely determined.

Theorem 49 : If f is a function and $x \in \mathrm{dom}(f)$, then

$$\{\, y \,\mathbb{!}\, (x,y) \in f \,\}$$

is a singleton.

Proof: Assume that f is a function and $x \in \mathrm{dom}(f)$. By Theorem 25, we just need to show that $\{\, y \,\mathbb{!}\, (x,y) \in f \,\}$ has a unique element. Since $x \in \mathrm{dom}(f)$, we can get a y such that $(x,y) \in f$. We thus have $y \in \{\, y \,\mathbb{!}\, (x,y) \in f \,\}$. Now we must show that y is unique. Suppose that $z \in \{\, y \,\mathbb{!}\, (x,y) \in f \,\}$. Then $(x,z) \in f$. Since f is a function and $(x,y),(x,z) \in f$, we conclude that $y = z$. ■

Definition 50 (Function Evaluation): Let f be a function and let $x \in \mathrm{dom}(f)$. By Theorem 49, there is a unique y such that $(x,y) \in f$. We denote this unique y by "$f(x)$", and we call it *the value of f at x*. Formally, we are making the definition

$$f(x) = \mathrm{occ}(\{\, y \,\mathbb{!}\, (x,y) \in f \,\}).$$

When f is a function, one thinks of $x \in \mathrm{dom}(f)$ as an "input" and one thinks of $f(x)$ as the "output" to which f "maps" x. Thus a function is a set of input-output pairs.

Theorem 51 (Essence of Evaluation): If f is a function then
(1) If $x \in \mathrm{dom}(f)$, then $(x, f(x)) \in f$.
(2) If $(x,y) \in f$, then $y = f(x)$.
(3) If $x \in \mathrm{dom}(f)$, then $(x,y) \in f \Leftrightarrow y = f(x)$.

Proof: Assume that f is a function.

To prove (1), assume that $x \in \mathrm{dom}(f)$. According to Theorem 49, then set $\{\, y \,\mathbb{!}\, (x,y) \in f \,\}$ is a singleton. Thus we can get some z so that $\{\, y \,\mathbb{!}\, (x,y) \in f \,\} = \{z\}$. Now, using Theorem 27,

$$f(x) = \mathrm{occ}(\{\, y \,\mathbb{!}\, (x,y) \in f \,\}) = \mathrm{occ}(\{z\}) = z.$$

Thus we have

$$f(x) \in \{z\} = \{\, y \,\mathbb{!}\, (x,y) \in f \,\}.$$

That is, we have $(x, f(x)) \in f$, proving (1).

To prove (2), assume that $(x, y) \in f$. Since there exists a y such that $(x, y) \in f$, we have $x \in \text{dom}(f)$, and so we may apply part (1) and conclude that $(x, f(x)) \in f$. Since f if a function and $(x, y), (x, f(x)) \in f$, we have $y = f(x)$.

Finally, (3) is simply a combination of (1) and (2). ■

Defining a Function by a Formula Often people will define a function by providing a formula that turns inputs into outputs. For example, one might say "Define f by $f(x) = x^2$ for $x \in A$," in order to define a squaring function. This is a way of making the definition "Let $f = \{ (x, x^2) \mid x \in A \}$." Note that in order for the "formula" style of definition to be a complete definition of a function, one needs to provide a domain (such as A in the example). We will sometimes adopt this style.

Theorem 52 : If f is a function, then $y \in \text{ran}(f)$ if and only if $y = f(x)$ for some $x \in \text{dom}(f)$.

Proof: Assume that f is a function.

$\Rightarrow$: Assume that $y \in \text{ran}(f)$. Then we can get some x so that $(x, y) \in f$. By Theorem 51, part (2), it follows that $y = f(x)$. Since $(x, y) \in f$, we have $(\exists y \mid (x, y) \in f)$. That is, $x \in \text{dom}(f)$.

$\Leftarrow$: Now assume that $y = f(x)$ and $x \in \text{dom}(f)$. By Theorem 51, part (1), it follows that $(x, y) \in f$. Thus we have $(\exists x \mid (x, y) \in f)$. That is, $y \in \text{ran}(f)$. ■

Theorem 53 (Equality of Functions): If f and g are functions, then $f = g$ if and only if $\text{dom}(f) = \text{dom}(g)$ and $f(x) = g(x)$ for all $x \in \text{dom}(f)$.

Proof: **Exercise 67**. Be careful in your proof to not attempt an evaluation before verifying that the input is in the domain of the function. ■

The notation $f : X \to Y$ is a proposition, read as "f maps X to Y" and defined as follows:

Definition 54 (Mapping):

$$f : X \to Y \quad \Leftrightarrow \quad \left(\begin{array}{ll} f \text{ is a function} & \wedge \\ \text{dom}(f) = X & \wedge \\ \text{ran}(f) \subseteq Y & \end{array} \right).$$

Pay special attention to the role of Y in this definition. Since X is the domain of f when $f : X \to Y$, it is tempting to think that Y is the range of f– but it is often not so. In the context of "$f : X \to Y$", the Y is referred to as a *codomain*.

Theorem 55 : If f is a function, then $f : X \to Y$ if and only if $f \subseteq X \times Y$ and $X \subseteq \text{dom}(f)$.

Proof: **Exercise 68**. ■

Exercise 69: Assume that x, y, z, u, v, w are distinct, and that none of them is a pair. For each of the following, determine whether it is a function. If it is, write a true statement of the form "$f : X \to Y$." If it is not, explain why not. The first two are done for you.

1. $f = \{(x, y), (v, w)\}$

   Answer: $f : \{x, v\} \to \{y, w\}$.

2. $f = \{(x, y), (x, w)\}$

   Answer: f is not a function, because (x, y) and (x, w) are in f while $y \neq w$.

3. $f = \{(x, y), (y, z), (z, w)\}$

4. $f = \{(x, x), (y, y), (v, v)\}$

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

6. $f = \{(x, y), (z, w), (u, w)\}$

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

8. $f = \{x, (y, z)\}$

9. $f = \{(u, v)\}$

10. $f = \{\}$

Exercise 70: Prove that if f is a function and $g \subseteq f$, then g is a function.

Exercise 71: Assume that $f : X \to Y$ and $A \subseteq X$. Define $g = \{\, (a, f(a)) \,!\, a \in A \,\}$.

1. Write out the full non-shorthand definition of g that includes the existential quantifer.

2. Prove that $g : A \to Y$.

Theorem 56 (Piecewise Function Definition):
If f and g are functions and $\text{dom}(f) \cap \text{dom}(g) = \{\}$, then $f \cup g$ is a function.

Proof: **Exercise 72.** ■

Definition 57 (Injectivity, Surjectivity, and Bijectivity):
Assume that $f : X \to Y$.
(1) f is *injective* iff for all $x, y \in X$, we have $f(x) = f(y) \Rightarrow x = y$.
(2) f is *surjective onto* Y iff $\text{ran}(f) = Y$.
(3) f is *bijective onto* Y iff f is both injective and surjective onto Y.

Injectivity To understand injectivity, it may help to look at a contraposed version of the definition: f is injective iff

$$(\forall x, y \mid (x, y \in \text{dom}(f) \ \wedge \ x \neq y) \ \Rightarrow \ (f(x) \neq f(y)))\,.$$

For an injective function, *different* inputs are always mapped to *different* outputs. For a non-injective function, two different inputs can get mapped to the same output.

Surjectivity When $f : X \to Y$, it is already known that $\text{ran}(f) \subseteq Y$. To say that f is surjective onto Y is then to say that $Y \subseteq f$, which is to say that every element of the codomain Y is arises as an output of the function f. For a function $f : X \to Y$ to *not* be surjective onto Y, there would have to be some element of Y that never arises as the output $f(x)$ for any $x \in X$.

When talking about surjectivity, people will sometimes omit the "surjective" and just say "f maps X onto Y," where the use of "*on*to" rather than "to" indicates surjectivity. Also, people will sometimes omit the "onto Y" and just say "f is surjective," leaving you to guess the codomain Y from context.

Theorem 58 : Assume that f is a function. Then f is injective if and only if

$$(\forall x, y, z \mid (x, y), (z, y) \in f \ \Rightarrow \ x = z)\,.$$

Proof: Assume that $f : X \to Y$.

$\Rightarrow$: Assume that f is injective. Consider any x, y, z such that $(x, y), (z, y) \in f$. We clearly have $x, z \in \text{dom}(f)$, and so we may apply Theorem 51 and conclude that $y = f(x)$ and $y = f(z)$. Since f is injective and $f(x) = f(z)$, we have $x = z$.

$\Leftarrow$: Assume that for all x, y, z such that $(x, y), (z, y) \in f$, we have $x = z$. To show that f is injective, consider any $x, y \in \text{dom}(f)$ such that $f(x) = f(y)$. Using Theorem 51, we have $(x, f(x)), (y, f(y)) \in f$. Since $f(x) = f(y)$, we actually have $(x, f(x)), (y, f(x)) \in f$.

Applying our assumption, it follows that $x = y$. ■

Thus injectivity is very similar to functionhood (Definition 48), except that the pairs have been flipped around.

Exercise 73: Assume that $f : X \to Y$ and $x \in \text{dom}(f)$. Assume also that f is injective. Define $g = f \setminus \{(x, f(x))\}$. Prove that $g : (X \setminus \{x\}) \to (Y \setminus \{f(x)\})$.

Theorem 59 : Assume that $f : X \to Y$. Then f is surjective onto Y if and only if

$$(\forall y \nmid y \in Y \Rightarrow (\exists x \nmid x \in X \wedge f(x) = y)).$$

Proof: **Exercise 74**. ■

Exercise 75: For each of the functions in Exercise 69, determine whether it is injective. If not, then explain why not.

Bijectivity As Theorem 59 suggests, surjectivity is a sort of existence statement. If $f : X \to Y$ and f is surjective onto Y, then for each $y \in Y$ there *exists* an $x \in X$ that maps to y. Injectivity, on the other hand, is a uniqueness statement. If f is injective, then when $f(x) = y$ we know that x is the *unique* thing that maps to y. Bijectivity is then existence and uniqueness together: If f is bijective, then for each $y \in Y$ *there exists a unique* $x \in X$ that maps to y.

When $f : X \to Y$ and f is bijective onto Y, we say that f gives a *one-to-one correspondence* between the elements of X and the elements of Y.

Exercise 76: Prove that if f is an injective function and $g \subseteq f$, then g is an injective function.

Exercise 77: Let $f = \{(a, c), (b, d)\}$ and assume that $a \neq b$ and $c \neq d$. Prove that $f : \{a, b\} \to \{c, d\}$ and f is bijective onto $\{c, d\}$.

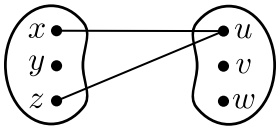
Exercise 78: Assume that $a \neq b$ and $f : \{a, b\} \to \{c\}$. Prove that f cannot be injective.

Exercise 79: Assume that $a \neq b$ and $f : \{c\} \to \{a, b\}$. Prove that f cannot be surjective onto $\{a, b\}$.

Exercise 80: Assume that x, y, z, u, v, w are distinct. Let S be a the cartesian product

$$\{x, y, z\} \times \{u, v, w\}.$$

In this exercise, we will use pictures like the following to describe various subsets of S.



The subset of S being described in this example is $\{(x,u),(z,u)\}$. Each line joining two dots represents a pair which is being included in the subset of S. For each of the following, provide a picture that describes a subset of S that meets the given specifications.

1. not a function
2. a function with domain $\{y,z\}$
3. a function with range $\{v\}$
4. a non-function with domain $\{y\}$ and range $\{u,v\}$
5. a function mapping $\{x,y,z\}$ to $\{u,w\}$ which is surjective onto $\{u,w\}$
6. a function mapping $\{x,y,z\}$ to $\{u,w\}$ which is not surjective onto $\{u,w\}$
7. a function mapping $\{x,y\}$ to $\{u,v,w\}$ which is injective
8. a function mapping $\{x,y\}$ to $\{u,v,w\}$ which is not injective
9. a function mapping $\{x,y,z\}$ to $\{u,v,w\}$ which is bijective onto $\{u,v,w\}$ and whose value at x is w

Exercise 81: Prove that if $X \times Y$ is a function, then either $X \times Y$ must be $\{\}$ or Y must be a singleton.

3.7 Composition and Inverse

Definition 60 (Composite):

$$S \circ T = \{\, (x,z) \mid (\exists y \mid (x,y) \in T \wedge (y,z) \in S) \,\}.$$

Recall that the right hand side above is a shorthand for

$$\{\, p \mid (\exists x, z \mid p = (x,z) \wedge (\exists y \mid (x,y) \in T \wedge (y,z) \in S)) \,\}.$$

Theorem 61 (Associativity of Composition): $S \circ (T \circ U) = (S \circ T) \circ U$

Proof: $\subseteq$: Consider any $(x, w) \in S \circ (T \circ U)$. Get y such that $(x, y) \in T \circ U$ and $(y, w) \in S$. Since $(x, y) \in T \circ U$, we can also get z such that $(x, z) \in U$ and $(z, y) \in T$. Now we have found a y satisfying $(z, y) \in T$ and $(y, w) \in S$, so we have shown that $(z, w) \in S \circ T$. Having found a z such that $(x, z) \in U$ and $(z, w) \in S \circ T$, we conclude that $(x, w) \in (S \circ T) \circ U$.

$\supseteq$: **Exercise 82**: Prove that $(S \circ T) \circ U \subseteq S \circ (T \circ U)$. ■

Theorem 62 (Domain and Range of Composite):
(1) If $\text{ran}(T) \subseteq \text{dom}(S)$, then $\text{dom}(S \circ T) = \text{dom}(T)$.
(2) $\text{ran}(S \circ T) \subseteq \text{ran}(S)$

Proof of (1) Assume that $\text{ran}(T) \subseteq \text{dom}(S)$.

$\subseteq$: Consider any $x \in \text{dom}(S \circ T)$. Get z such that $(x, z) \in S \circ T$. Get y such that $(x, y) \in T$ and $(y, z) \in S$. We have found a y such that $(x, y) \in T$. It follows that $x \in \text{dom}(T)$.

$\supseteq$: Consider any $x \in \text{dom}(T)$. Get y such that $(x, y) \in T$. Since there exists an x such that $(x, y) \in T$, we have $y \in \text{ran}(T)$. From our assumption $\text{ran}(T) \subseteq \text{dom}(S)$, it follows that $y \in \text{dom}(S)$. Get z such that $(y, z) \in S$. We have found a y such that $(x, y) \in T$ and $(y, z) \in S$. It follows that $(x, z) \in S \circ T$, so we have found a z such that $(x, z) \in S \circ T$. It follows that $x \in \text{dom}(S \circ T)$. ■

Proving (2) is **Exercise 83**.

Theorem 63 (Essence of Composition):
(1) If f and g are functions, then $g \circ f$ is a function and

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

for all $x \in \text{dom}(g \circ f)$.
(2) If $f : X \to Y$ and $g : Y \to Z$, then $g \circ f : X \to Z$.

Proof of (1): Assume that f and g are functions.

From Definition 60, it is clear that every element of $g \circ f$ is a pair. Thus $g \circ f$ is a set of pairs.

Consider any x, y, z such that (x, y) and (x, z) are in $g \circ f$. Using the fact that $(x, y) \in g \circ f$, we can get a such that $(x, a) \in f$ and $(a, y) \in g$. Using the fact that $(x, z) \in g \circ f$, we can get b such that $(x, b) \in f$ and $(b, z) \in g$. Since (x, a) and (x, b) are both in the function f, we must have $a = b$. Since (a, y) and $(b, z) = (a, z)$ are both in the function g, we must have $y = z$.

We have argued that $g \circ f$ is a set of pairs, and that whenever $(x, y), (x, z) \in g \circ f$, it follows

that $y = z$. Thus we have shown that $g \circ f$ is a function.

Now consider any $x \in \text{dom}(g \circ f)$. Get z such that $(x, z) \in g \circ f$. Get y such that $(x, y) \in f$ and $(y, z) \in g$. We will now make several uses of Theorem 51. From $(x, y) \in f$ and $(y, z) \in g$, we conclude that $y = f(x)$ and $z = g(y)$. From $(x, z) \in g \circ f$ (and the just-established fact that $g \circ f$ is a function), we conclude that $z = (g \circ f)(x)$. Thus we have

$$(g \circ f)(x) = z = g(y) = g(f(x)).$$ ■

Proof of (2): Assume that $f : X \to Y$ and $g : Y \to Z$. To show that $g \circ f : X \to Z$, we must argue that $g \circ f$ is a function, that its domain is X, and that it's range is contained in Z. We already know that $g \circ f$ is a function due to part (1) and the fact that f and g are functions.

To see that $\text{dom}(g \circ f) = X$, we will use Theorem 62. We have

$$\text{ran}(f) \subseteq Y = \text{dom}(g),$$

so part (1) of Theorem 62 applies and we conclude that $\text{dom}(g \circ f) = \text{dom}(f) = X$.

The fact that $\text{ran}(g \circ f) \subseteq Z$ is a consequence of part (2) of Theorem 62:

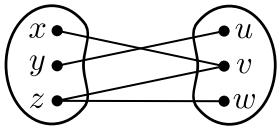
$$\text{ran}(g \circ f) \subseteq \text{ran}(g) \subseteq Z.$$ ■

The composite $g \circ f$ can be thought of as the function that, when given an input, applies f and then applies g.

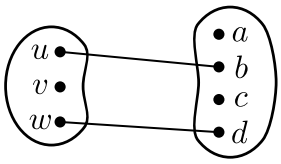
Exercise 84: Prove that if $S \subseteq A \times B$ and $T \subseteq B \times C$, then $T \circ S \subseteq A \times C$.

Exercise 85: Let $X = \{x, y, z\}$, let $U = \{u, v, w\}$, and let $A = \{a, b, c, d\}$. Assume that $x, y, z, u, v, w, a, b, c, d$ are distinct. In this exercise, we will depict subsets of $X \times U$, $U \times A$, and $X \times A$ in the manner of Exercise 80. This can give a helpful visual for composition. Let's do an example.

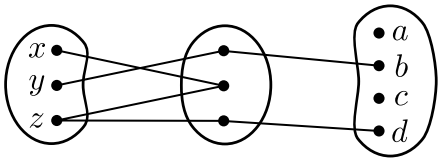
Let $f = \{(x, v), (y, u), (z, v), (z, w)\}$. Then $f \subseteq X \times U$ and f can be depicted by



Let $g = \{(u, b), (w, d)\}$. Then $g \subseteq U \times A$ and g can be depicted by

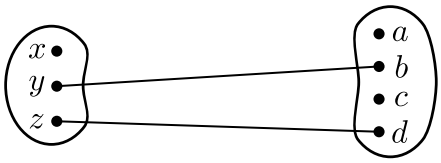


Now $g \circ f \subseteq X \times A$, and we can depict the composition by joining the two pictures together:



$(*)$

Then $g \circ f$ can be determined to have the picture



$(**)$

which is $\{(y, b), (z, d)\}$. Do you see how to get the picture $(**)$ from $(*)$?

1. Prove that if f and g are defined as in the example just given, then $\{(y, b), (z, d)\} \subseteq g \circ f$. No pictures allowed– give a real proof. You can also prove the reverse inclusion if you want, but it's... less fun.

2. For each f and g below, determine $g \circ f$ by producing images like $(*)$ and $(**)$. Your answer for each part below should include an image like $(*)$, an image like $(**)$, and a list of pairs that describes $g \circ f$.

   (a) $f = \{(x, u), (y, v), (z, w)\}$ and $g = \{(u, c), (v, a), (w, c)\}$

   (b) $f = \{(x, v), (y, v), (z, v)\}$ and $g = \{(u, a), (v, b), (w, d), (v, c)\}$

   (c) $f = \{(x, u), (y, w), (z, v)\}$ and $g = \{(v, b), (w, d)\}$

   (d) $f = \{(x, v), (y, v), (z, v)\}$ and $g = \{(u, c), (w, c)\}$

Definition 64 (Identity Function): The *identity function on* A is denoted by id_A and defined by

$$\mathrm{id}_A = \{\, (x,x) \mid x \in A \,\}.$$

Note that the right hand side above is short for

$$\{\, p \mid (\, \exists x \mid p = (x,x) \ \wedge \ x \in A \,) \,\}.$$

Theorem 65 (Facts about id_A):
(1) $\mathrm{id}_A : A \to A$.
(2) $\mathrm{id}_A(x) = x$ for all $x \in A$.
(3) If $f : A \to B$, then $f \circ \mathrm{id}_A = f$.
(4) If $g : B \to A$, then $\mathrm{id}_A \circ g = g$.

Proof: Proving (1), (2), and (3) is **Exercise 86**. We prove (4) here.

Assume that $g : B \to A$. Since $\mathrm{id}_A : A \to A$ by part (1), we have $\mathrm{id}_A \circ g : B \to A$ (Theorem 63 part (2)). In particular, the functions $\mathrm{id}_A \circ g$ and g have the same domain, B. For any $x \in B$, we have

$$\begin{array}{lll} (\mathrm{id}_A \circ g)(x) & = \mathrm{id}_A(g(x)) & \text{(Theorem 63 part (1))} \\ & = g(x). & \text{(part (2) of this theorem)} \end{array}$$

It follows from Theorem 53 that $\mathrm{id}_A \circ g = g$. ■

Definition 66 (Reverse): The *reverse* of S is denoted by $S^{\dashv}$ and defined by

$$S^{\dashv} = \{\, (y,x) \mid (x,y) \in S \,\}.$$

Note that the right hand side above is short for

$$\{\, p \mid (\, \exists x, y \mid p = (y,x) \ \wedge \ (x,y) \in S \,) \,\}.$$

Theorem 67 (Essence of Reversal): $(x,y) \in S \Leftrightarrow (y,x) \in S^{\dashv}$.

Proof: $\Rightarrow$: Assume that $(x,y) \in S$. We want to prove that $(y,x) \in S^{\dashv}$. This seems obvious but let us do it very carefully to avoid confusion. The proposition $(y,x) \in S^{\dashv}$ is equivalent to

$$(\, \exists a, b \mid (y,x) = (b,a) \ \wedge \ (a,b) \in S \,). \qquad (*)$$

Letting $b = y$ and $a = x$, we get $(y,x) = (b,a)$ and $(a,b) = (x,y) \in S$. We conclude (by an EG) that the condition $(*)$ holds and therefore that $(y,x) \in S^{\dashv}$.

$\Leftarrow$: Assume that $(y, x) \in S^{\dashv}$. Get a and b such that $(y, x) = (b, a)$ and $(a, b) \in S$ (carefully check that this is a correct use of Definition 66). Then $y = b$ and $x = a$, so $(x, y) \in S$. ■

Theorem 68 (Double Reversal): If S is a set of pairs, then

$$S^{\dashv\dashv} = S.$$

Proof: Assume that S is a set of pairs. We will make several uses of Theorem 67.

$\subseteq$: Consider any $(x, y) \in S^{\dashv\dashv}$. It follows that $(y, x) \in S^{\dashv}$, and from this it follows that $(x, y) \in S$.

$\supseteq$: Consider any $(x, y) \in S$. It follows that $(y, x) \in S^{\dashv}$, and from this it follows that $(x, y) \in S^{\dashv\dashv}$. ■

Exercise 87: Why is the assumption that S is a set of pairs needed in Theorem 68? Exactly what step of the proof would be in error if we did not have this assumption?

Theorem 69 (Reversal, Domain, and Range):
(1) $\text{dom}(S^{\dashv}) = \text{ran}(S)$.
(2) $\text{ran}(S^{\dashv}) = \text{dom}(S)$.

Proof: Proving (2) is **Exercise 88**. We prove (1) here.

$\subseteq$: Consider any $z \in \text{dom}(S^{\dashv})$. Get a such that $(z, a) \in S^{\dashv}$. Then $(a, z) \in S$. It follows that $z \in \text{ran}(S)$.

$\supseteq$: Consider any $z \in \text{ran}(S)$. Get a such that $(a, z) \in S$. Then $(z, a) \in S^{\dashv}$. It follows that $z \in \text{dom}(S^{\dashv})$. ■

Theorem 70 (Reversal and Composition): $(S \circ T)^{\dashv} = T^{\dashv} \circ S^{\dashv}$.

Proof: Proving that $(S \circ T)^{\dashv} \subseteq T^{\dashv} \circ S^{\dashv}$ is **Exercise 89**.

We will prove that $T^{\dashv} \circ S^{\dashv} \subseteq (S \circ T)^{\dashv}$. Consider any $(z, w) \in T^{\dashv} \circ S^{\dashv}$. Get a such that $(z, a) \in S^{\dashv}$ and $(a, w) \in T^{\dashv}$. Then we have $(w, a) \in T$ and $(a, z) \in S$. It follows that $(w, z) \in S \circ T$, and from this it follows that $(z, w) \in (S \circ T)^{\dashv}$. ■

Definition 71 (Invertibility): If f is a function, then f is said to be *invertible* if and only if $f^{\dashv}$ is also a function. In this context, we will refer to $f^{\dashv}$ as *the inverse* of f.

Theorem 72 (Invertibility of Injections): If f is a function, then $f^{\dashv}$ is a function if and only if f is injective.

Proof: Assume that f is a function.

Suppose that $f^{\dashv}$ is a function. We will use the criterion given in Theorem 58 to demonstrate that f is injective. Consider any x, y, z such that $(x, y), (z, y) \in f$. By Theorem 67, we have $(y, x), (y, z) \in f^{\dashv}$. Since $f^{\dashv}$ is a function, it follows that $x = z$. Thus we have proven that f is injective.

Conversely, suppose that f is injective. It is clear from Definition 66 that $f^{\dashv}$ is a set of pairs. To see that $f^{\dashv}$ is a function, suppose that $(x, y), (x, z) \in f^{\dashv}$. By Theorem 67, we have $(y, x), (z, x) \in f$. By Theorem 58 and the fact that f is injective, it follows that $y = z$. Thus we have proven that $f^{\dashv}$ is a function. ■

Note the role of the word "conversely" when it is used to introduce a paragraph. It serves to separate the "⇒" and "⇐" portions of the proof.

Theorem 73: If $f : X \to Y$ and f is injective, then $f^{\dashv} : \text{ran}(f) \to X$.

Proof: **Exercise 90**. ■

Theorem 74 : If f is an invertible function, $x \in \text{dom}(f)$, and $y \in \text{ran}(f)$, then

$$f(x) = y \;\Leftrightarrow\; x = f^{\dashv}(y)$$

Proof: Assume that f is an invertible function, $x \in \text{dom}(f)$, and $y \in \text{ran}(f)$. Theorem 73 tells us that $\text{ran}(f) = \text{dom}(f^{\dashv})$, so $y \in \text{dom}(f^{\dashv})$ and we are in a position to apply Theorem 51 as follows:

$$\begin{array}{rcll} f(x) = y & \Leftrightarrow & (x, y) \in f & \text{(Theorem 51)} \\ & \Leftrightarrow & (y, x) \in f^{\dashv} & \text{(Theorem 67)} \\ & \Leftrightarrow & f^{\dashv}(y) = x. & \text{(Theorem 51)} \end{array}$$

■

Theorem 75 : If $f : X \to Y$ and f is a bijection onto Y, then $f^{\dashv} : Y \to X$ and $f^{\dashv}$ is a bijection onto X.

Proof: Assume that $f : X \to Y$ and f is a bijection onto Y. Since f is injective, Theorem 73 tells us that $f^{\dashv} : \text{ran}(f) \to X$. Since f is surjective onto Y, we have $\text{ran}(f) = Y$, and so $f^{\dashv} : Y \to X$. It remains for us to argue that $f^{\dashv}$ is bijective onto X.

We know that f^{-1} is surjective onto X because $\text{ran}(f^{-1}) = \text{dom}(f) = X$, by Theorem 69.

Finally, we will use Theorem 72 to argue that f^{-1} is injective. We already know that f^{-1} is a function, and we also know that f^{-1-1}, which is f by Theorem 68, is a function. It follows from Theorem 72 that f^{-1} is injective. ■

Theorem 76 : If $f : X \to Y$ and f is injective, then $f^{-1} \circ f = \text{id}_X$.

Proof: Assume that $f : X \to Y$ and f is injective. From Theorem 73 we know that $f^{-1} : \text{ran}(f) \to X$. To prove that $f^{-1} \circ f = \text{id}_X$, we will use Theorem 53. This means we must show that the domains of $f^{-1} \circ f$ and id_X are equal, and that $f^{-1} \circ f$ and id_X take the same value on all elements of the common domain. We have $\text{dom}(\text{id}_X) = X = \text{dom}(f^{-1} \circ f)$ by Theorem 65 part (1) and Theorem 63 part (2).

Now consider any $x \in X$. Our basic argument is as follows:

$$\begin{array}{rcll} (f^{-1} \circ f)(x) & = & f^{-1}(f(x)) & \text{(Theorem 63 part (1))} \\ & = & x & \text{(Theorem 74)} \\ & = & \text{id}_X(x) & \text{(Theorem 65 part (2)).} \end{array}$$

However, some comments are needed to justify the middle line. Applying Theorem 74 to f^{-1} gives us

$$f^{-1}(f(x)) = x \;\Leftrightarrow\; f(x) = f^{-1-1}(x), \qquad (*)$$

but we should first check that the hypotheses of Theorem 74 are satisfied. Note that f^{-1} is an invertible function because $f^{-1-1} = f$ is a function. And note that $f(x) \in \text{ran}(f) = \text{dom}(f^{-1})$ and $x \in X = \text{dom}(f) = \text{ran}(f^{-1})$. Now Theorem 74 applies and we have $(*)$. The right hand side of $(*)$ holds thanks to Theorem 68, so we have $f^{-1}(f(x)) = x$ and our argument above is justified.

We have now proven that $(f^{-1} \circ f)(x) = \text{id}_X(x)$ for all $x \in X$. By Theorem 53, we have proven that $f^{-1} \circ f = \text{id}_X$. ■

Theorem 77 (Inverse and Composition): If $f : X \to Y$ and f is a bijection onto Y, then
(1) $f \circ f^{-1} = \text{id}_Y$.
(2) $f^{-1} \circ f = \text{id}_X$.

Proof: Assume that $f : X \to Y$ and f is a bijection onto Y.

Since f is injective, part (2) is Theorem 76.

By Theorem 75, we know that $f^{-1} : Y \to X$ and f^{-1} is a bijection onto X. Since f^{-1} is injective, we may apply Theorem 76 to conclude that $f^{-1-1} \circ f^{-1} = \text{id}_Y$. Using Theorem 68 to

rewrite this as $f \circ f^{\dashv} = \mathrm{id}_Y$, we have proven part (1). ■

Theorem 78 (Composition, Injectivity, and Surjectivity):
Assume that $f : X \to Y$ and $g : Y \to Z$.
(1) If f and g are injective, then $g \circ f$ is injective.
(2) If $g \circ f$ is injective, then f is injective.
(3) If f is surjective onto Y and g is surjective onto Z, then $g \circ f$ is surjective onto Z.
(4) If $g \circ f$ is surjective onto Z, then g is surjective onto Z.
(5) If f is bijective onto Y and g is bijective onto Z, then $g \circ f$ is bijective onto Z.

Proof: **Exercise 91**. ■

The notation "$f, g : X \to Y$" below is short for "$f : X \to Y \ \wedge \ g : X \to Y$".

Theorem 79 (Cancellation of Composite): Assume that $f, g : X \to Y$.
(1) If $h : Y \to Z$, h is injective, and $h \circ f = h \circ g$, then $f = g$.
(2) If $h : Z \to X$, h is surjective onto X, and $f \circ h = g \circ h$, then $f = g$.

Proof: Part (1) is **Exercise 92**. We prove (2) here.

Assume that $f, g : X \to Y$, $h : Z \to X$, h is surjective onto X, and $f \circ h = g \circ h$. Since f and g have the same domain X, all we need to do is prove that $f(x) = g(x)$ for all $x \in X$. Then we will be done by Theorem 53.

Consider any $x \in X$. Since h is surjective onto X, there is some $z \in Z$ such that $h(z) = x$ (Theorem 59). Note that $\mathrm{dom}(f \circ h) = Z$ (Theorem 63), so we may evaluate $f \circ h$ at z. We have

$$\begin{array}{rcll} f(h(z)) & = & (f \circ h)(z) & \text{(Theorem 63)} \\ & = & (g \circ h)(z) & \text{(since } f \circ h = g \circ h\text{)} \\ & = & g(h(z)) & \text{(Theorem 63).} \end{array}$$

That is, $f(x) = g(x)$. ■

Theorem 79 says that injective functions can be cancelled when they are on the left side of a composition, and surjective functions can be cancelled when they are on the right. These properties actually *characterize* injectivity and surjectivity. That is, a function is injective if and only if it is left-cancellable, and it is surjective if and only if it is right-cancellable. Proving this is **Exercise 93**, which is challenging and skippable. The precise assertion is this: If $h : Y \to Z$, then h is injective iff $h \circ f = h \circ g \Rightarrow f = g$ for all $f, g : X \to Y$, and h is surjective onto Z iff $f \circ h = g \circ h \Rightarrow f = g$ for all $f, g : X \to Y$.

Theorem 76 tells us that injective functions are "left-invertible." Precisely, this means that

they can be composed with something on the left to yield a suitable identity function. What follows is a sort of converse to Theorem 76.

Theorem 80 (Left-Invertible Functions): Assume that $f : X \to Y$. If

$$(\exists g \mid g : Y \to X \ \wedge \ g \circ f = \mathrm{id}_X),$$

then f is injective.

Proof: Assume that $f : X \to Y$ and that there is some g such that $g : Y \to X$ and $g \circ f = \mathrm{id}_X$. Get such a g. Consider any $x, x' \in X$ such that $f(x) = f(x')$. Then

$$x = \mathrm{id}_X(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = \mathrm{id}_X(x') = x'.$$

■

It is pleasing to know that there is a similar result for right-invertibility and surjectivity:

Theorem 81 (Right-Invertible Functions): Assume that $f : X \to Y$. If

$$(\exists g \mid g : Y \to X \ \wedge \ f \circ g = \mathrm{id}_Y),$$

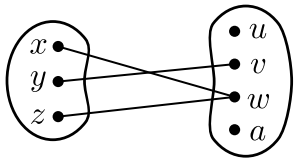
then f is surjective onto Y.

Proof: **Exercise 94**. ■

Exercise 95: Let $S = \{x, y, z\} \times \{u, v, w, a\}$. Assume that x, y, z, u, v, w, a are distinct. Define the following subsets of S:

$$\begin{array}{rcl} h & = & \{(x, w), (z, w), (y, v)\} \\ i & = & \{(x, v), (y, w), (z, a), (y, u)\} \\ j & = & \{(x, v), (y, w), (z, a)\} \end{array}$$

1. Depict each of h, i, j using a picture in the manner of Exercise 80. As an example, here is a depiction of h:



2. One of h, i, j is injective. Which one?

3. For the injection, find a left-inverse. That is, find a function $g : \{u, v, w, a\} \to \{x, y, z\}$ such that
$$g \circ (\text{the injection}) = \text{id}_{\{x,y,z\}}.$$
Depict this composition by joining pictures in the manner of Exercise 85.

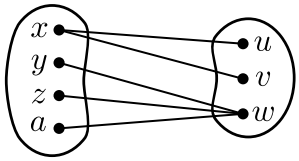
4. Redo question 3, but this time find a *different* left-inverse.

5. How many left inverses do you think there are?

Exercise 96: Let $S = \{x, y, z, a\} \times \{u, v, w\}$. Assume that x, y, z, u, v, w, a are distinct. Define the following subsets of S:

$$\begin{array}{rcl} h & = & \{(x,u),(x,v),(y,w),(z,w),(a,w)\} \\ i & = & \{(x,u),(y,u),(z,v),(a,w)\} \\ j & = & \{(x,u),(y,u),(z,w),(a,w)\} \end{array}$$

1. Depict each of h, i, j using a picture in the manner of Exercise 80. As an example, here is a depiction of h:



2. One of h, i, j is surjective onto $\{u, v, w\}$. Which one?

3. For the surjection, find a right-inverse. That is, find a function $g : \{u, v, w\} \to \{x, y, z, a\}$ such that
$$(\text{the surjection}) \circ g = \text{id}_{\{u,v,w\}}.$$
Depict this composition by joining pictures in the manner of Exercise 85.

4. Redo question 3, but this time find a *different* right-inverse.

5. How many right inverses do you think there are?

Theorems 76 and 80 tell us that left-invertibility is *equivalent* to injectivity. Theorem 81 tells us that right-invertibility *implies* surjectivity. You may now be wondering... are surjective functions always right-invertible?

If $f : X \to Y$ is surjective, then is there some $g : Y \to X$ such that $f \circ g = \text{id}_Y$? Letting $g = f^{\dashv}$ would not work, because $f^{\dashv}$ is probably not a function. If a g is to exist, then how can it be produced? Imposing various special conditions on Y can make it possible to

construct g. However, there is no hope for a general theorem. What is needed for the general statement is an axiom:

Axiom 82 (Axiom of Choice): If $f : X \to Y$ and f is surjective onto Y, then there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.

We will not use Axiom 82, but it is essential for much of modern mathematics.

Putting together Theorems 80 and 81 gives us a nice characterization of bijectivity in terms of composition:

Theorem 83 (Bijectivity and Isomorphism): Assume that $f : X \to Y$. Then f is a bijection onto Y if and only if

$$(\exists g \mid g : Y \to X \ \wedge \ g \circ f = \mathrm{id}_X \ \wedge \ f \circ g = \mathrm{id}_Y) .$$

Proof: Assume that $f : X \to Y$.

If f is a bijection onto Y, then letting $g = f^{-1}$ should work due to Theorems 75 and 77.

Conversely, assume that there exists $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. Then there exists $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$, so f is injective by Theorem 80. And there exists $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$, so f is surjective onto Y by Theorem 81. ■

Exercise 97: (Challenging) Prove that if $f : X \to Y$, f is injective, and X is nonempty, then there exists some $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$. (This is what it should really mean for f to be "left-invertible," rather than what is asserted by Theorem 76.)

Exercise 98: Prove that $\mathrm{id}_{\mathrm{dom}(B)} \subseteq B^{-1} \circ B$. Not a thrilling result, but good for practice with definitions.

3.8 Image

Definition 84 (Image): The *image of A under S* is denoted by $S[A]$ and defined by

$$S[A] = \{ y \mid (\exists x \mid x \in A \wedge (x, y) \in S) \} .$$

If S is a set of pairs, then $S[A]$ collects together the second entries of all the pairs in S whose

first entry is an element of A.

Exercise 99: Prove that $S[\mathrm{dom}(S)] = \mathrm{ran}(S)$

Exercise 100: Prove that $S[\{\}] = \{\}$

Exercise 101: Prove that if $f : X \to Y$, then $f^{\dashv}[Y] = X$.

The set $f^{\dashv}[B]$ appearing below is often called the *preimage* or the *inverse image* of B.

Theorem 85 (Image for Functions): Assume that $f : X \to Y$.

(1) If $A \subseteq X$, then

$$f[A] = \{\, f(a) \mid a \in A \,\}.$$

In other words,

$$y \in f[A] \;\Leftrightarrow\; (\exists a \mid y = f(a) \wedge a \in A\,).$$

(2)

$$f^{\dashv}[B] = \{\, x \mid x \in X \wedge f(x) \in B \,\}.$$

So if $x \in X$, then

$$x \in f^{\dashv}[B] \;\Leftrightarrow\; f(x) \in B.$$

Proof of (1): Assume that $f : X \to Y$ and $A \subseteq X$.

$\subseteq$: Consider any $z \in f[A]$. Get $a \in A$ such that $(a, z) \in f$. By Theorem 51, we have $z = f(a)$. We have shown that there exists an $a \in A$ for which $z = f(a)$, so $z \in \{\, f(a) \mid a \in A \,\}$.

$\supseteq$: Consider any $z \in \{\, f(a) \mid a \in A \,\}$. Get $a \in A$ such that $z = f(a)$. Observe that $a \in \mathrm{dom}(f)$, since $A \subseteq X$, so we are not breaching into undefined territory! By Theorem 51, we have $(a, z) \in f$. We have shown that there exists an $a \in A$ for which $(a, z) \in f$, so $z \in f[A]$. ■

Proof of (2): Assume that $f : X \to Y$.

$\subseteq$: Consider any $z \in f^{\dashv}[B]$. Get $b \in B$ such that $(b, z) \in f^{\dashv}$. Then $(z, b) \in f$. It follows that $f(z) = b$. And of course from $(z, b) \in f$ we know that $z \in \mathrm{dom}(f) = X$, so we have

$$z \in \{\, x \mid x \in X \wedge f(x) \in B \,\}.$$

$\supseteq$: Consider any $z \in X$ such that $f(z) \in B$. We have $(z, f(z)) \in f$, so $(f(z), z) \in f^{\dashv}$. Taking $x = f(z)$, we've shown there exists an $x \in B$ such that $(x, z) \in f^{\dashv}$. Therefore $z \in f^{\dashv}[B]$. ■

In the context of Theorem 85, where the set of pairs f is a function, it is tempting to refer

to $f^{\dashv}$ as an "inverse," but this would be a terrible mistake. The set of pairs $f^{\dashv}$ need not be a function, and so we just refer to it as the "reverse" of f.

Exercise 102: Prove that if $f : X \to Y$ and $x \in X$, then $f[\{x\}] = \{f(x)\}$.

Exercise 103: Prove that if $f : X \to Y$ and $A \subseteq B \subseteq Y$, then $f^{\dashv}[A] \subseteq f^{\dashv}[B]$.

Exercise 104: Prove that if $f : X \to Y$ and $A \subseteq B \subseteq X$, then $f[A] \subseteq f[B]$.

Theorem 86 (Image and Composition): $(g \circ f)[A] = g[f[A]]$.

Proof: $\subseteq$: Consider any $z \in (g \circ f)[A]$. Get $a \in A$ such that $(a, z) \in g \circ f$. Get c such that $(a, c) \in f$ and $(c, z) \in g$. From $a \in A$ and $(a, c) \in f$, it follows that $c \in f[A]$. From $c \in f[A]$ and $(c, z) \in g$, it follows that $z \in g[f[A]]$.

$\supseteq$: **Exercise 105**: Prove that $g[f[A]] \subseteq (g \circ f)[A]$. ■

Exercise 106: Prove that if $f : X \to Y$, then f is injective if and only if for all $y \in Y$, $f^{\dashv}[\{y\}]$ is either empty or it is a singleton.

Exercise 107: Prove that if $f : X \to Y$, then f is surjective onto Y if and only if for all $y \in Y$, $f^{\dashv}[\{y\}]$ is nonempty.

Theorem 87 : Assume that $f : X \to Y$, $A \subseteq X$, and $B \subseteq Y$.
(1) $f[f^{\dashv}[B]] \subseteq B$.
(2) $A \subseteq f^{\dashv}[f[A]]$.
(3) If $B \subseteq \text{ran}(f)$, then $f[f^{\dashv}[B]] = B$.
(4) If f is injective, then $f^{\dashv}[f[A]] = A$.

Proof: Proving parts (1) and (4) is **Exercise 108**. We prove (2) and (3). We will be relying on the descriptions of image and preimage that are given in Theorem 85.

To prove (2), consider any $a \in A$. By Theorem 85 part (1), we have $f(a) \in f[A]$. By Theorem 85 part (2), it follows that $a \in f^{\dashv}[f[A]]$.

To prove (3), assume that $B \subseteq \text{ran}(f)$. Note that we have one inclusion from part (1), so we only need to prove that $B \subseteq f[f^{\dashv}[B]]$. Consider any $b \in B$. Then by our assumption we have $b \in \text{ran}(f)$. Get x such that $(x, b) \in f$. Then $f(x) = b \in B$. By Theorem 85 part (2), the fact that $f(x) \in B$ gives us $x \in f^{\dashv}[B]$. By Theorem 85 part (1), the fact that $x \in f^{\dashv}[B]$ gives us $f(x) \in f[f^{\dashv}[B]]$. In other words, $b \in f[f^{\dashv}[B]]$. ■

Theorem 88 (Preimage Plays Nice): Assume that $f : X \to Y$, $A \subseteq Y$, and $B \subseteq Y$.
(1) $f^{-1}[A \cup B] = f^{-1}[A] \cup f^{-1}[B]$
(2) $f^{-1}[A \cap B] = f^{-1}[A] \cap f^{-1}[B]$
(3) $f^{-1}[A \setminus B] = f^{-1}[A] \setminus f^{-1}[B]$

Proof: Proving (2) and (3) is **Exercise 109**. We prove (1) here. Assume that $f : X \to Y$, $A \subseteq Y$, and $B \subseteq Y$.

$\subseteq$: Consider any $z \in f^{-1}[A \cup B]$. Then $z \in X$ and $f(z) \in A \cup B$. So either $f(z) \in A$ or $f(z) \in B$.

Case 1: If $f(z) \in A$, then $z \in f^{-1}[A] \subseteq f^{-1}[A] \cup f^{-1}[B]$.

Case 2: If $f(z) \in B$, then $z \in f^{-1}[B] \subseteq f^{-1}[A] \cup f^{-1}[B]$.

$\supseteq$: Consider any $z \in f^{-1}[A] \cup f^{-1}[B]$. Then either $z \in f^{-1}[A]$ or $z \in f^{-1}[B]$.

Case 1: If $z \in f^{-1}[A]$, then $z \in X$ and $f(z) \in A \subseteq A \cup B$, so $z \in f^{-1}[A \cup B]$.

Case 2: If $z \in f^{-1}[B]$, then $z \in X$ and $f(z) \in B \subseteq A \cup B$, so $z \in f^{-1}[A \cup B]$. ■

Exercise 110: Assume that $f : X \to Y$ and that A and B are subsets of X. One of the following two assertions has a proof, while the other does not.

$f[A \cup B] = f[A] \cup f[B]$
$f[A \cap B] = f[A] \cap f[B]$

Prove the one that has a proof. You should somehow find yourself blocked from proving the other one. (Open-ended question: What blocks the proof?)

Exercise 111: Given any function $f : A \to B$, let us define an operation "hat" as follows:

$$\widehat{f} = \{ (S, f[S]) \mid S \subseteq A \}.$$

1. Prove that if $f : A \to B$, then $\widehat{f} : \mathcal{P}(A) \to \mathcal{P}(B)$.
2. Prove that if $f : A \to B$ and $g : B \to C$, then $\widehat{g \circ f} = \widehat{g} \circ \widehat{f}$.

3.9 Natural Numbers

Given any term T, the string "next(T)" forms a term, defined as follows.

Definition 89 (Successor): $\text{next}(x) = x \cup \{x\}$.

We now introduce ten new constants into our language.

Definition 90 (Certain Numbers):

$$\begin{array}{ll} 0 = \{\} & 5 = \text{next}(4) \\ 1 = \text{next}(0) & 6 = \text{next}(5) \\ 2 = \text{next}(1) & 7 = \text{next}(6) \\ 3 = \text{next}(2) & 8 = \text{next}(7) \\ 4 = \text{next}(3) & 9 = \text{next}(8) \end{array}$$

Definition 91 (Inductive): A set J is said to be *inductive* if it contains 0 and it contains $\text{next}(n)$ for every n that it contains. That is,

$$J \text{ is inductive } \Leftrightarrow \ (0 \in J \ \wedge \ (\forall n \restriction n \in J \Rightarrow \text{next}(n) \in J\,))$$

We now define the constant $\mathbb{N}$. Elements of $\mathbb{N}$ are called *natural numbers*.

Definition 92: $\mathbb{N} = \{\, n \restriction (\forall J \restriction J \text{ is inductive } \Rightarrow \ n \in J\,)\,\}$.

The set $\mathbb{N}$ of natural numbers can be thought of as the "smallest" inductive set:

Theorem 93 (Essence of $\mathbb{N}$):
(1) $\mathbb{N}$ is inductive.
(2) If J is inductive, then $\mathbb{N} \subseteq J$.

Proof of (1): We must show that $0 \in \mathbb{N}$ and that $(\forall n \restriction n \in \mathbb{N} \Rightarrow \text{next}(n) \in \mathbb{N}\,)$.

Consider any inductive set J. By definition, $0 \in J$. Thus $(\forall J \restriction J \text{ is inductive } \Rightarrow \ 0 \in J\,)$. In other words, $0 \in \mathbb{N}$.

Now we prove that $(\forall n \restriction n \in \mathbb{N} \Rightarrow \text{next}(n) \in \mathbb{N}\,)$. Consider any $n \in \mathbb{N}$. Consider any inductive set J. Since $n \in \mathbb{N}$, we know that n is in every inductive set. In particular, $n \in J$. Sine J is inductive, it follows that $\text{next}(n) \in J$. Having shown that $\text{next}(n) \in J$ for an arbitrary inductive J, we conclude that $(\forall J \restriction J \text{ is inductive } \Rightarrow \ \text{next}(n) \in J\,)$. In other words, $\text{next}(n) \in \mathbb{N}$. ■

Proof of (2): Assume that J is inductive. Consider any $n \in \mathbb{N}$. Since n is an element of every inductive set, we have in particular that $n \in J$. ■

Theorem 94 (Mathematical Induction):
If

$$\Phi_{[x\to 0]}$$

and

$$\big(\,\forall n \,\mathbin{!}\, n \in \mathbb{N} \;\Rightarrow\; (\Phi_{[x\to n]} \;\Rightarrow\; \Phi_{[x\to \text{next}(n)]})\,\big)$$

both hold, then it follows that

$$\big(\,\forall n \,\mathbin{!}\, n \in \mathbb{N} \;\Rightarrow\; \Phi_{[x\to n]}\,\big)\,.$$

Proof: Assume that $\Phi_{[x\to 0]}$ and that $\big(\,\forall n \,\mathbin{!}\, n \in \mathbb{N} \;\Rightarrow\; (\Phi_{[x\to n]} \;\Rightarrow\; \Phi_{[x\to \text{next}(n)]})\,\big)$. Define

$$J = \{\, x \,\mathbin{!}\, (x \in \mathbb{N}) \wedge \Phi \,\}\,.$$

We argue that J is inductive.

First, we must show that $0 \in J$. This is equivalent to $(0 \in \mathbb{N}) \wedge \Phi_{[x\to 0]}$. We know that $0 \in \mathbb{N}$ since $\mathbb{N}$ is inductive (Theorem 93 part (1)). And we know that $\Phi_{[x\to 0]}$ holds because we assumed it. Therefore we have $0 \in J$.

Next, we must show that $(\,\forall n \,\mathbin{!}\, n \in J \Rightarrow \text{next}(n) \in J\,)$. Consider any $n \in J$. We have $n \in \mathbb{N}$ and $\Phi_{[x\to n]}$. By our assumption, it follows that $\Phi_{[x\to \text{next}(n)]}$. Since $\mathbb{N}$ is inductive and $n \in \mathbb{N}$, we have $\text{next}(n) \in \mathbb{N}$. From

$$(\text{next}(n) \in \mathbb{N}) \wedge \Phi_{[x\to \text{next}(n)]}$$

we see that $\text{next}(n) \in J$. Thus we have established that J is inductive.

By Theorem 93 part (2), it follows that $\mathbb{N} \subseteq J$. So

$$(\,\forall n \,\mathbin{!}\, n \in \mathbb{N} \Rightarrow n \in J\,)\,.$$

Since $n \in J$ is equivalent to $(n \in \mathbb{N}) \wedge \Phi_{[x\to n]}$, this proves our theorem. ■

Induction Theorem 94 is often used to prove things about natural numbers. The technique is called *mathematical induction*. Suppose you want to prove that all natural numbers are green. Then you can first prove that 0 is green; this is called the *base case*. Then prove that whenever a natural number n is green, it follows that $\text{next}(n)$ is also green; this is called the *induction step*. Then mathematical induction allows you to conclude that all natural numbers are green. Specifically, this would be an application of Theorem 94 with Φ being "x is green". One says that one is *doing induction on* x, since x is the variable that gets replaced by 0, n, and $\text{next}(n)$ in the application of Theorem 94.

To help you with reading and writing proofs that use induction, here is a base template applied to the nonsensical "all natural numbers are green" example:

Theorem: All natural numbers are green. In other words, $(\forall n \,\rfloor\, n \in \mathbb{N} \Rightarrow n \text{ is green})$.

Proof: We will prove this by doing induction on n in the proposition "n is green".

Base Case:

[insert argument convincing reader that 0 is green]

Induction Step: Suppose that $n \in \mathbb{N}$ and n is green.

[insert argument convincing reader that next(n) is green]

By induction (Theorem 94), it follows that $(\forall n \,\rfloor\, n \in \mathbb{N} \Rightarrow n \text{ is green})$. ■

Definition 95 (Order for $\mathbb{N}$):
(1) $x < y \;\Leftrightarrow\; x \in y$.
(2) $x \leq y \;\Leftrightarrow\; (x \in y \vee x = y)$.

Theorem 96 (Essence of Order and Succession):
(1) $x < \text{next}(x)$.
(2) $x < \text{next}(y) \;\Leftrightarrow\; x \leq y$.

Proof: **Exercise 112**. ■

Theorem 97 (About 0): If $n \in \mathbb{N}$, then
(1) $0 < \text{next}(n)$.
(2) $0 \leq n$.
(3) $0 \neq \text{next}(n)$.

Proof: We will prove that $0 < \text{next}(n)$ for all $n \in \mathbb{N}$, by doing induction on n.

Base Case: We have $0 < \text{next}(0)$ because it is equivalent to $0 \leq 0$.

Induction Step: Suppose that $n \in \mathbb{N}$ and $0 < \text{next}(n)$. Then $0 \leq \text{next}(n)$. It follows that $0 < \text{next}(\text{next}(n))$.

By induction (Theorem 94), we have proven that $0 < \text{next}(n)$ for every natural number n. This completes the proof of part (1).

Part (2) is equivalent to part (1).

To prove part (3), assume that $n \in \mathbb{N}$ and Suppose for the sake of contradiction that $0 = \text{next}(n)$. Then it follows from part (1) that $0 \in 0$. But $0 = \{\}$ is empty. ■

Theorem 98 (Predecessor): If $n \in \mathbb{N}$ and $n \neq 0$, then $n = \text{next}(m)$ for some $m \in \mathbb{N}$.

Proof: We must prove that

$$(\forall n \,\mathbf{!}\, n \in \mathbb{N} \Rightarrow (n \neq 0 \Rightarrow (\exists m \,\mathbf{!}\, m \in \mathbb{N} \wedge n = \text{next}(m)))). \qquad (*)$$

We will do this by doing an induction on n in the proposition

$$n \neq 0 \Rightarrow (\exists m \,\mathbf{!}\, m \in \mathbb{N} \wedge n = \text{next}(m)).$$

Base Case: It is vacuously true that $0 \neq 0 \Rightarrow (\exists m \,\mathbf{!}\, m \in \mathbb{N} \wedge 0 = \text{next}(m))$.

Induction Step: Suppose that $n \in \mathbb{N}$ and $n \neq 0 \Rightarrow (\exists m \,\mathbf{!}\, m \in \mathbb{N} \wedge n = \text{next}(m))$. We must now show that

$$\text{next}(n) \neq 0 \Rightarrow (\exists m \,\mathbf{!}\, m \in \mathbb{N} \wedge \text{next}(n) = \text{next}(m)).$$

Assume that $\text{next}(n) \neq 0$. Taking $m = n$ gives $m \in \mathbb{N}$ and $\text{next}(n) = \text{next}(m)$, so $(\exists m \,\mathbf{!}\, m \in \mathbb{N} \wedge \text{next}(n) = \text{next}(m))$. This completes the induction step.

By induction (Theorem 94), we have proven $(*)$. ■

Theorem 99 (Succession Preserves Order): Assume that $n \in \mathbb{N}$.
(1) If $m < n$, then $\text{next}(m) \leq n$.
(2) If $m < n$, then $\text{next}(m) < \text{next}(n)$.

Proof: Part (2) is equivalent to part (1). We prove part (1).

We will prove

$$m < n \;\Rightarrow\; \text{next}(m) \leq n$$

for all $n \in \mathbb{N}$ by doing induction on n.

Base Case: Since $\neg(m < 0)$, we have

$$m < 0 \;\Rightarrow\; \text{next}(m) \leq 0$$

and the base case is done.

Induction Step: Suppose that $n \in \mathbb{N}$ and

$$m < n \;\Rightarrow\; \text{next}(m) \leq n. \qquad (*)$$

Now assume that $m < \text{next}(n)$; we must prove that $\text{next}(m) \leq \text{next}(n)$. Our assumption $m < \text{next}(n)$ implies that $m \leq n$.

Case 1: Suppose that $m < n$. Then $\text{next}(m) \leq n$ by the induction hypothesis (∗). It follows that $\text{next}(m) < \text{next}(n)$, and therefore that $\text{next}(m) \leq \text{next}(n)$.

Case 2: Suppose that $m = n$. Then $\text{next}(m) = \text{next}(n)$, so we again have $\text{next}(m) \leq \text{next}(n)$. ■

Note the use of the words "induction hypothesis" to refer to the proposition that was assumed for the sake of establishing an induction step.

Theorem 100 (Transitivity for Order on $\mathbb{N}$): Assume that $n, m, k \in \mathbb{N}$.
(1) If $n < m$ and $m < k$, then $n < k$.
(2) If $n \leq m$ and $m < k$, then $n < k$.
(3) If $n < m$ and $m \leq k$, then $n < k$.
(4) If $n \leq m$ and $m \leq k$, then $n \leq k$.

Proof: Parts (2), (3), and (4) follow from part (1); showing this is **Exercise 113**. We prove (1) here. Assume that $n, m \in \mathbb{N}$. We will show that

$$(n < m \ \wedge \ m < k) \ \Rightarrow \ n < k$$

for all $k \in \mathbb{N}$, by doing induction on k.

Base Case: We have $(n < m \wedge m < 0) \Rightarrow n < 0$ simply because $\neg(m < 0)$.

Induction Step: Suppose that $k \in \mathbb{N}$ and

$$(n < m \ \wedge \ m < k) \ \Rightarrow \ n < k.$$

We will prove that

$$(n < m \ \wedge \ m < \text{next}(k)) \ \Rightarrow \ n < \text{next}(k).$$

Assume that $n < m$ and $m < \text{next}(k)$. Then $m \leq k$.

Case 1: Suppose that $m < k$. Then we have both $n < m$ and $m < k$, so it follows from the induction hypothesis that $n < k$.

Case 2: Suppose that $m = k$. Then, since $n < m$, we have $n < k$.

In both cases we obtained $n < k$, so it must be that $n < k$. It follows that $n \leq k$, and therefore that $n < \text{next}(k)$. This completes the induction step. ■

Theorem 101 : If $n < m$ and $m \in \mathbb{N}$, then $n \in \mathbb{N}$.

Proof: **Exercise 114**. Hint: Do an induction on m to prove "$n < m \Rightarrow n \in \mathbb{N}$" for all $m \in \mathbb{N}$. ■

Exercise 115: Prove that if $m \in \mathbb{N}$ then $m \subseteq \mathbb{N}$.

Theorem 102 (Irreflexivity for Order on $\mathbb{N}$): If $n \in \mathbb{N}$, then $\neg(n < n)$

Proof: We will use induction to prove that $(\forall n \, ! \, n \in \mathbb{N} \Rightarrow \neg(n < n))$.

Base Case: $\neg(0 < 0)$ holds because it is equivalent to $\{\} \notin \{\}$.

Induction Step: Suppose that $n \in \mathbb{N}$ and $\neg(n < n)$. Suppose, for the sake of obtaining a contradiction, that $\text{next}(n) < \text{next}(n)$. Then $\text{next}(n) \leq n$.

Case 1: If $\text{next}(n) = n$ then $\text{next}(n) < \text{next}(n)$ gives us $n < n$, which contradicts the induction hypothesis.

Case 2: Suppose that $\text{next}(n) < n$. Then since $n < \text{next}(n)$ and $\text{next}(n) < n$, it follows by transitivity (Theorem 100) that $n < n$. This contradicts the induction hypothesis. ■

Exercise 116: Prove that $\mathbb{N} \notin \mathbb{N}$. Hint: There is a very short proof.

Theorem 103 (Successor Cancels): Assume that $n, m \in \mathbb{N}$.
(1) If $\text{next}(m) < \text{next}(n)$, then $m < n$
(2) If $\text{next}(m) = \text{next}(n)$, then $m = n$.

Proof: Assume that $n, m \in \mathbb{N}$.

To prove (1), assume that $\text{next}(m) < \text{next}(n)$. Then $\text{next}(m) \leq n$, so we have

$$m < \text{next}(m) \leq n.$$

By transitivity (Theorem 100), it follows that $m < n$.

Now we prove (2). Assume that $\text{next}(m) = \text{next}(n)$. Since $m \in \text{next}(m) = \text{next}(n)$, we have $m \leq n$. Similarly, we have $n \leq m$. We will show that $m \subseteq n$ and $n \subseteq m$.

$\subseteq$: Consider any $k \in m$. By Theorem 101, it follows that $k \in \mathbb{N}$. We now have $k < m \leq n$ and we may apply transitivity to conclude that $k < n$. In other words, $k \in n$.

$\supseteq$: Consider any $k \in n$. By Theorem 101, it follows that $k \in \mathbb{N}$. We now have $k < n \leq m$ and we may apply transitivity to conclude that $k < m$. In other words, $k \in m$. ■

Theorem 104 (Trichotomy for Order on $\mathbb{N}$): Assume that $n, m \in \mathbb{N}$. Then either $m < n$, $n < m$, or $m = n$, and only *one* of these conditions holds. That is,
(1) $(m = n) \ \vee \ (m < n) \ \vee \ (n < m)$.
(2) $\neg(m = n \ \wedge \ m < n)$.
(3) $\neg(m = n \ \wedge \ n < m)$.
(4) $\neg(m < n \ \wedge \ n < m)$.

Proof: Assume that $m \in \mathbb{N}$. We will prove that

$$(\,\forall n \restriction n \in \mathbb{N} \ \Rightarrow \ ((m = n) \ \vee \ (m < n) \ \vee \ (n < m))\,)$$

by doing induction on n.

Base Case: We have

$$(m = 0) \ \vee \ (m < 0) \ \vee \ (0 < m)$$

because we have $0 \leq m$ from Theorem 97.

Induction Step: Suppose that $n \in \mathbb{N}$ and

$$(m = n) \ \vee \ (m < n) \ \vee \ (n < m).$$

Exercise 117: Complete the proof of (1) from here by proving that

$$(m = \text{next}(n)) \ \vee \ (m < \text{next}(n)) \ \vee \ (\text{next}(n) < m)$$

in each of the three cases.

Proving (2), (3), and (4) is **Exercise 118**. ■

Exercise 119: Prove that if $n, m \in \mathbb{N}$, then $(n \leq m \ \wedge \ m \leq n) \ \Rightarrow \ n = m$.

Exercise 120: Prove that if $n, m \in \mathbb{N}$, then $\neg(n \leq m) \ \Leftrightarrow \ m < n$.

Exercise 121: Prove that $2 < 5$. Prove that $4 \neq 7$.

Exercise 122: Assume that $n = \text{next}(m)$. Prove that $n \setminus \{m\} = m$.

Definition 105 (Minimum): Given $A \subseteq \mathbb{N}$, we say that n *is a minimum of* A if and only if $n \in A$ and $(\,\forall a \restriction a \in A \ \Rightarrow \ n \leq a\,)$.

Exercise 123: Prove that if a subset A of $\mathbb{N}$ has n and m as minima, then it follows that $n = m$. This justifies saying "the minimum of A" rather than "a minimum of A," when a minimum is known to exist.

Exercise 124: Assume that $A \subseteq \mathbb{N}$. To say that A has a minimum is to say that $(\,\exists n \restriction n \in A \ \wedge \ (\forall a \restriction a \in A \Rightarrow n \leq a\,)\,)$. Write down what it means for A to *not* have a

minimum. Do this by pushing the negation in all the way and applying the result from Exercise 120.

Theorem 106 (Well-Ordering of $\mathbb{N}$): Every nonempty set of natural numbers has a minimum. That is, if $A \subseteq \mathbb{N}$ then

$$A \neq \{\} \Rightarrow (\exists n \,!\, n \in A \ \wedge \ (\forall a \,!\, a \in A \Rightarrow n \leq a)).$$

Proof: Assume that $A \subseteq \mathbb{N}$. We will prove the contrapositive of the theorem: if A does not have a minimum, then A must be empty. Assume that A does not have a minimum.

We will now do an induction on k to prove that

$$(\forall m \,!\, (m \in \mathbb{N} \ \wedge \ m \leq k) \ \Rightarrow \ m \notin A) \qquad (*)$$

for all $k \in \mathbb{N}$. Then we will be done, as you will check in the following exercise.

Exercise 125: Prove that if $(*)$ holds for all $k \in \mathbb{N}$, then A is empty.

Base Case: We must show that

$$(\forall m \,!\, (m \in \mathbb{N} \ \wedge \ m \leq 0) \ \Rightarrow \ m \notin A).$$

Consider any $m \in \mathbb{N}$ such that $m \leq 0$. Suppose, for the sake of contradiction, that $m \in A$. Consider any $a \in A$. We have $0 \leq a$ by Theorem 97. From $m \leq 0 \leq a$ we get $m \leq a$. Since a is an arbitrary element of A, we have shown that $(\forall a \,!\, a \in A \Rightarrow m \leq a)$. In other words, m is a minimum of A. This contradicts our assumption that A has no minimum.

Induction Step: Suppose that

$$(\forall m \,!\, (m \in \mathbb{N} \ \wedge \ m \leq k) \ \Rightarrow \ m \notin A).$$

We must show that

$$(\forall m \,!\, (m \in \mathbb{N} \ \wedge \ m \leq \text{next}(k)) \ \Rightarrow \ m \notin A).$$

Consider any $m \in \mathbb{N}$ such that $m \leq \text{next}(k)$. Suppose, for the sake of contradiction, that $m \in A$. Consider any $a \in A$. By the induction hypothesis, we have $a \leq k \Rightarrow a \notin A$. Therefore we must have $\neg(a \leq k)$. By trichotomy (Theorem 104), it follows that $k < a$ (see also Exercise 120). By Theorem 99, we obtain $\text{next}(k) \leq a$. From $m \leq \text{next}(k) \leq a$ we get $m \leq a$. Since a is an arbitrary element of A, we have shown that $(\forall a \,!\, a \in A \Rightarrow m \leq a)$. In other words, m is a minimum of A. This contradicts our assumption that A has no minimum. ■

Exercise 126: (Open-ended) Why did $(*)$ have to be so complicated in the proof of Theorem 106? Why couldn't it just have been "$k \notin A$"? Try carrying out the proof with $(*)$ replaced by "$k \notin A$" and observe what blocks the proof from working.

The well-ordering theorem, Theorem 106, provides a new and sometimes more powerful way to carry out a proof by induction. Suppose you want to prove that all natural numbers are green. Then instead of proving a base case and an induction step, you can frame your argument like this:

Theorem: All natural numbers are green.

Proof: Define A to be the set of non-green natural numbers. Suppose, for the sake of contradiction, that A is nonempty. Then by well-ordering (Theorem 106), there is a minimum element n of A. That is, there is a minimum non-green natural number n.

[insert argument convincing reader that there exists $m < n$ such that m is non-green]

The fact that $m < n$ and $m \in A$ contradicts that n was the minimum of A. ■

3.10 Recursion

A function $f : \mathbb{N} \to X$ whose domain is $\mathbb{N}$ is called a *sequence*. Sequences are sometimes described by listing the first few outputs in order, and then putting "...". Here is an example:

$$f(0) = 2,\ f(1) = 3,\ f(2) = 4,\ f(3) = 5,\ \ldots$$

In this example, it seems that $f : \mathbb{N} \to \mathbb{N}$, and we can guess what f is intended to be. We can guess that the "..." are trying to communicate that $f(n) = \text{next}(\text{next}(n))$ for all $n \in \mathbb{N}$, or in other words that $f = \{\, (n, \text{next}(\text{next}(n))) \mid n \in \mathbb{N} \,\}$. It might be better to just define f explicitly like this, rather than create unnecessary guessing with "...".

Now consider the following example

$$f(0) = 2,\ f(1) = 4,\ f(2) = 6,\ f(3) = 8,\ \ldots$$

Now what in the world is f supposed to be? What is "..." trying to communicate here? You might want to write something like "$f(n) = 2 \cdot n + 2$", but "+" and "$\cdot$" have yet to be defined! The sort of pattern we *can* describe with the machinery built so far is that $f(\text{next}(n))$ seems to always equal $\text{next}(\text{next}(f(n)))$. That is, we can describe the output of f in terms of "previous" outputs. This is called a *recursion rule*. The list of outputs above is an attempt to communicate that f has the following two properties:

- $f(0) = 2$.
- $(\forall n \mid n \in \mathbb{N} \ \Rightarrow\ f(\text{next}(n)) = \text{next}(\text{next}(f(n))))$

Still, how is f *defined* exactly? The recursion rule is just some property that f is asserted to satisfy– how do we know that there even *is* a function satisfying that property? The following theorems are concerned with resolving this issue.

Theorem 107 (Definition by Recursion - Existence):
If $s \in X$ and $r : X \to X$, then there exists an $f : \mathbb{N} \to X$ such that $f(0) = s$ and

$$(\,\forall n \mid n \in \mathbb{N} \;\Rightarrow\; f(\text{next}(n)) = r(f(n))\,).$$

Proof: Assume that $s \in X$ and $r : X \to X$. Define

$$Z = \{\, h \mid h \subseteq \mathbb{N} \times X \;\wedge\; (0, s) \in h \;\wedge\; (\,\forall n, x \mid (n, x) \in h \;\Rightarrow\; (\text{next}(n), r(x)) \in h\,)\,\}.$$

The set Z can be thought of as collecting together all the sets of pairs that sort of have the properties that we want, except that they might contain more elements than they need in order to do so. For example, it is easy to see that $\mathbb{N} \times X$ is an element of Z. The main problem with elements of Z is that most of them are not functions. However, if we attempt to collect only the "essential" pairs that every element of Z must have in order to be an element of Z, then we may find that we have a function that has the desired properties. Define

$$f = \{\, p \mid (\,\forall h \mid h \in Z \Rightarrow p \in h\,)\,\}.$$

Since $\mathbb{N} \times X \in Z$, we have $p \in f \;\Rightarrow\; p \in \mathbb{N} \times X$ for all p, so $f \subseteq \mathbb{N} \times X$. Since we have $f \subseteq \mathbb{N} \times X$, if we want to prove that $f : \mathbb{N} \to X$ then we only need to show that f is a function and $\mathbb{N} \subseteq \text{dom}(f)$ (see Theorem 55). To finish the proof of this theorem, then, we need to prove the following claims:

(1) $\mathbb{N} \subseteq \text{dom}(f)$.

(2) f is a function.

(3) $f(0) = s$.

(4) $(\,\forall n \mid n \in \mathbb{N} \;\Rightarrow\; f(\text{next}(n)) = r(f(n))\,)$.

To do this, we will first prove some helper claims:

(5) $f \in Z$.

(6) $(0, s) \in f$ and s is unique with respect to this property. That is, $\{\, x \mid (0, x) \in f\,\} = \{s\}$.

Proof of Claim (5): We now argue that $f \in Z$. We already have $f \subseteq \mathbb{N} \times X$. We have $(0, s) \in f$ because whenever $h \in Z$, it follows that $(0, s) \in h$. Now consider any $(n, x) \in f$. We must show that $(\text{next}(n), r(x)) \in f$. Consider any $h \in Z$. Since $(n, x) \in f$, we have $(n, x) \in h$. It follows that $(\text{next}(n), r(x)) \in h$, because $h \in Z$. Since we have shown that $(\text{next}(n), r(x)) \in h$ for all $h \in Z$, we have shown that $(\text{next}(n), r(x)) \in f$. Thus we have shown that $f \in Z$.

Skippable Comment: It is easy to see from the construction of f that $f \subseteq h$ for every $h \in Z$.

So f is an element of Z which is a subset of every element of Z. Thus f can be thought of as the "smallest" set of pairs in Z.

Proof of Claim (6): We already have that $(0, s) \in f$ from Claim (5), so we only need to prove here that s is unique. Suppose that $(0, x) \in f$, and suppose for the sake of contradiction that $x \neq s$. Define $g = f \setminus \{(0, x)\}$.

Exercise 127: Prove that $g \in Z$.

Since $(0, x) \in f$ and $g \in Z$, we should have $(0, x) \in g$. We have arrived at a contradiction, so Claim (6) is proven.

Proof of Claim (1): We will do induction on n to prove that $(\forall n \nmid n \in \mathbb{N} \Rightarrow n \in \text{dom}(f))$.

Base Case: Since $(0, s) \in f$, we have $0 \in \text{dom}(f)$.

Induction Step: Suppose that $n \in \mathbb{N}$ and $n \in \text{dom}(f)$. Get x such that $(n, x) \in f$. Since $f \in Z$, it follows that $(\text{next}(n), r(x)) \in f$. Therefore $\text{next}(n) \in \text{dom}(f)$.

By induction, Claim (1) is proven.

Proof of Claim (2): Since $f \subseteq \mathbb{N} \times X$, we know that f is a set of pairs. We must prove that

$$(\forall x, y, z \nmid (x, y), (x, z) \in f \Rightarrow y = z).$$

This is equivalent to

$$(\forall n \nmid n \in \mathbb{N} \Rightarrow (\forall x, y \nmid (n, x), (n, y) \in f \Rightarrow x = y)),$$

which we will prove by doing induction on n.

Base Case: Suppose that $(0, x), (0, y) \in f$. Then by Claim (6) we have $x = s = y$.

Induction Step: Suppose that $n \in \mathbb{N}$ and that $(n, x), (n, y) \in f \Rightarrow x = y$ for all x, y. Consider any x, y such that $(\text{next}(n), x), (\text{next}(n), y) \in f$. By Claim (1), we can get z such that $(n, z) \in f$. We will argue that $x = r(z) = y$.

Suppose, for the sake of contradiction, that $x \neq r(z)$. Define $g = f \setminus \{(\text{next}(n), x)\}$.

> Subclaim: $g \in Z$.
> *Proof of Subclaim:* Since $g \subseteq f \subseteq \mathbb{N} \times X$, we have $g \subseteq \mathbb{N} \times X$. We know that $(0, s) \in f$ from Claim (6), and it cannot be that $(0, s) = (\text{next}(n), x)$ because it cannot be that $0 = \text{next}(n)$ (see Theorem 97). Therefore $(0, s) \in g$. Now we must show that $(\forall n, x \nmid (n, x) \in g \Rightarrow (\text{next}(n), r(x)) \in g)$. Consider any $(m, w) \in g$. Since $f \in Z$ and $(m, w) \in f$, we have $(\text{next}(m), r(w)) \in f$. In order to deduce $(\text{next}(m), r(w)) \in g$, we need to ensure that $(\text{next}(m), r(w))$ is not equal to $(\text{next}(n), x)$. Suppose, for the sake of contradiction, that $(\text{next}(m), r(w)) = (\text{next}(n), x)$. Then $\text{next}(m) = \text{next}(n)$ and $r(w) = x$.

By Theorem 103, it follows that $m = n$. Then our induction hypothesis applies to the situation $(n, z), (m, w) \in f$ and tells us that $z = w$. Thus $x = r(w) = r(z)$, contradicting our assumption that $x \neq r(z)$. This proves the subclaim.

Since $(\text{next}(n), x) \in f$ and $g \in Z$, we should have $(\text{next}(n), x) \in g$. We have arrived at a contradiction, and so we conclude that $x = r(z)$.

The same argument can be applied to y show that $y = r(z)$. Therefore $x = y$, and the induction step is complete.

By induction, Claim (2) is proven.

Claim (3) immediately follows from the fact that f is a function and $(0, s) \in f$.

Proof of Claim (4): Consider any $n \in \mathbb{N}$. Then $n \in \text{dom}(f)$, so $(n, f(n)) \in f$. Since $f \in Z$, it follows that $(\text{next}(n), r(f(n))) \in f$. Therefore, since f is a function, we have $f(\text{next}(n)) = r(f(n))$. ■

Theorem 108 (Definition by Recursion - Uniqueness):
Assume that $s \in X$ and $r : X \to X$. If
(1) $f, g : \mathbb{N} \to X$,
(2) $f(0) = g(0) = s$,
(3) $(\forall n, x \,\text{❙}\, n \in \mathbb{N} \Rightarrow f(\text{next}(n)) = r(f(n)))$, and
(4) $(\forall n, x \,\text{❙}\, n \in \mathbb{N} \Rightarrow g(\text{next}(n)) = r(g(n)))$,
then $f = g$.

Proof: Assume that $s \in X$, $r : X \to X$, and (1)-(4) hold. By Theorem 53, if we prove that

$$(\forall n \,\text{❙}\, n \in \mathbb{N} \;\Rightarrow\; f(n) = g(n))$$

then we will have $f = g$. We proceed with an induction on n.

Base Case: The base case $f(0) = g(0)$ is built into assumption (2).

Induction Step: Suppose that $n \in \mathbb{N}$ and $f(n) = g(n)$. Then

$$f(\text{next}(n)) = r(f(n)) = r(g(n)) = g(\text{next}(n)).$$ ■

We now have the ability to define a function (with domain $\mathbb{N}$) by specifying its value at 0 and specifying a recursion rule.

Exercise 128: Define $r : \mathbb{N} \to \mathbb{N}$ by $r(n) = \text{next}(\text{next}(n))$. Let $f : \mathbb{N} \to \mathbb{N}$ be the unique function that satisfies $f(0) = 2$ and $f(\text{next}(n)) = r(f(n))$ for all $n \in \mathbb{N}$.

1. Prove that $f(3) = 8$.

2. Prove that $2 \leq f(n)$ for all $n \in \mathbb{N}$.

Exercise 129: Define r and f as in Exercise 128. Assume that $x \neq y$. Define $r' = \{(x,y),(y,x)\}$. Let $g : \mathbb{N} \to \{x,y\}$ be the unique function that satisfies $g(0) = x$ and $g(\text{next}(n)) = r'(g(n))$.

1. Prove that $r' : \{x,y\} \to \{x,y\}$ and r' is a bijection onto $\{x,y\}$.

2. Prove that $r' \circ r' = \text{id}_{\{x,y\}}$

3. Prove that $g(3) = y$.

4. Prove that $g(f(n)) = x$ for all $n \in \mathbb{N}$.

3.11 Addition

Definition 109 (Adding One): $\ddagger = \{\, (n, \text{next}(n)) \restriction n \in \mathbb{N} \,\}$.

Exercise 130:

1. Prove that $\ddagger : \mathbb{N} \to \mathbb{N}$.

2. Prove that $\ddagger$ is injective

3. Prove that $\ddagger$ is not surjective onto $\mathbb{N}$.

Definition 110 (Adding n): Define $\mathcal{ADD} : \mathbb{N} \to \{\, f \restriction f : \mathbb{N} \to \mathbb{N} \,\}$ to be the unique function that satisfies

- $\mathcal{ADD}(0) = \text{id}_{\mathbb{N}}$ and
- $\mathcal{ADD}(\text{next}(n)) = \ddagger \circ (\mathcal{ADD}(n))$ for all $n \in \mathbb{N}$.

Exercise 131: The definition above is using Theorems 107 and 108, but some hypotheses need to be verified in order for those theorems to apply. Let $X = \{\, f \restriction f : \mathbb{N} \to \mathbb{N} \,\}$. Define the recursion rule that is being used in Definition 110. That is, define the function that plays the role of "r" in Theorem 107. Prove that the r that you define satisfies $r : X \to X$.

Exercise 132:

1. Prove that $\mathcal{ADD}(3) = \ddagger \circ (\ddagger \circ \ddagger)$.

2. Prove that $\mathcal{ADD}(3)(2) = 5$.

Definition 111 (Addition): Assume that $a, b \in \mathbb{N}$. Then we define

$$a + b = \mathcal{ADD}(b)(a).$$

Exercise 133:

1. Prove that $1 + 1 = 2$.
2. Prove that $2 + 3 = 5$.
3. Prove that $3 + 2 = 5$.

Theorem 112 (Essence of +): Assume that $m, n \in \mathbb{N}$. Then

(1) $m + n \in \mathbb{N}$.
(2) $m + 0 = m$.
(3) $m + \text{next}(n) = \text{next}(m + n)$.
(4) $\text{next}(n) = n + 1$.
(5) $m + (n + 1) = (m + n) + 1$.

Proof: **Exercise 134**. ■

From now on, whenever $n \in \mathbb{N}$ we may use "next(n)" and "$n + 1$" interchangeably.

Theorem 113 (Properties of +): Assume that $m, n, k \in \mathbb{N}$. Then

(1) $m + (n + k) = (m + n) + k$ (associativity for +)
(2) $n + 0 = n$ (0 is a right-identity for +)
(3) $0 + n = n$ (0 is a left-identity for +)
(4) $1 + n = n + 1$ (preliminary to commutativity)
(5) $m + n = n + m$ (commutativity for +)
(6) $m < n \;\Rightarrow\; m + k < n + k$ (+ respects <)
(7) $m + k = n + k \;\Rightarrow\; m = n$ (+ cancels under =)
(8) $m + k < n + k \;\Rightarrow\; m < n$ (+ cancels under <)
(9) $m + n = 0 \;\Rightarrow\; (m = 0 \wedge n = 0)$
(10) $m + n = 1 \;\Rightarrow\; ((m = 1 \wedge n = 0) \vee (m = 0 \wedge n = 1))$
(11) $m \leq m + k$
(12) $m \leq n \;\Rightarrow\; (\exists j \,\mathbf{!}\, j \in \mathbb{N} \wedge m + j = n)$ (solvability of certain equations)

We will prove (1), (6), and (7) here. Proving the rest of them is **Exercise 135**. Many (but not all!) of them are to be proved by induction.

Proof of (1): Assume that $m, n \in \mathbb{N}$. We will prove that

$$(\forall k \mid k \in \mathbb{N} \Rightarrow m + (n + k) = (m + n) + k)$$

by induction on k.

Base Case: We have

$$m + (n + 0) = m + n = (m + n) + 0,$$

by two applications of Theorem 112 part (2).

Induction Step: Suppose that $k \in \mathbb{N}$ and $m + (n + k) = (m + n) + k$. We can prove $m + (n + (k + 1)) = (m + n) + (k + 1)$ as follows:

$$\begin{array}{rcll} m + (n + (k + 1)) & = & m + ((n + k) + 1) & \text{(Theorem 112)} \\ & = & (m + (n + k)) + 1 & \text{(Theorem 112)} \\ & = & ((m + n) + k) + 1 & \text{(induction hypothesis)} \\ & = & (m + n) + (k + 1) & \text{(Theorem 112).} \end{array}$$

■

Proof of (6): Assume that $n, m \in \mathbb{N}$ an $m < n$. We will prove that

$$(\forall k \mid k \in \mathbb{N} \Rightarrow m + k < n + k)$$

by induction on k.

Base Case: We have $m + 0 < n + 0$ because $m < n$, $m + 0 = m$, and $n + 0 = n$.

Induction Step: Suppose that $k \in \mathbb{N}$ and $m + k < n + k$. We must prove that

$$m + (k + 1) < n + (k + 1).$$

Using associativity, we can rewrite what we want to prove as $(m + k) + 1 < (n + k) + 1$. In fact we have this, by Theorem 99. ■

Proof of (7): Assume that $n, m \in \mathbb{N}$. We will prove that

$$(\forall k \mid k \in \mathbb{N} \Rightarrow (m + k = n + k \Rightarrow m = n))$$

by induction on k.

Base Case: We have $m + 0 = n + 0 \Rightarrow m = n$ because $m + 0 = m$ and $n + 0 = n$.

Induction Step: Suppose that $k \in \mathbb{N}$ and $m + k = n + k \Rightarrow m = n$. We must prove that

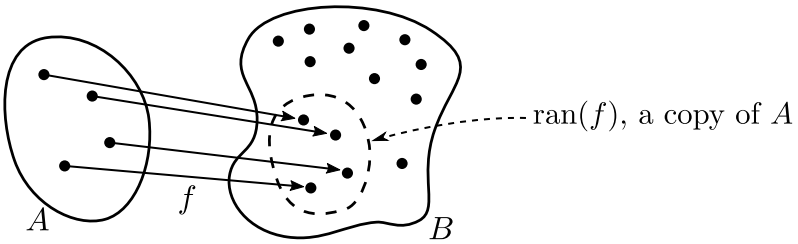
$$m + (k + 1) = n + (k + 1) \Rightarrow m = n.$$

Assume that $m+(k+1) = n+(k+1)$. By associativity, $(m+k)+1 = (n+k)+1$. By Theorem 103, it follows that $m+k = n+k$. By the induction hypothesis, it follows that $m = n$. ■

Exercise 136: Assume that $a \in \mathbb{N}$. Let $f : \mathbb{N} \to \mathbb{N}$ be the unique function satisfying $f(0) = 0$ and $f(n+1) = f(n) + a$ for all $n \in \mathbb{N}$. Prove that $f(m+k) = f(m) + f(k)$ for all $m, k \in \mathbb{N}$.

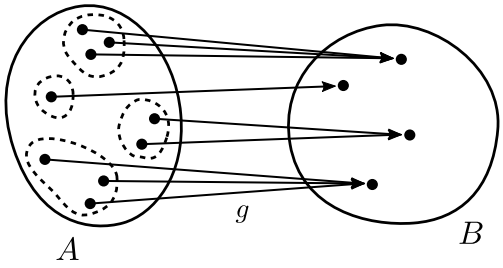
3.12 Cardinality

An injective function $f : A \to B$ associates to each element of A a unique element of B. We can imagine that an injection f *embeds* A into B, with $\text{ran}(f)$ being a subset of B that, via f, looks like a copy of A.



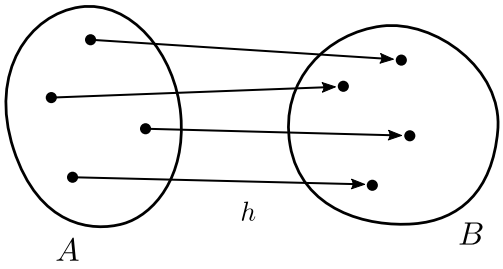
For A to embed into B like this, it seems that B must have at least as many elements as A, and B can possibly have more elements that don't get mapped to.

A surjective function $g : A \to B$ associates the elements of A to elements of B in such a way that every element of B has at least one element of A mapping to it. However, unless g is also injective, some elements of B can have multiple elements of A mapping to them. We can imagine that a surjection g collapses some bunches of elements of A onto all the individual elements of B.



For each element of B to receive at least one arrow, it seems that A must have at least as many elements as B, and A can possibly have more elements that get collapsed into some already-targeted elements of B.

A bijective function $h : A \to B$ associates all the elements of A to all the elements of B in a one-to-one way.



For a bijection to be possible, it seems that A must have exactly as many elements as B. If A had too few elements, then some elements of B would remain untargeted, ruling out surjectivity. If A had too many elements, then some collapsing would have to occur, ruling out injectivity.

This has been an imprecise discussion of some ideas that you can keep in mind for what is to come.

Definition 114 (Cardinality):
(1) $A \approx B \Leftrightarrow (\exists f \mathbin{!} f : A \to B \ \wedge \ f$ is a bijection onto $B)$.
(2) $A \preceq B \Leftrightarrow (\exists f \mathbin{!} f : A \to B \ \wedge \ f$ is injective$)$.
(3) $A \prec B \Leftrightarrow (A \preceq B \ \wedge \ \neg(A \approx B))$.

When $A \approx B$, we say that A and B *have the same cardinality*. As suggsted by the informal discussion above, we can think of "$A \approx B$" as saying that A and B have "the same number of elements." However, notice that there is no mention of $\mathbb{N}$ or its elements in the definition of "$A \approx B$". It is interesting that "having the same number of elements" can be defined without any reference to "number."

Theorem 115 :
(1) $A \approx A$ (reflexivity for $\approx$)
(2) If $A \approx B$ then $B \approx A$. (symmetry for $\approx$)
(3) If $A \approx B$ and $B \approx C$, then $A \approx C$. (transitivity for $\approx$)

Proof: Proving (1) and (3) is **Exercise 137**. We prove (2) here.

Assume that $A \approx B$. Get a bijection $f : A \to B$. By Theorem 75, the inverse $f^{\dashv} : B \to A$ is bijective. Therefore $B \approx A$. ■

Theorem 116 :
(1) $A \preceq A$ (reflexivity for $\preceq$)
(2) If $A \preceq B$ and $B \preceq C$, then $A \preceq C$. (transitivity for $\preceq$)

Proof: **Exercise 138**. ■

In the informal discussion at the beginning of this section, it is suggested that "$A \preceq B$" is a way of saying that B has at least as many elements as A. If B has at least as many elements as A, and A has at least as many elements as B, then one would expect that A and B must have the same amount of elements. This turns out to be correct, but it is not so easy to prove. This is the content of the next two theorems.

Theorem 117 (Preliminary to Cantor-Schroeder-Bernstein): If $C \subseteq A$ and $A \preceq C$, then $A \approx C$.

Proof: Assume that $C \subseteq A$ and $A \preceq C$. Get an injection $f : A \to C$. Let $S : \mathbb{N} \to \mathcal{P}(A)$ be the unique function that satisfies $S(0) = A \setminus C$ and $S(n+1) = f[S(n)]$ for all $n \in \mathbb{N}$. Define

$$D = \{\, d \mid (\exists n \mid n \in \mathbb{N} \ \wedge \ d \in S(n)) \,\}.$$

Define

$$g = \{\, (a, f(a)) \mid a \in D \,\} \ \cup \ \mathrm{id}_{A \setminus D}.$$

We claim that $g : A \to C$ and g is a bijection onto C. Our claims are:

(1) g is a function.

(2) $\mathrm{dom}(g) = A$.

(3) $\mathrm{ran}(g) = C$.

(4) g is injective.

Once we prove these claims, we can conclude that $A \approx C$ and the theorem is proven. We will establish a couple of useful facts along the way:

(5) $f[D] \subseteq D$.

(6) For all $a \in A$, we have $g(a) = f(a)$ if $a \in D$ and we have $g(a) = a$ if $a \notin D$.

Proof of Claim (5): Consider any $d \in D$; we must show that $f(d) \in D$. Get $n \in \mathbb{N}$ such that $d \in S(n)$. Then $f(d) \in f[S(n)] = S(n+1)$. Therefore $f(d) \in D$.

Proof of Claim (1): Since $\{\, (a, f(a)) \mid a \in D \,\}$ is a subset of f, it is a function (see Exercise 70). Observe that $\mathrm{dom}(\{\, (a, f(a)) \mid a \in D \,\}) = D$ and $\mathrm{dom}(\mathrm{id}_{A \setminus D}) = A \setminus D$ have empty intersection. Since g is the union of the two functions $\{\, (a, f(a)) \mid a \in D \,\}$ and $\mathrm{id}_{A \setminus D}$, and since the intersection of their domains is empty, it follows from Theorem 56 that g is a function.

Proof of Claim (2): Applying Exercise 66,

$$\mathrm{dom}(g) \ = \ \mathrm{dom}(\{\, (a, f(a)) \mid a \in D \,\}) \ \cup \ \mathrm{dom}(\mathrm{id}_{A \setminus D}) \ = \ D \cup (A \setminus D) \ = \ A.$$

Proof of Claim (6): Consider any $a \in A$. We will apply Theorem 51. If $a \in D$, then $(a, f(a)) \in \{ (a, f(a)) \mid a \in D \} \subseteq g$, so $f(a) = g(a)$. If $a \notin D$, then $(a, a) \in \mathrm{id}_{A \setminus D} \subseteq g$, so $a = g(a)$.

Proof of Claim (3): $\subseteq$: Consider any $z \in \mathrm{ran}(g)$. Get $x \in A$ such that $z = g(x)$. Either $x \in D$ or $x \notin D$.

Case 1: Suppose that $x \in D$. Then $z = g(x) = f(x) \in \mathrm{ran}(f) \subseteq C$.

Case 2: Suppose that $x \notin D$. Then $z = g(x) = x \in A \setminus D$. If we had $z \notin C$, then we would have $z \in A \setminus C = S(0) \subseteq D$. So it must be that $z \in C$.

In both cases we have shown that $z \in C$, so this proves that $\mathrm{ran}(g) \subseteq C$.

$\supseteq$: Now consider any $z \in C$. Either $z \in D$ or $z \notin D$.

Case 1: Suppose that $z \notin D$. Then $z \in A \setminus D$, and so we have $z = g(z) \in \mathrm{ran}(g)$.

Case 2: Suppose that $z \in D$. Get $n \in \mathbb{N}$ such that $z \in S(n)$. It cannot be that $n = 0$, for then we would have $z \in S(0) = A \setminus C$, which contradicts the assumption $z \in C$. Therefore we can get $m \in \mathbb{N}$ such that $n = m + 1$ (Theorem 98). Then $z \in S(m+1) = f[S(m)]$, so we can get a $d \in S(m)$ such that $z = f(d)$. Since $d \in D$, we have $g(d) = f(d) = z$.

In both cases we have shown that $z \in \mathrm{ran}(g)$, so this proves the claim.

Proof of Claim (4): Consider any $a, b \in A$ such that $g(a) = g(b)$. We will show that $a = b$. We consider four cases based on whether $a \in D$ and whether $b \in D$.

Case 1: Suppose that $a, b \in D$. Then $f(a) = g(a) = g(b) = f(b)$, so it follows that $a = b$ due to the injectivity of f.

Case 2: Suppose that $a, b \notin D$. Then $a = g(a) = g(b) = b$.

Case 3: Suppose that $a \in D$ and $b \notin D$. Then $g(a) = f(a)$ and $g(b) = b$, so we have $f(a) = b$. But this contradicts that $f[D] \subseteq D$, for we have $a \in D$ and $f(a) = b \notin D$. It turns out that Case 3 is not possible.

Case 4: Suppose that $b \in D$ and $a \notin D$. This is Case 3 with a and b swapped. Using the same argument, we see that Case 4 is not possible. ■

Theorem 118 (Cantor-Schroeder-Bernstein, AKA Antisymmetry for $\preceq$):
If $A \preceq B$ and $B \preceq A$, then $A \approx B$.

Proof: Assume that $A \preceq B$ and $B \preceq A$. Get an injection $f : A \to B$ and an injection $g : B \to A$. Define $C = \mathrm{ran}(g)$. Observe that $g : B \to C$ is a bijection onto C. Therefore we

have $B \approx C$.

Consider the composite $g \circ f : A \to A$. By Theorem 78, the composite $g \circ f$ is injective since f and g are injective. Since $\text{ran}(g \circ f) \subseteq \text{ran}(g) = C$, we actually have $g \circ f : A \to C$. That is, we have an injection from A into a subset C of A. Theorem 117 then applies and we conclude that $A \approx C$.

Since also $B \approx C$, we can apply symmetry and transitivity for $\approx$ to conclude that $A \approx B$. ■

Exercise 139: Prove that if $A \subseteq B$, then $A \preceq B$.

Exercise 140: Prove that if $A \approx B$ and $C \approx D$, then $A \times C \approx B \times D$.

Theorem 119: If $A \preceq B$, then there exists a surjection $g : B \to A$.

Proof: Assume that $A \preceq B$. Get an injection $f : A \to B$. By Exercise 97, we can get a function $g : B \to A$ such that $g \circ f = \text{id}_A$. It follows that $g \circ f$ is surjective, and so by Theorem 78 we conclude that g is surjective. ■

Exercise 141: Accepting Axiom 82 just for this exercise, prove that if $f : A \to B$ is surjective onto B, then $B \preceq A$.

3.13 Finite Sets

We next investigate finite sets. It may be useful to be aware of the elements of $0, 1, 2, \ldots$ based on Definition 90:

$0 = \{\}$
$1 = \text{next}(0) = 0 \cup \{0\} = \{\} \cup \{0\} = \{0\}$
$2 = \text{next}(1) = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$
$3 = \text{next}(2) = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$
$\ldots$

Definition 120 (Finiteness):
(1) We say that A *has* n *elements* iff $n \in \mathbb{N}$ and $A \approx n$.
(2) A set is *finite* iff it has n elements for some $n \in \mathbb{N}$.
(3) A set is *infinite* iff it is not finite.

Exercise 142: Prove that a set is empty if and only if it has 0 elements.

Exercise 143: Prove that a set is a singleton if and only if it has 1 element.

Exercise 144: Prove that if $\{x, y\}$ has 2 elements, then $x \neq y$.

In some of the proofs to come, it is useful to be able to quickly get bijections that swap elements:

Theorem 121 (Element Swap): If $p, q \in A$, then there is a bijection $f : A \to A$ such that $f(p) = q$ and $f(q) = p$.

Proof: **Exercise 145**. Hint: Prove that $(\mathrm{id}_A \setminus \{(p,p),(q,q)\}) \cup \{(p,q),(q,p)\}$ works. ■

Theorem 122 ($\preceq$ and $\leq$): If $n, m \in \mathbb{N}$, then

$$n \preceq m \;\Leftrightarrow\; n \leq m.$$

Proof: Assume that $n, m \in \mathbb{N}$.

$\Leftarrow$: Assume that $n \leq m$. Then whenever $k < n$, it follows that $k < m$. In other words, $n \subseteq m$. Therefore $n \preceq m$, by Exercise 139.

$\Rightarrow$: We will prove by induction on m that

$$(\,\forall n \,\mathbin{!}\, n \in \mathbb{N} \;\Rightarrow\; (n \preceq m \Rightarrow n \leq m)\,),$$

for all $m \in \mathbb{N}$.

Base Case: Consider any $n \in \mathbb{N}$ such that $n \preceq 0$. Get an injection $f : n \to 0$. We have $f \subseteq n \times \{\} = \{\}$, so $f = \{\}$. Therefore $n = \mathrm{dom}(f) = \{\} = 0$, and so $n \leq m$.

Induction Step: Suppose that $m \in \mathbb{N}$ and $(\,\forall n \,\mathbin{!}\, n \in \mathbb{N} \;\Rightarrow\; (n \preceq m \Rightarrow n \leq m)\,)$. Consider any $n \in \mathbb{N}$ such that $n \preceq m + 1$. Get an injection $f : n \to (m+1)$. Either $m \in \mathrm{ran}(f)$ or $m \notin \mathrm{ran}(f)$.

Case 1: Suppose that $m \notin \mathrm{ran}(f)$. Then $f : n \to m$, so $n \preceq m$. By the induction hypothesis, it follows that $n \leq m$. Therefore we also have $n \leq m + 1$.

Case 2: Suppose that $m \in \mathrm{ran}(f)$. Let k be the unique element of n such that $f(k) = m$. Since $k < n$, we know that $0 < n$, so we can get $s \in \mathbb{N}$ such that $n = s + 1$. Using Theorem 121, get a bijection $g : n \to n$ such that $g(s) = k$ and $g(k) = s$. Define $h = f \circ g$. Then we have that h is injective, $h : n \to m + 1$, and $h(s) = f(g(s)) = f(k) = m$. Define $j = h \setminus \{(s, m)\}$. Then j is injective (see Exercise 76), and $j : (n \setminus \{s\}) \to ((m+1) \setminus \{m\})$ (see Exercise 73). Therefore we have $j : s \to m$ (see Exercise 122). Since we have found an injection from s to m, we have $s \preceq m$. We may apply the induction hypothesis to s to conclude that $s \leq m$. It follows that $s + 1 \leq m + 1$. That is, $n \leq m + 1$. ■

Theorem 123 ($\approx$ and $=$ for Natural Numbers): If $n, m \in \mathbb{N}$, then

$$n \approx m \;\Leftrightarrow\; n = m.$$

Proof: The implication "$\Leftarrow$" is just Axiom 2 and Theorem 115. For "$\Rightarrow$", assume that $n \approx m$. Then $m \approx n$ (Theorem 115 again), and so we have both $n \preceq m$ and $m \preceq n$. Applying Theorem 122 to both of these, we get $n \leq m$ and $m \leq n$. It follows that $n = m$ (see Exercise 119). ■

Exercise 146: Prove that if X has n elements, Y has m elements, and $X \preceq Y$, then $n \leq m$.

Exercise 147: Assume that X has n elements, Y has m elements, and $m < n$. Prove that it is impossible for $f : X \to Y$ to be injective. This result is called "The Pigeonhole Principle."

The next two theorems are special cases of Axiom 82. Proofs are immediate if one chooses to accept Axiom 82. We do not officially accept Axiom 82 in these notes, and so we provide proofs.

Theorem 124 (Finite Choice - Preliminary Version): If $n \in \mathbb{N}$ and $f : A \to n$ surjectively, then there exists $g : n \to A$ such that $f \circ g = \mathrm{id}_n$.

Proof: We will prove that

$$(\,\forall A, f \restriction (f : A \to n \text{ surjectively}) \;\Rightarrow\; (\,\exists g \restriction (g : n \to A) \;\wedge\; (f \circ g = \mathrm{id}_n)\,)\,)$$

for all $n \in \mathbb{N}$, by doing induction on n.

Base Case: Consider any A and f such that $f : A \to 0$ surjectively. Then we have $f \subseteq A \times \{\} = \{\}$, so $f = \{\}$. Therefore $A = \mathrm{dom}(f) = \{\}$. Define $g = \{\}$. Then $g : 0 \to A$, and $f \circ g = \{\} = \mathrm{id}_{\{\}} = \mathrm{id}_0$.

Induction Step: Suppose that $n \in \mathbb{N}$ and that, for all A, f such that $f : A \to n$ surjectively, there exists $g : n \to A$ such that $f \circ g = \mathrm{id}_n$. Now consider any A and f such that $f : A \to (n+1)$ surjectively. Define $N = f^{\dashv}[\{n\}]$, and define $f' = \{\,(a, f(a)) \restriction a \in A \setminus N\,\}$. Then we have $f' : A \setminus N \to (n+1)$ (see Exercise 71). We claim that $\mathrm{ran}(f') = n$.

$\subseteq$: To see that $\mathrm{ran}(f') \subseteq n$, consider any $k \in \mathrm{ran}(f')$. Then $k \in (n+1)$. To show that $k \in n$, we only need to show that $k \neq n$. Get $a \in A \setminus N$ such that $f'(a) = k$. Since $f' \subseteq f$, we also have $f(a) = f'(a) = k$. If we had $k = n$, then we would have $a \in f^{\dashv}[\{n\}] = N$. Therefore $k \neq n$.

$\supseteq$: To see that $n \subseteq \mathrm{ran}(f')$, consider any $k \in n$. Then $k \in (n+1)$, so by the surjectivity

of f we can get some $a \in A$ such that $f(a) = k$. If we had $a \in N$, then we would have $k = f(a) = n$, and this would lead to the impossible situation $n \in n$. Therefore $a \in A \setminus N = \text{dom}(f')$. Since $f' \subseteq f$, we then have $f'(a) = f(a) = k$. Therefore $k \in \text{ran}(f')$.

Now we've established that $\text{ran}(f') = n$, so we have that $f' : A \setminus N \to n$ and that f' is surjective onto n. Our induction hypothesis allows us to get $g : n \to A \setminus N$ such that $f' \circ g = \text{id}_n$. Our remaining task is to construct a function $g' : (n+1) \to A$ such that $f \circ g' = \text{id}_{n+1}$. Since f is surjective, the set N is nonempty (see Exercise 107), and so we can get a_0 such that $a_0 \in N$. Define

$$g' = g \cup \{(n, a_0)\}.$$

We now claim that $g' : (n+1) \to A$ and that $f \circ g' = \text{id}_{n+1}$. Once this is established, the induction step will be complete and the theorem will be proven.

To see that g' is a function, we will use Theorem 56. It is clear that $\{(n, a_0)\}$ is a function. The intersection of $\text{dom}(g) = n$ and $\text{dom}(\{(n, a_0)\}) = \{n\}$ is empty by Theorem 102. By Theorem 56, we conclude that g' is a function.

To see that $\text{dom}(g') = n + 1$, we apply Exercise 66:

$$\text{dom}(g') = \text{dom}(g \cup \{(n, a_0)\}) = \text{dom}(g) \cup \text{dom}(\{(n, a_0)\}) = n \cup \{n\} = n + 1.$$

To see that $\text{ran}(g') \subseteq A$, consider any $a \in \text{ran}(g')$. Get $k \in (n+1)$ such that $g'(k) = a$. Then either $k = n$ or $k \in n$. In the case that $k = n$, we have $g'(k) = a_0 \in N \subseteq A$. In the case that $k \in n$, we have $g'(k) = g(k) \in \text{ran}(g) \subseteq A \setminus N \subseteq A$. In both cases, we ended up with $g'(k) \in A$. In other words, $a \in A$.

Finally, to see that $f \circ g' = \text{id}_{n+1}$ we consider any $k \in (n+1)$. Then either $k = n$ or $k \in n$.

Case 1: Suppose that $k = n$. Then we have

$$(f \circ g')(k) = (f \circ g')(n) = f(g'(n)) = f(a_0) = n = k.$$

Case 2: Suppose that $k \in n$. Since $g \subseteq g'$ and $k \in \text{dom}(g)$, we have $g(k) = g'(k)$. Since $k \in \text{dom}(g)$, we have $g(k) \in \text{ran}(g) = A \setminus N = \text{dom}(f')$. Since $f' \subseteq f$ and $g(k) \in \text{dom}(f')$, we have $f'(g(k)) = f(g(k))$. Putting these together, we have

$$(f \circ g')(k) = f(g'(k)) = f(g(k)) = f'(g(k)) = (f' \circ g)(k) = \text{id}_n(k) = k.$$

In both cases we ended up with

$$(f \circ g')(k) = k = \text{id}_{n+1}(k),$$

so by Theorem 53 we conclude that $f \circ g' = \text{id}_{n+1}$. ■

Theorem 125 (Finite Choice): If X is finite and $f : A \to X$ surjectively, then there exists $g : X \to A$ such that $f \circ g = \mathrm{id}_X$.

Proof: Assume that X is finite and $f : A \to X$ surjectively. Get $n \in \mathbb{N}$ such that $X \approx \mathbb{N}$. Get a bijection $h : X \to n$. Then $h \circ f : A \to n$, and $h \circ f$ is surjective by Theorem 78. Therefore we can apply Theorem 124 to get some $j : n \to A$ such that $(h \circ f) \circ j = \mathrm{id}_n$. Composing with h^{-1} on the left and h on the right completes the proof; here are the details:

$$\begin{array}{rcll} \mathrm{id}_X & = & h^{-1} \circ h & \text{(Theorem 77)} \\ & = & (h^{-1} \circ \mathrm{id}_n) \circ h & \text{(Theorem 65)} \\ & = & (h^{-1} \circ ((h \circ f) \circ j)) \circ h & \\ & = & (h^{-1} \circ h) \circ (f \circ (j \circ h)) & \text{(Theorem 61)} \\ & = & \mathrm{id}_X \circ (f \circ (j \circ h)) & \text{(Theorem 77)} \\ & = & f \circ (j \circ h) & \text{(Theorem 65).} \end{array}$$

We have found a function $j \circ h : X \to A$ such that $f \circ (j \circ h) = \mathrm{id}_X$. ■

Compare the following theorem to Exercise 141.

Theorem 126 : If X is finite and $f : A \to X$ surjectively, then $X \preceq A$.

Proof: Assume that X is finite and $f : A \to X$ surjectively. By Theorem 125, we can get $g : X \to A$ such that $f \circ g = \mathrm{id}_X$. By Theorem 78, the function g must be injective. ■

Exercise 148: Prove that if $n, m \in \mathbb{N}$ and there is a surjection $f : m \to n$, then $n \leq m$.

Theorem 127 (Adding One Element):
(1) If X has n elements and $a \notin X$, then $X \cup \{a\}$ has $n + 1$ elements.
(2) If X is finite, then $X \cup \{a\}$ is finite.

Proof: Assume that X has n elements and $a \notin X$. Get a bijection $f : X \to n$. Define $f' = f \cup \{(a, n)\}$.

Exercise 149: Prove that $f' : X \cup \{a\} \to (n + 1)$ and f' is bijective.

Exercise 150: Use (1) to prove (2). ■

Theorem 128 (Subsets Inherit Finiteness - Preliminary Version):
If $n \in \mathbb{N}$ and $S \subseteq n$, then S is finite.

Proof: We will prove "Every subset of n is finite" for all $n \in \mathbb{N}$ by doing induction on n.

Base Case: Consider any subset S of 0. Then $S = \{\}$, so $S \approx 0$.

Induction Step: Suppose that $n \in \mathbb{N}$, and that all subsets of n are finite. Consider any subset S of $n+1$. Either $n \in S$ or $n \notin S$.

Case 1: Suppose that $n \notin S$. Then $S \subseteq (n+1) \setminus \{n\} = n$. The induction hypothesis then ensures that S is finite.

Case 2: Suppose that $n \in S$. Define $T = S \setminus \{n\}$. Then $T \subseteq (n+1) \setminus \{n\} = n$, so the induction hypothesis ensures that T is finite. It follows that $T \cup \{n\}$ is finite, by Theorem 127. Since $T \cup \{n\} = (S \setminus \{n\}) \cup \{n\} = S$ (see Exercise 51 part 5), we have shown that S is finite. ■

Theorem 129 (Images Inherit Finiteness): If $f : A \to B$, $X \subseteq A$, and X is finite, then $f[X]$ is finite.

Proof: Assume that $f : A \to B$, $X \subseteq A$, and X is finite. Get $n \in \mathbb{N}$ such that $X \approx n$. Then $n \approx X$, so get a bijection $g : n \to X$. We will argue that $f \circ g : n \to f[X]$ and that $f \circ g$ is a bijection onto $f[X]$. This will prove that $n \approx f[X]$ and finish the proof of the theorem.

Since $X \subseteq A$, we do have $g : n \to A$, so $f \circ g : n \to B$. Since f and g are injective, we know that $f \circ g$ is injective.

Exercise 151: Prove that $\text{ran}(f \circ g) = f[X]$. ■

Theorem 130 (Subsets Inherit Finiteness): If X is finite and $S \subseteq X$, then S is finite.

Proof: Assume that X is finite and $S \subseteq X$. Get $n \in \mathbb{N}$ such that $X \approx n$. Get a bijection $f : X \to n$. Then $f[S] \subseteq n$, so $f[S]$ is finite by Theorem 128. By Theorem 87, we have $S = f^{-1}[f[S]]$. Since f^{-1} is a function and $f[S]$ is finite, it follows from Theorem 129 that $f^{-1}[f[S]]$ is finite. Therefore S is finite. ■

Exercise 152: Here is an idea for a simpler way to prove Theorem 130:

> Assume that X is finite and $S \subseteq X$. Then $S \preceq X$ by Exercise 139. So by Exercise 146, the set S must have fewer elements than the finite set X. Therefore S is finite.

Why doesn't this approach work?

Theorem 131 ($\cup$ and $+$): If the set X has n elements, the set Y has m elements, and $X \cap Y = \{\}$, then $X \cup Y$ has $n + m$ elements.

Proof: **Exercise 153** (Challenging). Hint: Use induction and Theorem 127. Be precise about exactly what it is that you are proving by induction. ■

Theorem 132: Assume that $n \in \mathbb{N}$ and $f : n \to n$. If f is injective, then f is surjective onto n.

Proof: Assume that $n \in \mathbb{N}$ and $f : n \to n$, and assume that f is injective. Suppose, for the sake of contradiction, that f is not surjective. Get $k \in n \setminus \text{ran}(f)$. Then n is nonempty, so $n = m + 1$ for some $m \in \mathbb{N}$ (Theorem 98). Using Theorem 121, get a bijection $g : n \to n$ such that $g(k) = m$ and $g(m) = k$. Then $g \circ f : n \to n$ and $g \circ f$ is injective. We will show that $\text{ran}(g \circ f) \subseteq m$.

Consider any $z \in \text{ran}(g \circ f)$. We already have $z \in n = m + 1$, so we just need to show that $z \neq m$ in order to conclude that $z \in m$. Get $\ell \in n$ such that $z = (g \circ f)(\ell) = g(f(\ell))$. Suppose, for the sake of contradicition, that $z = m$. Then $m = g(f(\ell))$ and $m = g(k)$, so since g is injective it follows that $f(\ell) = k$. But $k \notin \text{ran}(f)$, so we have reached a contradiction. Therefore z cannot be m, and we may conclude that $z \in m$.

We have now shown that $\text{ran}(g \circ f) \subseteq m$, so we have an injection $g \circ f : n \to m$. Therefore we have $n \preceq m$, and by Theorem 122 it follows that $n \leq m$. But $n = m + 1$, so we have reached a contradiction. Therfore f must be surjective. ■

Exercise 154: Prove that if X has $n + 1$ elements and $x \in X$, then $X \setminus \{x\}$ has n elements.

Exercise 155: (Challenging) In this exercise you will prove that every nonempty finite subset of $\mathbb{N}$ has a maximum. Here are the relevant definitions:

- If $A \subseteq \mathbb{N}$ and $n \in \mathbb{N}$, then n is an *upper bound* for A iff $(\forall k \restriction k \in A \Rightarrow k \leq n)$.
- If $A \subseteq \mathbb{N}$ and $n \in \mathbb{N}$, then n is a *maximum* for A iff $n \in A$ and n is an upper bound for A.

1. Prove that if a subset of $\mathbb{N}$ has a maximum, then the maximum is unique.
2. Prove that every finite subset of $\mathbb{N}$ has an upper bound. Hint: Use induction to prove that
$$(\forall A \restriction (A \subseteq \mathbb{N} \wedge A \approx n) \Rightarrow A \text{ has an upper bound})$$
for all $n \in \mathbb{N}$.
3. Assume that A is a nonempty finite subset of $\mathbb{N}$. Let
$$U = \{ n \restriction n \in \mathbb{N} \text{ and } n \text{ is an upper bound for } A \}.$$

Use well-ordering (Theorem 106) to argue that U has a minimum, and then prove that this minimum ends up being a maximum for A.

3.14 Infinite Sets

Theorem 133 (Infinitude of $\mathbb{N}$): $\mathbb{N}$ is infinite.

Proof: Suppose, for the sake of contradiciton, that $\mathbb{N}$ is finite. Get $n \in \mathbb{N}$ such that $\mathbb{N}$ has n elements. Since $n+1 \subseteq \mathbb{N}$, we have $n+1 \preceq \mathbb{N}$ (see Exercise 139). Since $n+1$ has $n+1$ elements, and $\mathbb{N}$ has n elements, it follows that $n+1 \leq n$ (see Exercise 146). This is a contradiction. Therefore $\mathbb{N}$ must be infinite. ■

Exercise 156: Theorem 129 does not work when "image" is replaced by "preimage." Give an example of A, B, f, and Y such that $f : A \to B$, $Y \subseteq B$, Y is finite, and $f^{\dashv}[Y]$ is infinite.

Definition 134 (Countability): A set A is said to be *countably infinite* iff $A \approx \mathbb{N}$.

We have now seen that two types of cardinalities can occur: finite cardinality, where a set has the same cardinality as n for some $n \in \mathbb{N}$, and infinite cardinality, where a set does not have the same cardinality as any $n \in \mathbb{N}$. There are many possible finite cardinalities: those of 0, 1, 2, etc. These are all distinct cardinalities, by Theorem 123. Is there just one infinite cardinality, or are there also many infinite cardinalities? If A and B are infinite sets, then do we necessarily have $A \approx B$? Or could we actually have $A \prec B$ with A and B being infinite sets?

Let us start with the countably infinite set $\mathbb{N}$ and attempt to build up a set with "greater" cardinality. Drawing inspiration from Theorem 127, the first thing we might try is to add one element to $\mathbb{N}$. This turns out not to affect the cardinality!

Theorem 135 (Hilbert's Hotel): $\text{next}(\mathbb{N}) \approx \mathbb{N}$.

Proof: Define $f = \ddagger \cup \{(\mathbb{N}, 0)\}$. (The diagram following this proof is a depiction of f.) Since $\mathbb{N} \notin \mathbb{N}$ (see Exercise 116), we may apply Theorem 56 to conclude that f is a function. We have

$$\text{dom}(f) = \text{dom}(\ddagger) \cup \{\mathbb{N}\} = \mathbb{N} \cup \{\mathbb{N}\} = \text{next}(\mathbb{N}),$$

and we have

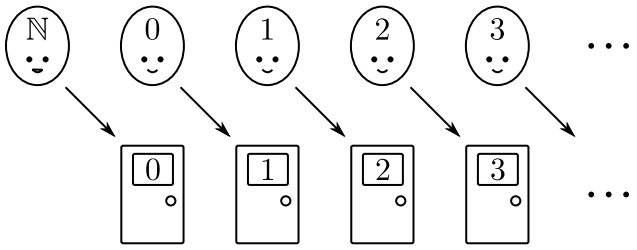
$$\text{ran}(f) = \text{ran}(\ddagger) \cup \{0\} \subseteq \mathbb{N},$$

so $f : \text{next}(\mathbb{N}) \to \mathbb{N}$. We will show that f is injective and surjective.

Suppose that $n, m \in \text{next}(\mathbb{N})$ and $f(n) = f(m)$. In the case that $n, m \in \mathbb{N}$, we have $n+1 = m+1$, so $n = m$. In the case that $n, m \in \{\mathbb{N}\}$, we obviously have $n = m$. In the

case that $n \in \mathbb{N}$ and $m = \mathbb{N}$, we have $n + 1 = 0$, which is impossible. Similarly, $n = \mathbb{N}$ and $m \in \mathbb{N}$ is impossible. Thus f is injective.

Consider any $n \in \mathbb{N}$. If $n = 0$, then $n = f(\mathbb{N})$. Otherwise, we can get $n' \in \mathbb{N}$ sich that $n = n' + 1$. Then $n = f(n')$. Thus f is surjective. ■



It follows from Theorem 135 that adding elements one-by-one to $\mathbb{N}$ is not going to yield new cardinalities. All of the sets $\mathbb{N}$, next($\mathbb{N}$), next(next(N)), etc. have the same cardinality; they are all countably infinite. The next thing one might try in order to produce a new cardinality is to "double" the set $\mathbb{N}$. We can do this by considering the set $2 \times \mathbb{N}$. This set consists of two distinct elements $(0, n)$ and $(1, n)$ for every $n \in \mathbb{N}$. The set $2 \times \mathbb{N}$ is sort of like a union of two separate copies of $\mathbb{N}$, so we might think it has "twice as many" elements. And yet, as we are about to see in Theorem 140, the cardinality has still not changed!

To help us prove this, we will introduce the concepts of even and odd numbers.

Definition 136 (Even and Odd):

(1) n is *even* iff $n = k + k$ for some $k \in \mathbb{N}$.
(2) n is *odd* iff $n = k + k + 1$ for some $k \in \mathbb{N}$.

Theorem 137 : Every natural number is either odd or even.

Proof: **Exercise 157**. Hint: Induction. ■

Theorem 138 : A natural number cannot be both odd and even.

Proof: Suppose, for the sake of contradiction, that there exists a natural number which is both odd and even. Let n be the smallest such natural number (we are using Theorem 106). Get $\ell, k \in \mathbb{N}$ such that $n = \ell + \ell + 1$ and $n = k + k$. Since $n = (\ell + \ell) + 1$, we cannot have $n = 0$. Since $n = k + k$ and $n \neq 0$, it must be that $k \neq 0$. Get $k' \in \mathbb{N}$ such that $k = k' + 1$. Then

$$k' + k' + 1 + 1 = (k' + 1) + (k' + 1) = k + k = n = \ell + \ell + 1,$$

so $k' + k' + 1 = \ell + \ell$. We see that $\ell + \ell$ is odd and even, and yet $\ell + \ell < \ell + \ell + 1 = n$. This contradicts the fact that n was the smallest odd-and-even natural number. ■

Theorem 139 : If $k, \ell \in \mathbb{N}$ and $k + k = \ell + \ell$ then $k = \ell$.

Proof: Assume that $k, \ell \in \mathbb{N}$ and $k + k = \ell + \ell$. If $k < \ell$, then

$$k + k < \ell + k < \ell + \ell$$

by Theorem 113, so we cannot have $k < \ell$. Similarly, we cannot have $\ell < k$. Thus $k = \ell$. ■

Theorem 140 (Doubling Countable Infinity): $2 \times \mathbb{N} \approx \mathbb{N}$.

Proof: Define

$$f = \{\, ((0, n), n + n) \mid n \in \mathbb{N} \,\} \cup \{\, ((1, n), n + n + 1) \mid n \in \mathbb{N} \,\}.$$

With the help of Theorem 56, it is straightforward to show that $f : 2 \times \mathbb{N} \to \mathbb{N}$. The diagram following this proof is a depiction of f.

To prove that f is injective, assume that $(i, n), (i', n') \in 2 \times \mathbb{N}$ and $f((i, n)) = f((i', n'))$. We cannot have $i = 0$ and $i' = 1$, for then we would have $n + n = n' + n' + 1$, and this contadicts Theorem 138. Similarly, we cannot have $i = 1$ and $i' = 0$. This leaves two cases.

Case 1: Suppose that $i = i' = 0$. Then $n + n = n' + n'$, so $n = n'$ by Theorem 139. Thus $(i, n) = (i', n')$.

Case 2: Suppose that $i = i' = 1$. Then $n + n + 1 = n' + n' + 1$, so $n + n = n' + n'$. It follows from Theorem 139 that $n = n'$. Thus $(i, n) = (i', n')$.

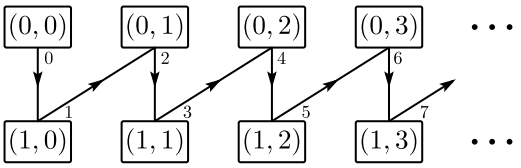
Since we get $(i, n) = (i', n')$ in all cases, we conclude that f is injective.

To prove that f is surjective, consider any $k \in \mathbb{N}$. By Theorem 137, k is either odd or even.

Case 1: Suppose that k is odd. Get $n \in \mathbb{N}$ such that $k = n + n + 1$. Then $k = f((1, n))$, so $k \in \text{ran}(f)$.

Case 2: Suppose that k is even. Get $n \in \mathbb{N}$ such that $k = n + n$. Then $k = f((0, n))$, so $k \in \text{ran}(f)$.

Since we get $k \in \text{ran}(f)$ either way, we conclude that f is surjective onto $\mathbb{N}$. Therefore f is a bijection, and we have shown that $2 \times \mathbb{N} \approx \mathbb{N}$. ■



So apparently mushing together two copies of $\mathbb{N}$ still leaves us with the same "amount" of elements– only countably infinitely many. Okay, what if we mush together *countably infinitely* many copies of the countably infinite set $\mathbb{N}$? What if instead of $2 \times \mathbb{N}$ we consider $\mathbb{N} \times \mathbb{N}$? This contains an entire copy of $\mathbb{N}$ for each element of $\mathbb{N}$! And yet, as we are about to see, it is still only countably infinite!

Theorem 141 (Squaring Countable Infinity): $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

Proof: We will start by constructing a useful function $a : \mathbb{N} \to \mathbb{N}$, and then we will construct a bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

First, define $r : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ by

$$r((k, n)) = (k + (n + 1), n + 1)$$

for all $k, n \in \mathbb{N}$. Let $a' : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be the unique function that satisfies

$$\begin{array}{ll} a'(0) = (0, 0) & \text{and} \\ a'(n + 1) = r(a'(n)) & \text{for all } n \in \mathbb{N}. \end{array}$$

Define $a = \{\, (n, k) \mid (n, (k, n)) \in a' \,\}$.

To see that a is a function, suppose that $(n, k), (n, k') \in a$. Then $(n, (k, n)), (n', (k', n)) \in a'$. Since a' is a function, we have $(k, n) = (k', n)$. It follows that $k = k'$. Thus a is a function.

Notice the following about a:

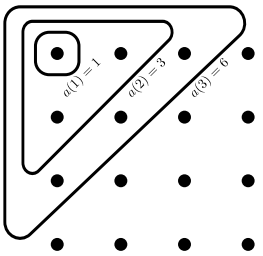
Fact 1: $(0, 0) \in a$. This is because $(0, (0, 0)) \in a'$.
Fact 2: For any $n \in \mathbb{N}$ and any k, if $(n, k) \in a$, then $(n + 1, k + (n + 1)) \in a$. This is because for any $n \in \mathbb{N}$ and any k we have

$$(n, (k, n)) \in a' \Rightarrow (n + 1, (k + (n + 1), n + 1)) = (n + 1, r((k, n))) \in a'.$$

One consequence of Fact 1 is that $0 \in \text{dom}(a)$. One consequence of Fact 2 is that for any $n \in \mathbb{N}$, if $n \in \text{dom}(a)$ then $n + 1 \in \text{dom}(a)$. It follows by induction that $\mathbb{N} \subseteq \text{dom}(a)$. It is clear from the definition of a that $\text{dom}(a) \subseteq \mathbb{N}$ and that $\text{ran}(a) \subseteq \mathbb{N}$, so we now have $a : \mathbb{N} \to \mathbb{N}$. We may now express Facts 1 and 2 as follows:

Fact 1: $a(0) = 0$.
Fact 2: For all $n \in \mathbb{N}$, we have $a(n + 1) = a(n) + (n + 1)$.

The idea is that a counts the number of dots in these triangular portions of a dot grid:



We will need one more useful fact about a before we construct our bijection:

Fact 3: For $n, n' \in \mathbb{N}$, if $n < n'$ then $a(n) + n < a(n')$.

To prove this, we fix $n \in \mathbb{N}$ and do induction on n'. The base case, $n' = 0$, is vacuous. Suppose, for the induction step, that $n' \in \mathbb{N}$ and $n < n' \Rightarrow a(n) + n < a(n')$. Assume that $n < n' + 1$. We must prove that $a(n) + n < a(n' + 1)$. We have $n \leq n'$, so we may proceed by cases as follows.

Case 1: Suppose that $n = n'$. Then

$$a(n) + n < a(n) + (n + 1) = a(n + 1) = a(n' + 1).$$

Case 2: Suppose that $n < n'$. Then we have $a(n) + n < a(n')$ by the induction hypothesis, so

$$a(n) + n < a(n') < a(n') + (n' + 1) = a(n' + 1).$$

We completed the induction step in both cases, so Fact 3 is proven.

Finally, we construct our bijection for the sake of proving $\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$. Define

$$\begin{aligned} f &= \{\, (a(n) + i, (i, j)) \mid i, j, n \in \mathbb{N} \ \wedge \ i + j = n \,\} \\ &= \{\, p \mid (\, \exists i, j, n \mid p = (a(n) + i, (i, j)) \ \wedge \ i, j, n \in \mathbb{N} \ \wedge \ i + j = n \,) \,\}. \end{aligned}$$

The diagram following this proof is a depiction of f. It is clear that $f \subseteq \mathbb{N} \times (\mathbb{N} \times \mathbb{N})$, so we are left needing to prove four things:

that f is a function,
that $\mathbb{N} \subseteq \text{dom}(f)$,
that f is injective,
and that f is surjective onto $\mathbb{N} \times \mathbb{N}$.

To prove that f is a function, consider any $(x, y), (x, y') \in f$. Get $i, j, n \in \mathbb{N}$ such that $i + j = n$ and $(x, y) = (a(n) + i, (i, j))$. Get $i', j', n' \in \mathbb{N}$ such that $i' + j' = n'$ and $(x, y') = (a(n') + i', (i', j'))$. Then $a(n) + i = x = a(n') + i'$. Now if we had $n < n'$, then it

would follow from Fact 3 above that $a(n) + n < a(n')$. But since $i \leq i + j = n$, this would lead to

$$a(n) + i \leq a(n) + n < a(n') \leq a(n') + i',$$

so it cannot be that $n < n'$. By a similar argument, it cannot be that $n' < n$. Therefore we must have $n = n'$. We then get $i = i'$ from

$$a(n) + i = a(n') + i' = a(n) + i'.$$

And finally we get $j = j'$ from

$$i + j = n = n' = i' + j' = i + j'.$$

Therefore $y = (i, j) = (i', j') = y'$, and we have proven that f is a function.

To prove that $\mathbb{N} \subseteq \text{dom}(f)$, we will use induction. Since $0 = a(0) + 0$, we have $(0, (0, 0)) \in f$. Therefore $0 \in \text{dom}(f)$. For an induction step, suppose that $m \in \mathbb{N}$ and $m \in \text{dom}(f)$. Get y such that $(m, y) \in f$. Get $i, j, n \in \mathbb{N}$ such that $i + j = n$ and $(m, y) = (a(n) + i, (i, j))$. Then $m = a(n) + i$. We have $i \leq i + j = n$, so either $i < n$ or $i = n$.

Case 1: Suppose that $i < n$. Then $0 < j$, for if $j = 0$ then $i = n$. Get $j' \in \mathbb{N}$ such that $j = j' + 1$. Define $i' = i + 1$. Then

$$i' + j' = (i + 1) + j' = i + (j' + 1) = i + j = n,$$

so $(a(n) + i', (i', j')) \in f$. Thus

$$m + 1 = (a(n) + i) + 1 = a(n) + i' \in \text{dom}(f).$$

Case 2: Suppose that $i = n$. Then $m = a(n) + n$, so $m + 1 = a(n) + (n + 1) = a(n + 1)$. Define $i' = 0$ and $j' = n + 1$. Then we have $i' + j' = n + 1$, so $(a(n + 1) + i', (i', j')) \in f$. Thus

$$m + 1 = a(n + 1) = a(n + 1) + i' \in \text{dom}(f).$$

We completed the induction step in both cases, so by induction we have proven that $\mathbb{N} \subseteq \text{dom}(f)$.

We now have $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, and it remains to prove that f is bijective.

To prove that f is injective, consider any $x, x' \in \text{dom}(f)$ such that $f(x) = f(x')$. Get $i, j, n \in \mathbb{N}$ such that $i + j = n$ and $(x, f(x)) = (a(n) + i, (i, j))$. Get $i', j', n' \in \mathbb{N}$ such that $i' + j' = n'$ and $(x', f(x')) = (a(n') + i', (i', j'))$. We have $(i, j) = f(x) = f(x') = (i', j')$, so $i = i'$, $j = j'$, and

$$n = i + j = i' + j' = n'.$$

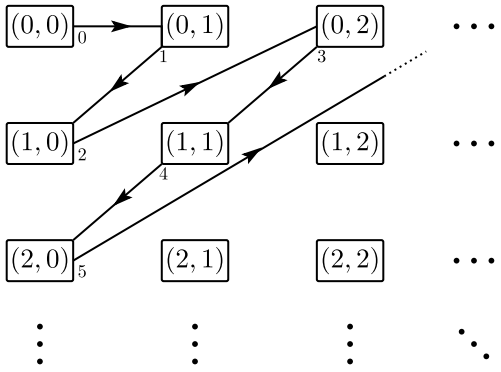
Since $i = i'$ and $n = n'$, we have

$$x = a(n) + i = a(n') + i' = x'.$$

Therefore f is injective.

To prove that f is surjective, consider any $(i, j) \in \mathbb{N} \times \mathbb{N}$. Define $n = i + j$. Then we have $f(a(n) + i) = (i, j)$, so f is surjective onto $\mathbb{N} \times \mathbb{N}$.

We have shown that there exists a bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$; we conclude that $\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$. ■



So even putting together countably infinitely many copies of a countably infinite set still does not yield a new cardinality– only another countably infinite set. It is starting to look like there is only one way for a set to be infinite, from the standpoint of cardinality. This turns out to be dead wrong, as we will see in Theorem 142!

Exercise 158: Prove that $A \preceq \mathcal{P}(A)$.

Theorem 142 (Cantor's Theorem): There does not exist a surjection $f : A \to \mathcal{P}(A)$.

Proof: Suppose for the sake of contradiction that $f : A \to \mathcal{P}(A)$ is surjective onto $\mathcal{P}(A)$. Define

$$C = \{\, a \mid a \in A \ \wedge \ a \notin f(a) \,\}.$$

Then $C \in \mathcal{P}(A)$, so since f is surjective we can get some $b \in A$ such that $f(b) = C$. Either $b \in C$ or $b \notin C$.

Case 1: Suppose that $b \in C$. Then $b \notin f(b) = C$. This a contradiction.

Case 2: Suppose that $b \notin C$. Then $b \in f(b) = C$. This is a contradiction. ■

Definition 143 (Uncountability): A set A is said to be *uncountably infinite* iff it is infinite, but it is not countably infinite.

Given Theorem 142 and Exercise 158, we see that there are many ways for a set to be infinite, from the standpoint of cardinality. We have the countably infinite set $\mathbb{N}$, and then we have

an unending ladder of uncountably infinite cardinalities beyond that:

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \prec \cdots$$

Exercise 159: (Challenging) In this exercise, you will prove that $\mathbb{N}$ is the "smallest" infinite set there is, from the standpoint of cardinality. You will prove that given any infinite set A, one has $\mathbb{N} \preceq A$. As far as I know, this requires Axiom 82, so you should accept Axiom 82 just for this exercise.

- Assume that A is an infinite set.
- Define $\mathscr{A} = \{ S \mid S \subseteq A \ \wedge \ S \neq \{\} \} = \mathcal{P}(A) \setminus \{\{\}\}$, the set of nonempty subsets of A.
- Define $\mathscr{A}^* = \{ (a, S) \mid (a, S) \in A \times \mathscr{A} \ \wedge \ a \in S \}$. Elements of $\mathscr{A}^*$ are sometimes called *pointed sets*, since they are pairs consisting of a set and a "point" in the set.
- Define $\pi_1 = \{ ((a, S), a) \mid (a, S) \in \mathscr{A}^* \}$ and $\pi_2 = \{ ((a, S), S) \mid (a, S) \in \mathscr{A}^* \}$. Then we have $\pi_1 : \mathscr{A}^* \to A$ and $\pi_2 : \mathscr{A}^* \to \mathscr{A}$. These two functions are called *projections*.

1. Prove that π_1 and π_2 are surjective.

- We may now use Axiom 82 to get some $g : \mathscr{A} \to \mathscr{A}^*$ such that $\pi_2 \circ g = \mathrm{id}_{\mathscr{A}}$.
- Define $c = \pi_1 \circ g$. Then $c : \mathscr{A} \to A$.

2. Prove that for all $S \in \mathscr{A}$, we have $c(S) \in S$. Thus the function c serves to "choose" an element of each $S \in \mathscr{A}$. This is why Axiom 82 is called the Axiom of Choice.

- Define $\mathscr{F} = \{ S \mid S \subseteq A \ \wedge \ S \text{ is finite} \}$, the set of finite subsets of A.
- The goal now is to construct $h : \mathbb{N} \to A \times \mathscr{F}$ such that

  $h(0) = (a_0, \{\})$, where $a_0 \in A$,
  $h(1) = (a_1, \{a_0\})$, where $a_1 \in A \setminus \{a_0\}$,
  $h(2) = (a_2, \{a_0, a_1\})$, where $a_2 \in A \setminus \{a_0, a_1\}$,
  etc.

  To do this, we first define a function $r : A \times \mathscr{F} \to A \times \mathscr{F}$ by

  $$r((a, F)) = (c(A \setminus (F \cup \{a\})), F \cup \{a\})$$

  for all $(a, F) \in A \times \mathscr{F}$.

3. Prove that this definition of r is okay by showing that for any $(a, F) \in A \times \mathscr{F}$, we have $A \setminus (F \cup \{a\}) \in \mathscr{A}$ and $F \cup \{a\} \in \mathscr{F}$.

- Now let $h : \mathbb{N} \to A \times \mathscr{F}$ be the unique function that satisfies

  $h(0) = (c(A), \{\})$ (note that $A \in \mathscr{A}$, because we assumed A is infinite) and $h(n+1) = r(h(n))$ for all $n \in \mathbb{N}$.

- Define $\pi_1' = \{\, ((a, F), a) \restriction (a, H) \in A \times \mathscr{F} \,\}$ and $\pi_2' = \{\, ((a, F), F) \restriction (a, F) \in A \times \mathscr{F} \,\}$. Then $\pi_1' : A \times \mathscr{F} \to A$ and $\pi_2' : A \times \mathscr{F} \to \mathscr{F}$.

- Define $f = \pi_1' \circ h$ and $H = \pi_2' \circ h$. Then $f : \mathbb{N} \to A$ and $H : \mathbb{N} \to \mathscr{F}$.

4. Prove that $f(0) = c(A)$, $H(0) = \{\}$, and

$$H(n+1) = H(n) \cup \{f(n)\} \qquad \text{and} \qquad f(n+1) = c(A \setminus H(n+1))$$

   for all $n \in \mathbb{N}$.

5. Prove that for all $n \in \mathbb{N}$, $f(n) \notin H(n)$.

6. Prove that for all $n, m \in \mathbb{N}$, $n < m \Rightarrow f(n) \in H(m)$.

7. Prove that f is injective.

- Thus $\mathbb{N} \preceq A$.

3.15 Relations

Given a set A, one can think of subsets of A as *unary predicates* about elements of A. For example if one defines $G = \{\, g \restriction g \in A \text{ and } g \text{ is green} \,\}$, then, for elements of A, to "be green" is to "be an element of G." This would be a *unary* predicate becuase the proposition "g is green" has just one variable in it– it is true or false depending on what g is. The set G is an object which represents the concept of "being green" for elements of A.

In a similar vein, one can think of subsets of $A \times A$ as *binary* predicates about elements of A. For example if one defines $L = \{\, (x, y) \restriction x, y \in A \text{ and } x \text{ loves } y \,\}$, then, for elements x, y of A, we have "x loves y" if and only if we have $(x, y) \in L$. The set L is an object which represents the concept of "loving" for elements of A. Instead of writing "$(x, y) \in L$," we will often use an infix notation and write "xLy." In this context, L is a *relation*.

Definition 144 (Relations):
(1) R is a *relation on* A if and only if $R \subseteq A \times A$.
(2) When R is a relation on A, we write "xRy" to mean "$(x, y) \in R$."

Instead of using letters like R or L for variables that stand for relations, we will often use the symbol "$\sim$". This is just because it looks pretty in the infix notation: $(x, y) \in \sim$ if and only if $x \sim y$. Bear in mind that even though the symbol $\sim$ is not a letter of the alphabet,

it is still a *variable* and not a constant. What "$\sim$" refers to and what assumptions about "$\sim$" are available all depends on context.

Definition 145 (Adjectives for Relations): Assume that $\sim \subseteq A \times A$.
(1) $\sim$ is *reflexive* on A iff $a \sim a$ for all $a \in A$.
(2) $\sim$ is *symmetric* iff $a \sim b \Rightarrow b \sim a$ for all a, b.
(3) $\sim$ is *transitive* iff $((a \sim b) \wedge (b \sim c)) \Rightarrow (a \sim c)$ for all a, b, c.
(4) $\sim$ is *antisymmetric* iff $((a \sim b) \wedge (b \sim a)) \Rightarrow (a = b)$ for all a, b.
(5) $\sim$ is *total* on A iff $(a \sim b) \vee (b \sim a)$ for all $a, b \in A$.

In the next definition, we will group some of these adjectives together in ways that have proven useful in practice. We will primarily be concerned with *equivalence relations*, but we also highlight some of the other types of relations that people often care about.

Definition 146 (Special Kinds of Relations): Assume that $\sim \subseteq A \times A$.
(1) $\sim$ is a *preorder* on A iff it is reflexive on A and transitive.
(2) $\sim$ is a *partial order* on A iff it is an *antisymmetric* preorder on A.
(3) $\sim$ is a *total order* on A iff it is a *total* partial order on A.
(4) $\sim$ is an *equivalence relation* on A iff it is a *symmetric* preorder on A.

So an equivalence relation (on A) is a relation (on A) that is reflexive (on A), transitive, and symmetric. When $\sim$ is an equivlanece relation on A, we say often read "$a \sim b$" as "a and b are *equivalent*."

Exercise 160: Assume that $\sim$ is a relation on A.

1. Prove that $\sim$ is a preorder on A if and only if $\mathrm{id}_A \subseteq \sim$ and $\sim \circ \sim \subseteq \sim$.

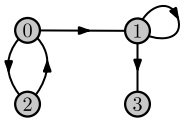
2. Prove that if $\sim$ is a preorder on A then $\sim \circ \sim = \sim$.

3. Prove that $\sim$ is an equivalence relation on A if and only if $\mathrm{id}_A \subseteq \sim$, $\sim \circ \sim \subseteq \sim$, and $\sim^{\dashv} \subseteq \sim$.

4. Prove that if $\sim$ is an equivalence relation on A then $\sim \circ \sim = \sim$ and $\sim^{\dashv} = \sim$.

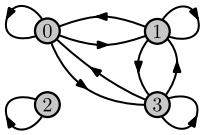
5. Prove that $\sim$ is total on A if and only if $\sim \cup \sim^{\dashv} = A \times A$.

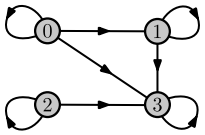
When A is a small finite set, we can depict relations $\sim$ on A by drawing a labeled dot for each element of A and then drawing an arrow from the the dot labeled x to the dot labeled y whenever $x \sim y$. For example,

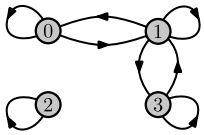


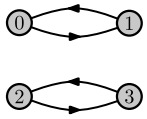
depicts the relation $\{(0,1),(1,1),(1,3),(0,2),(2,0)\}$ on the set $\{0,1,2,3\}$.

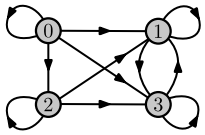
Exercise 161: Consider the following relations on $\{0,1,2,3\}$:

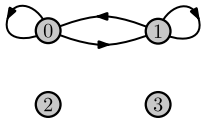
(a) 

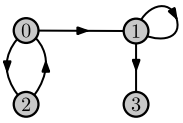
(b) 

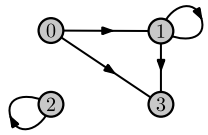
(c) 

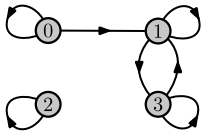
(d) 

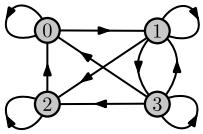
(e) 

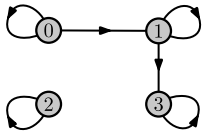
(f) 

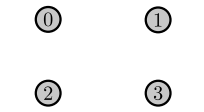
(g) 

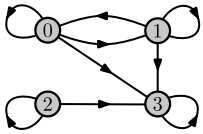
(h) 

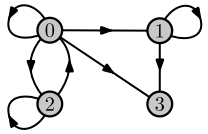
(i) 

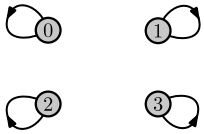
(j) 

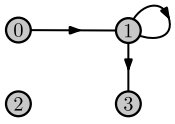
(k) 

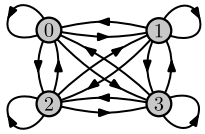
(l) 

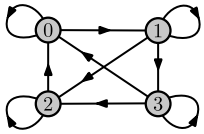
(m) 

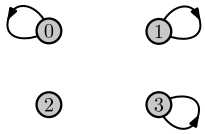
(n) 

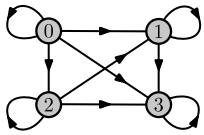
(o) 

(p) 

(q) 

(r) 

(s) 

(t) 

Answer the questions below. You do not need to prove anything.

1. Which relations are reflexive on $\{0,1,2,3\}$?
2. Which relations are symmetric?

3. Which relations are transitive?

4. Which relations are antisymmetric?

5. Which relations are total on $\{0, 1, 2, 3\}$?

6. Which relations are preorders on $\{0, 1, 2, 3\}$?

7. Which relations are partial orders on $\{0, 1, 2, 3\}$?

8. Which relations are total orders on $\{0, 1, 2, 3\}$?

9. Which relations are equivalence relations on $\{0, 1, 2, 3\}$?

Exercise 162: Assume that $\sim$ is a relation on A.

1. Prove that if $\sim$ is total on A, then $\sim$ is reflexive on A.

2. Prove that if $\sim$ is symmetric and antisymmetric, then $\sim \subseteq \mathrm{id}_A$.

3. Prove that id_A is the only relation on A which is reflexive, symmetric, and antisymmetric.

4. Prove that $A \times A$ is the only relation on A which is symmetric and total.

Exercise 163: For each of the following relations on $\mathbb{N}$, determine which of the adjectives in Definition 145 apply. Point out which relations are equivalence relations and which are partial orders.

1. $\sim = \{ (n, m) \mid n, m \in \mathbb{N} \ \wedge \ n \leq m \}$

2. $\sim = \{ (n, m) \mid n, m \in \mathbb{N} \ \wedge \ n < m \}$

3. $\sim = \{ (n, m) \mid n, m \in \mathbb{N} \ \wedge \ n = m \}$

4. $\sim = \{ (n, m) \mid n, m \in \mathbb{N} \ \wedge \ 4 < n + m \}$

5. $\sim = \{ (n, m) \mid n, m \in \mathbb{N} \ \wedge \ n \leq m + m \}$

6. $\sim = \{ (n, m) \mid n, m \in \mathbb{N} \ \wedge \ n + n \leq m \}$

7. $\sim = \{ (n, n + 1) \mid n \in \mathbb{N} \}$

8. $\sim = \{ (n, n + 1) \mid n \in \mathbb{N} \} \cup \{ (n + 1, n) \mid n \in \mathbb{N} \}$

9. $\sim = \{ (n, m) \mid n, m \in \mathbb{N}$ and $n + m$ is even $\}$ (recall Definition 136)

Exercise 164:

1. Define $\sim = \{\, (X,Y) \mid X,Y \subseteq A \ \wedge\ X \subseteq Y \,\}$. Prove that $\sim$ is a partial order on $\mathcal{P}(A)$.

2. Define $\sim = \{\, (X,Y) \mid X,Y \subseteq A \ \wedge\ X \preceq Y \,\}$ (recall Definition 114). Prove that $\sim$ is a partial order on $\mathcal{P}(A)$. (Hint: Much of the hard work has been done by previous theorems that you can reference.)

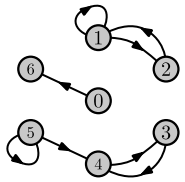
3. Define $\sim = \{\, (X,Y) \mid X,Y \subseteq A \ \wedge\ X \approx Y \,\}$. Prove that $\sim$ is an equivalence relation on $\mathcal{P}(A)$.

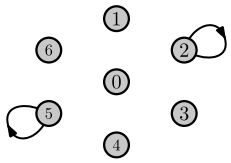
4. For each of the following relations on $\mathcal{P}(A)$, determine which of the adjectives in Definition 145 apply:

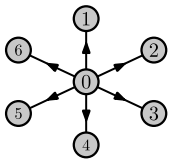
   (a) $\sim = \{\, (X,Y) \mid X,Y \subseteq A \ \wedge\ X \cap Y = \{\} \,\}$

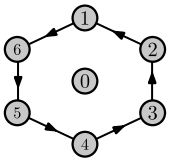
   (b) $\sim = \{\, (X,Y) \mid X,Y \subseteq A \ \wedge\ X \cap Y \neq \{\} \,\}$

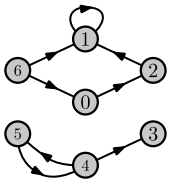
Exercise 165: For each of the following relations on 7, add a minimal number of arrows to turn them into equivalence relations. So do nothing if the given relation is already an equivalence relation, and otherwise draw in only the arrows that need to be included in order to ensure reflexivity, symmetry, and transitivity.

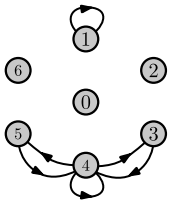
(a) 

(b) 

(c) 

(d) 

(e) 

(f) 

After doing Exercise 165, you might notice that an equivalence relation seems to partition a set into batches, where everything in any given batch is connected to everything else in the same batch, and where there are no connections between different batches. These batches are called *equivalence classes*.

Definition 147 (Equivalence Class): Assume that $\sim$ is an equivalence relation on A and $a \in A$. Then we define

$$[a]_\sim = \{\, x \mid x \sim a \,\}$$

and we call this the *equivalence class of* a, or the *equivalence class of* a *modulo* $\sim$. If the relation involved is clear from context, then we may simply write $[a]$ instead of $[a]_\sim$.

Exercise 166: For each part of Exercise 165, after you have added the arrows that are needed to have an equivalence relation, determine the equivalence classes [0] and [1]. ("Determine" means "list the elements.")

Exercise 167: Define $\sim = \{\, (X, Y) \mid X, Y \subseteq A \ \wedge\ X \approx Y \,\}$. You proved in Exercise 164 part 3 that $\sim$ is an equivalence relation on $\mathcal{P}(A)$. Now suppose that $x \in A$. Describe the equivalence classes $[\{\}]_\sim$ and $[\{x\}]_\sim$. (Hint: revisit the ideas around Definition 120.)

Exercise 168: Show that the following $\sim$ is an equivalence relation on $A \times B$, and then describe the equivalence classes:

$$\sim = \{\, ((a, b), (a', b)) \mid a, a' \in A \quad \wedge \quad b \in B \,\}.$$

Definition 148 (Set of Equivalence Classes): Assume that $\sim$ is an equivalence relation on A. Then we define

$$A/\sim \quad = \quad \{\, [a]_\sim \mid a \in A \,\}.$$

Referring back to the intuition from Exercise 165, an equivalence relation on a set *partitions* the set into batches called equivalence classes. We can make this concept precise. First, we make precise the concept of a *partition* of a set:

Definition 149 (Partition): A set $\mathcal{F} \subseteq \mathcal{P}(A)$ of subsets of A is a *partition of* A iff
(1) $\{\} \notin \mathcal{F}$,
(2) $(\forall a \mid a \in A \Rightarrow (\exists F \mid F \in \mathcal{F} \quad \wedge \quad a \in F))$, and
(3) $(\forall F, F' \mid F, F' \in \mathcal{F} \quad \Rightarrow \quad (F \neq F' \ \Rightarrow\ F \cap F' = \{\}))$.

Condition (2) says that the sets in $\mathcal{F}$ must "cover" all of A and condition (3) says that the sets in $\mathcal{F}$ must be pairwise disjoint. Condition (1) is an unimportant technicality that makes the upcoming Theorem 150 have a pretty statement. Next, we look at how equivalence relations give rise to partitions and vice versa:

Exercise 169: Suppose that $\sim$ is an equivalence relation on A. Prove that $A/\sim$ is a partition of A.

Exercise 170: Let $\mathcal{F}$ be a partition of A. Prove that

$$\{\, (a, b) \mid (\exists F \mid F \in \mathcal{F} \ \wedge\ a, b \in F) \,\}$$

is an equivalence relation on A.

Finally, we put the ideas together to see that equivalence relations and partitions are two ways of looking at the same information:

Theorem 150 (Correspondence between Equivalence Relations and Partitions): Given a set A, define

$$\begin{aligned} \mathcal{E} &= \{ \sim \mid \sim \text{ is an equivalence relation on } A \} \\ \mathcal{P} &= \{ \mathcal{F} \mid \mathcal{F} \text{ is a partition of } A \} \end{aligned}$$

and define a function f on $\mathcal{E}$ by

$$f(\sim) = A/\sim \qquad \text{for all } \sim \in \mathcal{E}.$$

Then $f : \mathcal{E} \to \mathcal{P}$ bijectively.

Proof: Exercise 169 proves that $\text{ran}(f) \subseteq \mathcal{P}$, so we have $f : \mathcal{E} \to \mathcal{P}$. It remains to prove that this mapping is bijective. We will use Theorem 83 to do this. Define a function g on $\mathcal{P}$ by

$$g(\mathcal{F}) = \{ (a,b) \mid (\exists F \mid F \in \mathcal{F} \ \wedge \ a,b \in F) \}$$

for all $\mathcal{F} \in \mathcal{P}$. Exercise 170 proves that $\text{ran}(g) \subseteq \mathcal{E}$, so we have $g : \mathcal{P} \to \mathcal{E}$.

Proof that $g \circ f = id_{\mathcal{E}}$: Consider any $\sim \in \mathcal{E}$. We will show that $g(f(\sim)) = \sim$.

For the inclusion $g(f(\sim)) \subseteq \sim$, consider any $(a,b) \in g(f(\sim))$. There is some $F \in f(\sim)$ such that $a,b \in F$. Since $F \in f(\sim) = A/\sim$, there is some $c \in A$ such that $F = [c]_\sim$. Since $a,b \in F = [c]_\sim$, we have $a \sim c$ and $b \sim c$. It follows that $a \sim b$, since $\sim$ is an equivalence relation. In other words, $(a,b) \in \sim$.

For the converse inclusion $g(f(\sim)) \supseteq \sim$, consider any $(a,b) \in \sim$. We have $a \sim b$ and, since $\sim$ is an equivalence relation, we also have $b \sim b$. It follows that $a,b \in [b]_\sim$. Since

$$a,b \in [b]_\sim \in A/\sim \ = f(\sim),$$

we have established that $(a,b) \in g(f(\sim))$.

We have shown that $g(f(\sim)) = \sim$, for arbitrary $\sim \in \mathcal{E}$. It follows that $g \circ f = \text{id}_{\mathcal{E}}$.

Claim: For any $a, F, \mathcal{F}$ with $a \in F \in \mathcal{F} \in \mathcal{P}$, we have $F = [a]_{g(\mathcal{F})}$.

Proof of claim: Suppose that $a \in F \in \mathcal{F} \in \mathcal{P}$.

Consider any $b \in F$. From the fact that $a,b \in F \in \mathcal{F}$ and from the definition of g, we get $(a,b) \in g(\mathcal{F})$. Hence $b \in [a]_{g(\mathcal{F})}$.

Conversely, consider any $b \in [a]_{g(\mathcal{F})}$. We have $(b, a) \in g(\mathcal{F})$, so there is some $F' \in \mathcal{F}$ such that $a, b \in F'$. Since $\mathcal{F}$ is a partition of A and $F, F' \in \mathcal{F}$, we have

$$F \neq F' \;\Rightarrow\; F \cap F' = \{\}.$$

We have seen that $a \in F \cap F'$, so $F \cap F' \neq \{\}$. It follows that $F = F'$, and so $b \in F$. This proves the claim.

Proof that $f \circ g = id_{\mathcal{P}}$: Now consider any $\mathcal{F} \in \mathcal{P}$. We will show that $f(g(\mathcal{F})) = \mathcal{F}$. For convenience of notation, define $\sim = g(\mathcal{F})$.

For the inclusion $f(\sim) \subseteq \mathcal{F}$, consider any $F \in f(\sim) = A/\sim$. There is some $a \in A$ such that $F = [a]_\sim$. Since $a \in A$ and $\mathcal{F}$ is a partition of A, there is some $G \in \mathcal{F}$ such that $a \in G$. By the claim above, we have $G = [a]_\sim$. Thus we have $F = G \in \mathcal{F}$.

For the converse inclusion $f(\sim) \supseteq \mathcal{F}$, consider any $F \in \mathcal{F}$. We required in Definition 149 that a partition consist of only nonempty sets, so there exists some $a \in F$. By the claim above, we have $F = [a]_\sim$. Hence $F \in A/\sim \; = f(\sim)$.

We have shown that $f(g(\mathcal{F})) = \mathcal{F}$, for arbitrary $\mathcal{F} \in \mathcal{P}$. It follows that $f \circ g = \mathrm{id}_{\mathcal{P}}$.

Since $f \circ g = \mathrm{id}_{\mathcal{P}}$ and $g \circ f = \mathrm{id}_{\mathcal{E}}$, we are done by Theorem 83. ■

3.16 Integers

You have now completed the main portion of this text. This final section will be a cursory preview of what you could pursue next.

Why might we want to define more numbers than $\mathbb{N}$ provides? Your first answer might be "because we are missing the negative numbers," but that's cheating! Imagine that you are the first human to come up with these ideas. Why are you not satisfied with $\mathbb{N}$? Now might be a good time to revisit Theorem 113 part (12).

If we were only interested in counting (finite collections), then $\mathbb{N}$ would be sufficient. But if we want to refer to changes between counts, also known as *differences*, then something is missing. A difference, unlike a distance, has a direction to it. The change from 3 to 5 is a *gain* of 2, while the change from 5 to 3 is a *loss* of 2. We'd like some mathematical objects that can represent gains and losses of various amounts– these will be the integers.

The following strategy is common throughout mathematics: First construct something that might be "too big" by introducing a symbol for every integer we could ever want to refer to, allowing for redundant symbols. Then cut down the redundancy by defining an equivalence relation and taking equivalence classes.

One symbolic way to refer to "the change from 3 to 5" is simply the pair $(3, 5)$. The pair $(5, 3)$ could refer to "the change from 5 to 3". We could think of $(3, 5)$ as sort of *being* the integer "gain-of-2," while $(5, 3)$ sort of *is* the integer "loss-of-2." In this view, an integer is just a pair of natural numbers. So the set $\mathbb{Z}$ of all integers could be defined to be $\mathbb{N} \times \mathbb{N}$.

But wait, this produces a lot of redundancy! The pair $(3, 5)$ represents a gain of 2, but so does the pair $(4, 6)$, so does the pair $(5, 7)$, and so on. For any given pair $(n, m) \in \mathbb{N} \times \mathbb{N}$, there is an infinite collection of pairs that represent the same gain or loss that one gets in the change from n to m.

How can we express the statement that two pairs (n, m) and (k, l) represent the same gain or loss? Let's cheat a little. Pretend that n and m are integers, even though they're not and even though we haven't defined what that means. Pretend that we have defined subtraction for integers. Then the change from n to m can be expressed as the difference $m - n$. The statement that two pairs (n, m) and (k, l) represent the same gain or loss can then (cheatingly) be written like this: $m - n = l - k$. Rearrangement leads to $m + k = l + n$, which is slightly less cheaty because it doesn't mention subtraction.

Okay, now stop cheating. We define an integer to be an *equivalence class* of pairs of natural numbers, where the equivalence relation being used is

$$(n, m) \sim (k, l) \;\Leftrightarrow\; m + k = l + n.$$

More formally:

Theorem 151: The following relation on the set $\mathbb{N} \times \mathbb{N}$ is an equivalence relation:

$$\{\, ((n, m), (k, l)) \;\mathbin{!}\; n, m, k, l \in \mathbb{N} \quad \wedge \quad m + k = l + n \,\}.$$

Proof: **Exercise 171**. ■

Definition 152 (Integers): Let $\sim$ be the equivalence relation on $\mathbb{N} \times \mathbb{N}$ defined in Theorem 151. We define

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

We end here. There's a lot more work to be done to give the integers $\mathbb{Z}$ the structure that makes them behave like integers. We only defined addition (Definition 111) for natural numbers– work is needed to see how $\mathbb{Z}$ can inherit the addition operation. Work is also needed to see how ordering for $\mathbb{N}$ (Definition 95) can be inherited by $\mathbb{Z}$.

Exercise 136 hints at how one could use recursion to define multiplication on $\mathbb{N}$. Further work can pass along the multiplication operation to $\mathbb{Z}$. Just as the need for subtraction led us to construct $\mathbb{Z}$ out of $\mathbb{N}$, a need for division can lead one to construct the rational

numbers, $\mathbb{Q}$, out of $\mathbb{Z}$. Eventually you can branch out to specific fields like abstract algebra or real analysis.

The adventure begins!

A The Bug

Axiom 5 makes it possible to prove a contradiction, and this breaks our entire system (recall Derived Rule 6). This bug was first encountered in 1897 when Burali-Forti unknowingly proved a theorem that directly contradicted an earlier theorem of Cantor. It caused quite a panic when Bertrand Russel pointed it out a few years later. The original path to the bug was complicated, but now thanks to Russell there is a much simpler way to see how a contradiction arises from Axiom 5.

Define a set $\mathcal{R} = \{\, x \mid x \notin x \,\}$. Now ask yourself: Is $\mathcal{R} \in \mathcal{R}$? By Axiom 5 we have

$$\mathcal{R} \in \mathcal{R} \quad \Leftrightarrow \quad \text{“ } x \notin x \text{ ”}_{[x \to \mathcal{R}]}.$$

In other words,

$$\mathcal{R} \in \mathcal{R} \quad \Leftrightarrow \quad \mathcal{R} \notin \mathcal{R} \tag{$*$}$$

Due to excluded middle, we have $(\mathcal{R} \in \mathcal{R}) \vee (\mathcal{R} \notin \mathcal{R})$. In the case that $\mathcal{R} \in \mathcal{R}$ we get $\mathcal{R} \notin \mathcal{R}$ from ($*$). In the case that $\mathcal{R} \notin \mathcal{R}$ we get $\mathcal{R} \in \mathcal{R}$ from ($*$). This completes a proof by cases in which we have proven the contradiction

$$(\mathcal{R} \in \mathcal{R}) \wedge (\mathcal{R} \notin \mathcal{R}).$$

What a disaster! The framework in this text is completely broken. That's why it's called *naive set theory*.

After the panic, people started coming up with different ways to fix the bug. Each approach led to a certain kind of set theory. Here we will briefly look at two popular flavors of set theory, NBG and ZF. Both fixes of the bug come down to the same basic idea: restrict who gets to be on the left hand side of "$\in$".

A.1 NBG

The NBG approach (Von Neumann–Bernays–Gödel set theory) is to replace Axiom 5 by the following:

Axiom (Membership, fixed version):

$$a \in \{\, x \mid \Phi \,\} \Leftrightarrow \ (\Phi_{[x \to a]} \ \wedge \ (\, \exists b \mid a \in b \,)).$$

This makes the proposition "$a \in \{\, x \mid \Phi \,\}$" harder to prove– one has to establish an extra condition $(\,\exists b \mid a \in b\,)$. In other words: For a to be a member of $\{\, x \mid \Phi \,\}$, in addition to satisfying the membership condition Φ it has to also be a known member of *something*.

At first glance this might not sound so hard. After all, isn't any given a at least a member of $\{a\}$? Not so! From Definition 16,

$$\{a\} = \{\, x \mid x = a \,\},$$

so by the new version of Axiom 5 we have

$$a \in \{a\} \;\Leftrightarrow\; (a = a \;\wedge\; (\,\exists b \mid a \in b\,)).$$

By Axiom 1 we can deduce

$$a \in \{a\} \;\Leftrightarrow\; (\,\exists b \mid a \in b\,),$$

but we are unable to reduce this to $a \in \{a\}$!

The extra condition "$(\,\exists b \mid a \in b\,)$" in the new Axiom 5 blocks us from ever proving the elementhood of a in anything. If we just knew that a is a member of *something* then $(\,\exists b \mid a \in b\,)$ becomes true and the new Axiom 5 reduces to the old Axiom 5 for "$a \in \ldots$" statements.

Some bootstrapping is needed to get our first "$a \in \ldots$" statements. This comes in the form of a whole bunch of new Axioms in NBG such as

Axiom: $(\,\exists b \mid \{\} \in b\,)$.

This forcibly admits $\{\}$ into the exclusive club of a's for which $(\,\exists b \mid a \in b\,)$. Being in this club means that "$\{\} \in \ldots$" statements effectively get to follow the rules of the old Axiom 5. For example, this makes it possible to use Defintion 16 to prove that $\{\} \in \{\{\}\}$. But we still can't prove $\{\{\}\} \in \{\{\{\}\}\}$– for that we might need another axiom like the following:

Axiom: $(\,\exists b \mid a \in b\,) \;\Rightarrow\; (\,\exists b \mid \{a\} \in b\,)$.

NBG has many more axioms like these to make set theoretic constructions such as doubleton, union, power set, etc. work properly with the new Axiom 5.

How does this repair the contradiciton in $(*)$ above? With the new Axiom 5, we replace $(*)$ by

$$\mathcal{R} \in \mathcal{R} \;\;\Leftrightarrow\;\; (\mathcal{R} \notin \mathcal{R} \;\wedge\; (\,\exists b \mid \mathcal{R} \in b\,)).$$

Assuming $\mathcal{R} \in \mathcal{R}$ still leads to a contradiction, so we must have $\mathcal{R} \notin \mathcal{R}$. Now assuming $(\,\exists b \mid \mathcal{R} \in b\,)$ leads back to $\mathcal{R} \in \mathcal{R}$ and another contradiction, so we must have

$$\neg\,(\,\exists b \mid \mathcal{R} \in b\,).$$

Instead of giving a contradiction when we ask whether $\mathcal{R} \in \mathcal{R}$, the new Axiom 5 simply tells us that $\mathcal{R}$ never gets to be a member of *anything*.

In NBG set theory, the word *set* is reserved only for those a's for which $(\exists b \,!\, a \in b)$. Otherwise the more general term *class* is used instead. What we've established above is that $\mathcal{R}$ is a class that is not a set.

A.2 ZF

ZF (Zermelo-Fraenkel) set theory is another very popular way to deal with the paradoxes of naive set theory. Instead of starting with a fix to Axiom 5, ZF set theory treats the notation "$\{\, x \,!\, \Phi \,\}$" in a completely different way.

When we write "$\{\, x \,!\, \Phi \,\}$," our intent is to refer to

$$\text{"a set } S \text{ with the property that } a \in S \Leftrightarrow \Phi_{[x \to a]} \text{ for all } a\text{"}.$$

ZF set theory wants us to stop and ask ourselves: Does such a set *exist*? In other words:

$$\big(\exists S \,!\, \big(\forall a \,!\, a \in S \Leftrightarrow \Phi_{[x \to a]}\big)\big)?$$

If yes, then a ZF axiom like our Axiom 2 can be used to prove that such an S is unique. In ZF set theory we think of the notation "$\{\, x \,!\, \Phi \,\}$" as a shorthand for

$$\text{"the unique set } S \text{ with the property that } a \in S \Leftrightarrow \Phi_{[x \to a]} \text{ for all } a\text{"}.$$

Just like with NBG, some bootstrapping is needed in ZF to get set theoretic constructions like doubleton, union, power set, etc. to work properly. This comes in the form of a bunch of axioms about the *existence* of various sets.

How does ZF help with the problematic set $\mathcal{R}$ at the beginning of this appendix? Well, due to the contradiction in $(*)$ we conclude that there *does not exist* a set $\mathcal{R}$ for which $x \in \mathcal{R} \Leftrightarrow x \notin x$ for all x. If you write "$\{\, x \,!\, x \notin x \,\}$" then you are trying to refer to

$$\text{"the unique set } \mathcal{R} \text{ for which } x \in \mathcal{R} \Leftrightarrow x \notin x \text{ for all } x\text{"}.$$

This is as nonsensical as trying to refer to "the unique element of the empty set." One can write the words, but they fail to refer to anything.

B Theorem Reference

All numbered definitions, axioms, and theorems for quick reference:

Axiom 1 (Reflexiveness for Equality): $x = x$.

Axiom 2 (Equality Used): If $x = y$, then $\Phi_{[a \to x]} \Leftrightarrow \Phi_{[a \to y]}$.

Theorem 3 (Symmetry and Transitivity for Equality):
(1) If $x = y$, then $y = x$.
(2) If $x = y$ and $y = z$, then $x = z$.

Theorem 4 (Equality Used): If $x = y$, then:
(1) $\Phi_{[a \to x]} \Leftrightarrow \Phi_{[a \to y]}$
(2) $☺_{[a \to x]} = ☺_{[a \to y]}$
(3) $\Phi \Leftrightarrow \Phi_{[x \to y]}$
(4) $☺ = ☺_{[x \to y]}$

Axiom 5 (Membership): $a \in \{\, x \mid \Phi \,\} \Leftrightarrow \Phi_{[x \to a]}$.
Warning: this axiom is broken.

Definition 6 (Inclusion): $a \subseteq b \Leftrightarrow (\, \forall z \mid z \in a \Rightarrow z \in b \,)$.

Theorem 7 (Reflexivity and Transitivity for Inclusion):
(1) $a \subseteq a$.
(2) If $a \subseteq b$ and $b \subseteq c$, then $a \subseteq c$.

Axiom 8 (Equality Gained): If $(\, \forall z \mid z \in a \Leftrightarrow z \in b \,)$, then $a = b$.

Theorem 9: $y = \{\, z \mid z \in y \,\}$.

Theorem 10 (Equality as Double Inclusion): $a = b$ if and only if $a \subseteq b$ and $b \subseteq a$.

Definition 11 (Empty Set): $\{\} = \{\, x \mid x \neq x \,\}$

Theorem 12 (Empty Set is Empty): $x \notin \{\}$.

Theorem 13 (Minimality of the Empty Set):
(1) $\{\} \subseteq a$.
(2) If $a \subseteq \{\}$, then $a = \{\}$.

Theorem 14 (Only the Empty Set is Empty): If $x \notin a$ for all x, then $a = \{\}$.

Theorem 15 (Nonemptiness): $a \neq \{\} \Leftrightarrow (\, \exists x \mid x \in a \,)$.

Definition 16 (Singleton): $\{x\} = \{\, a \mid a = x \,\}$.

Definition 17 (Doubleton): $\{x, y\} = \{\, a \mid (a = x) \vee (a = y) \,\}$.

Definition 18 (More Ways to List Elements):
(1) $\{x, y, z\} = \{\, a \mid (a = x) \vee (a = y) \vee (a = z) \,\}$
(2) $\{x, y, z, u\} = \{\, a \mid (a = x) \vee (a = y) \vee (a = z) \vee (a = u) \,\}$
(3) $\{x, y, z, u, v\} = \{\, a \mid (a = x) \vee (a = y) \vee (a = z) \vee (a = u) \vee (a = v) \,\}$
(4) $\{x, y, z, u, v, w\} = \{\, a \mid (a = x) \vee (a = y) \vee (a = z) \vee (a = u) \vee (a = v) \vee (a = w) \,\}$

Theorem 19 (Singleton and Inclusion): $x \in S$ if and only if $\{x\} \subseteq S$.

Theorem 20 : $\{x, y\} = \{y, x\}$

Theorem 21 : $\{x\} = \{y\}$ if and only if $x = y$.

Theorem 22 : $\{x, y\} = \{u\}$ if and only if $x = y = u$.

Theorem 23 : If $\{x, y\} = \{u, v\}$, then either $x = u$ and $y = v$, or $x = v$ and $y = u$.

Definition 24 (Being a Singleton): A set is said to be a *singleton* iff it has the form $\{x\}$ for some x. That is, we call s a singleton iff $(\, \exists x \mid s = \{x\} \,)$.

Theorem 25 (Existence and Uniqueness in Terms of Singleton):
A set s is a singleton if and only if it has a unique element. That is, s is a singleton if and only if

$$(\, \exists x \mid x \in s \wedge (\, \forall y \mid y \in s \Rightarrow y = x \,) \,).$$

Definition 26 (Occupant): Let s be a singleton. The *occupant* of s is denoted by $\mathrm{occ}(s)$ and defined by

$$\mathrm{occ}(s) = \{\, z \mid (\, \forall x \mid x \in s \Rightarrow z \in x \,) \,\}.$$

Theorem 27 (Essence of Occupant): $\mathrm{occ}(\{g\}) = g$.

Definition 28 (Intersection and Union):
(1) $a \cap b = \{\, x \mid (x \in a) \wedge (x \in b) \,\}$
(2) $a \cup b = \{\, x \mid (x \in a) \vee (x \in b) \,\}$

Theorem 29 (Algebraic Properties of Intersection and Union):

(1)	$a \cap b = b \cap a$	(commutativity of $\cap$)
(2)	$a \cup b = b \cup a$	(commutativity of $\cup$)
(3)	$(a \cap b) \cap c = a \cap (b \cap c)$	(associativity of $\cap$)
(4)	$(a \cup b) \cup c = a \cup (b \cup c)$	(associativity of $\cup$)
(5)	$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$	($\cup$ distributes over $\cap$)
(6)	$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$	($\cap$ distributes over $\cup$)
(7)	$a \cap a = a$	(idempotence of $\cap$)
(8)	$a \cup a = a$	(idempotence of $\cup$)
(9)	$a \cup \{\} = a$	($\{\}$ is an identity for $\cup$)
(10)	$a \cap \{\} = \{\}$	($\{\}$ is an annihilator for $\cap$)

Theorem 30 (Maximality of Intersection):

The set $b \cap c$ is a subset of both b and c, and it contains anything that is a subset of both b and c. That is,

(1) $b \cap c \subseteq b$
(2) $b \cap c \subseteq c$
(3) If $a \subseteq b$ and $a \subseteq c$, then $a \subseteq b \cap c$.

Theorem 31 (Minimality of Union):

The set $b \cup c$ contains both b and c, and it is a subset of any set that contains both b and c. That is,

(1) $b \subseteq b \cup c$
(2) $c \subseteq b \cup c$
(3) If $b \subseteq a$ and $c \subseteq a$, then $b \cup c \subseteq a$.

Theorem 32 (Inclusion in Terms of $\cap$ and $\cup$):

The following are equivalent:

(1) $a \subseteq b$
(2) $a \cap b = a$
(3) $a \cup b = b$

Definition 33 (Relative Complement): $a \setminus b = \{\, x \mid (x \in a) \wedge (x \notin b) \,\}$

Theorem 34 (De Morgan's Law - Set Theory Version):

(1) $a \setminus (b \cap c) = (a \setminus b) \cup (a \setminus c)$
(2) $a \setminus (b \cup c) = (a \setminus b) \cap (a \setminus c)$

Theorem 35 (Iterated Relative Complement): $a \setminus (a \setminus b) = a \cap b$.

Definition 36 (Power Set): $\mathcal{P}(x) = \{\, y \mid y \subseteq x \,\}$.

Theorem 37: $\mathcal{P}(\{x\}) = \{\{\}, \{x\}\}$.

Definition 38 (Ordered Pair): $(x, y) = \{\{x\}, \{x, y\}\}$.

Theorem 39 (Essence of Pairs):

$$(x, y) = (u, v) \text{ if and only if } x = u \text{ and } y = v.$$

Definition 40: A set is called a *pair* if and only if it has the form (a, b) for some a and b. That is, we call x a pair if and only if

$$(\, \exists a, b \mid x = (a, b)\,).$$

A set s is called a *set of pairs* or a *relation* if every element of s is a pair.

Definition 41 (Cartesian Product):

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

Theorem 42 (Essence of Cartesian Product):

$$(y, z) \in A \times B \text{ if and only if } y \in A \text{ and } z \in B.$$

Theorem 43 (Cartesian Products and Emptiness):
(1) $A \times B$ is nonempty if and only if A and B are both nonempty.
(2) $A \times B$ is empty if and only if either A is empty or B is empty.

Theorem 44: If $A \subseteq B$ and $C \subseteq D$, then $A \times C \subseteq B \times D$.

Theorem 45:

$$(A \times C) \cap (B \times D) \subseteq (A \cap B) \times (C \cap D).$$

Theorem 46: If A is nonempty and $A \times C \subseteq B \times D$, then $C \subseteq D$.

Definition 47 (Domain and Range): Let S be a set of pairs. The *domain* and the *range* of S are denoted respectively by $\mathrm{dom}(S)$ and $\mathrm{ran}(S)$, and they are defined as follows:

$$\begin{aligned} \mathrm{dom}(S) &= \{\, x \mid (\, \exists y \mid (x, y) \in S\,)\,\} \\ \mathrm{ran}(S) &= \{\, y \mid (\, \exists x \mid (x, y) \in S\,)\,\} \end{aligned}$$

Definition 48 (Function): A set f is said to be a *function* iff f is a set of pairs and

$$(\, \forall x, y, z \mid (x, y), (x, z) \in f \ \Rightarrow\ y = z\,).$$

Theorem 49 : If f is a function and $x \in \text{dom}(f)$, then

$$\{\, y \mid (x, y) \in f \,\}$$

is a singleton.

Definition 50 (Function Evaluation): Let f be a function and let $x \in \text{dom}(f)$. By Theorem 49, there is a unique y such that $(x, y) \in f$. We denote this unique y by "$f(x)$", and we call it *the value of f at x*. Formally, we are making the definition

$$f(x) = \text{occ}(\{\, y \mid (x, y) \in f \,\}).$$

Theorem 51 (Essence of Evaluation): If f is a function then
(1) If $x \in \text{dom}(f)$, then $(x, f(x)) \in f$.
(2) If $(x, y) \in f$, then $y = f(x)$.
(3) If $x \in \text{dom}(f)$, then $(x, y) \in f \Leftrightarrow y = f(x)$.

Theorem 52 : If f is a function, then $y \in \text{ran}(f)$ if and only if $y = f(x)$ for some $x \in \text{dom}(f)$.

Theorem 53 (Equality of Functions): If f and g are functions, then $f = g$ if and only if $\text{dom}(f) = \text{dom}(g)$ and $f(x) = g(x)$ for all $x \in \text{dom}(f)$.

Definition 54 (Mapping):

$$f : X \to Y \quad \Leftrightarrow \quad \left(\begin{array}{ll} f \text{ is a function} & \wedge \\ \text{dom}(f) = X & \wedge \\ \text{ran}(f) \subseteq Y & \end{array} \right).$$

Theorem 55 : If f is a function, then $f : X \to Y$ if and only if $f \subseteq X \times Y$ and $X \subseteq \text{dom}(f)$.

Theorem 56 (Piecewise Function Definition):
If f and g are functions and $\text{dom}(f) \cap \text{dom}(g) = \{\}$, then $f \cup g$ is a function.

Definition 57 (Injectivity, Surjectivity, and Bijectivity):
Assume that $f : X \to Y$.
(1) f is *injective* iff for all $x, y \in X$, we have $f(x) = f(y) \Rightarrow x = y$.
(2) f is *surjective onto* Y iff $\text{ran}(f) = Y$.
(3) f is *bijective onto* Y iff f is both injective and surjective onto Y.

Theorem 58 : Assume that f is a function. Then f is injective if and only if

$$(\, \forall x, y, z \mid (x, y), (z, y) \in f \;\Rightarrow\; x = z \,).$$

Theorem 59 : Assume that $f : X \to Y$. Then f is surjective onto Y if and only if

$$(\,\forall y \restriction y \in Y \;\Rightarrow\; (\,\exists x \restriction x \in X \;\wedge\; f(x) = y\,)\,).$$

Definition 60 (Composite):

$$S \circ T = \{\,(x, z) \restriction (\,\exists y \restriction (x, y) \in T \;\wedge\; (y, z) \in S\,)\,\}.$$

Theorem 61 (Associativity of Composition): $S \circ (T \circ U) = (S \circ T) \circ U$

Theorem 62 (Domain and Range of Composite):
(1) If $\mathrm{ran}(T) \subseteq \mathrm{dom}(S)$, then $\mathrm{dom}(S \circ T) = \mathrm{dom}(T)$.
(2) $\mathrm{ran}(S \circ T) \subseteq \mathrm{ran}(S)$

Theorem 63 (Essence of Composition):
(1) If f and g are functions, then $g \circ f$ is a function and

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

for all $x \in \mathrm{dom}(g \circ f)$.
(2) If $f : X \to Y$ and $g : Y \to Z$, then $g \circ f : X \to Z$.

Definition 64 (Identity Function): The *identity function on* A is denoted by id_A and defined by

$$\mathrm{id}_A = \{\,(x, x) \restriction x \in A\,\}.$$

Theorem 65 (Facts about id_A):
(1) $\mathrm{id}_A : A \to A$.
(2) $\mathrm{id}_A(x) = x$ for all $x \in A$.
(3) If $f : A \to B$, then $f \circ \mathrm{id}_A = f$.
(4) If $g : B \to A$, then $\mathrm{id}_A \circ g = g$.

Definition 66 (Reverse): The *reverse* of S is denoted by $S^{\dashv}$ and defined by

$$S^{\dashv} = \{\,(y, x) \restriction (x, y) \in S\,\}.$$

Theorem 67 (Essence of Reversal): $(x, y) \in S \Leftrightarrow (y, x) \in S^{\dashv}$.

Theorem 68 (Double Reversal): If S is a set of pairs, then

$$S^{\dashv\dashv} = S.$$

Theorem 69 (Reversal, Domain, and Range):
(1) $\mathrm{dom}(S^{\dashv}) = \mathrm{ran}(S)$.
(2) $\mathrm{ran}(S^{\dashv}) = \mathrm{dom}(S)$.

Theorem 70 (Reversal and Composition): $(S \circ T)^{\dashv} = T^{\dashv} \circ S^{\dashv}$.

Definition 71 (Invertibility): If f is a function, then f is said to be *invertible* if and only if $f^{\dashv}$ is also a function. In this context, we will refer to $f^{\dashv}$ as *the inverse* of f.

Theorem 72 (Invertibility of Injections): If f is a function, then $f^{\dashv}$ is a function if and only if f is injective.

Theorem 73: If $f : X \to Y$ and f is injective, then $f^{\dashv} : \mathrm{ran}(f) \to X$.

Theorem 74 : If f is an invertible function, $x \in \mathrm{dom}(f)$, and $y \in \mathrm{ran}(f)$, then

$$f(x) = y \;\Leftrightarrow\; x = f^{\dashv}(y)$$

Theorem 75 : If $f : X \to Y$ and f is a bijection onto Y, then $f^{\dashv} : Y \to X$ and $f^{\dashv}$ is a bijection onto X.

Theorem 76 : If $f : X \to Y$ and f is injective, then $f^{\dashv} \circ f = \mathrm{id}_X$.

Theorem 77 (Inverse and Composition): If $f : X \to Y$ and f is a bijection onto Y, then

(1) $f \circ f^{\dashv} = \mathrm{id}_Y$.
(2) $f^{\dashv} \circ f = \mathrm{id}_X$.

Theorem 78 (Composition, Injectivity, and Surjectivity):
Assume that $f : X \to Y$ and $g : Y \to Z$.

(1) If f and g are injective, then $g \circ f$ is injective.
(2) If $g \circ f$ is injective, then f is injective.
(3) If f is surjective onto Y and g is surjective onto Z, then $g \circ f$ is surjective onto Z.
(4) If $g \circ f$ is surjective onto Z, then g is surjective onto Z.
(5) If f is bijective onto Y and g is bijective onto Z, then $g \circ f$ is bijective onto Z.

Theorem 79 (Cancellation of Composite): Assume that $f, g : X \to Y$.

(1) If $h : Y \to Z$, h is injective, and $h \circ f = h \circ g$, then $f = g$.
(2) If $h : Z \to X$, h is surjective onto X, and $f \circ h = g \circ h$, then $f = g$.

Theorem 80 (Left-Invertible Functions): Assume that $f : X \to Y$. If

$$(\, \exists g \,!\, g : Y \to X \;\wedge\; g \circ f = \mathrm{id}_X \,),$$

then f is injective.

Theorem 81 (Right-Invertible Functions): Assume that $f : X \to Y$. If

$$(\exists g \mid g : Y \to X \ \wedge \ f \circ g = \mathrm{id}_Y),$$

then f is surjective onto Y.

Axiom 82 (Axiom of Choice): If $f : X \to Y$ and f is surjective onto Y, then there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.

Theorem 83 (Bijectivity and Isomorphism): Assume that $f : X \to Y$. Then f is a bijection onto Y if and only if

$$(\exists g \mid g : Y \to X \ \wedge \ g \circ f = \mathrm{id}_X \ \wedge \ f \circ g = \mathrm{id}_Y).$$

Definition 84 (Image): The *image of A under S* is denoted by $S[A]$ and defined by

$$S[A] = \{ y \mid (\exists x \mid x \in A \wedge (x, y) \in S) \}.$$

Theorem 85 (Image for Functions): Assume that $f : X \to Y$.

(1) If $A \subseteq X$, then

$$f[A] = \{ f(a) \mid a \in A \}.$$

In other words,

$$y \in f[A] \ \Leftrightarrow \ (\exists a \mid y = f(a) \wedge a \in A).$$

(2)

$$f^{\dashv}[B] = \{ x \mid x \in X \wedge f(x) \in B \}.$$

So if $x \in X$, then

$$x \in f^{\dashv}[B] \ \Leftrightarrow \ f(x) \in B.$$

Theorem 86 (Image and Composition): $(g \circ f)[A] = g[f[A]]$.

Theorem 87 : Assume that $f : X \to Y$, $A \subseteq X$, and $B \subseteq Y$.

(1) $f[f^{\dashv}[B]] \subseteq B$.
(2) $A \subseteq f^{\dashv}[f[A]]$.
(3) If $B \subseteq \mathrm{ran}(f)$, then $f[f^{\dashv}[B]] = B$.
(4) If f is injective, then $f^{\dashv}[f[A]] = A$.

Theorem 88 (Preimage Plays Nice): Assume that $f : X \to Y$, $A \subseteq Y$, and $B \subseteq Y$.

(1) $f^{\dashv}[A \cup B] = f^{\dashv}[A] \cup f^{\dashv}[B]$
(2) $f^{\dashv}[A \cap B] = f^{\dashv}[A] \cap f^{\dashv}[B]$
(3) $f^{\dashv}[A \setminus B] = f^{\dashv}[A] \setminus f^{\dashv}[B]$

Definition 89 (Successor): $\mathrm{next}(x) = x \cup \{x\}$.

Definition 90 (Certain Numbers):

$$\begin{array}{ll} 0 = \{\} & 5 = \text{next}(4) \\ 1 = \text{next}(0) & 6 = \text{next}(5) \\ 2 = \text{next}(1) & 7 = \text{next}(6) \\ 3 = \text{next}(2) & 8 = \text{next}(7) \\ 4 = \text{next}(3) & 9 = \text{next}(8) \end{array}$$

Definition 91 (Inductive): A set J is said to be *inductive* if it contains 0 and it contains $\text{next}(n)$ for every n that it contains. That is,

$$J \text{ is inductive } \Leftrightarrow \ (0 \in J \ \wedge \ (\, \forall n \restriction n \in J \Rightarrow \text{next}(n) \in J \,))$$

Definition 92: $\mathbb{N} = \{\, n \restriction (\, \forall J \restriction J \text{ is inductive } \Rightarrow \ n \in J \,) \,\}$.

Theorem 93 (Essence of $\mathbb{N}$):
(1) $\mathbb{N}$ is inductive.
(2) If J is inductive, then $\mathbb{N} \subseteq J$.

Theorem 94 (Mathematical Induction):
If

$$\Phi_{[x \to 0]}$$

and

$$\left(\forall n \restriction n \in \mathbb{N} \ \Rightarrow \ (\Phi_{[x \to n]} \ \Rightarrow \ \Phi_{[x \to \text{next}(n)]}) \right)$$

both hold, then it follows that

$$\left(\forall n \restriction n \in \mathbb{N} \ \Rightarrow \ \Phi_{[x \to n]} \right).$$

Definition 95 (Order for $\mathbb{N}$):
(1) $x < y \ \Leftrightarrow \ x \in y$.
(2) $x \leq y \ \Leftrightarrow \ (x \in y \ \vee \ x = y)$.

Theorem 96 (Essence of Order and Succession):
(1) $x < \text{next}(x)$.
(2) $x < \text{next}(y) \ \Leftrightarrow \ x \leq y$.

Theorem 97 (About 0): If $n \in \mathbb{N}$, then
(1) $0 < \text{next}(n)$.
(2) $0 \leq n$.
(3) $0 \neq \text{next}(n)$.

Theorem 98 (Predecessor): If $n \in \mathbb{N}$ and $n \neq 0$, then $n = \text{next}(m)$ for some $m \in \mathbb{N}$.

Theorem 99 (Succession Preserves Order): Assume that $n \in \mathbb{N}$.
(1) If $m < n$, then $\text{next}(m) \leq n$.
(2) If $m < n$, then $\text{next}(m) < \text{next}(n)$.

Theorem 100 (Transitivity for Order on $\mathbb{N}$): Assume that $n, m, k \in \mathbb{N}$.
(1) If $n < m$ and $m < k$, then $n < k$.
(2) If $n \leq m$ and $m < k$, then $n < k$.
(3) If $n < m$ and $m \leq k$, then $n < k$.
(4) If $n \leq m$ and $m \leq k$, then $n \leq k$.

Theorem 101 : If $n < m$ and $m \in \mathbb{N}$, then $n \in \mathbb{N}$.

Theorem 102 (Irreflexivity for Order on $\mathbb{N}$): If $n \in \mathbb{N}$, then $\neg(n < n)$

Theorem 103 (Successor Cancels): Assume that $n, m \in \mathbb{N}$.
(1) If $\text{next}(m) < \text{next}(n)$, then $m < n$
(2) If $\text{next}(m) = \text{next}(n)$, then $m = n$.

Theorem 104 (Trichotomy for Order on $\mathbb{N}$): Assume that $n, m \in \mathbb{N}$. Then either $m < n$, $n < m$, or $m = n$, and only *one* of these conditions holds. That is,
(1) $(m = n) \ \vee \ (m < n) \ \vee \ (n < m)$.
(2) $\neg(m = n \ \wedge \ m < n)$.
(3) $\neg(m = n \ \wedge \ n < m)$.
(4) $\neg(m < n \ \wedge \ n < m)$.

Definition 105 (Minimum): Given $A \subseteq \mathbb{N}$, we say that n *is a minimum of* A if and only if $n \in A$ and $(\, \forall a \restriction a \in A \ \Rightarrow \ n \leq a \,)$.

Theorem 106 (Well-Ordering of $\mathbb{N}$): Every nonempty set of natural numbers has a minimum. That is, if $A \subseteq \mathbb{N}$ then

$$A \neq \{\} \Rightarrow (\, \exists n \restriction n \in A \ \wedge \ (\, \forall a \restriction a \in A \Rightarrow n \leq a \,) \,) \,.$$

Theorem 107 (Definition by Recursion - Existence):
If $s \in X$ and $r : X \to X$, then there exists an $f : \mathbb{N} \to X$ such that $f(0) = s$ and

$$(\, \forall n \restriction n \in \mathbb{N} \ \Rightarrow \ f(\text{next}(n)) = r(f(n)) \,) \,.$$

Theorem 108 (Definition by Recursion - Uniqueness):
Assume that $s \in X$ and $r : X \to X$. If
(1) $f, g : \mathbb{N} \to X$,
(2) $f(0) = g(0) = s$,
(3) $(\, \forall n, x \restriction n \in \mathbb{N} \Rightarrow f(\text{next}(n)) = r(f(n)) \,)$, and
(4) $(\, \forall n, x \restriction n \in \mathbb{N} \Rightarrow g(\text{next}(n)) = r(g(n)) \,)$,
then $f = g$.

Definition 109 (Adding One): $\ddagger = \{\, (n, \text{next}(n)) \mid n \in \mathbb{N} \,\}$.

Definition 110 (Adding n): Define $\mathcal{ADD} : \mathbb{N} \to \{\, f \mid f : \mathbb{N} \to \mathbb{N} \,\}$ to be the unique function that satisfies

- $\mathcal{ADD}(0) = \text{id}_{\mathbb{N}}$ and
- $\mathcal{ADD}(\text{next}(n)) = \ddagger \circ (\mathcal{ADD}(n))$ for all $n \in \mathbb{N}$.

Definition 111 (Addition): Assume that $a, b \in \mathbb{N}$. Then we define

$$a + b = \mathcal{ADD}(b)(a).$$

Theorem 112 (Essence of $+$): Assume that $m, n \in \mathbb{N}$. Then

(1) $m + n \in \mathbb{N}$.
(2) $m + 0 = m$.
(3) $m + \text{next}(n) = \text{next}(m + n)$.
(4) $\text{next}(n) = n + 1$.
(5) $m + (n + 1) = (m + n) + 1$.

Theorem 113 (Properties of $+$): Assume that $m, n, k \in \mathbb{N}$. Then

(1) $m + (n + k) = (m + n) + k$ (associativity for $+$)
(2) $n + 0 = n$ (0 is a right-identity for $+$)
(3) $0 + n = n$ (0 is a left-identity for $+$)
(4) $1 + n = n + 1$ (preliminary to commutativity)
(5) $m + n = n + m$ (commutativity for $+$)
(6) $m < n \;\Rightarrow\; m + k < n + k$ ($+$ respects $<$)
(7) $m + k = n + k \;\Rightarrow\; m = n$ ($+$ cancels under $=$)
(8) $m + k < n + k \;\Rightarrow\; m < n$ ($+$ cancels under $<$)
(9) $m + n = 0 \;\Rightarrow\; (m = 0 \wedge n = 0)$
(10) $m + n = 1 \;\Rightarrow\; ((m = 1 \wedge n = 0) \vee (m = 0 \wedge n = 1))$
(11) $m \leq m + k$
(12) $m \leq n \;\Rightarrow\; (\,\exists j \mid j \in \mathbb{N} \;\wedge\; m + j = n\,)$ (solvability of certain equations)

Definition 114 (Cardinality):

(1) $A \approx B \;\Leftrightarrow\; (\,\exists f \mid f : A \to B \;\wedge\; f \text{ is a bijection onto } B\,)$.
(2) $A \preceq B \;\Leftrightarrow\; (\,\exists f \mid f : A \to B \;\wedge\; f \text{ is injective}\,)$.
(3) $A \prec B \;\Leftrightarrow\; (A \preceq B \;\wedge\; \neg(A \approx B))$.

Theorem 115 :

(1) $A \approx A$ (reflexivity for $\approx$)
(2) If $A \approx B$ then $B \approx A$. (symmetry for $\approx$)
(3) If $A \approx B$ and $B \approx C$, then $A \approx C$. (transitivity for $\approx$)

Theorem 116 :

(1) $A \preceq A$ (reflexivity for $\preceq$)
(2) If $A \preceq B$ and $B \preceq C$, then $A \preceq C$. (transitivity for $\preceq$)

Theorem 117 (Preliminary to Cantor-Schroeder-Bernstein): If $C \subseteq A$ and $A \preceq C$, then $A \approx C$.

Theorem 118 (Cantor-Schroeder-Bernstein, AKA Antisymmetry for $\preceq$): If $A \preceq B$ and $B \preceq A$, then $A \approx B$.

Theorem 119: If $A \preceq B$, then there exists a surjection $g : B \to A$.

Definition 120 (Finiteness):
(1) We say that A *has* n *elements* iff $n \in \mathbb{N}$ and $A \approx n$.
(2) A set is *finite* iff it has n elements for some $n \in \mathbb{N}$.
(3) A set is *infinite* iff it is not finite.

Theorem 121 (Element Swap): If $p, q \in A$, then there is a bijection $f : A \to A$ such that $f(p) = q$ and $f(q) = p$.

Theorem 122 ($\preceq$ and $\leq$): If $n, m \in \mathbb{N}$, then

$$n \preceq m \;\Leftrightarrow\; n \leq m.$$

Theorem 123 ($\approx$ and $=$ for Natural Numbers): If $n, m \in \mathbb{N}$, then

$$n \approx m \;\Leftrightarrow\; n = m.$$

Theorem 124 (Finite Choice - Preliminary Version): If $n \in \mathbb{N}$ and $f : A \to n$ surjectively, then there exists $g : n \to A$ such that $f \circ g = \mathrm{id}_n$.

Theorem 125 (Finite Choice): If X is finite and $f : A \to X$ surjectively, then there exists $g : X \to A$ such that $f \circ g = \mathrm{id}_X$.

Theorem 126 : If X is finite and $f : A \to X$ surjectively, then $X \preceq A$.

Theorem 127 (Adding One Element):
(1) If X has n elements and $a \notin X$, then $X \cup \{a\}$ has $n + 1$ elements.
(2) If X is finite, then $X \cup \{a\}$ is finite.

Theorem 128 (Subsets Inherit Finiteness - Preliminary Version): If $n \in \mathbb{N}$ and $S \subseteq n$, then S is finite.

Theorem 129 (Images Inherit Finiteness): If $f : A \to B$, $X \subseteq A$, and X is finite, then $f[X]$ is finite.

Theorem 130 (Subsets Inherit Finiteness): If X is finite and $S \subseteq X$, then S is finite.

Theorem 131 ($\cup$ and $+$): If the set X has n elements, the set Y has m elements, and $X \cap Y = \{\}$, then $X \cup Y$ has $n + m$ elements.

Theorem 132: Assume that $n \in \mathbb{N}$ and $f : n \to n$. If f is injective, then f is surjective onto n.

Theorem 133 (Infinitude of $\mathbb{N}$): $\mathbb{N}$ is infinite.

Definition 134 (Countability): A set A is said to be *countably infinite* iff $A \approx \mathbb{N}$.

Theorem 135 (Hilbert's Hotel): $\text{next}(\mathbb{N}) \approx \mathbb{N}$.

Definition 136 (Even and Odd):

(1) n is *even* iff $n = k + k$ for some $k \in \mathbb{N}$.
(2) n is *odd* iff $n = k + k + 1$ for some $k \in \mathbb{N}$.

Theorem 137 : Every natural number is either odd or even.

Theorem 138 : A natural number cannot be both odd and even.

Theorem 139 : If $k, \ell \in \mathbb{N}$ and $k + k = \ell + \ell$ then $k = \ell$.

Theorem 140 (Doubling Countable Infinity): $2 \times \mathbb{N} \approx \mathbb{N}$.

Theorem 141 (Squaring Countable Infinity): $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

Theorem 142 (Cantor's Theorem): There does not exist a surjection $f : A \to \mathcal{P}(A)$.

Definition 143 (Uncountability): A set A is said to be *uncountably infinite* iff it is infinite, but it is not countably infinite.

Definition 144 (Relations):

(1) R is a *relation on* A if and only if $R \subseteq A \times A$.
(2) When R is a relation on A, we write "xRy" to mean "$(x, y) \in R$."

Definition 145 (Adjectives for Relations): Assume that $\sim \subseteq A \times A$.

(1) $\sim$ is *reflexive* on A iff $a \sim a$ for all $a \in A$.
(2) $\sim$ is *symmetric* iff $a \sim b \Rightarrow b \sim a$ for all a, b.
(3) $\sim$ is *transitive* iff $((a \sim b) \wedge (b \sim c)) \Rightarrow (a \sim c)$ for all a, b, c.
(4) $\sim$ is *antisymmetric* iff $((a \sim b) \wedge (b \sim a)) \Rightarrow (a = b)$ for all a, b.
(5) $\sim$ is *total* on A iff $(a \sim b) \vee (b \sim a)$ for all $a, b \in A$.

Definition 146 (Special Kinds of Relations): Assume that $\sim \subseteq A \times A$.
(1) $\sim$ is a *preorder* on A iff it is reflexive on A and transitive.
(2) $\sim$ is a *partial order* on A iff it is an *antisymmetric* preorder on A.
(3) $\sim$ is a *total order* on A iff it is a *total* partial order on A.
(4) $\sim$ is an *equivalence relation* on A iff it is a *symmetric* preorder on A.

Definition 147 (Equivalence Class): Assume that $\sim$ is an equivalence relation on A and $a \in A$. Then we define

$$[a]_\sim = \{\, x \mid x \sim a \,\}$$

and we call this the *equivalence class of* a, or the *equivalence class of* a *modulo* $\sim$. If the relation involved is clear from context, then we may simply write $[a]$ instead of $[a]_\sim$.

Definition 148 (Set of Equivalence Classes): Assume that $\sim$ is an equivalence relation on A. Then we define

$$A/\sim \;=\; \{\, [a]_\sim \mid a \in A \,\}.$$

Definition 149 (Partition): A set $\mathcal{F} \subseteq \mathcal{P}(A)$ of subsets of A is a *partition of* A iff
(1) $\{\} \notin \mathcal{F}$,
(2) $(\forall a \mid a \in A \Rightarrow (\exists F \mid F \in \mathcal{F} \;\wedge\; a \in F))$, and
(3) $(\forall F, F' \mid F, F' \in \mathcal{F} \;\Rightarrow\; (F \neq F' \;\Rightarrow\; F \cap F' = \{\}))$.

Theorem 150 (Correspondence between Equivalence Relations and Partitions): Given a set A, define

$$\begin{aligned} \mathcal{E} &= \{\, \sim \mid \sim \text{ is an equivalence relation on } A \,\} \\ \mathcal{P} &= \{\, \mathcal{F} \mid \mathcal{F} \text{ is a partition of } A \,\} \end{aligned}$$

and define a function f on $\mathcal{E}$ by

$$f(\sim) = A/\sim \qquad \text{for all } \sim \in \mathcal{E}.$$

Then $f : \mathcal{E} \to \mathcal{P}$ bijectively.

Theorem 151: The following relation on the set $\mathbb{N} \times \mathbb{N}$ is an equivalence relation:

$$\{\, ((n,m),(k,l)) \mid n,m,k,l \in \mathbb{N} \;\wedge\; m+k = l+n \,\}.$$

Definition 152 (Integers): Let $\sim$ be the equivalence relation on $\mathbb{N}\times\mathbb{N}$ defined in Theorem 151. We define

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