A Beginning, a Muddle, and an End

An Introduction to Proofs

A Beginning, a Muddle, and an End

An Introduction to Proofs

Robert Vandermolen
Saint Mary-of-the-Woods College

Faith Molnar

January 1, 2025

[1] creativecommons.org/licenses/by-sa/4.0

Preface

The purpose for the course/book is to help the student that is about to transition from the traditional calculative courses, such as the calculus sequence, and begin their journey into the more abstract mathematics where proofs become prevalent.

Most students that would venture this far into the mathematics major have been enjoying these calculative classes, enjoying the comfort of an algorithm. Perhaps they were the student that loved Calculus III, where they pictured three dimensional shapes and loved the visualization. Whatever it was I have seen far too many students then reach the more "rigorous" classes and loose interest, change majors or just stop enjoying mathematics. In my opinion this is just a shame! And this text tries to give students an algorithm to hold on to as they move deeper and deeper into the muddle.

This transition from calculative to proving is why I choose instead of a combinatorial based course, such as discrete mathematics, we take our trip in the calculus student's favorite past time of numbers. So the student can rest assured that numbers are at the forefront of this course, even though we are exploring new and exciting paths where numbers may not take a leading role.

To the Teacher:

I don't know how you stumbled upon this book, but if you are reading this you are most likely deciding if you should adopt this textbook in your class. I'll save you the work: DO IT!

What? Are you still reading? Ohhh... you want more of an explanation. Well, first this book is free, stop making your students pay for expensive books!

Still here I see... You are more discerning. Well if you want to know if my exercises are of your taste, I assure you I broke no molds in the exercises. In this textbook Students will prove the traditional even, odd, divides, etc.

Wait... you are still reading... ok people might ask what you are doing... quick giggle and say:

"that's a funny tiktok"

That was close... didn't want your colleagues walking by to think you actually cared about student learning... so you want to know if this is different than those other introduction to proofs books... Well let me tell you a story...

I've had nights out at conferences with fellow mathematicians and have listened to these brilliant mathematicians lament on not understanding the purpose of a course on proof writing. And when these pillars of our mathematics community ever taught such a class it was with the outlook that someone learned to write proofs by seeing a lot of proofs. So the instructor would show off some proofs never really motivating why or how one would move from one line to the next then grab some questions from the exercise section and just hope their students would figure it out.

By my flippant description of this interaction you probably put together

that I don't feel this way. I feel like students can be led on the proving journey the same as they are led on their calculative journey. Just more care should be taken. I have attempted to create a text that allows the instructor to just "follow the chapters" in their present order and hopefully give the student's this journey!

Ok... but you are still reading... Yes, you may be asking why are my examples so "basic" I never once mention derivative like the popular texts in this subject by the big publishers... well this is because I save that for analysis... in this course I am just trying to introduce proving not introduce topics that cannot be picked up (almost) immediately. While these pithy examples can mislead the students that are still trying to "just get the answer" it is my hope that the treatment of these examples is what sets it apart.

Now, if you are curious of my ethos/outlook on proofs or that of advanced/ abstract mathematics to see if it aligns with yours and you have yet been scared away by this preface, then I can only assume that you either know me personally and are wondering if this rampant rambling will ever end or did he just blindly type on a keyboard and expect no one to ever read this. But perhaps brave traveler you are like me and are actually wondering...

How do you teach someone how to prove?

If you continue to read you will see that I wax poetic about undefined terms and tracing back conclusions to our assumptions, axioms and definitions... if this is all true then why not just teach a student to prove with a course in geometry? Or if this approach is too archaic start with a discrete math course where you can introduce them to fun brand new concepts like graphs and latin squares where they can start from first principles?

These are both amazing thoughts and in my personal opinion amazing classes, yet to go a little deeper than I had earlier in this preface, to me a discrete math course can take a lot of time playing with and learning these new concepts and the proofs are a side-kick to the combinatorics, which is awesome to the combinatorics lover, and this indeed can often soften the blow between the calculus and the notorious math major courses, but only slightly as the student still feels lost in their algebra and analysis and what happens a lot is the student shy's away from these subjects and clings to combinatorics where they first got those *good grades* or where they first felt *smart*. Yet, in this weird class which *feels like* it teaches them nothing new, its real goal is to make them look at the things they already knew differently, by giving them their college algebra to play with not only for a *safety blanket* ()as I will quite often refer to it) but in hopes to give them the space and time needed to see the deepness of the pond of proofs they are now peering into.

But... of course the critical reader, as I am sure you are, combined with years of mathematical knowledge, as I also assume you have, might just say: "wait isn't this just a baby's first number theory course?"

To which I scoff, a scoff more deeply than I have ever scoffed...

If you have read this far, I'm sure you have already looked me up... but I'm definetly not a number theorist... sorry in advance!

Contents

Chapter 0

What is a Proof?

We begin our journey at the beginning...

For the instructor: this chapter can be safely skipped!

0.1 In the Beginning We Had Shapes

As was true in ancient Athens, seems to ring true still in our sacred halls of academia, even more true after Bourbaki came in with their wrecking ball, and that is:

ΑΓΕΩΜΕΤΡΗΤΟΣ ΜΗΔΕΙΣ ΕΙΣΙΤΩ

Of course if that was "all Greek to you," do not fret fair Caesar, that was simply the author paying tribute to those that came before...

The history of math books are littered with reference to tax collectors and assessors, but besides the lousy adjectives that we call numbers we have had ***Geometry!***

0.2 Undefined Terms

It is our intention to be able to agree, beyond a shadow of doubt, on the truth of a litany of statements. These agreements are called proofs. As one first ventures on this journey they often take many things for granted, perhaps the most important is that we have a mutual agreement/understanding of the words and symbols being used in the discourse. This is easier said than done, as when one is defining a word they must of course use *more words*, then those words would of course need even more *words* to define them... and so on.... and so forth.

When would this pattern end? To ever have a discussion that went forward we would eventually need to stop. The *stopping* words, are commonly referred to as ***undefined terms***. For example, the almost universally agreed upon undefined terms for geometry are: **point**, **line**, and **incident**.

Surprisingly, as Aristotle had already explained the necessity of undefined terms, Euclid did attempt to define the words such as point and line. Luckily this did not effect his discourse as the definitions were vague and used at best to visualize a geometry rather than fix them with an immutable meaning.

0.3 Axioms

After we have all agreed on the undefined terms we would then need to set some *ground rules*. These rules that our new undefined terms must follow are known as **axioms**. Using our geometry example from above, one common axiom of euclidean geometry is:

1. For any two points there exists a line incident to both.

The etymology of the word axiom comes from a Greek word meaning to require. I find this apropos as axioms are required - otherwise we would have no footing to begin a discourse.

0.4 Definitions

Now once we have our undefined terms and axioms, we begin building perhaps the most important part of all proofs: the **definitions**. It is one of the ***major take-aways*** from this course that I would like the student to understand the importance of a definition. You can only prove something is true when you know that thing, when you know that thing's definition.

0.5 Proofs

There are two interpretations of what has been presented before you. One, hopefully how it has been presented here, is that of there is no other way one could argue/debate without this structure. Otherwise, a party could simply keep going backwards and backwards with no assumptions/axioms to back stop the debate.

The other point of view, perhaps most popular in textbooks, is to call this approach **deductive reasoning**, and draw contrast to that of **inductive reasoning**. Some how pitting the two against each other. The epitome of physicists versus mathematicians. Even, applied mathematicians vs theoretical mathematicians.

The differences attempting to be drawn between the world we have just set forward and that of collecting data and observing specific instances or phenomena, striving to form a theory, ***a model***, that reveals patterns or relationships among quantities and structures in nature. This process labeled as inductive reasoning, drawing general conclusions from particular cases/patterns. Which is supposed to be in stark opposition to deductive reasoning, where we draw conclusions based on statements accepted as true, our axioms and undefined terms. After which proofs are built, to ensure that conclusions are drawn logically to arrive at truth. Yet, it is impossible to separate these. It is the phenomena of our surrounding universe that Euclid yearned to define and describe in his geometries.

Yet, do not take these abstractions as something to be taken for granted. To quote Russell, "It is only at a high stage of civilization that we could take this series as a starting point". Or perhaps to quote another, "undoubtedly it took a million years to get the taste of an oyster just right".

In this class we will not explore the amazing world of tracing back every single conclusion to an undefined term or axiom, but instead we will start with A LOT of assumptions, assumptions students at this stage are used to making, namely "college algebra". Then later we will use fewer and fewer assumptions, only dipping our toe in the *endless* pond of abstraction.

0.6 Just Check a Bunch

Students are probably most familiar with the natural and social sciences, where theories are tested by comparing what happens in experiments to what was predicted, and checking that the results stay the same when the experiment is repeated. In math, often, the goal is to figure out whether a statement is always true. Even if a statement works for a lot of examples, there's still the chance that one example we haven't tested could show it's false. For example, you might notice that the expression

This example is inspired by an example that I absolutely fell in love with. I first came across the inspirational example in Smith, Douglas, Maurice Eggen, and Richard St Andre. "A transition to advanced mathematics." (1983).

$$x^2 - 7x + 53$$

produces a prime number for *many* values of x. The diligent student will check that for the first 10, 20, 30 or even 40 positive integers when we substitute our number for x we arrive at a prime number such as

$$(4)^2 - 7(4) + 53 = 41$$

which is prime! If this hard working student were to check with other numbers like 41, 42, and 43 they would also discover prime numbers as the solution.

However, this is not a conclusive proof, as it fails for $x = 44$, where the result is 1681, which is actually a square, that is it factors as 41×41.

I know for almost all of you, at least at one time in your life, it is enticing to just try specific examples. As well, it is undeniable that exploring these examples can, at times, offer valuable insights into mathematical concepts and relationships, it is not sufficient as a proof unless every possible case can be examined.

0.7 Obviously

When writing a proof a challenging task is to decipher what is obvious. The rule I make in my class is that you should write so that ANYONE in the class would have no questions to how you got to the next step.

Just to make things extra fun (and by fun, I mean slightly confusing), there will be moments when I'm pretty sure every single one of you will look at a step and think, "Well, obviously!" But then the next homework assignment will be to prove that very statement.

There will be moments where you are absolutely NOT allowed to just say, "Oh, that's obvious!" Furthermore, I will be very clear (especially at the beginning) on what you are allowed to take as given/obvious and everything else must be proven!

Chapter 1

Introduction to Logic

In this chapter we will see the foundation of proofs, namely propositional logic. Logic has become so prevalent in an invisible way as it is the underlying language of the technology that has began running our lives.

In more of a historical context logic was the primary tool for the original philosophers and debaters. The study of propositional logic teaches you how to argue! It is in simpliest terms the study of truth.

With that said, in propositional logic we have only 2 options:
True or ***False***
The quintessential ***1*** or ***0*** of computers.

Note 1.0.1 This chapter is quite verbose and the student has time early on in the course to find great algrorithms like truth tables, but these quick and low hanging algorithms have the danger of distracting the student from actually learning this bedrock portion of proofs, and treating this like their calculus class where they only *listen* when an example of algorithm is put on the jukebox.

1.1 Propositions and Connectives

I have heard many students say things like "I'm a math major not an English major". This sentiment becomes further and further from the truth as you continue your journey in the major of mathematics. For one, you begin to see mathematics as a language itself with its own grammar and rules, and in particular in this course you begin to only write paragraphs in exchange for the string of symbols and numbers from your calculus courses. As we begin our journey into abstract mathematics we need to do the exact opposite of this sentiment, and instead examine how language works, specifically how language handles truth.

In English, as in many languages, there are many types of sentences, some more complicated than others. We will now be concerning ourselves with if a sentence is true. This is the hallmark of proving, by only writing sentences that are true, so that our conclusions are then true.

1.2 Propositions and Negation

Even though many statements/sentences can be true or can be false, it doesn't make sense to say that any sentence that you could write is true or not. For example a *question* such as *"Where is my phone?"* or an *exclamation* like *"Oh*

No!". Both of these examples are indeed complete sentences, as in they express a complete thought, but are neither true nor false.

Definition 1.2.1 Proposition. A **proposition** is a sentence that can take only one of two values: truth or false. ◊

Example 1.2.2 Some Examples of Propostions. The following are examples of propositions:

(A) $2 + 5 = 4$

(B) The gazel will become the only living animal on earth by the year 2525.

(C) Galileo Galilei had bacon on his eleventh birthday.

□

Some propositions, like (A) in Example 1.2.2, p. 5 have clear truth values, that is we can easily determine if the statement is either True or False (but not both). Perhaps, to untangle the last sentence, it is clear that (A) in Example 1.2.2, p. 5 is False.

Yet, the remaining (B) and (C) in Example 1.2.2, p. 5, cannot be easily determined if they are True or False (unless of course you are reading this after 2525) but nonetheless they are either True or False (and not both) whether or not we can determine which one.

Example 1.2.3 Some Examples of Sentences that are not Propositions. The following are sentences that are NOT propositions:

(A) Stop!

(B) She has my phone.

(C) $x + 2 = 4$

(D) This sentence is false.

□

For examples (B) and (C) in Example 1.2.3, p. 5 are not propositions because (B) depends on who "She" is to determine its truth value, while in (C) it depends on what "x" is, for example when x is 2 it is True, but when x is 3 it is False. Example (A) from Example 1.2.3, p. 5 is an exclamation and is neither True nor False. Finally, (D) from Example 1.2.3, p. 5 is known as a **paradox**. If the statement "This sentence is false" is true, then by its meaning it must be false. On the other hand, if the given statement is false, then what it claims is false, so it must be true.

In our journey of learning propositional logic we will often find it necessary to discuss arbitrary propositions. To do so we will try and use capital letters such as: P, Q, R, S, and T.

There are many ways to create new propositions from old ones. Our first tool to do just that is the logical **negation**.

Definition 1.2.4 Negation. Given a proposition P,The **negation** of P, denoted $\sim P$, is the proposition

"***not*** P"

$\sim P$ is true exactly when P is false. ◊

It is noteworthy that the symbol $\neg$ can be found in many texts for the negation as well. The negation is simply the opposite of the proposition.

Example 1.2.5 Some Negation Examples.

(A) P: The sky is purple.

$\sim P$: The sky is not purple.

(B) P: It is raining right now at SMWC.

$\sim P$: It is not raining right now at SMWC.

□

1.3 Connectives and Compound Propositions

In Example 1.2.2, p. 5 the propositions are all **simple** or **atomic** in the sense that they do not have any other propositions as components. **Compound** propositions can be formed by using connective words, connecting more than one proposition.

Definition 1.3.1 Conjunction. Given propositions P and Q,The **conjunction** of P and Q, denoted $P \wedge Q$, is the proposition:

"P ***and*** Q"

$P \wedge Q$ is true exactly when *both* P and Q are true! ◊

We will see throughout this course that many different words in English can be used for our propositions with the same meaning. For example, but, while, and although are usually translated symbolically with the conjunction connective. An example of this, using the propositions from (A) in Example 1.3.2, p. 6, is we could write "It is not raining outside but I do have my umbrella" symbolically as "$(\sim P) \wedge Q$".

Example 1.3.2 Some Conjunction Examples.

(A) P : "It is raining outside."

Q : "I have an umbrella."

$P \wedge Q$: It is raining outside and I have an umbrella.

(B) P: "Leonardo di ser Piero da Vinci was born in Italy."

Q: "$\frac{\pi}{2}$ is rational."

$P \wedge Q$: "Leonardo di ser Piero da Vinci was born in Italy and $\frac{\pi}{2}$ is rational."

(C) P: "DNA stores information about how to build cells"

Q: "Archaea are prokaryotes"

$P \wedge Q$: "DNA stores information about how to build cells and Archaea are prokaryotes"

□

Definition 1.3.3 Disjunction. Given propositions P and Q,The **disjunction** of P and Q, denoted $P \vee Q$, is the proposition:

"P ***or*** Q"

$P \vee Q$ is true exactly when *at least one of* P or Q are true. ◊

The logical disjunction is often referred to as the **inclusive or**, as it is still true when both propositions are true. In English we often assume the use of the **exclusive or**, that is, when we use the word *or* we most often mean only one of two choices. For example "would you like chicken or steak". When someone

says this to you, you know immediately they do not mean that you can have both chicken and steak, that is not the case for the logical disjunction.

Example 1.3.4 Some Disjunction Examples.

(A) P: 10 is a composite.

Q: 4 is a prime.

$P \vee Q$: 10 is a composite or 4 is prime.

(B) P : "I will do my homework."

Q : "I will watch Star Wars."

$P \vee Q$: "I will do my homework or I will watch Star Wars."

(C) P : "I will do the dishes tonight."

Q : "I am cooking tonight."

$P \vee Q$: "I will do the dishes tonight or I am cooking tonight."

□

1.4 Conditionals and Biconditionals

In the last section we saw a few connectives. Using only these connectives is possible and is all you need for a **complete** logical system, but it ignores an important decree used quite often in logic/debate/mathematics. That is the implication.

1.5 Conditionals

Definition 1.5.1 Conditional. Given a propositions P and Q,the **conditional statement** $P \implies Q$ is the proposition

"If P then Q"

Proposition P is called the **antecedent** and Q is the **consequent**.

The conditional statement $P \implies Q$ is true exactly when P is false or Q is true. ◊

There are many ways of translating the conditional to english statements, which we will in the next table but perhaps the most popular is **implies**, that is "P implies Q".

$P \implies Q$:	Example:
If P then Q	If I am cooking tonight then I will do dishes
P implies Q	The water temperature is 100°C implies the water is boiling
P is sufficient for Q	The water temperature is 100°C is sufficient for the water is boiling
P only if Q	I am cooking tonight only if I will do the dishes
Q, if P	The water is boiling if the water temperature is 100°C
Q whenever P	The water is boiling whenever the water temperature is 100°C

Q is necessary for P	The water is boiling is necessary for the water temperature is 100°C
Q when P	The water is boiling when the water temperature is 100°C
Since P we get Q	Since we have seen that 4 is even we get that 2 divides 4.

I have found the truth values of this connective to be the most challenging for students. To help I suggest the student always think of the next example.

Example 1.5.2 The Lying Politician. P: I am elected
Q: I will lower taxes
$P \implies Q$: If I am elected then I will lower taxes.
So when is politician lying?
There are a couple of cases:

1. The politician is indeed elected:
   (a) The politician lowers taxes!
   The politiciian is not lying!
   (b) The politician does not lower taxes
   The politician is lying!
2. The politician is not elected:
   (a) The politician works hard with community leaders and lobbies to get taxes lowered
   The politician is not lying!
   (b) The politician sits on their couch all day eating Fruit Loops, and taxes are not lowered
   The politician is not lying!

□

Students seem to have the hardest time seeing that when the politician is not elected their is no obligation to do anything and hence the politician is not lying!

1.6 Biconditionals

Definition 1.6.1 Biconditional. Given a propositions P and Q,the **biconditional statement** $P \iff Q$ is the proposition
"P if and only if Q"
The biconditional statement $P \iff Q$ is true exactly when P and Q have the same truth value. ◊

Instead of writing "if and only if" we will often elect to only type ***"iff"***. Just as with the implication, the biconditional has many english translations:

$P \iff Q$:	Example:
P if and only if Q	I will buy dinner if and only if you buy the movie tickets
P if, but only if Q	The water temperature is 100°C if, but only if the water is boiling
P is equivalent to Q	The water temperature is 100°C is sufficient for the water is boiling

P is necessary and sufficient for Q	I am cooking tonight is necessary and sufficient for you to do the dishes

It is this biconditional that I believe many students hear when they hear the phrase: "If I am elected then I will lower taxes". When indeed they mean "Taxes will be lowered if, but only if I am elected".

1.7 Truth Tables

So far we have always looked at actual sentences, even when a letter like P was introduced it was immediately followed by an actual statement.

To recall our journey is to show/find the truth of statements, most often referred to as proofs. In this journey we will need to combine propositions which we already know their truth value to arrive at new propositions which we want to be true. To be able to do this we need to be able to know how combining different propositions with our connectives effect their truth value (truthiness). To keep track of this we now introduce truth tables.

1.8 Basic Tables

In a **truth table** we take arbitrary propositions indicated by letters, such as P, Q, R, S, and T, and consider all the cases of each being either True (T) or False (F). We then explore how coming them with connectives changes the truth value of the compound propositions.

We will call these arbitrary propositions/compound propositions, **propositional forms**. These propositional forms do not have a truth value. Instead, each form has a list of truth values that depend on the values assigned to its components. This list is displayed by presenting all possible combinations for the truth values of its components in a truth table.

To do this we will need to first be able to collect all the combinations of truth values of the basic components of a compound proposition. So for example, if the compound proposition has two components, lets name them P and Q then all combinations are:

P	Q
T	T
T	F
F	T
F	F

Figure 1.8.1

Now to see everything together we will begin with a couple of simple ones, first the conjunction ($P \wedge Q$). Since the conjunction involves two components (P and Q) their truth tables must include all combinations of their two truth values, just as collected above in figure Figure 1.8.1, p. 9.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Figure 1.8.2

Next the disjunction ($P \vee Q$). Since the disjunction also only involves two components (P and Q) their truth tables must again include all combinations of their two truth values, just as collected above in Figure 1.8.1, p. 9.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Figure 1.8.3

Next, we will see the truth table for the negation, $\sim P$. Since the negation only involves one component (P) we simply need the two truth values that P can obtain.

P	$\sim P$
T	F
F	T

Figure 1.8.4

Now, we see the implication, $P \implies Q$ in action. Again this has two components so we must list them all.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Figure 1.8.5

P	Q	$\sim P$	$(\sim P) \implies Q$
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

Figure 1.8.6

An important one is that of the biconditional, which we use as the word equivalent, this table shows us that this is an apt word use.

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

Figure 1.8.7

1.9 More Complicated Tables

Now let's dive into more complicated examples. As our examples get more complicated, I suggest that the student take time to break-it-down. That is

to create extra columns that are themselves components of compound propositions. A simple example of this is the compound proposition:

$$(\sim P) \implies Q$$

This example has only two *basic* components, namely P and Q. Yet, notice that the antecedent is $\sim P$, this is what I suggest you create a new column for namely after you make your P column and you Q column, then before you make your final column add a $\sim P$ column

P	Q	$\sim P$	$(\sim P) \implies Q$
T	T	F	
T	F	F	
F	T	T	
F	F	T	

Figure 1.9.1

Next, you can complete the table by only looking at the $\sim P$ and Q columns as they are the only ones now involved in the compound proposition $(\sim P) \implies Q$

P	Q	$\sim P$	$(\sim P) \implies Q$
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

Figure 1.9.2

For an even more complicated example consider:

$$(P \vee Q) \wedge (\sim (P \wedge Q))$$

This has two major pieces namely $P \vee Q$ as well as $P \wedge Q$. Again the atomic pieces are P and Q so we begin with our standard two columns, then we include a column for each of these major pieces:

P	Q	$P \vee Q$	$P \wedge Q$
T	T	T	T
T	F	T	F
F	T	T	F
F	F	F	F

Figure 1.9.3

Now recall that we are trying to build a table for

$$(P \vee Q) \wedge (\sim (P \wedge Q)).$$

The next major piece we see is that of $\sim (P \wedge Q)$

P	Q	$P \vee Q$	$P \wedge Q$	$\sim (P \wedge Q)$
T	T	T	T	F
T	F	T	F	T
F	T	T	F	T
F	F	F	F	T

Figure 1.9.4

Finally, we can simply look at the cells $P \vee Q$ as well as $\sim (P \wedge Q)$ to finish our table for:

$$(P \vee Q) \wedge [\sim (P \wedge Q)]$$

P	Q	$P \vee Q$	$P \wedge Q$	$\sim (P \wedge Q)$	$(P \vee Q) \wedge [\sim (P \wedge Q)]$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

Figure 1.9.5

From now on we will only show the finished tables.

Another way of making a more complicated table is to have a compound proposition which involves three atomic propositions: P, Q, and R. In this case all of the possible combinations of true and false are the following:

P	Q	R
T	T	T
T	T	F
T	F	T
T	F	F
F	T	T
F	T	F
F	F	T
F	F	F

Figure 1.9.6

Now we can do an example like

$$(P \wedge R) \implies Q$$

P	Q	R	$P \wedge R$	$(P \wedge R) \implies Q$
T	T	T	T	T
T	T	F	F	T
T	F	T	T	F
T	F	F	F	T
F	T	T	F	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

Figure 1.9.7

1.10 Tautologies and Contradictions

One of the strongest tools in proving are propositional statements that are either always true or always false.

Definition 1.10.1 Tautology. A **tautology** is a propositional form that is true for any assignment of truth value to its components ◊

One of the most famous, and most meme'd is the **Law of the Excluded Middle**, $P \vee (\sim P)$, which is a tautology. It is the classic "to be or not to be", "today I will do my homework or I will not". We can use a truth table to see that this statement is always true.

P	$\sim P$	$P \vee (\sim P)$
T	F	T
F	T	T

Figure 1.10.2

Another example, that may not immediately be as obvious is for

$$(P \vee Q) \vee [(\sim P) \wedge (\sim Q)]$$

P	Q	$P \vee Q$	$\sim P$	$\sim Q$	$(\sim P) \wedge (\sim Q)$	$(P \vee Q) \vee [(\sim P) \wedge (\sim Q)]$
T	T	T	F	F	F	T
T	F	T	F	T	F	T
F	T	T	T	F	F	T
F	F	F	T	T	T	T

Figure 1.10.3

Definition 1.10.4 Contradiction. A **contradiction** is a propositional form that is false for any assignment of truth value to its components ◊

For an example of a contradiction is the famous $P \wedge (\sim P)$, this is the classic "I will go to bed early and I will not go to bed early".

P	$\sim P$	$P \wedge (\sim P)$
T	F	F
F	T	F

Figure 1.10.5

Another example of a contradiction is: $\sim [P \vee (\sim P)]$, that is of course just a negation of a tautology.

P	$\sim P$	$P \vee (\sim P)$	$\sim [P \vee (\sim P)]$
T	F	T	F
F	T	T	F

Figure 1.10.6

1.11 Logical Equivalences

In this course students will often treat this beginning material of propositions and truth tables as not connected to the proofs, and just a way to get some good grades on early homework. I cannot blame the student for this, when thrown into an unknown world it is hard to hold on to everything.

Yet, we will now dive into equivalences. In the world of proving it may often be difficult to prove a statement how it appears in the homework, or how you first discovered it, but if you were to simply re-word it, now it becomes simpler to prove. These reworkings are the equivalences.

1.12 What is an equivalence?

Definition 1.12.1 Logically Equivalent. Two propositional forms are **logically equivalent** (or just **equivalent**) if and only if they have the same truth values. ◊

The notation, we will use, for two propositional forms begin equivalent is: $P \equiv Q$

To show that two propositional forms are indeed equivalent at the beginning we only have the tool of truth tables at our disposal. What we will see in this first example is that no matter our choice of truth value for P that $\sim (\sim P)$ we have the same truth value, that is

$$P \equiv \sim (\sim P)$$

Example 1.12.2

P	$\sim P$	$\sim (\sim P)$
T	F	T
F	T	F

Figure 1.12.3

□

For another example lets see if

$$[P \implies Q] \equiv [(\sim P) \vee Q]$$

Example 1.12.4

P	Q	$(P \implies Q)$	$\sim P$	$[(\sim P) \vee Q]$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Figure 1.12.5

Thus we see that the truth values are the same for $[P \implies Q]$ and $[(\sim P) \vee Q]$! □

1.13 Some Important Equivalences

There are a number of logical equivalences that are *very* important to become familiar with. We will build some of these truth tables for you, and leave the rest for exercises.

Augustus De Morgan (27 June 1806 - 18 March 1871) was a British mathematician and logician. He is best known for De Morgan's laws, relating logical conjunction, disjunction, and negation, and for coining the term "mathematical induction", the underlying principles of which he formalized. De Morgan's contributions to logic are heavily used in many branches of mathematics, including set theory and probability theory, as well as other related fields such as computer science.

∗information from Wikipedia∗

Theorem 1.13.1

- $\sim(\sim P) \equiv P$ — *Double negation Law*
- $P \wedge Q \equiv Q \wedge P$ — *Commutativity Laws*
- $P \vee Q \equiv Q \vee P$
- $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$ — *Distributivity Laws*
- $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

- $P \vee P \equiv P$ — *Absorption Laws*
- $P \wedge P \equiv P$
- $\sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q)$ — *DeMorgan's Law*
- $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$
- $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$ — *Associativity Laws*
- $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
- $[P \implies Q] \equiv [(\sim Q) \implies (\sim P)]$ — *Contrapositive*
- $P \implies Q \equiv (\sim P) \vee Q$ — *Rob's Law*

Proof. We saw the double negation law in Example 1.12.2, p. 14.
Next we will build the truth tables for two important ones, namely Rob's Law and contrapositive, then leave the rest as an exercise.

P	Q	$P \implies Q$	$\sim P$	$\sim Q$	$(\sim Q) \implies (\sim P)$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	T	T
F	F	T	T	T	T

Figure 1.13.2

P	Q	$P \implies Q$	$\sim P$	$(\sim P) \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Figure 1.13.3

■

1.14 The Algebra of Logic

Now that we have established the laws in Theorem 1.13.1, p. 15 we have a new way to prove two propositional forms are equivalent. It is what I playfully refer to as the algebra of logic.

Example 1.14.1 For a first example of this lets see a proof that

$$[(P \vee Q) \implies R] \equiv [(P \implies R) \wedge (Q \implies R)]$$

Proof.

$$\begin{aligned}
(P \vee Q) \implies R &\equiv [\sim (P \vee Q)] \vee R \text{ (Rob's Law)} \\
&\equiv [(\sim P) \wedge (\sim Q)] \vee R \text{ (De Morgan's)} \\
&\equiv R \vee [(\sim P) \wedge (\sim Q)] \text{ (commutativity)} \\
&\equiv [R \vee (\sim P)] \wedge [R \vee (\sim Q)] \text{ (distributivity)} \\
&\equiv [(\sim P) \vee R] \wedge [(\sim Q) \vee R] \text{ (commutativity)} \\
&\equiv [(P \implies R) \wedge (Q \implies R)] \text{ (Rob's Law)}
\end{aligned}$$

■
□

There are many examples for you to try in this chapter's exercises, but we will leave you with one more example.

Example 1.14.2

$$[P \implies (Q \implies R)] \equiv [(P \wedge Q) \implies R]$$

Proof.

$$\begin{aligned}
[P \implies (Q \implies R) &\equiv [(\sim P) \vee (Q \implies R)] \text{ (Rob's Law)} \\
&\equiv [(\sim P) \vee ((\sim Q) \vee R)] \text{ (Rob's Law)} \\
&\equiv [(\sim P) \vee (\sim Q)] \vee R \text{ (associativity)} \\
&\equiv \sim (P \wedge Q) \vee R \text{ (DeMorgan's)} \\
&\equiv [(P \wedge Q) \implies R] \text{ (Rob's Law)}
\end{aligned}$$

■
□

1.15 Quantifiers

It is now time to take care of those statements that were not propositions from Example 1.2.3, p. 5, but have probably been bugging you this whole time like: $x + 2 = 4$, which are known as an **open statement** or **predicate**. But, how on earth are we to do mathematics and these sentences not be in our lexicon? To handle these we need to quantify the x, by saying we can find a number so that $x + 2 = 4$. Before quantifying the statement you didn't even need to assume x was a number!

"But Dr. Rob I could tell x was a number by context!"

But, what context was that? Was it that this is a math class and I'm a math professor? Even so, what kind of number? A rational number (fractions)? A positive number? An imaginary number?

1.16 The Universe of Discourse

As many of you have assuredly yelled at the book by now, of course I can determine from context what we are talking about. But this is exactly the point of this next section, that before starting a discussion you must set your context. What we will call our **universe of discourse**.

The universe of discourse is our first example of a **set**.

So that we handle this playground with the respect it deserves, we will only give a very brief introduction to the topic right now, just what we need. We will dive deeper into set theory and use it as one of our major examples later on in the book!

Let's start with the very basics and *define* some things.

- **Set**: A collection of stuff (or nothing).
- **Element**: The stuff in the set.

The elements in a set do not have a particular order, so you can think of a set like a "magical bag" that holds things.

Set theory, like everything, comes with its own special notation. We often denote sets with a capital letter, and elements with a lower case letter.

The symbol $\in$ can be read as "in" or "is an element of" or "is a member of"

For example, "$x \in A$" would be read as "x is in A," or, "x is an element of the set A", or "x is a member of the set A"

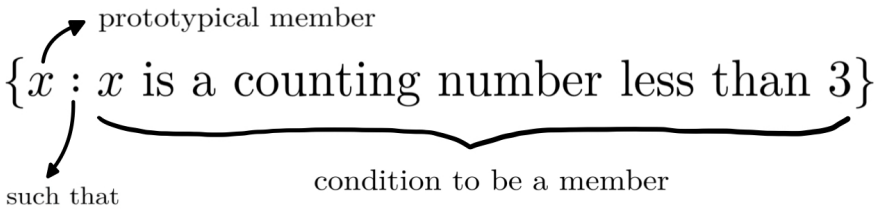
Besides just arbitrarily naming a set in attempts to define a set we can also describe what is the set by capturing all the elements in the set between the symbols { and } then listing the elements separated by commas. For example if we just wanted to collect the following numbers in a set:

$$A = \{3, 7, 8, 9\}$$

Or if we were to collect the set of all counting numbers we could use ... to indicate continuing a pattern:

$$\{1, 2, 3, ...\}$$

We could also use what is known as set builder notation:



1.17 Common Universes

Throughout the text we will use a lot of common universes in our text, but also to really drive home the wide application of these theories we will use some less common universes as well. The most common universes we will deal with is the numbers, by which we will mostly discuss the following:

$\mathbb{N} = \{0, 1, 2, 3, ...\}$		The Natural Numbers
$\mathbb{Z}$ $\{..., -3, -2, -2, 0, 1, 2, 3, ...\}$	=	The Integers
$\mathbb{Z}^+ = \{1, 2, 3, ...\}$		The Counting Numbers
$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, \text{ with } b \neq 0\}$		The Rational Numbers
$\mathbb{R}$		The Real Numbers
$\mathbb{C}$		The Complex Numbers

Notice that I take the extremely divisive standpoint that $\mathbb{N}$ contains 0. Later in the book we will justify this, but now, I am your teacher and thus you are in my camp on this issue!

1.18 Truth Sets and Predicate Forms

When we are discussing a general universe of discourse we will denote it as $\mathcal{U}$. We will also often need to speak of a predicate in general terms so we will use the *function* notation for predicates. Such as for the predicate $x \geq 3$ we can denote it by $P(x)$. And thus we can now determine that a statement like $P(2)$ which is $2 \geq 3$ is false.

After setting our universe can now talk about the **truth set** of a predicate $P(x)$, that is collecting all of the elements of our universe that make $P(x)$ true.

Example 1.18.1 The truth set for the open sentence "$x^2 < 3$" depends on the universe of discourse. When the universe is set as $\mathcal{U} = \mathbb{N}$ then the truth set is $\{0, 1\}$. When the universe is $\mathcal{U} = \mathbb{Z}$ then the truth set is $\{-1, 0, 1\}$. If the universe was to be $\mathcal{U} = \mathbb{R}$ then the truth set would be the open interval $(-\sqrt{3}, \sqrt{3})$. □

Definition 1.18.2 Equivalent Predicates. For a fixed universe of discord, we say that two predicates, $P(x)$ and $Q(x)$, are **equivalent** iff they have the same truth set.

We will denote this as $P(x) \equiv Q(x)$ ◊

Now lets see an example of this in play with some, perhaps, unexpected results.

Example 1.18.3 The predicates $P(x) : x^2 + 2x = -1$ and $Q(x) : x \leq 1$ are equivalent in the universe $\mathcal{U} = \mathbb{Z}^+$. They are not equivalent in the universe $\mathcal{U} = \mathbb{Z}$. □

This next example should work the way you expected.

Example 1.18.4 The open statements $R(x) : x^2 = 9$ and $S(x) : x = 3$ are equivalent in the universe $\mathcal{U} = \mathbb{N}$ but they again are not equivalent in the universe $\mathcal{U} = \mathbb{Z}$ □

1.19 The Existential Quantifier

Consider the predicate $3x = 12$ is, again, not a proposition as it depends on the universe and which x from this universe we are talking about. But, there is a way of not choosing an x from the universe to turn this into a proposition, that is to consider the statement:

$$\text{There is an } x \text{ such that } 3x = 12$$

This proposition is still treated differently than other propositions we have considered, as it still depends on the universe. This new proposition can be formed from the predicate by applying a quantifier, that is we qualify our open sentence before saying it.

Definition 1.19.1 Existential Quantifier. For a predicate $P(x)$, the sentence

$$\exists x \; P(x)$$

is read

$$\text{"There exists an } x \text{ such that } P(x)\text{"}$$

or

$$\text{"For some } x, \; P(x)\text{"}$$

or

$$\text{"We can find an } x \text{ so that } P(x)\text{"}$$

The proposition $\exists x \; P(x)$ is true iff the truth set of $P(x)$ is nonempty. The symbol $\exists$ is called the **existential quantifier** ◊

One way to show that $\exists x \; P(x)$ is true for a specific universe is to identify an object $a \in \mathcal{U}$ such that $P(a)$ is true.

Example 1.19.2 For this example lets consider the following predicates

(A) $P(x) : x$ loves books

(B) $Q(x)$: x eats pizza

(C) $R(x) : x > 4$

For (C) the statement $\exists x\ R(X)$ is true in the universe $\mathcal{U} = \mathbb{R}$ is true as $4.5 \in \mathbb{R}$ as well as many other numbers. In statement (A) there are no real numbers that have any opinions on books for my understanding, but if the universe was all people then $\exists x\ P(x)$ is true as I am a person and I love books. Similarly for (B) the proposition, $\exists x\ Q(x)$ in the universe of all people is also true, as I also eat pizza! □

In English there are many ways to say the existential quantifier, such as:

- "some"
- "at least one"
- "there is"

and so many more.

I'd like to end this subsection with the symbolization of a statement

$$\text{Some } P(x) \text{ are } Q(x)$$

which should be

$$(\exists x)(P(x) \wedge Q(x)$$

1.20 The Universal Quantifier

The statement "everyone reads books" is being qualified by something different than an exists, yet does have a truth value and hence is a proposition. It is this quantifier that we call the universal quantifier.

Definition 1.20.1 Universal Quantifier. For a predicate $P(x)$, the statement

$$\forall x\ P(x)$$

is read

$$\text{"For all } x\ P(x)\text{"}$$

and is true iff the truth set of $P(x)$ is the *entire* universe. The symbol $\forall$ is called the **universal quantifier**. ◊

In English there are many ways to say the universal quantifier, such as:

- "for all"
- "for every"
- "for each"

and so many more.

Example 1.20.2 For this example lets consider the following predicates

(A) $P(x)$: x loves math textbooks

(B) $Q(x)$: x eats pizza

(C) $R(x) : x > 4$

In (C) for the universe $\mathcal{U} = \mathbb{R}$ the proposition $\forall x\ R(x)$ is false as $2 \in \mathbb{R}$ yet 2 is not greater than 4. For (A) in the universe of all people, the proposition

$\forall x\ P(x)$ is also false as I have met many students who dislike most math textbooks. Similarly for (B) in the universe of all people the proposition $\forall x\ Q(x)$ is also false as I have met a health conscious person who does not eat pizza. □

There are many many many examples of the use of the universal quantifier, but one popular one that I'd like to take a moment to discuss is:

$$\text{All } P(x) \text{ are } Q(x)$$

this can be symbolized by

$$(\forall x)(P(x) \implies Q(x))$$

1.21 Negating Quantifiers

It is also important to note what the negation of each of these quantifiers are.

$$\sim [\exists\ P(x)]$$

read literally says, "There does not exist." Sometimes it is helpful to read this as "everybody doesn't." That is

$$\sim [\exists x\ P(x)] \equiv [\forall x\ (\sim P(x))]$$

$$\sim \forall\ P(x)$$

says "not all," which can be thought of as, "somebody does." That is

$$\sim [\forall x\ P(x)] \equiv \exists x\ (\sim P(x))$$

Example 1.21.1 For these examples we will see multiple ways to write them.

1. $\sim (\forall n \in \mathbb{Z}\ \sqrt{n} \in \mathbb{Z}) \equiv (\exists n \in \mathbb{Z}\ \sqrt{n} \notin \mathbb{Z})$
   - $*$NOT$*$(For all integers n, $\sqrt{n}$ is an integer)
   - For some integers n, $\sqrt{n}$ is not an integer.
2. $\sim (\exists n \in \mathbb{Z}\ n^2 = 5) \equiv [\forall n \in \mathbb{Z}\ n^2 \neq 5]$
   - $*$NOT$*$(There exists an integer n such that $n^2 = 5$
   - For all integers n, n^2 does not equal 5.

□

1.22 Unique Existence

There is a special case of the existential quantifier, that is used when you want to be very clear that there is only one special member of the universe that satisfies your predicate.

Definition 1.22.1 Unique Existential Quantifier. For a predicate $P(x)$, the proposition

$$\exists! x\ P(x)$$

is read

"there exists a unique x such that $P(x)$"

and is true iff the truth set of $P(x)$ has *exactly one* element form the universe. The symbol $\exists!$ is called the **unique existential quantifier**. $\Diamond$

The difference between the existential and unique existential quantifier is the number of elements of the universe that satisfy your open statement.

Example 1.22.2 Consider the next two predicates:

- $P(x) : x$ is even
- $Q(x) : x$ is prime
- $R(x) : x^2 = 4$

The statement

$$\exists! x \ (P(x) \wedge Q(x))$$

is true in the universe $\mathcal{U} = \mathbb{N}$ as the only number satisfying the statement $P(x) \wedge Q(x)$, that is x is even and prime, is $2 \in \mathbb{N}$ The proposition

$$\exists! x \ R(x)$$

on the other hand, is true for the universe $\mathcal{U} = \mathbb{N}$, as the only natural number to satisfy this propostion is 2, but not true for the universe $\mathcal{U} = \mathbb{Z}$ as there are two numbers, namely +2 and -2 in the integers which make the predicate true. $\square$

1.23 More Examples

Now we will give some more examples:

Example 1.23.1

(A) For every Indiana resident x older than 18, x can vote

$$(\forall x)(x \text{ Indiana resident } \wedge x \text{ is older than 18 } \wedge x < 10) \implies x \text{ can vote}$$

(B) Some functions defined at 0 are not differentiable at zero

$$(\exists f)(f \text{ is defined at } 0 \wedge f \text{ is not differentiable at } 0)$$

(C) Some students are math majors and some students are business majors

$$(\exists x)(x \text{ is a math majors}) \wedge (\exists y)(y \text{ is a business major})$$

$\square$

1.24 Exercises

1. Write truth tables for the following:
   (a) $(\sim P) \implies Q$
   (b) $P \iff Q$
   (c) $(P \vee Q) \wedge [\sim (P \wedge Q)]$

(d) $(P \implies Q) \vee Q$
(e) $(P \wedge R) \implies Q$
(f) $(\sim Q) \implies Q$
(g) $P \vee (\sim P)$
(h) $\sim (P \wedge Q)$
(i) $(\sim P) \vee (\sim Q)$
(j) $(\sim P) \implies (R \wedge Q)$

2. Show the remaining laws are from Theorem 1.13.1, p. 15 are true, using truth tables.

3. Use a truth table to show whether the following are or are not equivalent:

(a) $[P \implies ((\sim Q) \wedge R)]$, $[(P \implies (\sim Q)) \vee (P \implies R)]$
(b) $[((\sim P) \vee Q) \implies R]$, $[((\sim R) \implies P) \wedge (Q \implies R)]$
(c) $[(P \wedge (\sim Q)) \implies R]$, $[P \implies (Q \vee R)]$
(d) $[(P \implies Q) \wedge (\sim R)]$, $[(R \vee P) \implies ((\sim R) \wedge Q)]$

4. Turn the first statement into the second one. Show your steps and state which equivalence rule from 1.3.2 you used to get there.

(a) $[P \implies ((\sim Q) \wedge R)] \equiv [(P \implies (\sim Q)) \wedge (P \implies R)]$
(b) $[((\sim P) \vee Q) \implies R] \equiv [((\sim R) \implies P) \wedge (Q \implies R)]$
(c) $[(P \wedge (\sim Q)) \implies R] \equiv [P \implies (Q \vee R)]$
(d) $[(P \implies Q) \wedge (\sim R)] \equiv [(R \vee P) \implies ((\sim R) \wedge Q)]$

5. Consider the statement

$$\exists x \in \mathbb{R} \text{ such that } x^3 = 3.$$

Which of the following are also ways of saying this statement? (identify all that apply)

(a) There is at least one real number whose cube is 3.
(b) The cube of each real number is 3.
(c) Some real numbers have cube 3.
(d) The number x has cube 3, for some real number x.
(e) If x is a real number, then $x^3 = 3$.
(f) Some real number has cube 3.

6. Consider the statement

$$\forall n \in \mathbb{Z} \text{ if } n + 1 \text{ is even then } n \text{ is odd.}$$

Which of the following are also ways of saying this statement? (identify all that apply)

(a) If the sum of an integer and one is even, then that integer is odd.
(b) All integers are even once you add one and are odd.
(c) Given any integer which once adding one is even, that integer must be odd.
(d) For all integers, there are some which you add one then it is even.

(e) Any integer which is even once adding one is odd.

(f) All odd integers are even once adding one.

7. Translate the following English statements into symbolic sentences with quantifiers. The universe for each is given in the parenthetical.

   (a) Not all math students are hardworking. ($\mathcal{U}$ =all students)

   (b) All math students are not hardworking. ($\mathcal{U}$ =all students)

   (c) There is a smallest positive integer ($\mathcal{U} = \mathbb{R}$)

   (d) Some people are happy and some people are not happy. ($\mathcal{U}$ =all people)

   (e) No one loves everybody

8. Rewrite the statement in English without using the symbols $\forall$ or $\exists$. Express your answer as simply as possible. Then write a negation for the statement. Determine which statement is true, the original or the negation.

   (a) $\exists$ a book $b, \forall$ people p, p has read b.

   (b) $\forall$ odd integers $n, \exists$ an integer k such that $n = 2k + 1$.

   (c) $\forall r \in \mathbb{Q}, \exists$ integers a and b such that $r = a/b$.

9. Rewrite the statement formally using quantifiers and variables. Write the negation of the statement.

   (a) Everybody believes somebody.

   (b) Somebody believes everybody.

   (c) Any even integer equals some other integer plus 1.

   (d) The number of rows in any truth-table is 2^n for some integer n.

Chapter 2

How to Argue

One could characterize a proof as arguing to the most skeptical person you have ever met that something is true. Now that we have our logic background, we are ready to start stringing propositions together to make these arguments.

2.1 Arguments

Arguments are so important, they merit their own chapter. They are the essence of your future proofs, these are your "steps" you long for from your calculus class.

2.2 Validness

To begin you give the most general form for these *steps*.

Definition 2.2.1 Argument. The general form of an **argument** is:

$$\begin{array}{c} A \\ B \\ \hline \therefore C \end{array}$$

A and B are the assumptions and C is the conclusion. The symbol $\therefore$ is read "therefore". ◊

Arguments are simply propositions listed in an order, so we will need to make sense of this in our logical framework. To do so so we have the following definition.

Definition 2.2.2 Valid. We will say an argument is **valid** whenever

$$(A \wedge B) \implies C$$

is a tautology. ◊

Definition 2.2.3 Invalid. We will say an argument is **invalid** whenever

$$(A \wedge B) \implies C$$

is a contradiction. ◊

Recall, what it takes for an implication to be true, that is either the antecedent is false or the consequent is true.

Example 2.2.4 Here are some examples of valid arguments:

$$\frac{\begin{array}{c}\text{All parabolas are functions of degree 2}\\ \text{All functions of degree 2 are quadratic}\end{array}}{\therefore \text{All parabolas are quadratic}}$$

$$\frac{\begin{array}{c}\text{An apple is purple}\\ \text{An apple is a fruit}\end{array}}{\therefore \text{An apple is purple}}$$

$$\frac{\begin{array}{c}\text{All spiders have 8 legs}\\ \text{A poodle is a spider}\end{array}}{\therefore \text{A poodle has 8 legs}}$$

Here is an example of an invalid argument:

$$\frac{\begin{array}{c}\text{All chickens are animals that eat corn}\\ \text{All chickens are animals that have wings}\end{array}}{\therefore \text{All animals that eat corn have wings}}$$

□

Notice that it is not the truth of the premises that makes an argument valid or invalid, but rather the truth of the conclusion.

2.3 Arguments with Propositional Forms

In this section we will "pull open the hood" a bit, and explore the inner workings of the arguments with general propositional forms.

We begin with perhaps the most famous arguments. These are surely not the only tools we will use, but definitely some of the more important ones.

Modus Ponens.

Modus Ponens is a specific type of argument with two premises: $P \implies Q$, and P, and concludes Q. That is

$$\frac{\begin{array}{c}P \implies Q\\ P\end{array}}{\therefore Q}$$

An example of this is "If it is raining then the ground is wet. It is raining. Therefore the ground is wet."

Modus Tollens.

Modus Tollens is simply the application of the contrapositive, specifically: $P \implies Q$, and $\sim Q$, and conludes $\sim P$. That is

$$\frac{\begin{array}{c}P \implies Q\\ \sim Q\end{array}}{\therefore \ \sim P}$$

A similar example of this is "If it is raining then the ground is wet. The ground is not wet. Therefore the ground it is not raining."

Even though these happen to be the most famous they are far from the only. Here is a not so complete list:

Argument:	Name:
$\dfrac{P}{\therefore\ P \vee Q}$	Addition
$\dfrac{P \wedge Q}{\therefore\ P}$	Simplification
$\dfrac{\begin{array}{c}P\\Q\end{array}}{\therefore\ P \wedge Q}$	Conjunction
$\dfrac{\begin{array}{c}P \implies Q\\P\end{array}}{\therefore\ Q}$	Modus Ponens
$\dfrac{\begin{array}{c}P \implies Q\\\sim Q\end{array}}{\therefore\ \sim P}$	Modus Tollens
$\dfrac{\begin{array}{c}P \implies Q\\Q \implies R\end{array}}{\therefore\ P \implies R}$	Hypothetical Syllogism
$\dfrac{\begin{array}{c}P \vee Q\\\sim P\end{array}}{\therefore\ Q}$	Disjunctive Syllogism

Figure 2.3.1

Now lets see some examples of these in play.

Now that we have our arguments written using propositional forms we can verify that each of these arguments are valid using a truth table, that is seeing they are all tautologies, or that they are always true.

We will do *Hypothetical Syllogism* and leave the rest as an exercise to the reader.

P	Q	R	$P \implies Q$	$Q \implies R$	$P \implies R$	$[(P \implies Q) \wedge (Q \implies R)] \implies (P \implies R)$
T	T	T	T	T	T	T
T	T	F	T	F	F	T
T	F	T	F	T	T	T
T	F	F	F	T	F	T
F	T	T	T	T	T	T
F	T	F	T	F	T	T
F	F	T	T	T	T	T
F	F	F	T	T	T	T

Figure 2.3.2

Example 2.3.3 For this example lets set a few propositions:

$$P: \text{ It is sunny today}$$
$$Q: \text{ It is colder than yesterday}$$
$$R: \text{ We will go hiking}$$
$$S: \text{ We will go for a bike ride}$$
$$W: \text{ We will be home by dark}$$

Next consider the list of premises.

- $\sim P \wedge Q:$ It is not sunny today and it is colder than yesterday
- $R \implies P:$ We will go hiking only if it is sunny
- $(\sim R) \implies S:$ If we do not go swimming then we will go hiking
- $S \implies W:$ If we go on a bike ride then we will be home before dark

When can then make the following arguments:

(A) To start we will only consider the first premise.

$$\frac{(\sim P) \wedge Q}{\therefore \ \sim P}$$

Since we have assumed that it is not sunny and colder than yesterday we can conclude it is not sunny outside, using conjunction.

(B) Now Let's use the conclusion from (A), with the next premise.

$$\frac{\begin{array}{c}(\sim P) \\ R \implies P\end{array}}{\therefore \ \sim R}$$

That is if we assume that it is not sunny and that we will go hiking only if it is sunny, then we can conclude that we do not go hiking, using Modus Tollens.

(C) Now using the conclusion from (B) and our next premises we see

$$\frac{\begin{array}{c}(\sim R) \\ (\sim R) \implies S\end{array}}{\therefore \ S}$$

Since we have assumed that we are not hiking and that if we don't hike then we will go on a bike ride we can thus conclude that we will go on a bike ride by Modus Ponens.

(D) Now using the conclusion of (C) and our next premise.

$$\frac{\begin{array}{c}S \\ S \implies T\end{array}}{\therefore \ W}$$

Hence since we assumed that we are going on a bike ride and if we go on a bike ride we will be back home by dark we can conclude that we will be back by dark again by Modus Ponens.

We have just done our first proof, and shown if all the statements are assumed then we can conclude that we will be home before dark! □

2.4 The Bad and the Ugly

There are many ways to make a valid argument, and many ways to make an invalid argument. As a student of proofs it is inevitable that you will make all of the mistakes, and find new and amazing ways of making invalid arguments, it is unavoidable. But, don't fret, that is the beautiful learning journey you are on!

A very common mistake that students will make when arguing is what is known as **circular reasoning**.

Catch 22.

Circular reasoning or **begging the question** or **catch 22** happens when we *assume* the statement we are trying to conclude.

The term *Catch 22* was coined by the character Doc Daneeka, an army psychiatrist, in the novel Catch 22, to describe a governmental loophole that prevented pilots from requesting a mental evaluation to avoid dangerous missions.

This fallacy comes from the very valid argument:

$$\frac{P}{\therefore\ P}$$

It's just this argument doesn't get you very far.

Consider the next example of circular reasoning.

Example 2.4.1 Say I was trying to conclude that a number x is even, then circular reasoning would be: "Assume that x is even, thus x is even" □

Another misstep that students are bound to take is almost a misapplication of the contrapositive, or thinking the implication is stronger than it is.

Denying the Antecedent.

Denying the antecedent is the invalid argument

$$\frac{\begin{array}{c}P \implies Q \\ \sim P\end{array}}{\therefore\ \sim Q}$$

Recall that the contraposition is

$$[P \implies Q] \equiv [(\sim Q) \implies (\sim P)]$$

but not $(\sim P) \implies (\sim Q)$.

Example 2.4.2 Consider the statement: "If it is sunny then we will go on a bike ride". We still might go on a bike ride if it's not sunny, I was just saying if it's sunny we will definitely go! □

Another mistake in a similar fashion is again mistaking the power of the implication.

Affirming the Conclusion.

Affirming the conclusion is the invalid argument

$$\begin{array}{c} P \implies Q \\ Q \\ \hline \therefore\ P \end{array}$$

Recall that $Q \implies P$ is NOT the same as $P \implies Q$.

Example 2.4.3 Consider the statement: "If it is sunny then we will go on a bike ride". Just because we go on a bike ride doesn't some how make it sunny, again I was just saying if it's sunny we will definitely go! □

2.5 Arguments with Quantifiers

We have seen in Section 2.1, p. 25 that quantified statements can lead to interesting arguments. For example

$$\begin{array}{c} \text{All } A \text{ are } B \\ \text{All } B \text{ are } C \\ \hline \therefore\ \text{All } A \text{ are } C \end{array}$$

For example "All longshoremen are in a union" and "All unions have dues" thus we can conclude that "All longshoremen pay dues".

Next we have a far from complete list:

Argument:	Name:
$\dfrac{\forall x\ P(x)}{\therefore\ P(c) \text{ where } c \in \mathcal{U}}$	Universal Instantiation
$\dfrac{P(c) \text{ for an arbitrary } c \in \mathcal{U}}{\therefore\ \forall x\ P(x)}$	Universal Generalization
$\dfrac{\exists x\ P(x)}{\therefore\ P(c) \text{ for some } c \in \mathcal{U}}$	Existential Instantiation
$\dfrac{P(c) \text{ for some } c \in \mathcal{U}}{\therefore\ \exists x\ P(x) \vee Q}$	Existential Generalization

These will be instrumental to our proofs involving quantifiers shortly! And since we will attempt to put them in more plain language...

The How-To's with Assuming quantifiers:

Assuming	Can do	Name
$\forall$	It always works so use it for one that you *already have*	Universal Instantiation
$\exists$	Can *produce* an element it works for and then you can use it	Existential Instantiation

The How-To's with Concluding quantifiers:

Want to Conclude	Must do	Name
$\forall$	choose an arbitrary one and then show it works for that one	Universal Generaliza
$\exists$	*GIVE* an element and *then* show it works for that one	Existential Generaliz

Figure 2.5.1

2.6 Exercises

1. Assume that the truth value assignments for each statement are correct.

   - All math students are smart. (True)
   - All smart people are goofy. (True)
   - All smart people are math students. (False)
   - All math students are silly. (True)

   Now given these assigned truth values, determine the validity and soundness of each of the following arguments:

   (a)
   All math students are smart.
   All smart people are silly.
   $\therefore$ All math students are silly.

   (b)
   All math students are silly.
   All smart people are silly.
   $\therefore$ All math students are smart.

   (c)
   All smart people are math students.
   All math students are silly.
   $\therefore$ All smart people are silly.

   (d)
   All smart people are silly.
   All math students are silly.
   $\therefore$ All math students are silly.

2. Using truth tables show that the remaining arguments are valid in Figure 2.3.1, p. 27

3. Use the following as premises

   - Consider the following propositions.
     - P : Today is Sunday
     - Q : I go shopping
     - R : I go shopping at the mall
     - S : I go shopping at Micro Center
     - W : I will buy a gaming computer

   Next, we will make the following assumptions:

(A) I'll go shopping if it is Sunday.

(B) If I go to Micro Center then I will not go to the mall.

(C) I am not going to the mall.

(D) I buy a gaming computer whenever I go to Micro Center.

Using the arguments (and naming when you use them) in Figure 2.3.1, p. 27 conclude W.

Chapter 3

Direct Proofs

In this chapter we will begin to actually prove!

What one proves in an introduction to proofs class varies. But for this book we start by letting the student use college algebra as a crutch to lean on as they enter this new and scary world of proving.

3.1 Where We Start

The biggest pain and question of all beginning proofs student is:

"What can I assume?"

To help answer that we will begin every chapter with either a quick note or a detailed list.

3.2 What We Can Assume

As this is the first chapter of actual proving we will begin with a detailed list!

Things you can assume without mentioning:

1. That adding/subtraction/multiplication of integers works like you think. For example
$$2 - 3 = -3 + 2$$
(Notice I did not say division! DO NOT use division in this chapter!)

2. Basic college algebra like:
$$x^2 - 3x = x(x - 3)$$

3. Basic ordering properties of the integers such as:
$$1 < 2 \text{ or } 12 \geq 7, \text{ etc.}$$

Things you can assume but MUST mention:

1. Closure of addition in the Integers:
If $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ then $(x + y) \in \mathbb{Z}$
"when you add two integers you get an integer..."

2. Closure of subtraction in the Integers:

   If $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ then $(x - y) \in \mathbb{Z}$

   "when you subtract two integers you get an integer..."

3. Closure of multiplication in the Integers:

   If $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ then $(x \cdot y) \in \mathbb{Z}$

   "when you multiply two integers you get an integer..."

4. Any Theorem/Lemma/Corollary given in this chapter, unless otherwise stated.

5. **The Division Algorithm**

   $\forall a, b \in \mathbb{Z}$, with $a \neq 0$, $\exists! q, r \in \mathbb{Z}$ such that

   $$b = aq + r$$

   where $0 \leq r \leq |a|$. The q is called the **quotient** and the r is called the **remainder**.

   (once we have enough tools we will prove this Proposition 6.12.6, p. 121 but for now we will assume it)

For anything else... just don't assume it! If you can't do a proof without making the assumption you want just write that in your proof! We can work on it from there!

3.3 Our Terms

Now, in order to start proving things we need the objects we are going to prove them about. In addition when we begin our journey in proving, I'd like to limit the moving pieces to those few assumptions just listed, and ***most importantly*** these following definitions.

I begin by being this limiting to make sure our playground is small enough that no one hurts themselves by falling off monkey bars that are too high, but also large enough that we can actually get some *real* proving in. We'll start with a few common definitions, namely odd, even, and divides.

Definition 3.3.1 Even. $\forall x \in \mathbb{Z}, x$ is **even** iff $\exists k \in \mathbb{Z}$ such that $x = 2k$ $\Diamond$

Definition 3.3.2 Odd. $\forall x \in \mathbb{Z}, x$ is **even** iff $\exists k \in \mathbb{Z}$ such that $x = 2k + 1$ $\Diamond$

Definition 3.3.3 Divides. $\forall x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, we say x **divides** y iff $\exists k \in \mathbb{Z}$ such that $y = kx$

The notation for x divides y is $x|y$ $\Diamond$

It is important to become so familiar with these that you could say them in your sleep.

Note 3.3.4 ***Definitions*** are ***ASSUMPTIONS/PREMISES***, so when using arguments from the previous chapter use them as such.

3.4 Direct Proof

Our first method before proving is known as direct proof, it is the student's go-to throughout their career.

Most often we will be proving statements that look like:

$$P \implies Q$$

So, before we dive into it I'd like to give the song that we will sing whenever we start proving.

- What's the P? (The "if" part)
- What's the Q? (The "then" part)
- What're the definitions?
- Now, what to do? (Which proving method - until we learn more this will always be direct proof)

3.5 What is a Direct Proof?

Now without further ado the direct proof.

Direct Proof of $P \implies Q$.

Assume P
$\vdots$
Therefore Q
Thus $P \implies Q$

Here is where the title of the text becomes clear:
Beginning -- Assume P
Muddle -- ...
End -- Therefore Q

3.6 Does it Work?

We have an entire chapter about arguments, so does this *direct proof* work?
Is the *direct proof* a valid argument?

$$\begin{array}{l} P \\ Q \\ \hline \therefore\ P \implies Q \end{array}$$

To see this the "long way" lets build a truth table:

P	Q	$P \wedge Q$	$P \implies Q$	$[P \wedge Q] \implies [P \implies Q]$
T	T	T	T	T
T	F	F	F	T
F	T	F	T	T
F	F	F	T	T

And we see that

$$[P \wedge Q] \implies [P \implies Q]$$

is a tautology! I.e. the direct proof is a valid argument!

Note 3.6.1 Yes, your eyes do not deceive you, I did just *prove* that the *direct proof* is a proof.

3.7 Our First Proof

Now that we have our first weapon in hand (the direct proof) let's start to slay our first dragon.

Prove: For all integers x, whenever x is odd then $x+1$ is even.

Before we begin any proof we sing our song (play-along):

"What's the P?"**1.** x is odd

"What's the Q?"**2.** $x+1$ is even

"What're the definitions?"**3.** Odd (Definition 3.3.2, p. 34) and even (Definition 3.3.1, p. 34)!

"Now, what to do?"**4.** A direct proof! (it is the only method we know so far)

3.8 The Beginning

One purpose of our fun song is for us to to split what we want to prove into the Beginning and the End.

Once we have it split like that we see something left over... this is the beginning quantifier. This quantifier is quite often forgotten/assumed when it is not written, but assumed nonetheless, therefore we call it the *hidden quantifier*. Either way the statement we are trying to prove is now broken up as follows:

$$\forall x \in \mathbb{Z} \text{ if } x \text{ is odd then } x+1 \text{ is even}$$

To prove our statement with this beginning quantifier, according to Universal Generalization from Figure 2.5.1, p. 31 we need to show it works with an arbitrary integer.

To indicate this in our proof we may begin with either of the sentences:

"Let x be an integer."

or

"Choose an arbitrary integer x"

Now, we can take care of the Beginning from the direct proof:

Assume the "P"

"Assume that x is odd."

3.9 The Muddle

To proceed with our proof we don't have much except the definitions. (It can be helpful, especially in these early stages of proof writing, to write the relevant definitions to the side in your scratch work - this is why it's part of the song!)

From the definition odd (Definition 3.3.2, p. 34) we can make the conclusion that:

x must look like:

$$x = 2k+1$$

for some integer k.

Invoking this definition in this manner is an application of Existential Instantiation from Figure 2.5.1, p. 31

To continue *muddling along* we can use some college algebra, as is allowed by Section 3.2, p. 33 and calculate:

$$\begin{aligned} x+1 &= (2k+1)+1 \\ &= k+2 \end{aligned}$$

$$= 2(k+1)$$

The $x+1$ on the left of this equation is the end conclusion we're *aiming* for! (*"What's the Q"* from the song)

The stuff on the right is what we manipulate to make it "look like," or "fit," the definition of even. We will attempt to make this more clear in the next subsection.

Remark 3.9.1 I choose these as the first *types* of proofs to show/have students do first, because the muddle is basically the same for all of them: "invoke a definition then calculate". It gives the students something to hold on to as they are still trying to digest the previous chapters...

3.10 The End

From the muddle, we have:

$$x+1 = 2(k+1)$$

To be able to make our conclusion

$$Q: \ x+1 \text{ is even}$$

we must use defintion of even (Definition 3.3.1, p. 34), which uses an existential quantifier so we must (Figure 2.5.1, p. 31) be able to produce/point at an integer, so that $x+1$ is this integer times 2.

We have exactly that, because (Section 3.2, p. 33) $k+1$ is an integer!

To write this in our proof we can say:

"Since $k+1$ is an integer (this is where./how we "assume but mention" the *closure of addition in the integers*), by definition of even, $x+1$ is even."

Finally we should end every proof with a wrap-up sentence. This sentence is to summarize the proof, most importantly laying out your proving method, in this example a direct proof.

For this proof our wrap-up could look like:

"Since we assumed that an arbitrary integer x was odd and showed that $x+1$ is even, we can conclude that for all integers x, whenever x is odd then $x+1$ is even, by direct proof."

At last we indicate that our proofs are over with a:

QED

When a proof is finished, customarily, we either write "QED" or □ at the bottom. This comes from the Latin "quod erat demonstrandum," which means "that which was to be demonstrated."

To wrap-up everything in a pretty bow, lets see the whole proof in one spot.

Example 3.10.1 ***Prove:*** For all integers x, whenever x is odd then $x+1$ is even.

Let x be an integer. Assume x is odd. Thus, by the definition of odd, we can find an integer k so that $x = 2k+1$.

Calculate:

$$\begin{aligned} x+1 &= (2k+1)+1 \\ &= k+2 \\ &= 2(k+1) \end{aligned}$$

Since $k+1$ is an integer, by definition of even, $x+1$ is even.

Since we assumed that an arbitrary integer x was odd and showed that $x+1$ is even, we can conclude that for all integers x, whenever x is odd then $x+1$ is even, by direct proof. □ □

3.11 More Direct Proof Examples

We will give each of these examples a subsection, then further subdivide the sections for their in-depth explanations.

3.12 Direct Proof Example 2

Prove: For all integers x and y, if x and y are both odd then $x+y$ is even.

Before we begin any proof we sing our song (play-along):

"What's the P?"**1.** x and y are both odd

"What's the Q?"**2.** $x+y$ is even

"What're the definitions?"**3.** Odd(Definition 3.3.2, p. 34) and even (Definition 3.3.1, p. 34)!

"Now, what to do?"**4.** A direct proof! (it is the only method we know so far)

The Breakdown:

$$\forall x, y \in \mathbb{Z} \text{ if } x \text{ and } y \text{ are both odd then } x+y \text{ is even}$$

3.13 The Beginning

Just as before we begin by "shoveling off" our beginning quantifier (Section 2.5, p. 30) by saying something along the lines of:

"Choose arbitrary integers x and y."

Now, we take care of the beginning of our direct proof...

Assume the P

So in our example we would write:

"Assume both x and y are odd."

3.14 The Muddle

Again, as will be quite often even after this class, we do not have much but the definitions (Section 3.3, p. 34), so we will apply these definitions (making note they involve quantifiers Figure 2.5.1, p. 31).

To apply the definition of odd (Definition 3.3.2, p. 34) to our integer x we *use* the *exists* from the proof to produce a new integer which will need a name, lets name it t. This t can be found so that $x = 2t+1$.

Some questions that often arise here are: "but the proof says k?" Yet, in fear of sounding like a broken record we are *using/applying* the definition of odd, and when using the $\exists$ (by Figure 2.5.1, p. 31) we can *find* some integer (in this example) to do the job. The k in the definition is just a stand-in for *some integer*.

So for our proof we could write:

"By the definition of odd we can find an integer t so that $x = 2t+1$."

Next, we do the exact same procedure with the y, but because y is a new number and it is a brand new *application* of the definition of odd we can produce a a new integer (Figure 2.5.1, p. 31), so this time lets name it s.

That is in our proof we could write:

"Again, by the definition of odd, we can find an integer s such that $y = 2s + 1$."

Having successfully applied our definitions we now have *something* we can calculate with, so lets try to add what is in our Q, namely $x + y$

$$\begin{aligned} x + y &= (2t + 1) + (2s + 1) \\ &= 2s + 2t + 1 + 1 \\ &= 2s + 2t + 2 \\ &= 2(s + t + 1) \end{aligned}$$

Now, we can (hopefully) *see* our definition of even at the last equality, signalling that we are ready for our end.

3.15 The End

From the muddle, we have:

$$x + y = 2(s + t + 1)$$

To be able to make our conclusion

$$Q : \ x + y \text{ is even}$$

we must, again, use definition of even (Definition 3.3.1, p. 34), which uses an existential quantifier so we must (Section 2.5, p. 30) , be able to produce/point at an integer, so that $x + y$ is this integer times 2.

We have exactly that, because (Section 3.2, p. 33) $s + t + 1$ is an integer!

To write this in our proof we can say:

"Since $s + t + 1$ is an integer, by definition of even, $x + y$ is even."

Finally we should end every proof with a wrap-up sentence. This sentence is to summarize the proof, most importantly laying out your proving method, in this example a direct proof.

For this proof our wrap-up could look like:

"Since we assumed that an arbitrary two integers x and y were odd and showed that $x + y$ is even, we can conclude that for all integers x and y, whenever x and y are odd then $x + 1$ is even, by direct proof."

Now lets see everything written together in a single spot.

Example 3.15.1 **1.** ***Prove:*** For all integers x and y, if x and y are both odd then $x + y$ is even

Choose arbitrary integers x and y. Assume both x and y are odd. By the definition of odd we can find an integer t so that $x = 2t + 1$. Again, by the definition of odd, we can find an integer s such that $y = 2s + 1$.

Now calculate:

$$\begin{aligned} x + y &= (2t + 1) + (2s + 1) \\ &= 2s + 2t + 1 + 1 \\ &= 2s + 2t + 2 \\ &= 2(s + t + 1) \end{aligned}$$

Since $s + t + 1$ is an integer, by definition of even, $x + y$ is even.

Since we assumed that an arbitrary two integers x and y were odd and showed that $x + y$ is even, we can conclude that for all integers x and y, whenever x and y are odd then $x + 1$ is even, by direct proof. □

3.16 Direct Proof Example 3

The last two examples had even in the P and even in the Q. In fear of students thinking this is some sort of immutable law/pattern lets change that pattern this time.

Prove: For all integers x and y if x and y are both odd then $x \cdot y$ is odd.

Before we begin any proof we sing our song (play-along):

"What's the P?"**1.** x and y are both odd

"What's the Q?"**2.** $x \cdot y$ is odd

"What're the definitions?"**3.** Odd (Definition 3.3.2, p. 34)!

"Now, what to do?"**4.** A direct proof! (it is the only method we know so far)

The Breakdown:

$$\forall x, y \in \mathbb{Z} \text{ if } x \text{ and } y \text{ are both odd then } x + y \text{ is odd.}$$

3.17 The Beginning

We begin by taking care of our leading quantifier, $\forall x, y \in \mathbb{Z}$, trying our best to never forget Figure 2.5.1, p. 31. To do this we could use a variety of english statements to do this, for example:

- "Select two random integers x and y"
- "Choose two arbitrary integers x and y"
- "Let x and y be integers"

Next, we do the first step of a direct proof, that is Assume the P. From our song we already know this, and that is:

"Assume x and y are both odd"

3.18 The Muddle

Now, as we see in this first class of proofs so often, the only tools we really have at our disposal are the definitions from Section 3.3, p. 34. In this proof we have to apply a definition twice from our previous line/assumption namely:

- x is odd
- y is odd

Something that bares repeating over and over and over and over again, is to always remember Figure 2.5.1, p. 31. Right now we need to remember this because the definition of (Definition 3.3.2, p. 34) invoke an existential quantifier. So to apply the definition of odd for x we can use language like:

"We can find an $a \in \mathbb{Z}$ so that $x = 2a + 1$."

To use the definition of odd for our y we can use language like:

"We can also find a $b \in \mathbb{Z}$ so that $y = 2b + 1$."

Now that we have used our definitions we can move to our usual muddle where we use some good ole *college algebra*. In a more general look at proofs at a whole is that you should keep in mind what we are trying to conclude, i.e. the Q, namely that $x + y$ is odd. So we should calculate $x + y$.

Calculate:

$$\begin{aligned} x+y &= (2a+1)\cdot(2b+1) \\ &= 4ab+2a+2b+1 \\ &= 2(2ab+a+b)+1 \end{aligned}$$

3.19 The End

From the muddle we know have:

$$x+y = 2(2ab+a+b)+1$$

Now, using the definition of odd (Definition 3.3.2, p. 34) and of course Figure 2.5.1, p. 31 we can conclude that from the muddle that $x+y$ is odd, as $2ab$ is an integer and thus $(2ab+a+b)$ is an integer, and hence we have that $x+y$ is an integer times 2 then plus one.

Now lets see everything written together in a single spot, with a proper wrap-up.

Example 3.19.1 **2.** ***Prove:*** For all integers x and y if x and y are both odd then $x \cdot y$ is odd.

Select two random integers x and y. Assume that x is even and y is odd. By definition of even we can find an integer a so that $x = 2a+1$. Also, by the definition of odd we can find an integer b so that $y = 2b+1$. Now we calculate:

$$\begin{aligned} x+y &= (2a+1)\cdot(2b+1) \\ &= 4ab+2a+2b+1 \\ &= 2(2ab+a+b)+1 \end{aligned}$$

Now since $2ab+a+b$ is an integer, we see that $x+y$ is odd.

To summarize, since we chose arbitrary integers x and y which we assumed were even and odd, respectively, by direct proof we proved that for all integers x and y, if x is even and y is odd, then $x+y$ is odd. □ □

3.20 Direct Proof Example 4

Now let's see an example that is *not* even nor odd.

Prove: $\forall x, y \in \mathbb{Z}$ if $5|x$ and $5|y$ then $5|(x-2y)$

Before we begin any proof we sing our song (play-along):

"What's the P?"**1.** $5|x$ and $5|y$

"What's the Q?"**2.** $5|(x-2y)$

"What're the definitions?"**3.** divides (Definition 3.3.3, p. 34)

"Now, what to do?"**4.** A direct proof! (it is the only method we know so far)

The Breakdown:

$$\forall x, y \in \mathbb{Z}\ 5|x \text{ and } 5|y \implies 5|(x+y)$$

3.21 The Beginning

This proof is the same as we have been doing at the beginning as it starts with our beginning quantifier. As usual we take care of that using:

"Let x and y be integers."

As we are still doing a direct proof our first step involving this is Assume the P, and for this example it is:

"Assume that both $5|x$ and $5|y$."

3.22 The Muddle

In this example we go to our definitions again (being careful for the quantifier Figure 2.5.1, p. 31), specifically for $5|x$ we use the definition of divides (Definition 3.3.3, p. 34) as follows:

"By definition of divides we can find an $a \in \mathbb{Z}$ so that $x = 5a$."

For $5|y$ we apply the definition of divides (Definition 3.3.3, p. 34) as:

"By definition of divides we can find a $b \in \mathbb{Z}$ so that $y = 5b$."

Something I have seen students do here is write "exists an integer b". You are using the existential quantifier to produce a specific integer (Figure 2.5.1, p. 31), by saying exists you are just telling me that you could theoretically find one, not telling that you are producing one to use.

So now that we have something we can use, like usual we can calculate:

$$\begin{aligned}(x - 2y) &= (5a) - (2 \cdot (5b)) \\ &= 5(a - 2b)\end{aligned}$$

3.23 The End

From muddle we have

$$x + y = 5(a - 2b)$$

and then we can reference a couple of our assumptions from Section 3.2, p. 33, and say:

"Since $2b$ is an integer a $a - 2b$ is an integer by the definition of divides 5 divides $x - 2y$."

Now let's see everything written together in a single spot, with an appropriate wrap-up.

Example 3.23.1 **3.** ***Prove:*** $\forall x, y \in \mathbb{Z}$ if $5|x$ and $5|y$ then $5|(x - 2y)$

Let x and y be integers. Assume that 5 divides both x and y. Next, we calculate:

$$\begin{aligned}(x - 2y) &= (5a) - (2 \cdot (5b)) \\ &= 5(a - 2b)\end{aligned}$$

Since $2b$ is an integer it follows that $a - 2b$ is an integer, thus by the definition of divides, 5 divides $x - y$.

To summarize, since we chose arbitrary integers x and y and assume that 5 divides both of them, and have shown that $5|(x - 2y)$, by direct proof we have shown that for any integers x and y, if $5|x$ and $5|y$ then $5|(x - 2y)$ □

3.24 Direct Proof Example 5

Our last detailed example of a direct proof it is a classic inequality. Inequalities will play a large role in your future analysis class.

Prove: For all positive real numbers x and y, if $a < b$ then $b^2 - a^2 > 0$.

Before we begin any proof we sing our song (play-along):

"What's the P?"**1.** $a < b$

"What's the Q?"**2.** $b^2 - a^2 > 0$

"What're the definitions?"**3.** x is positive mean $x > 0$

"Now, what to do?"**4.** A direct proof! (it is the only method we know so far)

The Breakdown:

$$\forall x, y \in \mathbb{R} \text{ with } x > 0 \text{ and } y > 0 \; a < b \implies 0 < (a^2 - b^2)$$

3.25 The Beginning

This beginning is the same as the others. We take care of the beginning quantifier by:

"Let x and y be positive real numbers."

For our approach of a direct proof we need to start by assuming the P, that is:

"Assume that $a < b$"

3.26 The Muddle

Now, as is in most inequality proofs first we need to work backwards. That is notice:

$$b^2 - a^2 = (b - a)(b + a)$$

by our allowed assumptions of basic *college algebra*. But we have that $b+a > 0$ since both $a > 0$, and $b > 0$, then again with our assumptions of *college algebra*. That is we can, lets say, add b to the left side of $a > 0$ and add 0 to the right side. Also, $b - a > 0$ since subtracting a from both sides of our assumption results in $a < b$.

3.27 The End

To write our proof in a logical format we will have to go the opposite direction, as otherwise we will have said our conclusion before we concluded it, essentially falling for circular reasoning, that is:

Subtracting a from both sides of our assumption $a < b$ we see that $b-a > 0$, and by adding b to the left and 0 to the right of $a > 0$ we get that $b + a > 0$. Finally, since $b + a > 0$ we can multiply both sides of $b - a > 0$ by $(b + a)$ and arrive at:

$$b^2 - a^2 = (b - a)(b + a) > 0.$$

Now let's see everything written together in a single spot.

Example 3.27.1 **4.** ***Prove:*** For all positive real numbers x and y, if $a < b$ then $b^2 - a^2 > 0$.

Let x and y be positive real numbers. Assume that $a < b$.

Since subtracting a from both sides of our assumption $a < b$ we see that

$b - a > 0$, and by adding b to the left and 0 to the right of $a > 0$ we get that $b + a > 0$. Finally, since $b + a > 0$ we can multiply both side of $b - a > 0$ by $(b + a)$ and arrive at:

$$b^2 - a^2 = (b - a)(b + a) > 0.$$

Since we assumed x and y are positive real numbers and $a < b$, then we showed that $(b^2 - a^2) > 0$, by direct proof we can conclude, that for all positive real numbers x and y if $a < b$ then $(b^2 - a^2) > 0$. □

3.28 Proofs with Conjunctions and Disjunctions

So far we have been proving the prototypical

$$P \implies Q$$

as it is perhaps one of the most common propositional forms used in mathematics, and otherwise. Yet, in all of our examples thus far both P and Q have been atomic propositions. In this section we will be substituting the antecedent and consequent with compound propositions.

Assuming an Or.

For propositions P, Q, and R, to prove a statement in the form of

$$(P \vee R) \implies Q$$

First we:
Prove: $P \implies Q$
then we:
Prove: $R \implies Q$

To verify that this argument is valid, we will use a truth table to show:

$$[(P \implies Q) \wedge (R \implies Q)] \implies [(P \vee R) \implies Q]$$

is a tautology. To do so we will show a stronger result using the tricks of Section 1.14, p. 16.

$$\begin{aligned}(P \vee R) \implies Q &\equiv [\sim (P \vee R)] \vee Q \text{ (Rob's Law)}\\ &\equiv [(\sim P) \wedge (\sim R)] \vee Q \text{ (De Morgan's)}\\ &\equiv [(\sim P) \vee Q] \wedge [(\sim R) \vee Q] \text{ (distribution)}\\ &\equiv [P \implies Q] \wedge [R \implies Q] \text{ (Rob's Law)}\end{aligned}$$

Now lets see an example of this in play.

Example 3.28.1 ***Prove:*** for any two integers x and y if x is even or y is even then $x \cdot y$ is even.

Proof. Let x and y be integers.
First assume that x is even. By definition of even (Definition 3.3.1, p. 34) we can find an integer k so that $x = 2k$. Calculate:

$$\begin{aligned} x \cdot y &= (2k) \cdot y \\ &= 2(ky) \end{aligned}$$

since ky is an integer by the definition of even, $x \cdot y$ is even.
Next, we instead assume y is even. By definition of even we can find an integer t so that $y = 2t$. Calculate:

$$\begin{aligned} x \cdot y &= x \cdot (2t) \\ &= 2(xt) \end{aligned}$$

since xt is an integer by the definition of even, $x \cdot y$ is even.
Now since we have shown that for $\forall x, y \in \mathbb{Z}$ that both x is even implies $x \cdot y$ is even and y is even implies $x \cdot y$ is even, we have shown that $\forall x, y \in \mathbb{Z}$. ■

□

Another interesting scenario is when we are trying to conclude a disjunction.

Concluding an Or.

For propositions P, Q, and R, to prove a statement in the form of

$$P \implies (Q \vee R)$$

We instead
Prove: $[P \wedge (\sim R)] \implies Q$

That this argument is valid can be seen by showing that

$$[P \implies (Q \vee R)] \equiv [[P \wedge (\sim R)] \implies Q]$$

To do that we will again use the tricks of Section 1.14, p. 16.

$$\begin{aligned} P \implies (Q \vee R) &\equiv (\sim P) \vee (Q \vee R) \text{ (Rob's Law)} \\ &\equiv (\sim P) \vee (R \vee Q) \text{ (commutativity)} \\ &\equiv [(\sim P) \vee R] \vee Q \text{ (associativity)} \\ &\equiv \sim [P \wedge (\sim R)] \vee Q \text{ (De Morgan's)} \\ &\equiv (P \wedge (\sim R)) \implies Q \text{ (Rob's Law)} \end{aligned}$$

Now lets see an example.

Example 3.28.2 ***Prove:*** For all integers x and y if x is even then y is odd or $x + y$ is even

Proof. Let x and y be arbitrary integers. Assume that x is even and that y is not odd. By the definition of even (Definition 3.3.1, p. 34) we can find an integer k so that $x = 2k$. By the division algorithm (Section 3.2, p. 33) we can find integers q and r such that $0 \leq r < 2$ such that $y = 2q + r$. Yet since we assumed y is not odd $r \neq 1$, and since r is an integer and $0 \leq r < 2$ and the only integers which satisfy this inequality are 0 and 1, which only leaves $r = 0$ thus $y = 2q$. Now calculate:

$$\begin{aligned} x + y &= 2k + 2q \\ &= 2(k + q) \end{aligned}$$

Since $k + q$ is an integer by the definition of even $x + y$ is even.
Since we have assumed for two arbitrary integers x and y that x is even and y is not odd, and we have concluded that $x + y$ is even, we can conclude that for all integers x and y, if x is even then y is odd or $x + y$ is even. ■

□

The last propositional form we consider in this section is the following.

Concluding an And.

For propositions P, Q, and R, one way to prove a statment in the form of

$$P \implies (Q \wedge R)$$

First we:
Prove: $P \implies Q$
then we:
Prove: $P \implies R$

To see that this is a valid way of proving, we once again show an even stronger result using the methods of Section 1.14, p. 16.

$$\begin{aligned} P \implies (Q \wedge R) &\equiv (\sim P) \vee (Q \wedge R) \text{ (Rob's Law)} \\ &\equiv [(\sim P) \vee Q] \wedge [(\sim P) \vee R] \text{ (distribution)} \\ &\equiv [P \implies Q] \wedge [P \implies R] \text{ (Rob's Law)} \end{aligned}$$

Example 3.28.3 ***Prove:*** For all integers a and b, if $3|(a - 2)$ and $3|(b - 1)$ then $3|(a + b)$ and $3|(a - 2b)$

Proof. Let a and b be arbitrary integers.
Assume that $3|(a-2)$, also assume that $3|(b-1)$. By definition of divides (Definition 3.3.3, p. 34) we can produce an integer k such that $a-2=3k$, and hence by adding 2 to both sides of this equation we get $a=3k+2$. As well by the definition of divides we can come forth with another integer t with the property that $b-1=3t$, this time adding 1 to both sides of the equation we see that $b=3t+1$.
Now, we will prove: if $3|(a-2)$ and $3|(b-1)$ then $3|(a+b)$, by calculating:

$$\begin{aligned} a+b &= (3k+2)+(3t+1) \\ &= 3k+3t+3 \\ &= 3(k+t+1) \end{aligned}$$

and since $k+t+1$ is an integer by the definition of divides $3|(a+b)$.
Next, we will prove: if $3|(a-2)$ and $3|(b-1)$ then $3|(a-2b)$, instead by calculating:

$$\begin{aligned} a+b &= (3k+2)-2(3t+1) \\ &= 3k+2-6t-2 \\ &= 3k-6t \\ &= 3(k-2t) \end{aligned}$$

and since $k-2t$ is an integer by the definition of divides $3|(a-2b)$.
Now that we have assumed that a and b are arbitrary integers and assumed that $3|(a-2)$ and $3|(b-1)$ then we showed that both $3|(a+b)$ and that $3|(a-2b)$ we can conclude that for all integers a and b, if $3|(a-2)$ and $3|(b-1)$ then $3|(a+b)$ and $3|(a-2b)$. ■

□

3.29 More Examples

To end this chapter we give some more examples without all of the commentary of our song nor the beginning, muddle, and end.

Example 3.29.1 ***Prove:*** For all integers a, b, and c if a divides b and b divides c then a divides c

Find some integers a, b, and c. Assume a divides b and b divides c. Thus by definition of divides, we can find an integer k such that $b=ak$. Also by definition of divides, we can find an integer l such that $c=bl$

Calculate:

$$\begin{aligned} c &= bl \\ &= (ak)l \\ &= a(kl) \end{aligned}$$

Since kl is an integer, by definition of divides, a divides c. Thus by direct proof, according to the definition of divides, if if a divides b and b divides c then a divides c. □ □

Example 3.29.2 ***Prove:*** For all integers x and y, if x and y are even, $x+y$ is even.

Let x and y be integers. Assume x and y are even. Thus, by definition of even, we can find an integer k so that $x=2k$, and we can find an integer l so that $y=2l$.

Calculate:

$$\begin{aligned} x + y &= 2k + 2l \\ &= 2(k + l) \end{aligned}$$

Since $k + l$ is an integer, by definition of even, $x + y$ is even. □ □

Example 3.29.3 ***Prove:*** an odd integer plus 2 is odd.

Let x be an integer. Assume x is odd. Hence, by the definition of odd, we can find an integer k such that $x = 2k + 1$

Calculate:

$$\begin{aligned} x + 2 &= (2k + 1) + 2 \\ &= 2(k + 1) + 1 \end{aligned}$$

Thus, since $k + 1$ is an integer, by definition of odd, $x + 2$ is odd. □ □

Example 3.29.4 ***Prove:*** if 5 divides x and 5 divides y then 5 divides $x + y$

Let x and y be integers. Assume 5 divides x and 5 divides y. Hence, by the definition of divides, we can find an integer k so that $x = 5k$ and we can find an integer l so that $y + 5l$

Calculate:

$$\begin{aligned} x + y &= 5k + 5l \\ &= 5(k + l) \end{aligned}$$

Since $k + l$ is an integer, by definition of divides, 5 divides $x + y$.

Thus, by direct proof, if 5 divides x and 5 divides y, then 5 divides $x + y$. □ □

Example 3.29.5 ***Prove:*** If 5 divides $x - 1$ and 5 divides $y - 4$ then 5 divides $x + y$.

Let x and y be integers. Assume divides $x - 1$ and 5 divides $y - 4$. By definition of divides, we can find an integer k such that $x - 1 = 5k$ By definition of divides, we can find an integer m such that $y - 4 = 5k$.

Calculate:

$$\begin{aligned} x + y(x - 1) + (y - 4) + 5 \\ + 5k + 5m + 5 \\ + 5(k + m + 1) \end{aligned}$$

Since $k + m + 1$ is an integer, by definition of divides, 5 divides $x + y$

Thus, by direct proof, if 5 divides $x - 1$ and 5 divides $y - 4$ then 5 divides $x + y$. □ □

Example 3.29.6 ***Prove:*** For all integers a, b, and c if a divides b and a divides c then a divides $b - c$

Let a, b, and c be integers. Assume a divides b and a divides c. By the definition of divides, we can find an integer h so that $b = ah$ and an integer d so that $c = ad$.

calculate

$$\begin{aligned} b - c &= ah - ad \\ &= a(h - d) \end{aligned}$$

Since $h - d$ is an integer, by definition of divides, a divides $b - c$. Hence by direct proof, if a divides b and a divides c then a divides $b - c$. □ □

3.30 Exercises

Direct proofs with just even and odd

1. $\forall w, x, y, z \in \mathbb{Z}$ prove the following.
   (a) if $x + y$ is even, then $x - y$ is even
   (b) if x and y are odd, then $x * y$ is odd
   (c) if x is even, and y and z are odd, then $(x * y) + z$ is odd
   (d) if x and y are even then xy is divisible by 4.
   (e) if x and y are odd then $x + y$ is even.
   (f) if x and y are even then $3x - 5y$ is even.
   (g) if x is odd then $x + 2$ is odd
   (h) if $x|y$ then $x|yz$
   (i) if $x|y$ and $w|z$ then $xw|yz$
   (j) if x is odd then $x^2 + 1$ is even
2. $\forall a, b, c \in \mathbb{Z}$, prove the following with techniques from Section 3.28, p. 44
   (a) If $5|(a - 2)$ and $5|(b - 3)$ then $5|(a + b)$ and $5|(a - b + 1)$.
   (b) If $7|a$ then 7 does not divide b or $7|(a + b)$.
   (c) If a is even or $4|b$ then $4|(2a \cdot b)$.
3. Suppose that you would use a direct proof if you were to prove the following statements. For each only write " the beginning " and " the end"
   (a) For every real valued function f, if f is differentiable then f is continuous.
   (b) For all slompins, a, if a is an insteredment then $a^2 - 5$ is flooxin.
   (c) If m is an annsubmir and p is a curric-fac then $3m - 5p + 1$ is a divisper.
   (d) For every two integers x and y, if x is threeven and y is thud, then $x + y + 2$ is thodd.

Direct proofs with divides and proof by cases

1. If x and y are even, then $4|xy$
2. $2x - 1$ is odd (Proof by cases)
3. $x^2 + x + 3$ is odd (Proof by cases)
4. If $x|y$ and $z|w$ then $xz|yw$
5. If $xy|z$ then $x|z$

Contradiction, Contraposition, Bi-conditional

1. If $4 \nmid x^2$ then x is odd. (Contraposition)
2. If xy is odd then xx and y are odd. (Proof by cases)
3. If $5|x^2$ then $5|x$ (Contraposition)
4. If ab is odd then a and b are odd. (Contradiction)
5. If $a - b$ is odd, then $a + b$ is odd. (Contradiction)
6. $\sqrt{5}$ is irrational. (Contradiction)
7. $ac|bd$ if and only if $a|b$. (bi-conditional)

Chapter 4

Indirect Proofs

The students go-to proof is most commonly the direct proof, yet there are many methods of proving that do not involve this method, they are broadly described as indirect proofs. In this chapter we will go through a few examples.

4.1 Our Assumptions

In this chapter you can assume anything you had in Section 3.2, p. 33. We also include a few more defintitons for this chapter.

Definition 4.1.1 Common Divisor. $\forall a, b, c \in \mathbb{Z}$, all non-zero, we call c a **common divisor** of a and b iff c divides a and c divides b. $\Diamond$

Definition 4.1.2 Greatest Common Divisor. $\forall a, b, c \in \mathbb{Z}$, all non-zero, we call c the **greatest common divisor** of a and b, denoted $c = \text{GCD}(a, b)$ iff

1. c is a common divisor of a and b
2. every common divisor of $d \in \mathbb{Z}$ of a and b has the property $d \leq c$. (every other divisor is smaller)

$\Diamond$

Definition 4.1.3 Rational. $x \in \mathbb{Q}$ iff $\exists p, q \in \mathbb{Z}$ with $q \neq 0$ such that $x = \frac{p}{q}$ and $\text{GCD}(p, q) = 1$ $\Diamond$

Definition 4.1.4 1-d Integer Cone. For any integers x_1, x_2, ..., x_n for some natural number n we say an integer y is in the **1-d integer cone formed by** x_1, x_2, ..., x_n if and only if there exists integers a_1, a_2, ..., a_n so that

$$y = a_1x_1 + a_2x_2 + ... + a_nx_n$$

$\Diamond$

4.2 Contrapositive

This first example of an indirect proof is quite close to the indirect proof. It takes some of our ingenuity from Section 1.13, p. 14 and puts it to work.

4.3 What is a Proof by Contraposition?

A proof by contraposition uses (of course) the contraposition from Section 1.13, p. 14

$$[P \implies Q] \equiv [(\sim Q) \implies (\sim P)]$$

So that we can prove $P \implies Q$ by instead proving $(\sim Q) \implies (\sim P)$. To prove this equivalent statement we will use direct proof. We summarize this in the following.

Proof by Contrapositive of $P \implies Q$.

Assume $\sim Q$
$\vdots$
Therefore $\sim P$
Thus $P \implies Q$

Again, the title of the text becomes clear:
Beginning -- Assume $\sim Q$
Muddle -- ...
End -- Therefore $\sim P$

4.4 First Example of Contrapositive

For our first example, just as in Section 3.4, p. 34, we will give as many *gory* details as we can think of to help the eager student of proofs.

Prove: $\forall m \in \mathbb{Z}$ if m^2 is odd, then m is odd.
Before we begin any proof we sing our song (play-along):
"What's the P?"**1.** m^2 is odd
But... for this question we need to really know the $\sim P$:
m is not odd odd

"What's the Q?"**2.** m is odd
But... again... for this question we need to really know the $\sim Q$:
m^2 is not odd odd

"What're the definitions?"**3.** Odd and even! (found in Section 3.3, p. 34)

"Now, what to do?"**4.** Proof by contraposition - because we are trying to learn it ***The Breakdown of the original:***

$$\forall m \in \mathbb{Z} \text{ if } m^2 \text{ is odd} \quad \text{then } m \text{ is odd}$$

The Breakdown of the contrapositive:

$$\forall m \in \mathbb{Z} \text{ if } m \text{ is not odd} \quad \text{then } m^2 \text{ is not odd}$$

Note 4.4.1 When first getting used to the contrapositive students have at times made the mistake of negating the beginning quantifier which in this case would be $\exists m \in \mathbb{Z}$. Be careful as the statement actually has the form $\forall m \in \mathbb{Z}$ $R(m)$ where

$$R(m): \text{ if } m^2 \text{ is odd then } m \text{ is odd}$$

4.5 The Beginning

Just like before, "shovel off" the beginning quantifier

$$\forall m \in \mathbb{Z}$$

using the guidance of Figure 2.5.1, p. 31 by choosing an arbitrary element, with language like:

- Let m be an integer
- Choose an arbitrary integer m
- Pick an integer m
- Take any integer m of your choice
- Let m be a freely chosen integer
- Assume m is an integer, chosen arbitrarily
- Designate an integer m of arbitrary selection
- Grab yerself any ol' integer, and let it be called m!
- Hark! Select an integer, and let it bear the name m, chosen as thou wilt
- Pick an integer, any integer, and call it m. Doesn't matter which—it could be lurking anywhere, but m is the one we'll follow
- Aye, take m, an integer, any integer, an m of no particular choosing but of the choosing all the same—floating through the mind like a thought barely caught, yet caught still: m it is.

Now we take care of our beginning of our proof using this new method of proof by contraposition, by assuming $\sim Q$.

Assume m is not odd.

Now, many of you may be reading this last line yelling with your fist in the air saying, "who says not odd, just say even". Yet, we must of course consult our *allowed assumptions* section (Section 4.1, p. 50) and the assumption that "not odd" is equivalent to "even" is not one of those!

4.6 The Muddle

As the pain point of even vs odd is not lost to me and it will be helpful to be able to write proofs without having to prove that not odd is the same as even every single time. This want to not prove something over and over again, or to separate a smaller proof from a different result comes up a lot, so when we want to do this we create a Lemma.

The word *Lemma* comes from the Ancient Greek , (perfect passive) something received or taken. Thus something taken for granted in an argument.

Lemma 4.6.1 *Let y be an integer, then y is either even or odd.*

Proof. By the division algorithm (Section 3.2, p. 33) we can find integers q and r such that $0 \leq r < 2$ such that $y = 2q + r$. Yet since r is an integer and $0 \leq r < 2$ and the only integers which satisfy this inequality are 0 and 1, we are left only with $y = 2q + 0 = 2q$ (even) or $y = 2q + 1$ (odd). ■

With our assumption that m is not odd and this Lemma in hand we could use Disjunctive Syllogism (Figure 2.3.1, p. 27) in our proof to write:

Since we assumed that m is not odd by Lemma 4.6.1, p. 52 we can conclude that m is even.

Now we finally have in our proof that m is even so we can go back to what we have come accustomed to: using the definitions. Specifically in this example we could write something like:

Thus by definition of even we can find an integer k such that $m = 2k$

Then, we could continue *following our nose* to do the common muddle so far in this text, and that is to *calculate*.

Calculate:

$$\begin{aligned} m^2 &= (2k)(2k) \\ &= 2(2k^2) \end{aligned}$$

4.7 The End

From the muddle we have that

$$m^2 = 2(2k^2)$$

from the definitoin of even (Definition 3.3.1, p. 34) we can now conclude:

Since $2k^2$ is an integer, according to the definition of even, m^2 is even.

Now this is not exactly what we want to conclude. We want to conclude that: m^2 is not odd so again using Disjunctive Syllogism (Figure 2.3.1, p. 27) and our newest lemma we could write:

Because we have concluded that m^2 is even by Lemma 4.6.1, p. 52 we can now conclude that m^2 is not odd.

Finally, we can write our wrap up sentence!

Hence, by proof by contraposition if m^2 is odd then m is odd. □

Now let's see everything written together in a single spot.

Example 4.7.1 ***Prove:*** For any integer m, if m^2 is odd, then m is odd.

Let m be an integer. Assume m is not odd. Hence, by Lemma 4.6.1, p. 52 we can conclude that m is even.

By definition of even we can find an integer k such that $m = 2k$

Calculate:

$$\begin{aligned} m^2 &= (2k)(2k) \\ &= 2(2k^2) \end{aligned}$$

Since $2k^2$ is an integer, according to the definition of even, m^2 is even. Because we have concluded that m^2 is even by Lemma 4.6.1, p. 52 we can now conclude that m^2 is not odd.

Hence, by proof by contraposition if m^2 is odd then m is odd. □ □

4.8 Contradiction

Our next method for proving is known as proof by contradiction. It is an extremely powerful example of an indirect proof. It plays off the concept of the excluded middle, in more plain language a statement is either true of false and nothing between.

The excluded middle is also known as the law / principle of the excluded third, in Latin principium tertii exclusi. Another Latin designation for this law is tertium non datur or "no third [possibility] is given".

4.9 What is a contradiction?

Proof by contradiction is the most different than the direct proof yet. The first big difference is that before now we have always considered the case where we were proving $P \implies Q$ yet this time we will be only considering proving any proposition R. This does not mean that we will not use it to prove propositions in the form of an implication, because we definitely will, it is just that we set up the proof not separating the implication as we have done before.

Proof by Contradiction of R.

Assume $\sim R$
$\vdots$
Therefore T
$\vdots$
Therefore $\sim T$
Hence $T \wedge \sim T$ which is a contradiction.
Thus R

On first look it might also seem to not follow our title, but of course:
Beginning -- Assume $\sim R$
Muddle -- conclude T ... conclude $\sim T$
End -- Therefore $T \wedge (\sim T)$ is a contradiction

This proving method may also not seem to fit immediately into our argument section (Chapter 2, p. 25). To see how it fits in first notice that before the conclusion this method is simply the direct proof of the statement

$$(\sim R) \implies [T \wedge (\sim T)]$$

Yet, this is equivalent to R, to see that consider the following truth table.

R	T	$[T \wedge (\sim T)]$	$(\sim R) \implies [T \wedge (\sim T)]$
T	T	F	T
T	F	F	T
F	T	F	F
F	F	F	F

Figure 4.9.1

Finally, before we move on, when we want to use contradiction to prove a statement in the form of $P \implies Q$ we will need to assume that $\sim [P \implies Q]$. So it may be helpful to review how to negate such a statement, using our techniques from Section 1.14, p. 16

$$\begin{aligned} \sim [P \implies Q] &\equiv [\sim ((\sim P) \vee Q)] \text{ (Rob's Law)} \\ &\equiv [\sim (\sim P) \wedge (\sim Q)] \text{ (De Morgan's)} \\ &\equiv P \wedge (\sim Q) \text{ (double negation)} \end{aligned}$$

and hence we have the equivalence:

$$\sim [P \implies Q] \equiv [P \wedge (\sim Q)]$$

4.10 First Example of Proof by Contradiction

For our first example of contradiction we will stick with our safety blanket of the integers.

Prove: For all integers a and b if $a - b$ is odd then $a + b$ is odd.

Before we begin any proof we sing our song (play-along):

"What's the P?"**1.** $a - b$ is odd

"What's the Q?"**2.** $a + b$ is odd

"What're the definitions?"**3.** even (Definition 3.3.1, p. 34) and odd (Definition 3.3.2, p. 34)

"Now, what to do?"**4.** Proof by contradiction - so we can try and learn it!***The Breakdown:***

$$\forall a, b \in \mathbb{Z} \text{ if } a - b \text{ is odd then } a + b \text{ is odd.}$$

4.11 The Beginning

To begin our proof we first take care of the beginning quantifier. As usual we will do this by choosing arbitrary integers, that is we will use language like:

Let a and b be arbitrary integers.

Note 4.11.1 Again be careful, even though we will be negating we DO NOT negate the quantifier!

Now to begin our proof by contraposition we need to Assume $\sim R$

But R is not in our song! Yes that's true, but R is just "what we want to prove". In this example we want to prove if $a-b$ is odd then $a+b$ is odd. So we will need to assume $\sim$ (if $a - b$ is odd then $a + b$ is odd) or using our analysis above we will:

Assume that $a - b$ is odd yet $a + b$ is not odd.

Now this is false, and it is our job to confirm that, yet a reader with no warning might be very alarmed that you began your proof with such a blatantly false assumption. To quell our reader's troubled stomach, and let them know what we're doing, we can start the sentence with:

For the sake of contradiction...

Or for those more inclined to the classics we can simply at the beginning of our proof write:

[RAA]

which stands for *reductio ad absurdum*, that is, "reduction to absurdity."

4.12 The Muddle

Next, almost right away we can react almost with *knee jerk* and play off our assumption with:

Since we assumed that $a+b$ is not odd, by Lemma 4.6.1, p. 52 we have that $a + b$ is even.

Now, again, as if we were to *knee jerk* we could then apply our definitions of even (Definition 3.3.1, p. 34) and odd (Definition 3.3.2, p. 34) with language similar to:

By the definition of odd we can obtain an integer ℓ so that $a - b = 2\ell + 1$. As well, by the definition odd (Definition 3.3.2, p. 34) we are able to select an integer s so that $a + b = 2s$.

Yet, this is where our quick reactions or just using the definitions we have sung in our song ends. In other examples we would look to the quintessential Q as our target to set up a calculation. Unfortunately in a proof by contradiction we are in search of a brand new proposition (which we have lovingly named T) further more we also need to find its negation ($\sim T$). This search is not always easy, and where to begin isn't always clear.

For this example we wandered in the woods and simply added the two things from our assumption together...

Calculate:

$$\begin{aligned}(a-b)+(a+b) &= (2\ell+1)+(2s)\\ &= 2\ell+2s+1\\ &= 2(\ell+s)+1\end{aligned}$$

and similar to many proofs that came before this we can conclude that since $\ell+s$ is an integer by the definition of odd, we have that

$$T:\ (a-b)+(a+b) \text{ is odd}$$

But, there is of course another way of calculating this sum with no consideration of these newly found integers, ℓ and s, that is...

$$(a-b)+(a+b) = (a+a)+(b-b) = 2a$$

yet, since a is an integer by the definition of even we have that $(a-b)+(a+b)$ is even, or in light of Lemma 4.6.1, p. 52 we have:

$$\sim T:\ (a-b)+(a+b) \text{ is not odd}$$

Therefore we have stumbled upon our contradiction, our T *and* not T.

4.13 The End

Now that we have found our contradiction of $T\wedge(\sim T)$ we should make sure to point out this contradiction just in case our reader missed this, letting everyone know we have come to the end of our proof by contradiction. We, of course, can do this by following numerous linguistic paths but we must choose one so:

Yet, $(a-b)+(a+b)$ is an integer and cannot be both even and odd, which is a contradiction. Thus using proof by contradiction we have successfully shown that for all integers a and b if $a-b$ is odd then $a+b$ is odd.

As usual we collect it in our tldr boxes...

Example 4.13.1 ***Prove:*** For all integers a and b if $a-b$ is odd then $a+b$ is odd.

Let a and b be arbitrary integers. For the sake of contradiction assume that $a-b$ is odd yet $a+b$ is not odd. Since we assumed that $a+b$ is not odd, by Lemma 4.6.1, p. 52 we have that $a+b$ is even. By the definition of odd we can obtain an integer ℓ so that $a-b=2\ell+1$. As well, by the definition odd (Definition 3.3.2, p. 34) we are able to select an integer s so that $a+b=2s$. Calculate:

$$\begin{aligned}(a-b)+(a+b) &= (2\ell+1)+(2s)\\ &= 2\ell+2s+1\\ &= 2(\ell+s)+1\end{aligned}$$

since $\ell+s$ is an integer by the definition of odd, we have that $(a-b)+(a+b)$

is odd. Yet, we can also calculate as:

$$(a-b)+(a+b) = (a+a)+(b-b) = 2a$$

yet, since a is an integer by the definition of even we have that $(a-b)+(a+b)$ is even, or in light of Lemma 4.6.1, p. 52 we have that $(a-b)+(a+b)$ is even.

Yet, $(a-b)+(a+b)$ is an integer and cannot be both even and odd, which is a contradiction. Thus using proof by contradiction we have successfully shown that for all integers a and b if $a-b$ is odd then $a+b$ is odd. □

4.14 $\sqrt{2}$ is Irrational

This next proof is a proof that I believe every single student in mathematics should know and love. It is this proof that I learned very early on in my math career that shaped how I understood mathematics. I would meet people and tell them "I'm a math major" and they would say things like "ugh I always hated math" and I would tell them "no, math is not what you think math is." It is about truths. For example take an extremely simple shape the right triangle, literally just put two sticks at a sharp angle and connect the two edges with another stick. This third stick has a length that is not a fraction of either of the other sides. Pythagoras went to his grave believing that it must, but we can show beyond a shadow of a doubt it is not.

Before we jump into that proof it will be helpful to have a lemma that we can call on, in all honesty to shorten our work load (what lemma's are best for).

Lemma 4.14.1 *If 2 divides m^2 then 2 divides m*

Proof. Let m be an integer. We will prove this using contraposition, that is we will assume 2 does not divide m, thus by Lemma 4.6.1, p. 52 m is odd. Hence we can find an integer k such that $m = 2k+1$.
Calculate:

$$\begin{aligned} m^2 &= m \cdot m \\ &= (2k+1)(2k+1) \\ &= 4k^2+4k+1 \\ &= 2(2k^2+2k)+1 \end{aligned}$$

Since $2k^2+2k$ is an integer, by definition of odd, m^2 is odd, hence by Lemma 4.6.1, p. 52 m^2 is not even. Thus by proof by contraposition, if 2 divides m^2 then 2 divides m. ■

Prove: $\sqrt{2}$ is irrational.

Before we begin any proof we sing our song, although it is a little different when we're using contradiction (play-along):

"What's the P?"**1.** $\sqrt{2}$ is irrational

"What's the Q?"**2.** There is no Q this time!

"What're the definitions?"**3.** Rational, relatively prime, and divides (create reference here!)

"Now, what to do?"**4.** Proof by contradiction - because I said so!

4.15 The Beginning

For a proof by contradiction we need to begin by assuming what we need to prove is false, and to remind you this could be jarring to a reader so let them know what you are doing, for example we could write:

For the sake of contradiction assume that $\sqrt{2}$ is rational. That is, it is not true that $\sqrt{2}$ is irrational

4.16 The Muddle

Now, we continue with our song by applying the definitions we can, per the definition of rational (Definition 4.1.3, p. 50), we can find two integers p and q so that $\sqrt{2} = \frac{p}{q}$ and

$$T: \ \text{GCD}(p, q) = 1$$

Next, we will do exactly what any good calculus student would do and that is "get-rid-of" that square root.

Calculate:

$$\text{square both sides: } 2 = \frac{p^2}{q^2}$$
$$\text{multiply both sides by } q^2 : 2q^2 = p^2$$

But, q^2 is an integer, thus by the definition of even, p^2 is even. Hence, by Lemma 4.14.1, p. 57 we can conclude that p is even

Thus, by the definition of even we can find an integer m so that $p = 2m$.

Now, we can play our common replacement game.

Calculate again:

$$\begin{aligned} 2q^2 &= (2m)^2 \\ &= 4m^2 \\ \text{Divide both sides by 2 } q^2 &= 2m^2 \end{aligned}$$

But m^2 is an integer, so, by definition of even, q^2 is even, and again by Lemma 4.14.1, p. 57, q is even.

Since $2 \mid p$ and $2 \mid q$, 2 is a common divisor, and thus by definition of greatest common divisor (Definition 4.1.2, p. 50) we have that $\text{GCD}(p, q) \geq 2$, yet this means that

$$\sim T: \ \text{GCD}(p, q) \neq 1$$

4.17 The End

So now that we have found our contradiction $T \wedge (\sim T)$ we are done, but just incase the reader missed this contradiction as you unwrapped it, lets put it all in one place.

Thus we have shown $\text{GCD}(p, q) = 1$ ***and*** $\text{GCD}(p, q) \neq 1$ which is a contradiction. Thus by proof by contradiction, we have shown that $\sqrt{2}$ is irrational.

Now let's see everything written together in a single spot.

Example 4.17.1 ***Prove:*** $\sqrt{2}$ is irrational.

For the sake of contradiction assume that $\sqrt{2}$ is rational. That is, it is not true that $\sqrt{2}$ is irrational. By the definition of rational (Definition 4.1.3, p. 50),

we can find two integers p and q so that $\sqrt{2} = \frac{p}{q}$ and $\text{GCD}(p, q) = 1$

Calculate:

$$\text{square both sides: } 2 = \frac{p^2}{q^2}$$
$$\text{multiply both sides by } q^2 : 2q^2 = p^2$$

But, q^2 is an integer, thus by the definition of even, p^2 is even. Hence, by Lemma 4.14.1, p. 57 we can conclude that p is even

Thus, by the definition of even we can find an integer m so that $p = 2m$.

Calculate again:

$$\begin{aligned} 2q^2 &= (2m)^2 \\ &= 4m^2 \\ \text{Divide both sides by 2 } q^2 &= 2m^2 \end{aligned}$$

But m^2 is an integer, so, by definition of even, q^2 is even, and again by Lemma 4.14.1, p. 57, q is even.

Since $2 \mid p$ and $2 \mid q$, 2 is a common divisor, and thus by definition of greatest common divisor (Definition 4.1.2, p. 50) we have that $\text{GCD}(p, q) \geq 2$, yet this means that $\text{GCD}(p, q) \neq 1$

Thus we have shown $\text{GCD}(p, q) = 1$ ***and*** $\text{GCD}(p, q) \neq 1$ which is a contradiction. Thus by proof by contradiction, we have shown that $\sqrt{2}$ is irrational. □

4.18 Biconditional Proofs

Proofs of statements with a biconditional are ubiquitous in mathematics. As you have seen all of our definitions are biconditional statements. We use the biconditional to me mean equivalent. These equivalences in future math classes give tools for proving conditions without working to more intuitive definitions, instead by giving more usable ones.

You can prove biconditionals in many ways; the one we will take time to examine the what I tell my students is the "safe way". It is the two-way proof.

Two-Way proof of $P \iff Q$.

Prove: $P \implies Q$
Prove: $Q \implies P$
Therefore, $P \iff Q$

That this proof method is valid follows from the fact that the following is an equivalence:

$$[P \iff Q] \equiv [(P \implies Q) \wedge (Q \implies P)]$$

to verify this equivalence we have the following truth table.

P	Q	$P \implies Q$	$Q \implies P$	$[P \implies Q] \wedge [Q \implies P]$	$P \iff Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Figure 4.18.1

For our next examples we spare the reader the in-depth treatment as it is simply two direct proofs.

Example 4.18.2 ***Prove:*** a is odd if and only if $a+1$ is even.

Proof. Let a be an integer
$[\implies]$ (if a is odd then $a+1$ is even)
Assume a is odd. Hence, by definition of odd (Definition 3.3.2, p. 34) we can find an integer k so that $a = 2k+1$
Calculate

$$\begin{aligned} a+1 &= 2k+1+1 \\ &= 2k+2 \\ &= 2(k+1) \end{aligned}$$

Since $k+1$ is an integer, by definition of even, $a+1$ is even. Hence by direct proof, if a is odd then $a+1$ is even.
$[\impliedby]$ (if $a+1$ is even, then a is odd)
Assume $a+1$ is even. Hence, by definition of even we can find an integer m such that $a+1 = 2m$
Calculate:

$$\begin{aligned} a+1 &= 2m \\ a &= 2m-1 \\ &= 2m-1-1+1 \\ &= 2m-2+1 \\ &= 2(m-1)+1 \end{aligned}$$

Thus, since $m-1$ is an integer, by definition of odd, a is odd. Thus by direct proof if $a+1$ is even, then a is odd.
Since we showed by direct proof that if a is odd then $a+1$ is even ***and*** if $a+1$ is even, then a is odd, then a is odd ***if and only if*** $a+1$ is even.□ ■

□

Example 4.18.3 ***Prove:*** For any integer a; a is odd if and only if a^3 is odd.

Proof. Let a be arbitrary integer.
$[\implies]$ (if a is odd then a^3 is odd)
Assume that a is odd, by the definition of odd (Definition 3.3.2, p. 34) we can find an integer k so that $a = 2k + 1$. Now calculate:

$$\begin{aligned} a^3 &= (2k+1)^3 \\ &= (2k+1)(2k+1)(2k+1) \\ &= (4k^2+4k+1)(2k+1) \\ &= 8k^3+12k^2+6k+1 \\ &2(4k^3+6k^2+3k)+1 \end{aligned}$$

since $(4k^3 + 6k^2 + 3k)$ is an integer a^3 is odd.
$[\impliedby]$ (if a^3 is odd then a is odd.)
For the sake of contraposition assume that a is not odd, thus by Lemma 4.6.1, p. 52 we have that a is even. By the definition of even we can find an integer t so that $a = 2t$. Now calculate:

$$a^3 = (2k)^3 = 8k^3 = 2[4k^3]$$

since $4k^3$ is an integer, we can conclude a^3 is even, thus by Lemma 4.6.1, p. 52 we have that a^3 is not odd. Therefore by contraposition we have that if a^3 is odd then a is odd. ■
□

There is another method for proving an *if and only if* statement it is not recommended for the student who is just starting their proving journey, but for completeness I would be remiss if I did not include it.

One-Way Proof of $P \iff Q$.

P iff T_1
T_1 iff T_2
...
T_{n-1} iff T_n
T_n iff Q

The reason I warn beginning students away from this is that too often students get it in their head that the faster way is better, in calculus they see the limit definition for the derivative then learn the power rule and say to themselves well I'm never going back to the limit.

Again for the sake of completion we provide an example, the diligent hard working student will do their best to see why a backwards proof would be *boring*.

Example 4.18.4 ***Prove:*** For any two integers a and b; $a^2 < -b^2$ if and only if $(a-b)^2 < -2ab$

Proof. Let a and b be arbitrary integers, not that
$a^2 < -b^2$
if and only if
$a^2 + b^2 < 0$
if and only if
$a^2 + b^2 - 2ab < -2ab$
if and only if
$(a-b)^2 < -2ab$
Therefore $a^2 < -b^2$ if and only if $(a-b)^2 < -2ab$ ■

□

4.19 Proof by Exhaustion

Our next proof method is not really a standalone method; other methods will need to accompany it. We will introduce it using the direct proof as the accompaniment. Proof by cases can also be viewed as specific example of Section 3.28, p. 44.

4.20 What are Cases?

Unlike the example in Section 0.6, p. 3 where the are an unlimited amount of integers to choose from, sometimes we have a finite and more tenable collection of possibilities than we could actually check or prove in each of these situations.

The following is the basic *shape* of a proof by cases.

Proof by Cases.

Case 1: a proof of the first case
Case 2: a proof of the second case
⋮
Case n: a proof of the n^{th} case

At its most basic a proof by cases is an instance of proofs "Assuming an Or" from Section 3.28, p. 44 where one is tasked to prove $(P \vee R) \implies Q$, then we would split the problem into proving $P \implies Q$ as our *first case* and then $R \implies Q$ as our *secondcase*. For examples of this the reader is reffered to Section 3.28, p. 44.

Another common place proof by cases comes up are when we are trying to prove propositions in the form of:

$$\forall x \; P(x)$$

for some predicate $P(x)$. There are many common places that proof by cases in the previous form come up, for example the following:

- $\forall x \in \mathbb{Z}$ we have either x is even or x is odd.
- $\forall x, y \in \mathbb{Z}$ either $x|y$ or $x|(y - r)$ for some integer $0 < r < |x|$
- $\forall x \in \mathbb{R}$ either $x \geq 0$ or $x < 0$

We have already proven that the first point is true in Lemma 4.6.1, p. 52. For the second point, a more general result, we provide the following lemma.

Lemma 4.20.1 *For any two integers x and y, there exists an $r \in \mathbb{Z}$ such that $0 \leq r < |x|$ and $x|(y - r)$*

Proof. Let x and y be integers. By the division algorithm from Section 3.2, p. 33 we can find a $q, r \in \mathbb{Z}$ such that $0 \leq r < |x|$ and $y = qx + r$. Hence subtracting both sides by r we get $y - r = qx$ since q is an integer by the definition of divides (Definition 3.3.3, p. 34) we have that $x|(y - r)$. ■

4.21 Exhaustive Examples

We now include some examples, the first one is an example of breaking into the cases of even and odd.

Example 4.21.1 ***Prove:*** for any integer a, $a(a+1)$ is even.

Proof. Let a be an integer. a is either even, or odd.
Case 1: Assume a is even.
Hence by definition of even, we can find an integer k such that $a = 2k$.
Calculate:

$$\begin{aligned} a(a+1) &= 2k(2k+1) \\ &= 4k^2 + 2k \\ &= 2(2k^2 + k) \end{aligned}$$

Thus, since $k^2 + k$ is an integer, by definition of even, $a(a+1)$ is even. Thus by direct proof, if a is even then $a(a+1)$ is even.
Case 2: Assume a is odd. Thus by definition of odd, we can find an integer m such that $a = 2m + 1$
Calculate

$$\begin{aligned} a(a+1) &= (2m+1)(2m+1+1) \\ &= (2m+1)(2(m+1)) \\ &= 2[(2m+1)(m+1)] \end{aligned}$$

Thus since $(2m+1)(m+1)$ is an integer, according to the definition of even, $a(a+1)$ is even. Thus by direct proof if a is odd then $a(a+1)$ is even.
Thus since case 1 and case 2 hold, by proof by cases, and by direct proof, $a(a+1)$ is even. □ ■

□

Example 4.21.2 ***Prove:*** for any integer n, if n is odd, then there exists an integer j so that $n = 4j - 1$ or $n = 4j + 1$

Proof. Let n be an integer. Assume n is odd. By definition of odd we can find an integer m such that $n = 2m + 1$
Case 1: Assume m is even. By definition of even we can find an integer j such that $m = 2j$.

$$\begin{aligned} n &= 2m + 1 \\ &= 2(2j) + 1 \\ &= 4j + 1 \end{aligned}$$

Hence case 1 holds by direct proof.
Case 2: Assume m is odd. Thus by definition of odd we can find an integer k so taht $m = 2k + 1$
Calculate:

$$\begin{aligned} n &= 2n + 1 \\ &= 2(2k + 1) \\ &= 4k + 3 \\ &= 4k + 4 - 2 \\ &= 4(k + 1) - 1 \end{aligned}$$

Hence case 2 holds by direct proof.
Thus, since case 1 and case 2 hold, by proof by cases, if n is odd, then we can find an integer$j$ so that $n = 4j - 1$ or $n = 4j + 1$ ■

□

Example 4.21.3 ***Prove:*** For every integer a, if $3|a^2$ then $3|a$.

Proof. Let a be an arbitrary integer. For the sake of contrapositive assume that 3 does not divide a. By Lemma 4.20.1, p. 62 since the only numbers greater than zero and strictly less than 3 are 1 and 2 either $3|(a-1)$ or $3|(a-2)$
Case 1: Assume $3|(a-1)$.
By definition of divides we can find an integer k so that $a-1=3k$, hence by adding 1 to both sides of the equation we get $a=3k+1$. Now calculate:

$$\begin{aligned} a^2 &= (3k+1)^2 \\ &= 9k^2+6k+1 \\ &= 3(3k^2+2k)+1 \end{aligned}$$

Hence $a^2-1=3(3k^2+2k)$. Since $3k^2+2k$ is an integer by definition of divides $3|(a^2-1)$ thus by Lemma 4.20.1, p. 62 we have that 3 does not divide a^2
Case 2: Assume $3|(a-2)$.
By definition of divides we can find an integer t so that $a-2=3t$, hence by adding 2 to both sides of the equation we get $a=3t+2$. Now calculate:

$$\begin{aligned} a^2 &= (3t+2)^2 \\ &= 9t^2+12t+4 \\ &= 9t^2+12t+3+1 \\ &= 3(3t^2+4t+1)+1 \end{aligned}$$

Hence $a^2-1=3(3t^2+4t+1)$. Since $3t^2+4t+1$ is an integer by definition of divides $3|(a^2-1)$ thus by Lemma 4.20.1, p. 62 we have that 3 does not divide a^2
Therefore by proof by cases 3 does not divide a^2, and hence by proof by contraposition if $3|a^2$ then $3|a$. □ ■
□

4.22 Existential Proofs

In this section we will we discuss some proofs surrounding the existential quantifier. We begin by explaining the basics of proving statements that involve an existential.

Proving $\exists x \in \mathcal{U}\ P(x)$.

Produce an actual candidate $c \in \mathcal{U}$
show $P(c)$ is true
Therefore $\exists x \in \mathcal{U}\ P(x)$

It's the old saying of just "show me". Proving existentials in this manner come up in your future algebra and analysis courses repeatedly as some of their most important concepts are defined with an exists. The following example is perhaps not the most enlightening but it does serve the purpose of a first example.

Example 4.22.1 ***Prove:*** There exists a rational number x such that $x+\frac{3}{4}=2$

Proof. I now present for your consideration the rational number:

$$\frac{5}{4}$$

One can see that this is indeed a rational number as both 5 and 4 are integers and $\text{GCD}(5, 4) = 1$ thus it satisfies the definition of a rational number (Definition 4.1.3, p. 50). To see that this rational number indeed does the job for our statement notice that

$$\begin{aligned}\frac{5}{4} + \frac{3}{4} &= \frac{5+3}{4} \\ &= \frac{8}{4} \\ &= 2\end{aligned}$$

therefore there truly does exist a rational number x so that $x + \frac{3}{4} = 2$ ■

□

For our next example we will dig a little deeper into the existential proof in more of a mock experience to your future courses. But first, we will need to take advantage of the following lemma, which we present with proof here, even though the proof does not involve an existential.

Lemma 4.22.2 *For all positive integers a and b if $a|b$ then $a \leq b$*

Proof. Let a and b be positive integers. For the sake of contradiction assume that $a|b$ and $b < a$. By the definition of divides (Definition 3.3.3, p. 34) we can find an integer k so that $b = ak$, now since $b < a$ then $b = 0 \cdot a + b$ where 0 is the quotient and b is the remainder satisfies the division algorithm (Section 3.2, p. 33), yet since both a and b are positive the k also satisfies the condition of quotient. This is a contradiction as the quotient from the division algorithm is unique. □ ■

Example 4.22.3 ***Prove:*** For any integers x and y, there exists a smallest positive integer that is in the 1-d integer cone formed by x and y.

Proof. Let x and y be integers, next we need to provide an integer which is smallest among all integers in the 1-d integer cone formed by x and y. We present for your scrutiny the integer

$$d = \text{GCD}(x, y)$$

Now, we are left with the task to show that d is the smallest positive integer in the 1-d integer cone formed by x and y. To say this another way we need to prove that the greatest common divisor of x and y is the smallest positive integer in the 1-d integer cone formed by x and y.
To prove this let d be the smallest positive integer in the 1-d integer cone formed by x and y (it will be our goal to show it is our d from above). By the definition of the 1-d integer cone (Definition 4.1.4, p. 50) we can find integers s and t such that

$$d = sx + ty$$

To show that this smallest positive integer is the greatest common divisor by the definition of greatest common divisor (Definition 4.1.2, p. 50) first it must be a divisor of both x and y.
By the division algorithm (Section 3.2, p. 33) we can find positive integers q and r such that $0 \leq r < d$ such that $x = qd + r$ yet by substituting in the form of d above we see $x = q(sx + ty) + r$ and hence

$$r = x - q(sx + ty) = (1 - qs)x + (qt)y$$

and since $(1 - qs)$ and qt are both integers by the definition of 1-d integer cone, then r is in the 1-d integer cone formed by x and y yet we assumed d was the smallest positive one, so because we assumed $0 \leq r < d$ then $r = 0$ hence $a = qd$ and since q is an integer by the definition of divides $d|x$.
similarly by the division algorithm (Section 3.2, p. 33) we can find positive integers z and w such that $0 \leq w < d$ such that $y = zd + w$ yet by substituting in the form of d above we see $y = z(sx + ty) + w$ and hence

$$w = y - z(sx + ty) = (zs)x + (1 - zt)y$$

and since $(1 - zt)$ and zs are both integers by the definition of 1-d integer cone, then w is in the 1-d integer cone formed by x and y yet we assumed d was the smallest positive one, so because we assumed $0 \leq w < d$ then $w = 0$ hence $y = zd$ and since z is an integer by the definition of divides $d|y$.
Therefore by the definition of common divisor (Definition 4.1.1, p. 50) d is a common divisor of x and y.
By the definition of greatest common divisor (Definition 4.1.2, p. 50) we still need to show that any other divisor is smaller than d. To do this let c be a common divisor of x and y. By definition of common divisor both $c|x$ and $c|y$ hence by definition of divides (Definition 3.3.3, p. 34) we can find integers a and b so that $x = ac$ and $y = bc$ thus substituting in our above relations we have

$$d = sac + tbc = (sa + tb)c$$

and since $sa + tb$ is an integer by the definition of divides $c|d$. Finally by Lemma 4.22.2, p. 65 we have $c < d$ as desired.
Since we have verified both parts in the definition of greatest common divisor we have that

$$d = \text{GCD}(x, y)$$

□ ■
□

Next, we will discuss unique existence. This quantifier adds a step to our proving method as we are not simply saying there is an element out there we are saying there is only one of those elements. Uniqueness is a common theme in algebra and analysis as well.

Proof of $\exists! x \in \mathcal{U}\ P(x)$.

Prove $\exists x \in \mathcal{U}\ P(x)$
Assume you have $a \in \mathcal{U}$ and $b \in \mathcal{U}$ so that $P(a)$ is true and $P(b)$ is true.
Prove $a = b$

For our first example we will explore a common theme from your future algebra courses.

Example 4.22.4 ***Prove:*** There exists a unique integer, a, so that for all integers b

$$a + b = b$$

Proof. The integer that we submit for your deliberation is:

$$0$$

To see that zero works, to satisfy the existence, notice that when we choose an arbitrary integer x that: $0 + x = x$.
Now to prove the uniqueness, assume that we have two integers c and d so that for any integer b both $c + b = b$ and $d + b = b$. So in particular

$$c = d + c = c + d = d$$

that is $c = d$.
Therefore, we have shown that there exists an integer with the desired property and that this integer is unique. □ ■

□

4.23 Exercises

1. Using contraposition for the following prove for every integer a that
   (a) if a is even then $a + 1$ is odd
   (b) if a is odd then $a + 2$ is odd
   (c) if a^2 is not divisible by 4 then a is odd
2. Using contradiction for the following prove for any integer a that
   (a) if ab is odd then both a and b are odd
   (b) if a is odd then $a + 1$ is even.
3. Using proof by cases for the following prove for any integer a that
   (a) If 5 does not divide a then 5 does not divide a^2
   (b) $a(a - 1)$ is even
   (c) $2a - 1$ is odd
   (d) $a^2 + a + 3$ is odd

4. Prove the following biconditional statments for any integers a, b, c, and d (you are allowed to divide for this exercise)
   (a) a is odd if and only if $a + 1$ is even
   (b) $ac|bc$ if and only if $a|b$
   (c) $a + c = b$ and $2b - a = d$ if and only if $a = b - c$ and $b + c = d$
5. Prove the following statements involving existential
   (a) For any integer a there exists an unique integer b so that $a + b = 0$
   (b) There exists a rational number x such that $x + \frac{3}{2} = 4$
6. Prove that $\sqrt{3}$ is not a rational number.

Chapter 5

Set Theory

Now in this second half of the course we move our adventure of exploring proofs by diving deeper into the new playground of *naive set theory*. This adventure will begin by considering sets of numbers, toys, animals and all sort of creations. To gently introduce our students to the proofs involved with such creatures we will provide the (now) familiar sets of numbers.

While indeed we gave the reader the minimum needed from set theory to play with quantifiers in Section 1.16, p. 17 in this chapter we essentially start over re-defining it all.

5.1 What is a Set?

While set theory has been rigorously defined axiomatically, in this course we choose to only skim the surface using a whole lot of intuition and the propositional logic that we developed in Chapter 1, p. 4. The main object of study in set theory is the *set*. Intuitively a set is a magic bag filled with stuff... or nothing... Georg Cantor the russian mathematician, credited as the father of set theory, first defined the set as:

A set is a gathering together into a whole of definite, distinct objects of our perception or of our thought—which are called elements of the set.

We include a much more boring description.

Definition 5.1.1 Set. A **set** is a well defined collection of objects. ◊

Definition 5.1.2 Element. The objects in a set are called **elements** or *members*. ◊

We will most often denote sets with capital letters like: A, B, C etc. Furthermore we will denote elements with lowercase letters like a, b, x, etc.

$\in$ Notation.

To indicate that x is an element of a set A we will write:

$$x \in A$$

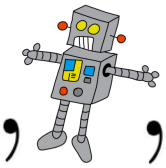
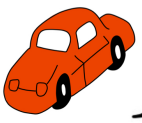
To indicate that x is not an element of a set A we will write:

$$x \notin A$$

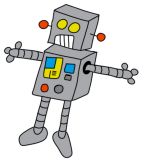
Membership to a set is a ***proposition*** as it is either true or false.

To define a specific set we can simply list all of it's elements. To do so we encompass the elements we wish to include between braces: { and } and separate the elements with a comma.

Example 5.1.3 Consider the following set A

$A = \{ 3, $  $, $  $, $  $\}$

and note the following example of the membership notation.

 $\in A$

You can also indicate the negation of membership

 $\notin A$

□

Note 5.1.4 A set has no order, and you cannot repeat elements.

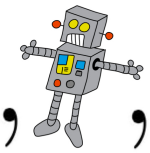
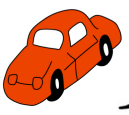
Definition 5.1.5 Cardinality. For a set A we call the **cardinality** or **order** of A is the number of elements in the set A, denoted as

$$|A|$$

◊

In this course we will only mention this concept when the sets are finite, when sets are infinite the cardinality of a set flourishes a beautiful theory, one which we will not dive into in this text but is quite amazing.

Example 5.1.6 Consider the following set

$A = \{ 3, $  $, $  $, $  $\}$

We see that the number of elements in the set A is 4 hence, $|A| = 4$. □

Sets come in many different shapes and flavors and throughout your mathematical career you will need to become extremely comfortable with sets, and depending on the discipline you will either love or hate the following set, but you will never deny that it is perhaps one of the most important sets.

Definition 5.1.7 Empty Set. We will call the set containing no elements

the **empty set**, we denote the empty set as $\emptyset$, that is

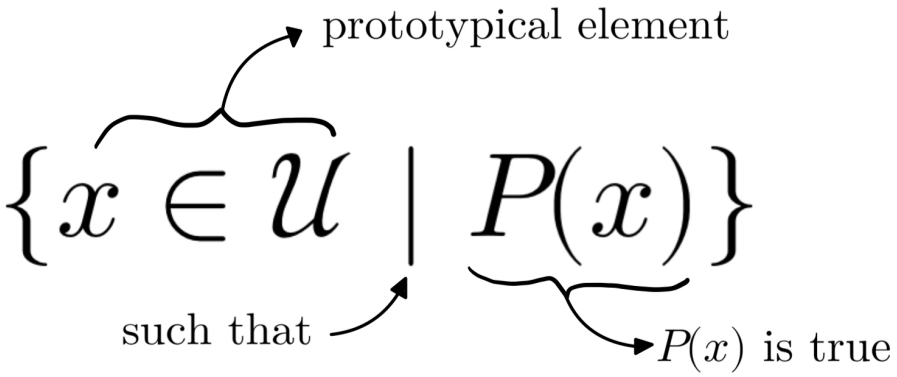
$$\emptyset = \{\}$$

$\Diamond$

As there are no elements in $\emptyset$, therefore $|\emptyset| = 0$, as well, to the the disjoy of all combinatorists, the statement $x \in \emptyset$ is a contradiction (that is always false).

5.2 Set Builder Notation

Membership is the defining characteristic of a set, thus it is helpful to define a set by conditions for membership. One way to do that we call **set-builder notation**.



This is our way of defining membership $a \in \{x \mid P(x)\}$ if and only if $P(a)$ is true.

Example 5.2.1 We include some sets defined with set-builder notation.

(A) $\{x \in \mathbb{Z} \mid -5 < x < 5\}$

(B) $\{y \in \mathbb{Z} \mid y = 3a + 1 \text{ for some } a \in \mathbb{Z}\}$

(C) $\{z \in \mathbb{Q} \mid |z| < \sqrt{7}\}$

$\square$

In Example 5.2.1, p. 71 (B) we defined the condition with a quantifier, specifically $\exists a \in \mathbb{Z}$. This is an extremely common use-case in mathematics. I bring this up here to warn the student that this is perhaps the most common quantifier to be *hidden*. That is, we would most likely see it presented as:

$$\{y \in \mathbb{Z} \mid y = 3a + 1,\ a \in \mathbb{Z}\}$$

To defend the mathematician which chooses to present it in this manner, we mostly study objects with a well defined and unique multiplication, that is there is only one unique integer a that satisfies $y = 3a + 1$ for a given y.

Adding to the possible confusion yet important to understand, for this *same* set it is true that

$$\forall k \in \mathbb{Z}\ (3k + 1) \in \{y \in \mathbb{Z} \mid y = 3a + 1,\ a \in \mathbb{Z}\}$$

that is, by defining a set with an existential condition we are actually defining a universal relationship. To top it off we often do not even mention the universal relationship and *hide* the existential one, all in the sake of brevity and the word *obvious*.

5.3 Comparing and Combining Sets

Now we will begin comparing sets. Our first tool of comparison is the concept of subset.

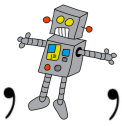
Definition 5.3.1 Subset. We say that the set A is a **subset** of a set B, denoted $A \subseteq B$, if and only if for all $x \in \mathcal{U}$,

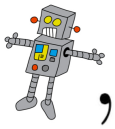
$$x \in A \implies x \in B$$

$\Diamond$

To say that in more plain language, $A \subseteq B$ means B contains all the elements of A, it is noteworthy that B may contain more than just those elements from A.

Example 5.3.2 Consider the sets

$A = \{3,$    $\}$

$B = \{$      $, 3\}$

notice that every element from A can also be found in B, that is $A \subseteq B$. $\square$

Example 5.3.3 Define the sets

$$A = \{3, 6, 9, 12, 15\}$$

$$B = \{x \in \mathbb{Z} \mid x = 3a \text{ for some } a \in \mathbb{Z}\}$$

Notice that $A \subseteq B$ since

$$\begin{aligned} 3 &= 3 \cdot 1 \\ 6 &= 3 \cdot 2 \\ 9 &= 3 \cdot 3 \\ 12 &= 3 \cdot 4 \\ 15 &= 3 \cdot 5 \end{aligned}$$

that is, every element of A is also an element of B. $\square$

When a set A has exactly the same elements of a set B we say those set are equal. The following definition makes this more rigorous

Definition 5.3.4 Equal Sets. We say that a set A is **equal** to a set B, denoted $A = B$, if and only if both

$$A \subseteq B$$

and

$$B \subseteq A$$

or equivalently by:

$$\forall x \in \mathcal{U}\ x \in A \iff x \in B$$

$\Diamond$

Sets are equal exactly when you would think they are, when they are the same set. Yet, as hopefully you have been piecing together in this journey, to prove things like "they are the same" we need a bit more rigor and propositional *guidance* to prove truth. Shortly we will venture into the world of proving with these sets, yet lets take a little time not just to build rigorous definitions but to build our intuition further.

We now venture into combining sets, that is making new sets given one or more sets.

Definition 5.3.5 Union. We define the **union** of two sets A and B, denoted $A \cup B$ as the set:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

◊

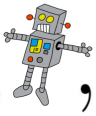
As is done for a set, we must define what it takes for membership to this set. For the union membership is allowed when membership of either A or B is established. In more common vernacular, this says that the union of two sets is anything from either set.

Example 5.3.6 Consider the following sets

$A = \{3, $  $, $  $, $  $\}$

$B = \{$  $, $  $, $  $\}$

then the union of A and B is as follows

$A \cup B = \{$  $, $  $, $  $, $  $, $  $, 3\}$

□

Example 5.3.7 Define the sets

$$A = \{x \in \mathbb{R} \mid 0 \leq x < 10\}$$

$$B = \{x \in \mathbb{R} \mid -10 < x < 0\}$$

Thus the union of these two sets is

$$A \cup B = \{x \in \mathbb{Z} \mid -10 < x < 10\}$$

since any real number between -10 and 10 are either included between 0 and 10 or between -10 and 0. □

Another way to combine sets is to consider only the elements in which they share, this is our next definition.

Definition 5.3.8 Intersection. The **intersection** of two sets A and B, denoted $A \cap B$, is defined as

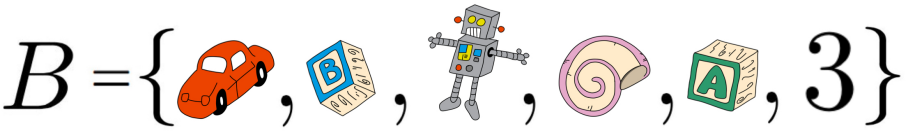
$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

◊

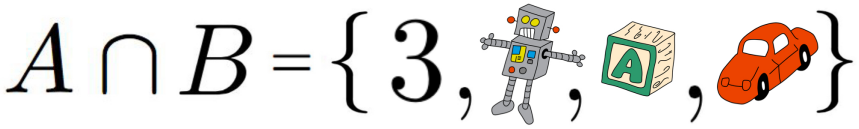
Again, as these are sets, we must define what it means to be a member of this set. For the intersection membership is defined for those elements that have membership to both the sets A and B. Or in other words, the intersection only has the things that are shared between two sets.

Example 5.3.9 Consider the following sets

$A =$ 

$B =$ 

therefore the intersection of these two sets are

$A \cap B =$ 

Notice that elements in the intersection are exactly those that show up in both A and B. □

Example 5.3.10 Define the sets

$$A = \{x \in \mathbb{Z} \mid 0 < x \leq 10\}$$

$$B = \{x \in \mathbb{Z} \mid x = 2y \text{ for some } y \in \mathbb{Z}\}$$

Thus the intersection of these two sets is

$$A \cap B = \{2, 4, 6, 8, 10\}$$

since those are the only even integers between 0 and 10 (including 10). □

The last construction showed where two sets were the same yet, now we explore where they differ.

Definition 5.3.11 Difference. The **difference** of a set A and a set B, denoted $A - B$, is the set defined as

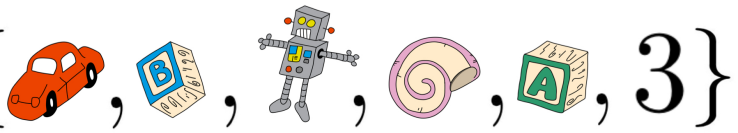
$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

◊

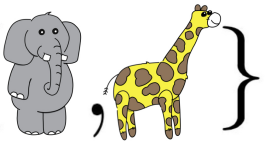
The difference of A and B consists of the things that are in A, but not in B.

Example 5.3.12 Consider the sets

$A =$ 

$B =$  $3\}$

thus the set difference of A and B is

$A - B =$ 

notice that the difference is made up only of elements that appear in A yet do not appear in B. □

Example 5.3.13 Define the sets

$$A = \{x \in \mathbb{Z} \mid 0 < x < 10\}$$

$$B = \{x \in \mathbb{Z} \mid x = 2y \text{ for some } y \in \mathbb{Z}\}$$

Thus the difference of these two sets is

$$A - B = \{1, 3, 5, 7, 9\}$$

since these are there integers between 0 and 10 that are not even. □

To end this section we have been quite flippant on our universe of discourse, yet with a well defined one we can look at the set difference involving the universe.

Definition 5.3.14 Compliment. The **compliment** of a set A in the universe $\mathcal{U}$, is defined as the following set,

$$A^c = \{x \in \mathcal{U} \mid x \notin A\}$$

or

$$A^c = \mathcal{U} - A$$

◊

The compliment can, perhaps, most simply be stated as everything that is not in A.

Example 5.3.15 For this example consider the universe of discourse as the integers, $\mathcal{U} = \mathbb{Z}$, and consider the set of all even numbers, that is the set

$$A = \{x \in \mathbb{Z} \mid x = 2y \text{ for some } y \in \mathbb{Z}\}$$

Then the compliment of A is all the integers that are not even, or in lieu of Lemma 4.6.1, p. 52 we have that

$$A^c = \{x \in \mathbb{Z} \mid x = 2y + 1 \text{ for some } y \in \mathbb{Z}\}$$

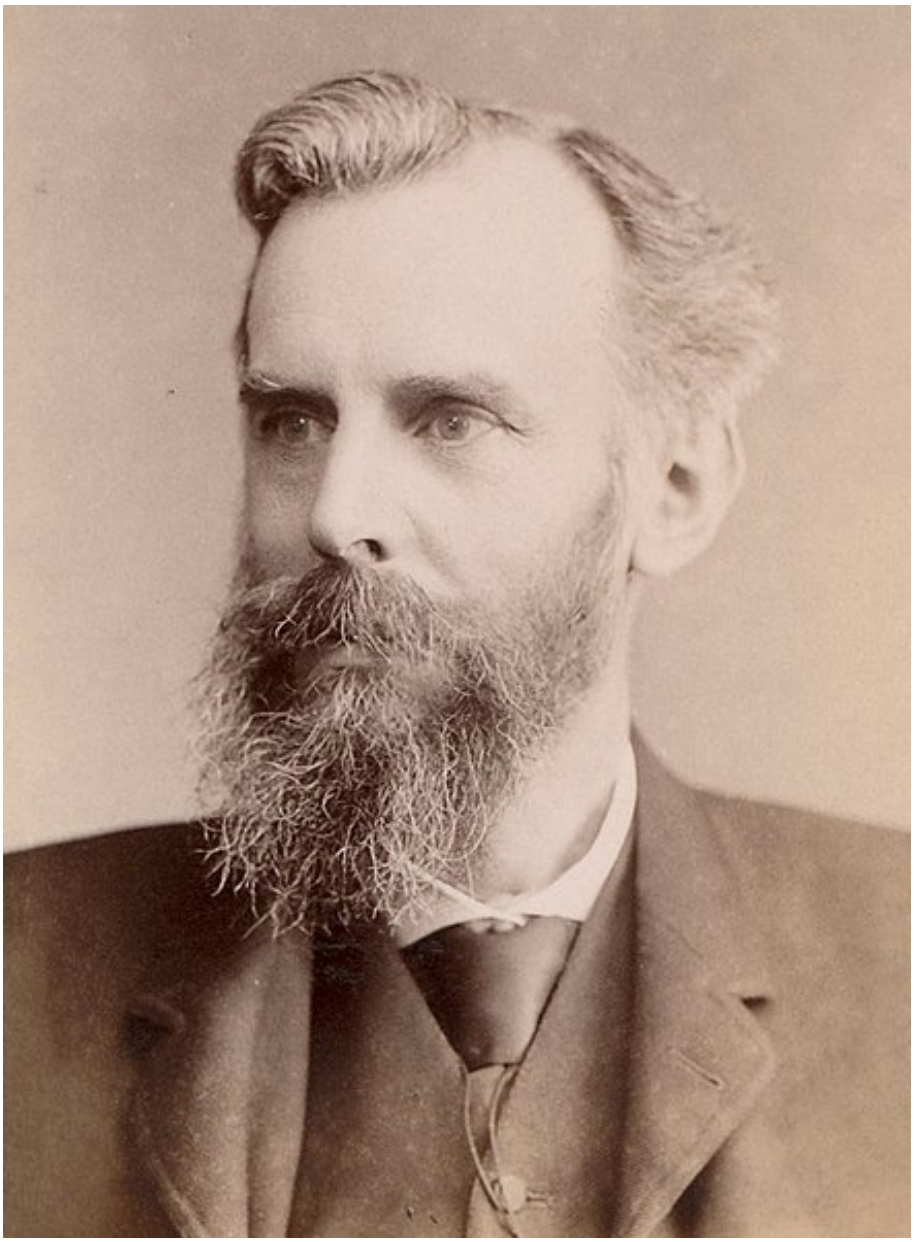
□

5.4 Venn Diagrams and Logic of Sets

To understand/describe the relationship between sets we often use a tool known as **Venn Diagrams**. In simplest terms a Venn diagram is a drawing repre-

senting the sets we are considering, we draw a circle for each set, and imagine the elements are inside the circle. Further, in this section we will use the basic underpinning of propositional logic to pick apart some logical conclusions from set theory.

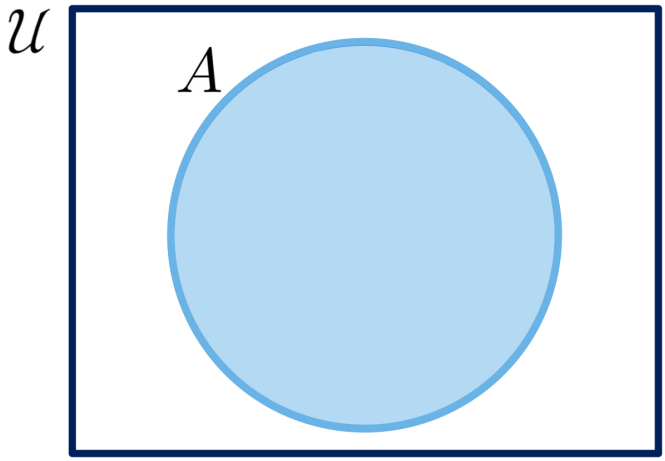
John Venn was an English mathematician that in the 1800's introduced Eulerian Circles, which we now don with his name.



5.5 Venn Diagrams

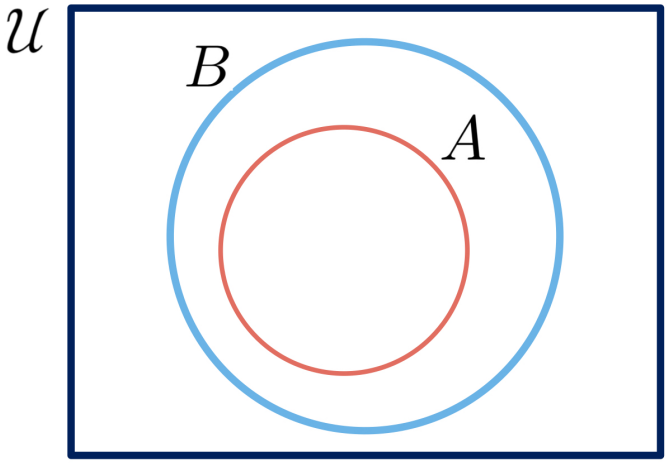
We now provide some basic examples of Venn diagrams.

Example 5.5.1 A Venn diagram for a singular set A



□

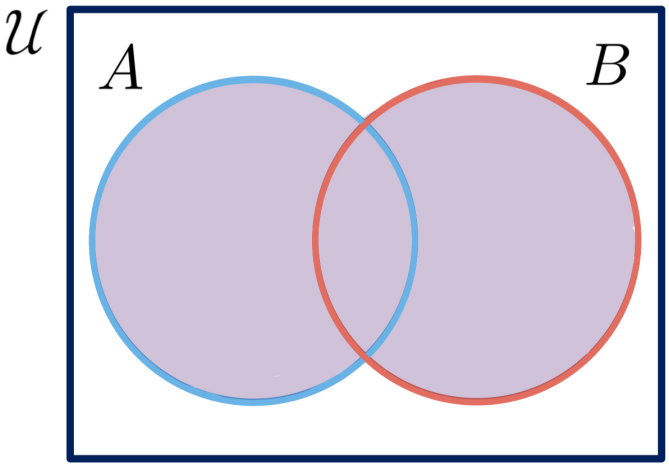
Example 5.5.2 A Venn diagram for $A \subseteq B$



□

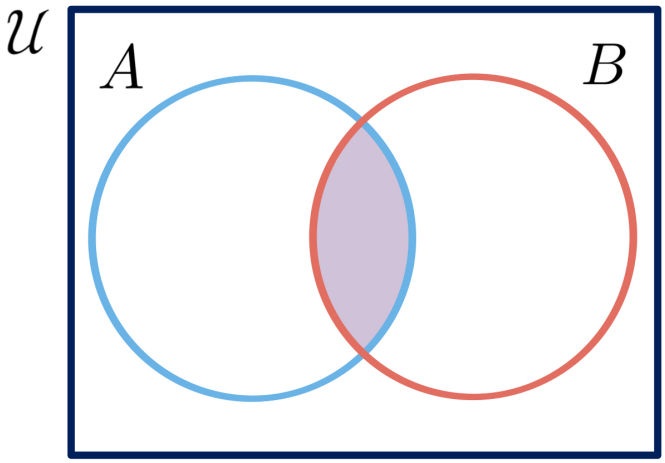
When we are indicating a specific portion of the Venn diagram we will use shading, such as the following examples.

Example 5.5.3 A Venn diagram for $A \cup B$



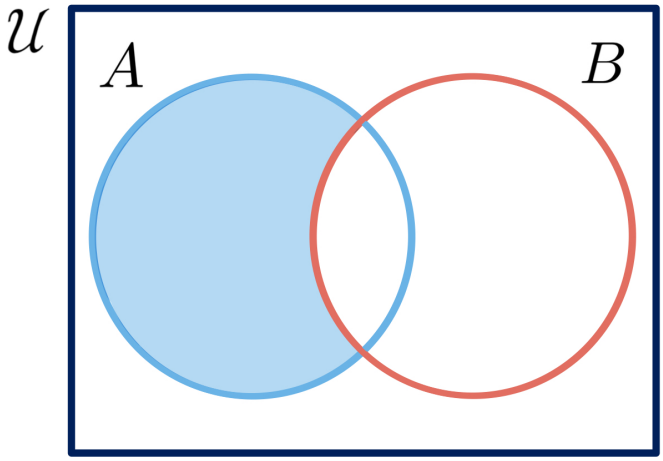
□

Example 5.5.4 A Venn diagram for $A \cap B$



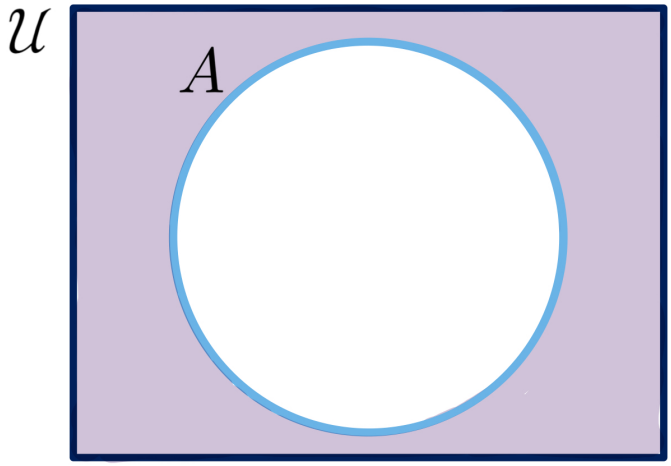
□

Example 5.5.5 A Venn diagram for $A - B$



□

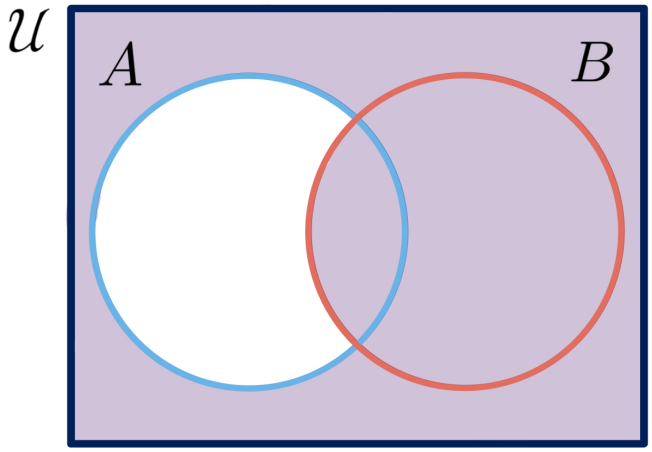
Example 5.5.6 A Venn diagram for A^c



□

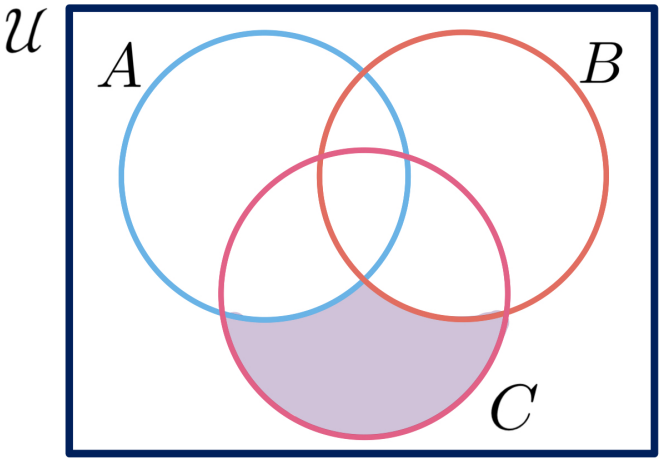
In this chapter's exercises (Section 5.26, p. 101) you will be asked to identify different sets in a Venn diagram. To help the student still attempting to take a grasp of set theory we give a few more creative examples next.

Example 5.5.7 The set: $(A - B)^c$



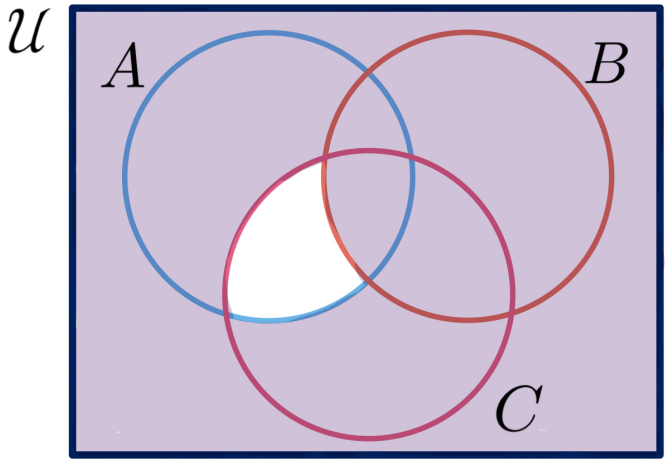
Here consider the set that contains A yet not that, that is in B, this is exactly the part that is not shaded, as it is the compliment. □

Example 5.5.8 The set: $(A \cup B)^c \cap C$



This time we consider the place which is neither A nor B yet is in C □

Example 5.5.9 The set: $(A \cap C)^c \cup B$



In this example consider the set that avoids where A intersects C yet does include all of B. □

5.6 The Logic of Sets

To the teacher: Be careful in this section... don't lose them... maybe even skip or just quickly note these? Or perhaps challenge the brave student, the student who has been staring deeply into the ripples of the pond to venture here...

As we have built set theory directly from propositional logic we can approach some basic properties very similarly to that of Section 1.14, p. 16 and Chapter 2, p. 25. Now we have the tools to start proving, we begin with the reason that most people hate the empty set.

Proposition 5.6.1 *Let A be a set then*

$$\emptyset \subseteq A$$

Proof. To prove this statement, we first fix a universe of discourse $\mathcal{U}$ and a set A. Now we examine the definition of subset; which applied to our scenario would say, for any $x \in \mathcal{U}$

$$x \in \emptyset \implies x \in A$$

Yet, $x \in \emptyset$ is a contradiction, that is always false, no matter the element, no matter the universe of discourse, as $\emptyset$ is empty, containing no elements.
So, the proof of this statement falls to the fact that if C is a contradiction then for any proposition P, the following argument is valid

$$\frac{C}{\therefore P}$$

Of course this means that $C \implies P$ is a tautology, to see this consider the following truth table.

C	P	$C \implies P$
F	T	T
F	F	T

Figure 5.6.2

■

To reiterate, it is this contradiction of $x \in \emptyset$ which really is the sticking point for the empty set, and why it is always a fringe case that becomes the dismay of mathematicians world round. Next, we present a few more subset conditions.

Proposition 5.6.3 *Let A, B, and C be sets, then the following are true*

(a) $A \subseteq A$

(b) if $A \subseteq B$ *and* $B \subseteq C$, *then* $A \subseteq C$

Proof. (a) $x \in A \implies x \in A$ is the argument

$$\frac{P}{\therefore P}$$

hence we need $P \implies P$ to be a tautology, yet

P	$P \implies P$
T	T
F	T

Figure 5.6.4

(b) This one is

$$\frac{\begin{array}{c} P \implies Q \\ Q \implies R \end{array}}{\therefore P \implies R}$$

which is just Hypothetical Syllogism from Figure 2.3.1, p. 27. ■

Next we give a somewhat analogous treatment to that of Theorem 1.13.1, p. 15, and leave it to the diligent reader to draw the direct comparisons.

Proposition 5.6.5 *Let A, B, and C be sets, then the following are true*

(a) $(A^c)^c = A$

(b) $A \cup B = B \cup A$ *(commutativity)*

(c) $A \cap B = B \cap A$ *(commutativity)*

(d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(distributivity)*

(e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(distributivity)*

(f) $A \cap A = A$ *(absorption)*

(g) $A \cup A = A$ *(absorption)*

(h) $(A \cup B)^c = A^c \cap B^c$

(i) $(A \cap B)^c = A^c \cup B^c$

(j) $A \cup (B \cup C) = (A \cup B) \cup C$ *(associativity)*

(k) $A \cap (B \cap C) = (A \cap B) \cap C$ *(associativity)*

(l) $A \subseteq B$ *iff* $B^c \subseteq A^c$

In a similar fashion the following conditions are the consequences of the arguments in Figure 2.3.1, p. 27.

Proposition 5.6.6

(a) $A \subseteq A \cup B$

(b) $A \cap B \subseteq A$

These final properties are unique to sets, yet have the same logical progressions as the previous ones.

Proposition 5.6.7

(a) $A \cap \emptyset = \emptyset$

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

(c) $A - \emptyset = A$

(d) $\emptyset - A = \emptyset$

(e) $A \subseteq B$ *if and only if* $A \cup B = B$

(f) $A \subseteq B$ *if and only if* $A \cap B = A$

(g) If $A \subseteq B$ *then* $A \cup C \subseteq B \cup C$

(h) If $A \subseteq B$ *then* $A \cap C \subseteq B \cap C$

We leave these last ones without proof, nor the challenge for a hard working reader to try and work it out, but instead we hope the student's intuition will guide them.

5.7 First Proofs with Sets

In the previous section we looked at many basic properties of sets. Now we will venture into some proofs that are more indicative of your future classes, and return (momentarily) back to the safety of numbers.

We first examine how one would prove a subset to be true.

Proving $A \subseteq B$.

Let $x \in A$
...
Therefore $x \in B$

The keen-eyed student will notice that this is simply the direct proof applied to the definition of subset, specifically:

$$\forall x \in \mathcal{U}\ x \in A \implies x \in B$$

We will see many examples of this proving method throughout out the class, yet before we jump in, I'd like to note for either the instructor or the diligent student who has been paying very close attention to the journey. I used to try and teach this by taking away the numbers, and instead using the beginning, muddle and the end in Section 5.6, p. 80 instead of the now off-handed way you see presented here, but I believe the students felt like it was too jarring and then leaned away from subsets and set proofs, which was detrimental to their learning once we got to abstract algebra. So now I introduce these proofs with numbers in hopes that you leave the set theory section with the love that you left from the even and odd proofs.

5.8 The First Proof

Define the sets

$$A = \{x \in \mathbb{Z} \mid x = 6a \text{ for some } a \in \mathbb{Z}\}$$

$$B = \{x \in \mathbb{Z} \mid x = 2a \text{ for some } a \in \mathbb{Z}\}$$

Prove: $A \subseteq B$

Before we begin any proof we sing our song (play-along):

"What's the P?"**1.** $x \in A$

"What's the Q?"**2.** $x \in B$

"What're the definitions?"**3.** The definition of the sets written directly above silly goose!

"Now, what to do?"**4.** A direct proof! (proof of a subset!)

5.9 The Beginning

To begin this proof we follow our procedure above, by choosing an arbitrary element of the set A, using words in the manner of:

Let $s \in A$

Thats all there is to it, we abscond with a random element of A, then drudge forward with our journey to show it is a member of B.

5.10 The Muddle

I chose to begin with this example as the muddle is almost identical to most other of our examples. That is we simply state what it takes for s to belong to A. From the definition above of the set A, we see in the *condition* part of the set-builder notation it tells us that there must be an integer so that s is 6 times this integer (sound familiar?). To invoke this we could write something like:

By the definition of membership of A, we can produce some integer t so that $s = 6t$.

5.11 The End

Now, for the end we need to finally get to the finish line, that is finally conclude that our element s is indeed a member of B. For this notice that

$$s = 6t = 2 \cdot (3t)$$

and since 3 is an integer and t is an integer we have that $3t$ is an integer and hence s satisfies the condition to be in B.

Next, we present it all in one place.

Example 5.11.1 Define the sets

$$A = \{x \in \mathbb{Z} \mid x = 6a \text{ for some } a \in \mathbb{Z}\}$$

$$B = \{x \in \mathbb{Z} \mid x = 2a \text{ for some } a \in \mathbb{Z}\}$$

Prove: $A \subseteq B$

Proof:

Let $s \in A$, by definition of the set A we can find an integer t so that $s = 6t$, yet note since $6 = 2 \cdot 3$ we have $s = 6t = 2 \cdot (3t)$. Now, since 3 and t are integers we can conclude $3t$ is an integer. Therefore by the definition of the set B we have that $s \in B$ □

5.12 More Examples

This is an important concept of your future mathematics courses so we will now provide a couple more abbreviated examples of subset.

Example 5.12.1 Consider the sets:

$$A = \{x \in \mathbb{Z} \mid x = 6a + 4 \text{ for some } a \in \mathbb{Z}\}$$

$$B = \{y \in \mathbb{Z} \mid y = 3a + 1 \text{ for some } a \in \mathbb{Z}\}$$

Prove: $A \subseteq B$

Proof. We begin by selecting a completely arbitrary element of A, which we will denote as $n \in A$. Applying the condition of membership to A we can find an integer m such that $n = 6m + 4$. By factoring we see that

$$n = 6m + 4 = 6m + 3 + 1 = 3(2m + 1) + 1$$

and since $2m + 1$ is an integer we see that n satisfies the condition to be a member of B.
Therefore, we have chosen an arbitrary $n \in A$, and successfully shown that $n \in B$, hence we have shown that $A \subseteq B$. ■

□

For our next example we will look at proof involving the intersection (Definition 5.3.8, p. 73).

Example 5.12.2 Consider the sets:

$$A = \{x \in \mathbb{Z} \mid x = 2a + 1 \text{ for some } a \in \mathbb{Z}\}$$

$$B = \{y \in \mathbb{Z} \mid y = 5a + 2 \text{ for some } a \in \mathbb{Z}\}$$

$$C = \{z \in \mathbb{Z} \mid z = 10a + 7 \text{ for some } a \in \mathbb{Z}\}$$

Prove: $C \subseteq A \cap B$

Proof. We first choose an arbitrary element of C in attempts to show it also belongs to $A \cap B$, name this element $x \in C$.
Using the definition of the set C we see that we can fix a specific $s \in \mathbb{Z}$ so that $x = 10s + 7$.
Now, to show membership of the intersection, $A \cap B$, we need to show that our element x is both a member of A ***and*** that it is a member of B, by the definition of intersection (Definition 5.3.8, p. 73). Thus we break the remainder of the proof into two parts.
[Membership of* A*]
Notice that we can factor

$$x = 10s + 7 = 10s + 6 + 1 = 2(5s + 3) + 1$$

and as $5s+3$ is an integer we see that x satisfies the conditions to be a member of A.
[Membership of* B*]
Similarly, notice that we can again factor

$$x = 10s + 7 = 10s + 5 + 2 = 5(2s + 1) + 2$$

and as $2s+1$ is an integer we see that x satisfies the conditions to be a member of B.
Finally, since we have chosen a completely arbitrary element $x \in C$ and then have shown that $x \in A$ and that $x \in B$ we can conclude that $x \in A \cap B$, therefore we have shown that $C \subseteq A \cap B$. ■

□

Our next example will work through a proof that involves a union (Definition 5.3.5, p. 73).

Example 5.12.3 Consider the sets

$$A = \{c \in \mathbb{Z} \mid c = 6g + 4 \text{ for some } g \in \mathbb{Z}\}$$

$$B = \{d \in \mathbb{Z} \mid d = 15h - 8 \text{ for some } h \in \mathbb{Z}\}$$

$$C = \{f \in \mathbb{Z} \mid f = 3j + 1 \text{ for some } j \in \mathbb{Z}\}$$

Prove: $A \cup B \subseteq C$

Proof. To start the proof we will choose an arbitrary element of $A \cup B$, we will name this random member $y \in A \cup B$. By the definition of union (Definition 5.3.5, p. 73) we have that $y \in A$ ***or*** $y \in B$, thus we split our proof in to two cases.

[Case 1: $\mathbf{y \in A}$***]***

For this first case, assume that $y \in A$, by the condition defining the set A we can find an integer t such that $y = 6t + 4$. Next, we calculate:

$$y = 6t + 4 = 6t + 3 + 1 = 3(2t + 1) + 1$$

since $2t + 1$ is an integer we see that y satisfies the condition to be a member of C, that is $y \in C$.

[Case 2: $\mathbf{y \in B}$***]***

For this case we will instead assume $y \in B$. This time by the condition defining the set B we can locate a special integer s so that $y = 15s - 8$. Now we can calculate:

$$y = 15s - 8 = 15s - 9 + 1 = 3(5s - 3) + 1$$

and since $5s - 3$ is an integer we see that, as the condition for membership of C is satisfied, $y \in C$.

To wrap-up, since we have chosen a random element $y \in A \cup B$ and have shown that this same element must have the property that $y \in C$ we can conclude that $A \cup B \subseteq C$. ■

□

Now we will explore the process of showing when sets are equal.

Definition 5.12.4 Equals. We say that two sets A and B are **equal**, denoted

$$A = B$$

if and only if

$$A \subseteq B \text{ and } B \subseteq A$$

◊

Therefore to prove the statement $A = B$ we must have two proofs, one proof for $A \subseteq B$ and one proof for $B \subseteq A$.

Our next couple of examples aim to show this.

Example 5.12.5 Consider the set

$$X = \{x \in \mathbb{Z} \mid x = 3g + 2h \text{ for some } g, h \in \mathbb{Z}\}$$

Prove: $X = \mathbb{Z}$

Proof. We will again need to break this proof into two parts.
[Want to Show: $\mathbf{X \subseteq \mathbb{Z}}$***]***
For the first part, let $c \in X$ and hence by the definition of the set X we have that $x \in \mathbb{Z}$, therefore $X \subseteq \mathbb{Z}$. (this is of course what many refer to as the *easy part*)
[Want to Show: $\mathbb{Z} \subseteq \mathbf{X}$***]***
In this next part, assume $m \in \mathbb{Z}$. It is now our objective to show membership in X, to do such we will need to produce two integers, the way in which we discovered these integers is irrelevant to the proof, so for the sake of argument, lets just assume angels whispered it to me in my sleep.
Notice that since m is an integer and $-m$ is an integer, then we can calculate:

$$3m - 2m = m$$

and hence by the condition of set X we have that $m \in X$, therefore $\mathbb{Z} \subseteq X$.
To wrap-up, since we have shown that both $X \subseteq \mathbb{Z}$ and $\mathbb{Z} \subseteq X$ we may conclude that $X = \mathbb{Z}$. ■
□

5.13 Power Set

The power set includes all the subsets of a given set. To help make this clearer, we'll now work through a couple of examples together.

Definition 5.13.1 Power Set. Let A be a set. The **power set** of A is the set whose elements are the subsets of A and is denoted $\mathscr{P}(A)$

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

◊

The power set is made up of all the subsets of a given set. Let's explore some examples to help make this clear.

Example 5.13.2 Consider the set:

$$A = \left\{ \text{  }, \text{  } \right\}$$

To build the power set, it is customary to begin with the empty set, $\emptyset$, which we know must be a member of the power set from Proposition 5.6.1, p. 80 we know that $\emptyset \subseteq A$. Hence, $\emptyset \in \mathscr{P}(A)$

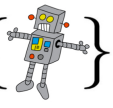
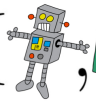
Next, we will of course need all of the **singletons**, that is all the sets containing a single element from A

$$\left\{ \text{  } \right\} \in \mathscr{P}(A)$$

$$\left\{ \text{  } \right\} \in \mathscr{P}(A)$$

Finally, since for any set $A \subseteq A$, as any element of A is surely an element of A, we have $A \in \mathscr{P}(A)$

thus the power set is:

$\mathscr{P}(A) = \{\emptyset, \{$  $\}, \{$  $\}, \{$  $\}\}$

□

Our next example, though a bit more straightforward, uses our familiar numbers with a slightly larger set to help solidify the concept.

Example 5.13.3 Let's look at an example of a power set: the power set of $B = \{1, 2, 3\}$.

Just, as in the last example, in every power set we must find the empty set, that is $\emptyset \in \mathscr{P}(B)$.

Next, we will work through each singleton:

$$\{1\} \in \mathscr{P}(B)$$

$$\{2\} \in \mathscr{P}(B)$$

$$\{3\} \in \mathscr{P}(B)$$

As our set has three elements there are a few subsets which have two elements this time:

$$\{1, 2\} \in \mathscr{P}(B)$$

$$\{1, 3\} \in \mathscr{P}(B)$$

$$\{2, 3\} \in \mathscr{P}(B)$$

Finally, as $B \subseteq B$, we have that $B \in \mathscr{P}(B)$.

Thus the power set of B is:

$$\mathscr{P}(B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

□

The curious counter, will notice by the procedural way in which we construct these power sets that when we start with finite sets, that they are indeed easy enough to count.

Theorem 5.13.4 *For a finite set A the size of the power set is*

$$|\mathscr{P}(A)| = 2^{|A|}$$

We leave the proof of this to a course in counting, or the studious reader may work it out themselves.

5.14 First Proof

For our very first proof using the power set we will now shed the numbers and prove for arbitrary sets A and B.

Prove: $A \subseteq B$ if and only if $\mathscr{P}(A) \subseteq \mathscr{P}(B)$

This is a biconditional proof so it is like we are working with two proofs, so we will use it as such and prove each statement separately.

5.15 Proof of: $A \subseteq B \implies \mathscr{P}(A) \subseteq \mathscr{P}(B)$

Before we begin any proof we sing our song (play-along):

"What's the P?" **1.** $A \subseteq B$

"What's the Q?" **2.** $\mathscr{P}(A) \subseteq \mathscr{P}(B)$

"What're the definitions?"**3.** The definition of power set (Definition 5.13.1, p. 87) and the definition of subset (Definition 5.3.1, p. 72)

"Now, what to do?"**4.** A direct proof

5.16 The Beginning

To begin, there is nothing fancy we simply assume the "P" that is we would write something simple like:

Assume $A \subseteq B$

Our goal is to prove that $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, thus we need to prove a subset, to do this we must choose an arbitrary element of $\mathscr{P}(A)$ with language like:

Let $x \in \mathscr{P}(A)$

it will be our objective to show that this element x also belongs to $\mathscr{P}(B)$.

5.17 The Muddle

I know, we have no numbers what are we to do?

stay calm we have not completely disregarded the mold, usually in the muddle we invoke some definitions, so let's do that now, namely the definition of membership to the power set. We do this with language like:

By definition of the power set of A, we have that $x \subseteq A$.

As it is our objective to show that this element x also belongs to $\mathscr{P}(B)$, this means we need to show that x is a subset of B. To do this we do so like any proof of subset (kinda like the one we are in the middle of...) and choose an random element of x, we can do this with language like:

Choose an arbitrary $a \in x$.

Where to go from here?? Well, right before this we unraveled the fact that $x \subseteq A$ and hence by defintion of subset we have $a \in A$. We could express this in our proof with the following language:

Since $x \subseteq A$ and that we have assumed $a \in x$, by the definition of subset we can make the conclusion that $a \in A$.

Hark! Our very first assumption was 'bout how the fair set A compares to the set B, more specifically that $A \subseteq B$, hence in a similar fashion we could write the following conclusion:

Since we assumed $A \subseteq B$ and since we have discovered that $a \in A$ by definition of subset we can conclude that $a \in B$. Hence, since we chose an arbitrary element $a \in x$ and have shown that $a \in B$ as well, by definition of subset we can conclude $x \subseteq B$.

5.18 The End

Finally, we have just concluded that $x \subseteq B$, which is the defining condition for membership to the power set of B, thus we can conclude:

By defintion of power set since $x \subseteq B$ we have that $x \in \mathscr{P}(B)$. Therefore as we chose $x \in \mathscr{P}(A)$ arbitrarily, by definition of subset we have our desired result that $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

5.19 Proof of: $\mathscr{P}(A) \subseteq \mathscr{P}(B) \implies A \subseteq B$

Before we begin any proof we sing our song (play-along):

"What's the P?"**1.** $\mathscr{P}(A) \subseteq \mathscr{P}(B)$

"What's the Q?"**2.** $\mathscr{P}(A) \subseteq \mathscr{P}(B)$

"What're the definitions?"**3.** The definition of power set (Definition 5.13.1, p. 87) and the definition of subset (Definition 5.3.1, p. 72)

"Now, what to do?"**4.** direct proof

5.20 The Beginning

This time to begin, we must assume this *new* "P" that is we would write something simple like:

Assume $\mathscr{P}(A) \subseteq \mathscr{P}(B)$

Our goal is to prove that $A \subseteq B$, thus we need to *prove a subset*, to do this we must choose an arbitrary element of A with language like:

Let $y \in A$

5.21 The Muddle

Now, what do we do?!

This time we don't even have any useful definitions to lean on... all we know is that A is a set, literally one of the most general objects ever, it can be anything...

As we take a breath or two, we see that all we really have at this time is our assumption about power sets. Luckily we have just completed working our way through our examples of power set and recall that the singletons were one of the first sets we looked at, and hence we have that:

Since $y \in A$ by the definition of subset $\{y\} \subseteq A$, thus by the definition of power set we have that $\{y\} \in \mathscr{P}(A)$. Now, since we have assumed that $\mathscr{P}(A) \subseteq \mathscr{P}(B)$ by the definition of subset we have that $\{y\} \in \mathscr{P}(B)$.

5.22 The End

Given that $\{y\} \in \mathscr{P}(B)$ by the definition of power set we can conclude that $\{y\} \subseteq B$, and by the definition of subset, since $y \in \{y\}$ we have that $y \in B$.

Yet, since we have chosen $y \in A$ arbitrarily and have shown that $y \in B$ by the definition of subset we can conclude that $A \subseteq B$ as desired. Now that we have shown that both

$$A \subseteq B \implies \mathscr{P}(A) \subseteq \mathscr{P}(B)$$

and that

$$\mathscr{P}(A) \subseteq \mathscr{P}(B) \implies A \subseteq B$$

we can conclude that

$$A \subseteq B \iff \mathscr{P}(A) \subseteq \mathscr{P}(B)$$

We now give an abbreviated proof in a single location for the ease of the reader.

Example 5.22.1 ***Prove:*** $A \subseteq B$ if and only if $\mathscr{P}(A) \subseteq \mathscr{P}(B)$

$[\implies]$

Assume $A \subseteq B$ Let $x \in \mathscr{P}(A)$. Hence by definition of power set, $x \subseteq A$

By Proposition 5.6.3, p. 81 (b), since $x \subseteq A$ and $A \subseteq B$ we can conclude $x \subseteq B$. Thus by definition of power set, $x \in \mathscr{P}(B)$

Thus by direct proof, if $A \subseteq B$ then $\mathscr{P}(A) \subseteq P(B)$

[$\Longleftarrow$]

Assume that $\mathscr{P}(A) \subseteq \mathscr{P}(B)$. Let $y \in A$ By definition of power set, $\{y\} \in P(A)$. Hence by our assumption, $\{y\} \in \mathscr{P}(B)$. Hence by our assumption and the definition of power set, $\{y\} \in \mathscr{P}(A)$, hence $\{y\} \in \mathscr{P}(B)$. By definition of subset, since $y \in \{y\}$ then $y \in B$.

Thus by direct and bi-directional proof, $A \subseteq B$ if and only if $\mathscr{P}(A) \subseteq \mathscr{P}(B)$ □

5.23 The Natural Numbers

This subsection can be safely skipped, but it is a fun construction using only the empty set to build the natural numbers, also why I insist that $0 \in \mathbb{N}$.

For this construction we begin with the empty set:

$$|\emptyset| = 0$$

then we consider the set which has a singular element, the empty set,

$$|\{\emptyset\}| = 1$$

now we consider the set which contains these previous two sets, namely:

$$|\{\emptyset, \{\emptyset\}\}| = 2$$

next lets collect all these sets in a set, that is

$$|\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}| = 3$$

and continue

$$|\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}| = 4$$

and continue

$$|\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}\}| = 5$$

and continue... the diligent student will complete this exercise...

5.24 Cross Product

In this section we introduce the concept of cross product, this is yet another way of making new sets from old sets.

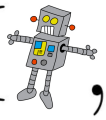
Definition 5.24.1 Cross Product. Given two sets A and B we can define a new set which we will call the **cross product** of A and B (or the **cartesian product**) defined as

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

◊

This is the collection of all ordered pairs. We explore this new construction in the following examples.

Example 5.24.2 Consider the sets

$$A = \{ \text{  }, \text{  } \}$$

$$B = \{ \text{  }, \text{  }, 3 \}$$

thus the cross product is the following set:

$$A \times B = \left\{ \begin{array}{l} (\text{  }, \text{  }), (\text{  }, \text{  }), (3, \text{  }), \\ (\text{  }, \text{  }), (\text{  }, \text{  }), (3, \text{  }) \end{array} \right\}$$

□

Our next example explores the lack of commutation of the cross product.

Example 5.24.3 Let's look at another cross product of some sets. Calculate $A \times B$ and $B \times A$ given the sets $A = \{2, G, E\}$ and $B = \{\pi, e, P\}$

$$A \times B = \{(2, \pi), (2, e), (2, P), (G, \pi), (G, e), (G, P), (E, \pi), (E, e), (E, P)\}$$

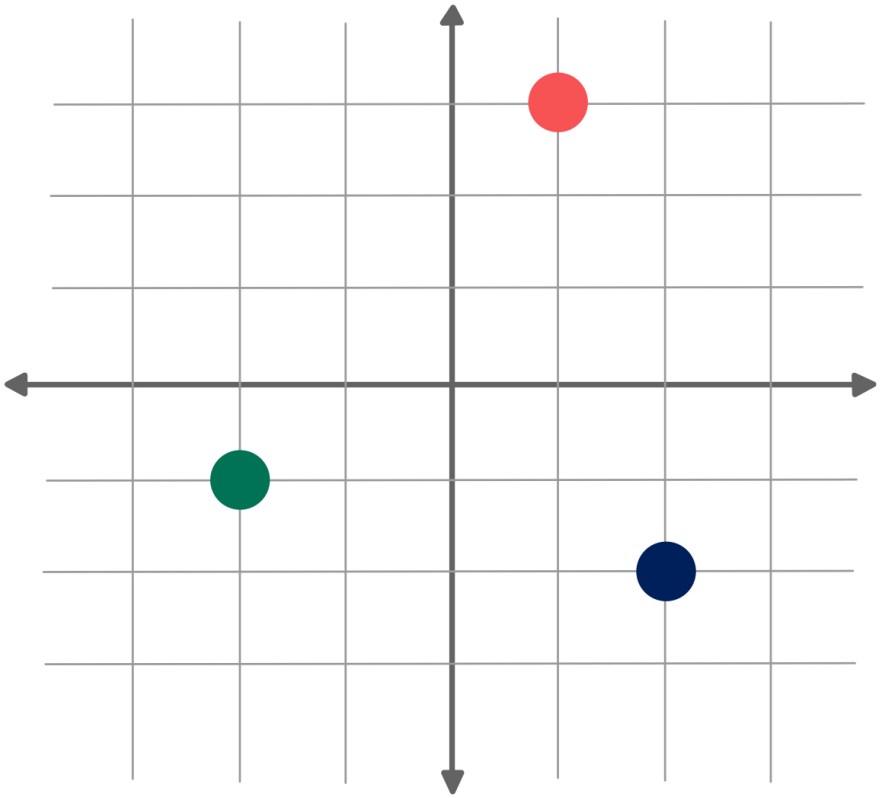
$$B \times A = \{(\pi, 2), (\pi, G), (\pi, E), (e, 2), (e, G), (e, E), (P, 2), (P, G), (P, E)\}$$

□

The cross product has been shown since very early on in your mathematical education mostly the ordered pairs you would consider was the cartesian plane, the good ol' x and y axis.

Example 5.24.4 This time if we consider a set I've tried very hard to stay away from, namely the real numbers, $\mathbb{R}$, then the cartesian plane is the set $\mathbb{R} \times \mathbb{R}$.

Throughout your youth you have surely seen many points illustrated on this cartesian plane, such as the elements $(1, 3)$, $(2, -2)$, and $(-2, -1)$



□

With this basic understanding of the cross-product we are ready to start proving with it.

Example 5.24.5 ***Prove:*** For sets A, B, C, and D, if $A \subseteq C$ and $B \subseteq D$ then $A \times B \subseteq C \times D$

Proof. We begin by assuming that $A \subseteq C$ and that $B \subseteq D$. Our objective is to prove that $A \times B \subseteq C \times D$, that is we need to show a subset, we do this by choosing an arbitrary element, $x \in A \times B$.
To understand this element we of course refer to the definition (Definition 5.24.1, p. 91), from which we see the defining condition promises that we can find two elements, one from A and one from B, name these elements, $a \in A$ and $b \in B$, such that $x = (a, b)$.
By our assumption that $A \subseteq C$, since we established $a \in A$ by definition of subset we get that $a \in C$. Similarly, by our assumption that $B \subseteq D$ and since we established that $b \in B$ again by the definition of subset $b \in D$.
Therefore, by the definition of cross product $x = (a, b) \in C \times D$ as desired. ■

□

Example 5.24.6 ***Prove:*** Let A and B be sets, then $A \times (B \cup C) = (A \times B) \cup (A \times C)$

Proof. ***[Want to show:*** $\mathbf{A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)}$***]***
We begin by choosing an arbitrary element $x \in A \times (B \cup C)$. By the definition of cross product, we can find $m \in A$ and $\ell \in B \cup C$ such that $x = (m, \ell)$. By definition of union, $\ell \in B$ or $\ell \in C$.
Hence $(m, \ell) \in A \times B$, when $\ell \in B$, or $(m, \ell) \in A \times C$, when $\ell \in C$. Thus, by definition of union, $x = (m, \ell) \in (A \times B) \cup (A \times C)$ Thus by definition of subset, since $x \in A \times (B \cup C)$ and $x \in (A \times B) \cup (A \times C)$, hence we have that $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$.
[Want to show: $\mathbf{(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)}$***]***
This time let $y \in (A \times B) \cup (A \times C)$. Hence by definition of union, $y \in (A \times B)$ or $y \in (A \times C)$. Hence, by definition of cross product, we can find $s \in A$ and $t \in B$ such that $y = (s, t)$ ***or*** $d \in A$ and $r \in C$ such that $y = (d, r)$.
Case 1: $\mathbf{y = (s, t)}$
Since $t \in B$, by definition of union, $t \in B \cup C$ and since $s \in A$, $y = (s, t) \in A \times (B \cup C)$ by definition of cross product. Thus by definition of subset, since $y \in (A \times B) \cup (A \times C)$ and $y \in A \times (B \cup C)$, therefore we can conclude that $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$
Case 2: $\mathbf{y = (d, r)}$
Since $l \in C$, by definition of union, $r \in B \cup C$. And since $d \in A$, by definition of cross prodcut, $y = (d, r) \in A \times (B \cup C)$. Thus by definition of subset, since $y \in (A \times B) \cup (A \times C)$ and $y \in A \times (B \cup C)$, thus we have $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$
Thus, since both cases hold, by direct proof and proof by cases, $A \times (B \cup C) = (A \times B) \cup (A \times C)$ ■

□

5.25 Families

We now consider, basic constructions like union, intersection and the cross product between many sets at once. We consider these over a **family of sets**, which is just a fancy way of saying a set whose members are sets. We will most often use the *script font* to indicate a family, for example $\mathscr{A}$.

Definition 5.25.1 Union over a Family. Let $\mathscr{A}$ be a family of sets. We define the **union over** $\mathscr{A}$ as

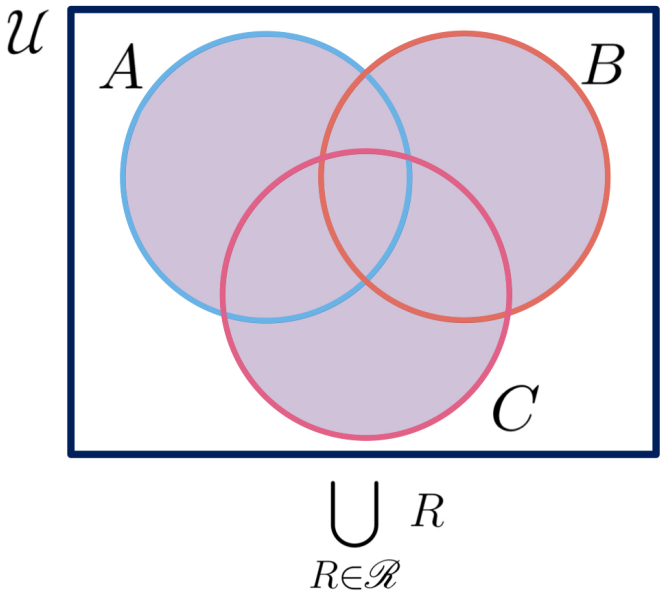
$$\bigcup_{A \in \mathscr{A}} A = \{x \mid x \in A \text{ for some } A \in \mathscr{A}\}$$

◊

As we are still learning set-builder notation, to help us be able to unpack the condition in the previous definition, note the following condition of membership:

$$x \in \bigcup_{A \in \mathscr{A}} A \text{ if and only if } [\exists A \in \mathscr{A}\ x \in A]$$

Example 5.25.2 We now illustrate the union over a family with a Venn diagram below for the family of sets $\mathscr{R} = \{A, B, C\}$



□

Example 5.25.3 Consider the family of sets $\mathscr{B} = \{R, S, T\}$ where each set is defined as follows

$$R = \{1, 3, G, \square, \triangle, \Omega\}$$
$$S = \{\alpha, \Gamma, H, 7, 900\}$$
$$T = \{1, \Gamma, \triangle, 200, 16\}$$

Thus the union over $\mathscr{B}$ is

$$\bigcup_{B\in\mathscr{B}} B = (R \cup S) \cup T = \{1, 3, G, \square, \triangle, \Omega, \alpha, \Gamma, H, 7, 900, 200, 16\}$$

□

Our next topic examines intersections within this new concept of families of sets.

Definition 5.25.4 Intersection over a Family. Let $\mathscr{A}$ be a family of sets. We define the **intersection over** $\mathscr{A}$ as

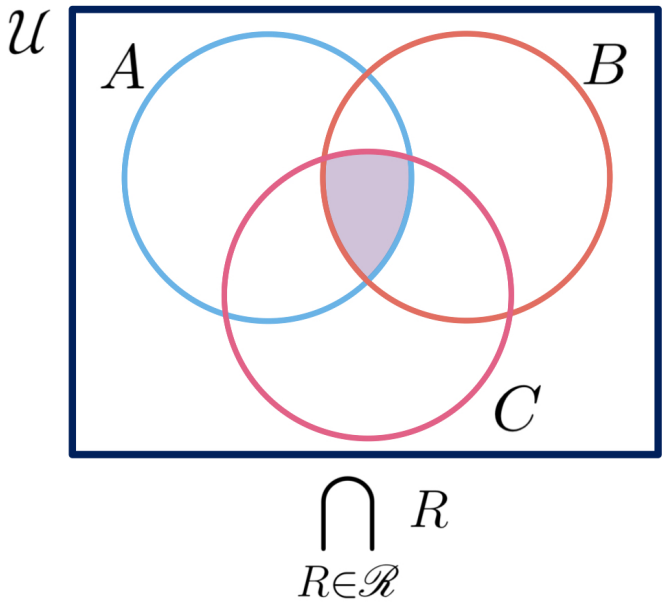
$$\bigcap_{A\in\mathscr{A}} = \{x \mid x \in A \text{ for every } A \in \mathscr{A}\}$$

◊

To help again we unpack the condition in the previous definition, note the following condition of membership:

$$x \in \bigcap_{A\in\mathscr{A}} A \text{ if and only if } [\forall A \in \mathscr{A}\ x \in A]$$

Example 5.25.5 We now illustrate the intersection over a family with Venn diagram below, again, for the family of sets $\mathscr{R} = \{A, B, C\}$



□

Example 5.25.6 Consider the family of sets $\mathscr{B} = \{R, S, T\}$ where each set is defined as follows

$$R = \{1, 3, G, \square, \triangle, \Omega\}$$
$$S = \{3, \alpha, \Gamma, H, \Omega, 900, \triangle\}$$
$$T = \{1, 3, \Gamma, \Omega, \triangle, 200, 16\}$$

Thus the union over $\mathscr{B}$ is

$$\bigcap_{B\in\mathscr{B}} B = (R \cap S) \cap T = \{\Omega, 3, \triangle\}$$

□

Now lets explore a general proof involving these constructions.

Example 5.25.7 ***Prove:*** For a non-empty family of sets $\mathscr{A}$

$$\bigcap_{A\in\mathscr{A}} A \subseteq \bigcup_{A\in\mathscr{A}} A$$

Proof. We begin as we do for any subset proof, and that is, we choose an arbitrary element $x \in \bigcap_{A\in\mathscr{A}} A$
By definition of the intersection over a family for any member of the family x must belong to it. So choose an arbitrary $C \in \mathscr{A}$ thus $x \in C$, which by defintion of union, since $x \in C$ we have that $x \in \bigcup_{A\in\mathscr{A}} A$.
Therefore since we chose an arbitrary element $x \in \bigcap_{A\in\mathscr{A}} A$ and have shown $x \in \bigcup_{A\in\mathscr{A}} A$, we can conclude $\bigcap_{A\in\mathscr{A}} A \subseteq \bigcup_{A\in\mathscr{A}} A$ as desired. □ ■

□

If this is still a bit too abstract for our dear reader we will now introduce a concept which allows us to look at these constructions a bit more like the summation from our calculus classes.

Definition 5.25.8 Indexed Family of Sets. Let Δ be a nonempty set such that for every $i \in \Delta$ we correspond a set A_i, an **indexed family of sets** over Δ, is the family of sets,

$$\mathscr{A} = \{A_i \mid i \in \Delta\}$$

We call the set Δ **the indexing set**. $\Diamond$

The most common case of an index set is when $\Delta \subseteq \mathbb{N}$ in the form of

$$\Delta = \{0, 1, 2, 3, ..., n\}$$

for some $n \in \mathbb{N}$, in this case we will often write the intersections as

$$\bigcap_{i \in \Delta} A_i = \bigcap_{i=0}^{n} A_i$$

and the union as

$$\bigcup_{i \in \Delta} A_i = \bigcup_{i=0}^{n} A_i$$

With this new construction lets visit another example.

Example 5.25.9 Consider the indexing set $\Delta = \{0, 1, 2\}$, and the family of sets $\mathscr{C} = \{C_0, C_1, C_2\}$ where each set is defined as follows

$$C_0 = \left\{7, 15, H, \triangle, \pi, \frac{1}{3}\right\}$$

$$C_1 = \left\{15, \triangle, \square, H, \frac{1}{3}, 0, \pi\right\}$$

$$C_2 = \left\{7, 15, \Gamma, \frac{1}{3}, \pi, 0, 16\right\}$$

Thus the union over $\mathscr{C}$ is

$$\begin{aligned}\bigcap_{i \in \Delta} = C_i \bigcap_{i=0}^{2} C_i &= (C_0 \cap C_1) \cap C_2 \\ &= \left\{\frac{1}{3}, 15, \pi\right\}\end{aligned}$$

□

Of course this basic use case of an index set is far from the only one, in the next example we leave the case of a finite indexing set by setting $\Delta = \mathbb{N}$. To build these with ease, and to show the reader a use case from future mathematics courses where each set in our family is a subset of the real numbers.

Example 5.25.10 Consider the indexing set $\mathbb{N}$ and the family of sets $\mathscr{A} = \{A_i \mid i \in \mathbb{N}\}$ defined as the following intervals,

$$A_i = \left[\frac{1}{i+2}, \frac{1}{i+1}\right) = \left\{x \in \mathbb{R} \;\middle|\; \frac{1}{i+1} \leq x < \frac{1}{i}\right\}$$

thus we have

$$\bigcup_{i \in \mathbb{N}} A_i = \bigcup_{i=0}^{\infty} A_i = (0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$$

and

$$\bigcap_{i \in \mathbb{N}} A_i = \bigcap_{i=0}^{\infty} A_i = \emptyset$$

□

In your next example we leave the natural numbers for our index set and instead explore the example where our indexing set of $\mathbb{Q}$.

Example 5.25.11 Consider the the indexing set $\mathbb{Q}$ Now define the indexed family of sets $\mathscr{B} = \{B_n \mid n \in \Gamma\}$, defined as the following closed intervals,

$$B_\alpha = \big[\alpha, \alpha + 1\big] = \{x \in \mathbb{R} \mid \alpha \leq x \leq \alpha + 1\}$$

thus we have

$$\bigcup_{\alpha \in \mathbb{Q}} B_\alpha = [0, \infty) = \{x \in \mathbb{R} \mid 0 \leq x < \infty\}$$

and

$$\bigcap_{\alpha \in \mathbb{Q}} B_\alpha = \{0\}$$

□

Now that we have built our intuition on unions and intersections over families, lets prove a result about them.

Example 5.25.12 Let Δ be an indexing set, and $\mathscr{A} = \{A_i \mid i \in \Delta\}$ be an indexed family of sets.

Prove: If B is a set then

$$B \cap \left(\bigcup_{i \in \Delta} A_i \right) = \bigcup_{i \in \Delta} (B \cap A_i)$$

Proof. This is a proof of the equality of two sets so we will need to break up the proof into two parts, namely we will need to show two subsets.
Proving: $B \cap \left(\bigcup_{i\in\Delta} A_i\right) \subseteq \bigcup_{i\in\Delta}(B \cap A_i)$
To prove this we will start like most subset proofs, namely by choosing an arbitrary element $s \in B \cap \left(\bigcup_{i\in\Delta} A_i\right)$. By the definition of intersection both $s \in B$ and $s \in \bigcup_{i\in\Delta} A_i$. By the definition of union over a family if we choose an arbitrary $j \in \Delta$ we have $s \in A_j$, thus since $s \in B$ and $s \in A_j$ by the definition of intersection we have that $s \in B \cap A_j$. Because we chose $j \in \Delta$ arbitrary it is true the for any $i \in \Delta$ $s \in B \cap A_i$ and hence the definition of union over a family is satisfied, that is

$$s \in \bigcup_{i\in\Delta}(B \cap A_i)$$

as desired.
Proving: $\bigcup_{i\in\Delta}(B \cap A_i) \subseteq B \cap \left(\bigcup_{i\in\Delta} A_i\right)$
To prove this we will start like most subset proofs, namely by choosing an arbitrary element $y \in \bigcup_{i\in\Delta}(B \cap A_i)$. By definition of union over a family when we choose an arbitrary element $k \in \Delta$ we must have that $y \in (B \cap A_k)$ by definition of intersection this means that both $y \in B$ and $y \in A_k$. Since we chose $k \in \Delta$ arbitrarily we have shown that for any $i \in \Delta$ that $y \in A_i$ that is we have shown the definition of membership to a union over a family, namely that

$$y \in \bigcup_{i\in\Delta} A_i$$

Yet, we have also shown that $y \in B$, thus by definition of intersection we have that

$$y \in B \cap \left(\bigcup_{i\in\Delta} A_i)\right)$$

as desired.
Since we have shown both the subsets

$$B \cap \left(\bigcup_{i\in\Delta} A_i\right) \subseteq \bigcup_{i\in\Delta}(B \cap A_i)$$

and

$$\bigcup_{i\in\Delta}(B \cap A_i) \subseteq B \cap \left(\bigcup_{i\in\Delta} A_i\right)$$

we can conclude the desired equality of:

$$B \cap \left(\bigcup_{i\in\Delta} A_i\right) = \bigcup_{i\in\Delta}(B \cap A_i)$$

□ ■
□

We finish up this section with a concept which will come into play when we discuss partitions later in the course.

Definition 5.25.13 Pairwise Disjoint. The indexed family $\mathscr{A} = \{A_\alpha | \alpha \in \Delta\}$ of sets is **pairwise disjoint** if and only if for all α and β in Δ, either

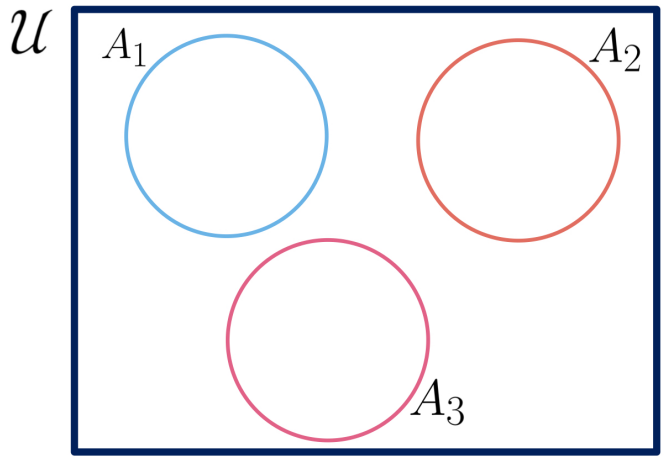
$$A_\alpha = A_\beta$$

or

$$A_\alpha \cap A_\beta = \emptyset$$

In other words, the sets are completely the same, or completely different. ◊

Example 5.25.14 First consider the indexing set $\Delta = \{1, 2, 3\}$ and the indexed family of sets $\mathscr{A} = \{A_1, A_2, A_3\}$

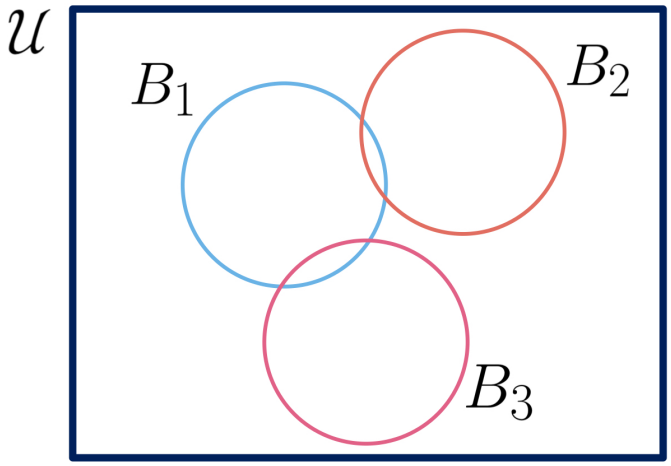


Notice that

$$A_1 \cap A_2 = \emptyset$$
$$A_1 \cap A_3 = \emptyset$$
$$A_2 \cap A_3 = \emptyset$$

and thus this family is pairwise disjoint.

Next, consider the same index set of $\Delta = \{1, 2, 3\}$ yet this time the indexed family $\mathscr{B} = \{B_1, B_2, B_3\}$



This time notice that

$$\bigcap_{i \in \Delta} B_i = \emptyset$$

and

$$B_2 \cap B_3 = \emptyset$$

yet

$$B_1 \cap B_3 \neq \emptyset$$

yet

$$B_1 \neq B_3$$

thus $\mathscr{B}$ is *not* pairwise disjoint □

We could not end the section without a proof, so here is your obligatory proof.

Example 5.25.15 Let Δ be an indexing set, and let both $\mathscr{A} = \{A_i \mid i \in \Delta\}$ and $\mathscr{B} = \{B_i \mid i \in \Delta\}$ be indexed family of sets.

Prove: If $\mathscr{A}$ is pairwise disjoint and $\mathscr{B} \subseteq \mathscr{A}$ then $\mathscr{B}$ is pairwise disjoint.

Proof. We begin this proof by assuming our antecedent.
Assume that $\mathscr{A}$ is pairwise disjoint and $\mathscr{B} \subseteq \mathscr{A}$. It is our objective to prove that $\mathscr{B}$ is pairwise disjoint, but looking above and seeing the definition of pairwise disjoint we see that we need to prove a universal quantifier, thus we choose arbitrary $j \in \Delta$ and $k \in \Delta$. Now since we have assumed that $\mathscr{B} \subseteq \mathscr{A}$ we have that both $B_j \in \mathscr{A}$ and $B_k \in \mathscr{A}$, thus by definition of membership to $\mathscr{A}$ we can find $s \in \Delta$ and $t \in \Delta$ so that $B_j = A_s$ and $B_k = A_t$.
Since we have assumed that $\mathscr{A}$ is pairwise disjoint then either

$$B_j \cap B_k = A_s \cap A_t = \emptyset$$

or

$$B_j = A_s = A_t = B_k$$

hence we have satisfied the definition of pairwise disjoint of $\mathscr{B}$. □ ■

□

Note 5.25.16 For the proofs in this section we see a common muddle that I like to call *chasing the definitions*, I know it can be jarring at first not having your warm and safe calculative muddle, but I promise you it will be ok! And I promise you in the next chapter there will *always* be a very solid calculative step!

5.26 Exercises

1. For the sets A, B, and C, for the following draw a Venn diagram shading the appropriate regions
   (a) $A \cup (B \cap C)^c$
   (b) $(A \cap B)^c - C$
   (c) $A \cap (B - C)$
2. For the following prove that $A \subseteq B$
   (a)
   $$A = \{a \in \mathbb{Z} \mid a = 12k \text{ for some } k \in \mathbb{Z}\}$$
   $$B = \{b \in \mathbb{Z} \mid b = 6s \text{ for some } s \in \mathbb{Z}\}$$
   (b)
   $$A = \{a \in \mathbb{Z} \mid a = 7k + 1 \text{ for some } k \in \mathbb{Z}\}$$
   $$B = \{b \in \mathbb{Z} \mid b = 14s + 8 \text{ for some } s \in \mathbb{Z}\}$$
   (c)
   $$A = \{a \in \mathbb{Z} \mid a = 6k + 15s \text{ for some } k \in \mathbb{Z} \text{ and some } s \in \mathbb{Z}\}$$
   $$B = \{b \in \mathbb{Z} \mid 3t \text{ for some } t \in \mathbb{Z}\}$$
3. For the following sets write out all elements of *both* $A \times B$ and $B \times A$

(a)

$$A = \{1, 3, 23, \square\}$$
$$B = \{\square, \triangle, \alpha\}$$

(b)

$$A = \{12, \pi, \Gamma\}$$
$$B = \{\sigma, \varphi, \theta\}$$

Chapter 6

Principle of Mathematical Induction

Here, we turn our attention to a proof technique that is extremely powerful and a favorite of students for its deceptively straightforward algorithmic approach, known as *induction*. This method is essential to your future mathematics courses, and allows us to prove statements that extend across infinite scenarios by using repetition as its backbone. Interestingly, it all begins with a concept we've known since our earliest days with numbers... counting!

6.1 What We Will Use

In this chapter you can, as usual, assume anything you had in Section 3.2, p. 33.

We will be using some constructions from your previous math courses a good bit in this chapter so we will review/establish a bit of notation before we enter this chapter.

6.2 Summation

We use the summation notation to add up a collection of indexed numbers.

Summation Notation.

For any $n \in \mathbb{N}$ and any collection of indexed numbers: $a_0, a_1, a_2, ..., a_n$, define

$$\sum_{i=0}^{n} a_i = a_0 + a_1 + a_2 + a_3 + ... + a_n$$

The most basic examples arise when the a_i satisfy some formula with an input of i.

Example 6.2.1 Let $a_i = 2i - 1$, now we calculate:

$$\begin{aligned}\sum_{i=0}^{3} a_i &= \sum_{i=0}^{3} (2i - 1) \\ &= (2 \cdot (0) - 1) + (2 \cdot (1) - 1) + (2 \cdot (2) - 1) + (2 \cdot (3) - 1)\end{aligned}$$

$$= -1 + 1 + 3 + 5$$
$$= 8$$

□

The summation does not need to *start at 0*; it can start anywhere, the point is that it moves through the successors wherever it is you start, for example:

$$\sum_{i=2}^{5} a_i = a_2 + a_3 + a_4 + a_5$$

or in a more general fashion for any $k \in \mathbb{N}$ and any $m \in \mathbb{N}$, with $k \leq m$,

$$\sum_{i=k}^{m} a_i = a_k + a_{k+1} + a_{k+2} + ... + a_m$$

This construction lends itself to the use of induction (the object of this chapter) so well as it has a property I like to refer to as *peeling off a factor*.

Peeling Off a Summation.

Notice for any $k \in \mathbb{N}$ and any $m \in \mathbb{N}$, with $k \leq m$, we can *peel off the first term*

$$\sum_{i=k}^{m} a_i = a_k + \left(\sum_{i=(k+1)}^{m} a_i \right)$$

or this time *peeling off the last term*

$$\sum_{i=k}^{m} a_i = \left(\sum_{i=k}^{m-1} a_i \right) + a_m$$

6.3 Product

We use the product notation to multiply together a collection of indexed numbers.

Product Notation.

For all $n \in \mathbb{N}$ and any collection of indexed numbers: $a_0, a_1, a_2, ..., a_n$

$$\prod_{i=0}^{n} a_i = a_0 \cdot a_1 \cdot a_2 \cdot a_3 \cdot \ ... \ \cdot a_n$$

Our use case of this notation will be again when a_i satisfy some equation in i.

Example 6.3.1 Again, for a simple first example consider $a_i = 2i - 1$, now we calculate:

$$\prod_{i=0}^{3} a_i = \prod_{i=0}^{3} (2i - 1)$$
$$= (2 \cdot (0) - 1) \cdot (2 \cdot (1) - 1) \cdot (2 \cdot (2) - 1) \cdot (2 \cdot (3) - 1)$$
$$= -1 \cdot 1 \cdot 3 \cdot 5$$
$$= -15$$

□

In a similar fashion to the summation, the product does not need to *start at 0* it can start any where, the point is that it moves through the successors wherever it is you start, for example:

$$\prod_{i=2}^{5} a_i = a_2 \cdot a_3 \cdot a_4 \cdot a_5$$

or in a more general fashion for any $k \in \mathbb{N}$ and any $m \in \mathbb{N}$, with $k \leq m$,

$$\prod_{i=k}^{m} a_i = a_k \cdot a_{k+1} \cdot a_{k+2} \cdot \ ... \ \cdot a_m$$

Just as with the summation the main characteristic we will involve is *peeling.*

Peeling Off a Product.

Notice, this time, for any $k \in \mathbb{N}$ and any $m \in \mathbb{N}$ with $k \leq m$, we can *peel off the first term*

$$\prod_{i=k}^{m} a_i = a_k \cdot \left(\prod_{i=(k+1)}^{m} a_i \right)$$

or this time *peeling off the last term*

$$\prod_{i=k}^{m} a_i = \left(\prod_{i=k}^{m-1} a_i \right) \cdot a_m$$

6.4 Factorial

We use the factorial notation to count the number of ways to permute a collection of objects.

Factorial.

We define

$$0! = 1$$

and for any $n \in \mathbb{N}$ with $n > 0$ we define

$$n! = \prod_{i=0}^{n-1} (n - i) = n \cdot (n-1) \cdot (n-2) \cdot \ ... \ \cdot 1$$

Example 6.4.1 For this example we will calculate some factorials:

$$2! = 2 \cdot 1 = 2$$

$$3! = 3 \cdot 2 \cdot 1 = 6$$

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$

□

As is the theme of this chapter, there is definitely a pattern.

Peeling Off a Factorial.

For any $m \in \mathbb{N}$ we can *peel off leading terms* of the factorial

$$m! = (m) \cdot [(m-1)!] = (m \cdot (m-1)) \cdot [(m-2)!]$$

and so on.

6.5 Introduction to Induction

We begin with a couple of definitions that are fundamental, yet this technique we are building to is so algorithmic I believe students can become extremely proficient at applying mathematical induction with little found here.

Definition 6.5.1 Successor. Let $n \in \mathbb{N}$ we call $(n+1) \in \mathbb{N}$ the successor of n. ◊

In the late 1800's an Italian mathematician Giuseppe Peano developed five axioms which can create all of the basic ordering and arithmetic properties we all know and love of the natural numbers, using an undefined term of *successor*, our definition of course captures the heart of his construction. Let it be said, Peano did not consider 0 a natural number, but we will forgive him. It is through these axioms which one verifies induction, this is out side the scope of this text but, such a fun exercise for the dedicated reader!

Definition 6.5.2 Inductive Set. Let $S \subseteq \mathbb{N}$, we call S an **inductive set** if and only if S has the property

$$n \in S \implies (n+1) \in S$$

◊

This says that a set S is an inductive set whenever it contains all of its successors.

It is inductive sets that are the underpinning of mathematical induction.

Definition 6.5.3 Principle of Mathematical Induction. Let $k \in \mathbb{N}$, and let $S \subseteq \mathbb{N}$ with the following properties:

(i) $k \in S$

(ii) S is an inductive set

Then S contains all natural numbers greater than or equal to k, that is

$$S = \{n \in \mathbb{N} \mid n \geq k\}$$

◊

In some texts this is referred to as a *generalized* version of induction, those people also usually follow in the footsteps of Peano and naively assume 0 is not a natural number, we instead give the following example.

Example 6.5.4 Let $S \subseteq \mathbb{N}$ and assume that both $0 \in S$ and S is an inductive set. By the Principle of Mathematical Induction (PMI) we can conclude that $S = \mathbb{N}$. □

It has now been my experience that students have clocked out at this point in the lecture, no matter how much I have promised them that their algorithmic

tendencies will be returning. So let's let the rubber hit the road and actual do some proofs!

The basic idea of PMI is to prove that the truth set, $S \subset \mathbb{N}$, of a predicate $P(x)$ is equal to an inductive set. Or to hopefully make this sound less like a riddle,

Proof of $\forall m \geq k$ $P(m)$ Using PMI.

Proof:

(i) ***(Base Step)*** Show that $P(k)$ is true

(ii) ***(Induction Assumption)*** Assume we can find an $n \in \mathbb{N}$ such that $P(n)$ is true

(iii) (***Prove:*** $\mathbf{P(n+1)}$) ... thus $P(n+1)$ is true

Therefore $\forall m \in \mathbb{N}$ such that $m \geq k$ then $P(m)$ is true.

Hopefully you can at least start to see the algorithm forming, there are 3 steps, and we take these steps every time!

6.6 First Proof with Induction

For our first example of induction we will use a summation (Section 6.2, p. 103)

Prove: For any $m \in \mathbb{N}$ with $m \geq 1$

$$\sum_{i=1}^{m}(2i-1) = m^2$$

Before we begin this proof we sing a slightly different song for induction (play-along):

"What's the Base Case?"**1.** $m = 1$

"What's the $P(m)$?"**2.**

$$P(m) : \sum_{i=1}^{m}(2i-1) = m^2$$

"What're the definitions?"**3.** summation (Section 6.2, p. 103)!

"Now, what to do?"**4.** Principle of Mathematical Induction! (it is the point of the chapter, also we usually just call it *induction*)

6.7 The Beginning

In *Induction* we always begin with showing the base case, in our song we identified the base case as $m = 1$, so for our first step we need to show that $P(1)$ is true

(i) (Base Case):

$$\begin{aligned}\sum_{i=1}^{1}(2i-1) &= 2\cdot(1)-1\\ &= 1\\ &= 1^2\end{aligned}$$

hence $P(1) : \sum_{i=1}^{1}(2i-1) = 1^2$,that is we have shown the base case

After our base case step we use our most crucial step of them all the induction assumption, this is where we just assume it works for some arbitrary number that is at least the size of our base case. For this example I will name that *arbitrary* number n.

(ii) (Induction Assumption):

Assume we can find an $n \in \mathbb{N}$ such that

$$\sum_{i=1}^{n}(2i-1) = n^2$$

6.8 The Muddle

The muddle for an induction always has the same purpose an often is done with a calculation. The purpose of the muddle is to satisfy the last part of an induction proof, the $n+1$ case.

(iii) (***Prove:*** $\mathbf{P(n+1)}$)

Now we (use the student's favorite word...) *calculate*

$$\begin{aligned}
\sum_{i=1}^{n+1}(2i-1) &= \left(\sum_{i=1}^{n}(2i-1)\right) + (2(n+1)-1) && \text{(peel off)}\\
&= n^2 + (2(n+1)-1) && \text{(induction assumption!)}\\
&= n^2 + 2n + 2 - 1\\
&= n^1 + 2n + 1\\
&= (n+1)^2 && \text{(factoring)}
\end{aligned}$$

6.9 The End

Using *Induction* the muddle should have always endend with a calculation which showed our desired result. In this example we have shown

$$P(n+1) : \sum_{i=1}^{n+1}(2i-1) = (n+1)^2$$

therefore by proof by induction we have shown for any $m \in \mathbb{N}$ with $n \geq 1$ that

$$\sum_{i=1}^{m}(2i-1) = m^2$$

QED

6.10 Basic Induciton Examples

In this section we will give some basic examples of induction using the tools from Section 6.1, p. 103

Example 6.10.1 ***Prove:*** For any $m \in \mathbb{N}$ with $m \geq 1$

$$\sum_{i=1}^{m}(8i-5) = 4m^2 - m$$

Proof. ***(i) (Base Case):***
Note that as we are tasked to show our result holds for any $m \geq 1$, our base case is 1!

$$\begin{aligned}\sum_{i=1}^{1}(8i-5) &= (8\cdot(1)-5)\\ &= 3\\ &= 4\cdot(1)^2-(1)\end{aligned}$$

thus we have shown

$$P(1): \sum_{i=1}^{1}(8i-5) = 4\cdot(1)^2-(1)$$

(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$\sum_{i=1}^{n}(8i-5) = 4n^2 - n$$

(iii) (***Prove:*** $\mathbf{P(n+1)}$)
Calculate:

$$\begin{aligned}\sum_{i=1}^{n+1}(8i-5) &= \left(\sum_{i=1}^{n}(8i-5)\right) + (8(n+1)-5) && \text{(peel off)}\\ &= (4n^2-n)+(8n+3) && \text{(induction assumption)}\\ &= 4n^2+7n+3\end{aligned}$$

For this example I find it easiest to also work *backwards*

$$\begin{aligned}4(n+1)^2-(n+1) &= 4(n^2+2n+1)-(n+1)\\ &= 4n^2+8n+4-n-1\\ &= 4n^2+7n+3\end{aligned}$$

Thus, we have shown $\sum_{i=1}^{n+1}(8i-5) = 4(n+1)^2-(n+1)$.
Hence, by proof by principle of mathematical induction, $\sum_{i=1}^{m}(8i-5) = 4m^2 - m$ for any $m \in \mathbb{N}$ with $m \geq 1$. □ ■

□

Example 6.10.2 ***Prove:*** For any $m \in \mathbb{N}$ with $m \geq 1$

$$\sum_{i=1}^{m}(3i-2) = \frac{m}{2}(3m-1)$$

Proof. ***(i) (Base Case):***

$$\begin{aligned}\sum_{i=1}^{1}(3i-2) &= 3(1)-2\\ &= 1\\ &= \frac{1}{2}(3(1)-1)\end{aligned}$$

hence we have established:

$$P(1): \sum_{i=1}^{1}(3i-2) = \frac{1}{2}(3(1)-1)$$

(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$\sum_{i=1}^{n}(3i-2) = \frac{n}{2}(3n-1)$$

(iii) (***Prove:*** $\mathbf{P(n+1)}$)
Calculate:

$$\begin{aligned}\sum_{i=1}^{n+1}(3i-2) &= (\sum_{i=1}^{n}(3i-2)) + (3(n+1)-2)\\ &= \frac{n}{2}(3n-1) + (3(n+1)-2) \qquad \text{(induction assumption)}\\ &= \frac{n}{2}(3n-1) + (3n+1)\\ &= \frac{n}{2}(3n-1) + \frac{2}{2}(3n+1)\\ &= \frac{n(3n-1)+2(3n+1)}{2}\\ &= \frac{3n^2-n+6n+2}{2}\\ &= \frac{3n^2+5n+2}{2}\\ &= \frac{(n+1)(3n+2)}{2}\\ &= \frac{(n+1)(3(n+1)-1)}{2}\end{aligned}$$

Thus, we have shown $\sum_{i=1}^{n+1}(3i-2) = \frac{(n+1)}{2}(3(n+1)-1)$.
Hence, by proof by principle of mathematical induction, $\sum_{i=1}^{m}(3i-2) = \frac{m}{2}(3m-1)$ for any $m \in \mathbb{N}$ with $m \geq 1$. □ ■

□

Example 6.10.3 ***Prove:*** For any $m \in \mathbb{N}$ with $m \geq 1$

$$\sum_{i=1}^{m}\frac{1}{i(i+1)} = \frac{m}{m+1}$$

Proof. ***(i) (Base Case):***
Note that as we are tasked to show our result holds for any $m \geq 1$, our base case is again 1!

$$\begin{aligned}\sum_{i=1}^{1} \frac{1}{i(i+1)} &= \frac{1}{(1)\cdot((1)+1)} \\ &= \frac{1}{2} \\ &= \frac{(1)}{((1)+1)}\end{aligned}$$

hence we have established

$$P(1) : \sum_{i=1}^{1} \frac{1}{i(i+1)} = \frac{(1)}{((1)+1)}$$

(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

(iii) (***Prove:*** $\mathbf{P(n+1)}$)
Calculate:

$$\begin{aligned}\sum_{i=1}^{n+1} \frac{1}{i(i+1)} &= \left(\sum_{i=1}^{n} \frac{1}{i(i+1)}\right) + \frac{1}{(n+1)((n+1)+1)} && \text{(peel off)} \\ &= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} && \text{(Induction Assumption)} \\ &= \frac{n(n+2)+1}{(n+1)(n+2)} && \text{(common denominator)} \\ &= \frac{n^2+2n+1}{(n+1)(n+2)} \\ &= \frac{(n+1)^2}{(n+1)(n+2)} && \text{(factoring)} \\ &= \frac{n+1}{(n+1)+1}\end{aligned}$$

Thus, we have shown $\sum_{i=1}^{n+1} \frac{1}{i(i+1)} = \frac{n+1}{(n+1)+1}$.
Hence, by proof by principle of mathematical induction, $\sum_{i=1}^{m} \frac{1}{i(i+1)} = \frac{m}{m+1}$ for any $m \in \mathbb{N}$ with $m \geq 1$. □ ■

□

Now let's see some examples using the product Section 6.1, p. 103

Example 6.10.4 ***Prove:*** For any $m \in \mathbb{N}$ with $m \geq 1$

$$\prod_{i=1}^{m} \left(1 - \frac{1}{i+1}\right) = \frac{1}{m+1}$$

Proof. ***(i) (Base Case):***
Note that as we are tasked to show our result holds for any $m \geq 1$, our base case is again 1!

$$\begin{aligned}\prod_{i=1}^{1}\left(1-\frac{1}{i+1}\right) &= 1-\frac{1}{(1)+1}\\ &= 1-\frac{1}{2}\\ &= \frac{2-1}{2}\\ &= \frac{1}{(1)+1}\end{aligned}$$

hence we have established our based case, that is:

$$P(1): \prod_{i=1}^{1}\left(1-\frac{1}{i+1}\right) = \frac{1}{(1)+1}$$

(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$\prod_{i=1}^{n}\left(1-\frac{1}{i+1}\right) = \frac{1}{n+1}$$

(iii) (***Prove:*** $\mathbf{P(n+1)}$)
Calculate:

$$\begin{aligned}\prod_{i=1}^{n+1}\left(1-\frac{1}{i+1}\right) &= \left(\prod_{i=1}^{n}\left(1-\frac{1}{i+1}\right)\right)\cdot\left(1-\frac{1}{(n+1)+1}\right) && \text{(peel off)}\\ &= \left(\frac{1}{n+1}\right)\cdot\left(1-\frac{1}{n+2}\right) && \text{(induction assumption)}\\ &= \frac{1}{n+1}-\frac{1}{n+1}\cdot\frac{1}{n+2}\\ &= \frac{(n+2)-1}{(n+1)(n+2)} && \text{(common denominator)}\\ &= \frac{n+1}{(n+1)(n+2)}\\ &= \frac{1}{(n+1)+1}\end{aligned}$$

Thus, we have shown $\prod_{i=1}^{n+1}\left(1-\frac{1}{i+1}\right) = \frac{1}{(n+1)+1}$.
Hence, by proof by principle of mathematical induction, $\prod_{i=1}^{m}\left(1-\frac{1}{i+1}\right) = \frac{1}{m+1}$ for any $m \in \mathbb{N}$ with $m \geq 1$. □ ■

□

Next, we explore an example with a base case not 1.

Example 6.10.5 ***Prove:*** For any $m \in \mathbb{N}$ with $m \geq 2$

$$\prod_{i=2}^{m}\frac{i^2-1}{i^2} = \frac{m+1}{2m}$$

Proof. ***(i) (Base Case):***
For this example as we are asked to prove this for all $m \geq 2$, our base case is 2.

$$\begin{aligned}\prod_{i=2}^{2} \frac{i^2-1}{i^2} &= \frac{(2)^2-1}{(2)^2} \\ &= \frac{4-1}{4} \\ &= \frac{3}{4} \\ &= \frac{(2)+1}{2\cdot(2)}\end{aligned}$$

hence we have established:

$$P(2): \prod_{i=2}^{2} \frac{i^2-1}{i^2} = \frac{(2)+1}{2\cdot(2)}$$

(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$\prod_{i=1}^{n} \frac{i^2-1}{i^2} = \frac{n+1}{2n}$$

(iii) (***Prove:*** $\mathbf{P(n+1)}$)
Calculate:

$$\begin{aligned}\prod_{i=2}^{n+1} \frac{i^2-1}{i^2} &= \left(\prod_{i=1}^{n} \frac{i^2-1}{i^2}\right) \cdot \frac{(n+1)^2-1}{(n+1)^2)}() && \text{(peel off)} \\ &= \left(\frac{n+1}{2n}\right) \cdot \frac{(n+1)^2-1}{(n+1)^2)} && \text{(induction assumption)}\end{aligned}$$

$$\frac{(n+1)(n^2+2n+1-1)}{(2n)(n+1)^2}$$

$$\begin{aligned}&= \frac{n^2+2n}{2n(n+1)} \\ &= \frac{n(n+2)}{2n(n+1)} \\ &= \frac{(n+1)+1}{2(n+1)}\end{aligned}$$

Thus, we have shown $\prod_{i=2}^{n+1} \frac{i^2-1}{i^2} = \frac{(n+1)+1}{2(n+1)}$.
Hence, by proof by principle of mathematical induction, $\prod_{i=2}^{m} \frac{i^2-1}{i^2} = \frac{m+1}{2m}$ for any $m \in \mathbb{N}$ with $m \geq 2$. □ ■

□

Next, lets see some examples with the factorial Section 6.1, p. 103

Example 6.10.6 ***Prove:*** For any $m \in \mathbb{N}$ with $m \geq 1$

$$\prod_{i=1}^{m}(4i-2) = \frac{(2m)!}{(m!)}$$

Proof. ***(i) (Base Case):***
Let $n = 1$. Calculate $\prod_{i=1}^{1}(4i-2) = \frac{2(1)!}{(1)!}$:

$$4(1) - 2 = 2$$

(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$\prod_{i=1}^{n}(4i-2) = \frac{(2n)!}{(n!)}$$

(iii) (***Prove:*** $\mathbf{P(n+1)}$)
Calculate:

$$\begin{aligned}
\prod_{i=1}^{n+1}(4i-2) = \frac{2(n+1)!}{(n+1)!} &= (\prod_{i=1}^{n}(4i-2))((4(n+1)-2) \\
&= \frac{2n!}{n!}((4(n+1)-2) \qquad \text{(induction assumption)} \\
&= (\frac{2n!}{n!})(4n+2) \\
&= (\frac{2n!}{n!})(2(2n+1)) \\
&= (2)\frac{(2n+1)((2n)!)}{n!} \\
&= \frac{(2n+1)!}{n!}(2) \\
&= \frac{(2n+2)!}{\frac{1}{2}(2n+2)n!} \\
&= \frac{(2n+2)!}{(n+1)n!} \\
&= \frac{(2n+2)!}{(n+1)!}
\end{aligned}$$

Thus, we have shown $\prod_{i=1}^{n+1}(4i-2) = \frac{2(n+1)!}{(n+1)!}$.
Hence, by proof by principle of mathematical induction, $\prod_{i=1}^{m}(4i-2) = \frac{(2m)!}{m!}$ for any $m \in \mathbb{N}$ with $m \geq 1$. □ ■

□

Example 6.10.7 ***Prove:*** For any $m \in \mathbb{N}$ with $m \geq 1$

$$\sum_{i=1}^{m}\frac{i}{(i+1)!} = 1 - \frac{1}{(m+1)!}$$

Proof. ***(i) (Base Case):***
Note that as we are tasked to show our result holds for any $m \geq 1$, our base case is again 1!

$$\sum_{i=1}^{1} \frac{i}{(i+1)!} = \frac{(1)}{(1)+1}$$

hence we have verified the condition $P(1)$
(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$\sum_{i=1}^{n} \frac{i}{(i+1)!} = 1 - \frac{1}{(n+1)!}$$

(iii) (***Prove:*** $\mathbf{P(n+1)}$)
Calculate:

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{i}{(i+1)!} &= \left(\sum_{i=1}^{n} \frac{i}{(i+1)!}\right) + \frac{(n+1)}{[(n+1)+1]!} && \text{(peel off)} \\
&= \left(1 - \frac{1}{(n+1)!}\right) + \frac{n+1}{(n+2)!} && \text{(induction assumption)} \\
&= 1 + \frac{-(n+2)+(n+1)}{(n+2)!} && \text{(common denominator)} \\
&= 1 - \frac{1}{((n+1)+1)!}
\end{aligned}$$

Thus, we have shown $\sum_{i=1}^{n+1} \frac{i}{(i+1)!} = 1 - \frac{1}{((n+1)+1)!}$.
Hence, by proof by principle of mathematical induction, $\sum_{i=1}^{m} \frac{i}{(i+1)!} = 1 - \frac{1}{(m+1)!}$ for any $m \in \mathbb{N}$ with $m \geq 1$. □ ■

□

I really like this next example as it exemplifies how induction is often used in your future algebra courses, namely the union is defined as something between two sets, so to do it to multiple sets we need do two at a time. This *two at a time* is an example of *peeling off*, just as the previous examples.

Example 6.10.8 ***Prove:*** Let $\mathscr{A} = \{A_i \mid i \in \Delta\}$ be an indexed family of sets, and For any $m \in \mathbb{N}$ with $m \geq 1$ such that $\Delta = \{1, 2, ..., m\}$

$$\left(\bigcap_{i=1}^{m} A_i\right)^c = \bigcup_{i=1}^{m} A_i^c$$

Proof. ***(i) (Base Case):***
Note that as we are tasked to show our result holds for any $m \geq 1$, our base case is again 1!

$$\left(\bigcap_{i=1}^{1} A_i\right)^c = (A_1)^c$$

hence we have established the base case $P(1)$
(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$\left(\bigcap_{i=1}^{n} A_i\right)^c = \bigcup_{i=1}^{n} A_i^c$$

(iii) (***Prove:*** $\mathbf{P(n+1)}$)
Calculate:

$$\begin{aligned}
\left(\bigcap_{i=1}^{n+1} A_i\right)^c &= \left(\left(\bigcap_{i=1}^{n} A_i\right) \cap A_{n+1}\right) && \text{(peel off)} \\
&= \left(\bigcap_{i=1}^{n} A_i\right)^c \cup A_{n+1}^c && \text{(DeMogran's Law)} \\
&= \left(\bigcup_{i=1}^{n} A_i^c\right) \cup A_{n+1}^c && \text{(induction assumption)} \\
&= \bigcup_{i=1}^{n+1} A_i^c
\end{aligned}$$

Thus, we have shown $\left(\bigcap_{i=1}^{n+1} A_i\right)^c = \bigcup_{i=1}^{n+1} A_i^c$.
Hence, by proof by principle of mathematical induction, $\left(\bigcap_{i=1}^{m} A_i\right)^c = \bigcup_{i=1}^{m} A_i^c$ for any $m \in \mathbb{N}$ with $m \geq 1$. □ ■

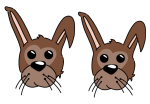
□

6.11 The Fibonacci Sequence

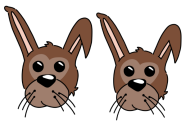
This next topic is one that stuck with me from my undergraduate experience. I was lucky enough to be taught by the Italian mathematician Dr. Annalisa Calini. She told us the story of her fellow Italian mathematician Fibonacci with such enthusiasm that I could never hope to match. Yet, here is my poor attempt.

The Story of Fibonacci.

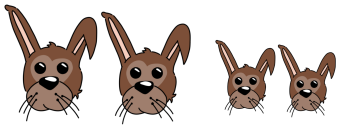
Our story begins on ***Day 1*** with Fibonacci sitting in a park on a beautiful day. He notices *1 pair* young bunnies, male and female, hopping by.



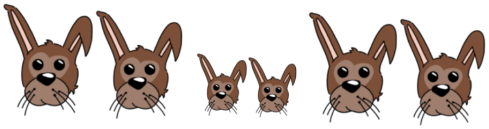
The next day, on ***Day 2*** Fibonacci returned to the same park and noticed the same *1 pair*, yet this time they have grown to rabbits, now biologically capable of procreating.



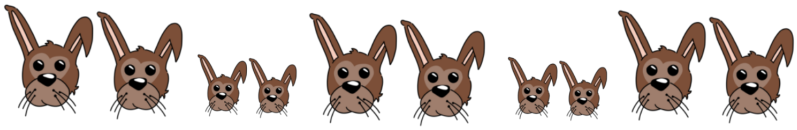
He again returned the following day, on ***Day 3***, and on this day he noticed his pair of rabbits, but also another pair of bunnies, again paired as in one male and one female, giving us a total of *2 pair* of rabbits.



Now on ***Day 4*** Fibonacci noticed his original pair had given birth again, as well as the first litter was now grown to the age of reproduction, giving us *3 pairs* of rabbits total. He deduced that it took one day for the rabbits to mature, and then another day for the rabbits to give birth to a new pair of bunnies.



On ***Day 5*** returning once again to this same park he noticed that his original pair was there, and their first litter but not the original pair and the first litter have both produced pairs of bunnies, leaving a total of *5 pairs* of rabbits at the park.



Later on Day 5, Fibonacci returns to his home and comes up with perhaps the greatest mathematical assumption in all of history,

Assume that rabbits never die!

Then asked himself how many rabbits would be there on day 6, or 7, or 8, or even 1000...

To create a formal definition of the fibonacci we use the concept of inductive definitions. An inductive definition is one which takes the form of PMI, specifically where we first define a base case and then we define the inductive step

Definition 6.11.1 The Fibonacci Numbers. ***(i) (Bases Cases)***

$$f_1 = 1 \text{ and } f_2 = 1$$

(ii) (Inductive Case)

To calculate any Fibonacci number, f_n, we add the two numbers that preceded it:

$$f_n = f_{n-1} + f_{n-2}$$

$\Diamond$

For fun let's count some more rabbits.

Example 6.11.2 By definition

$$f_1 = 1$$
$$f_2 = 1$$

then

$$f_3 = f_2 + f_1 = 1 + 1 = 2$$
$$f_4 = f_3 + f_2 = 2 + 1 = 3$$
$$f_5 = f_4 + f_3 = 3 + 2 = 5$$
$$f_6 = f_5 + f_4 = 5 + 3 = 8$$
$$f_7 = f_6 + f_5 = 8 + 5 = 13$$
$$f_8 = f_7 + f_6 = 13 + 8 = 21$$

so many bunnies... $\square$

The awake student, usually sitting somewhere right off the front row, will notice that when we defined the Fibonacci numbers we didn't just have a singular base case, and we didn't define the $n+1$ case, which is slightly different from the procedure of induction. To this student I applaud you, that is correct; we instead used a slightly different version of induction, known commonly as complete induction.

Definition 6.11.3 Principle of Complete Induction. Let $k \in \mathbb{N}$ and suppose S is a subset of $\mathbb{N}$ with the following property:

$\forall n \in \mathbb{N}$ with $k < n$

if $\{k, k+1, k+2, k+3, ..., n-1\} \subset S$ then $n \in S$

Then $S = \{n \in \mathbb{N} \mid n \geq k\}$ $\Diamond$

Proving using complete induction amounts to a procedure almost identical to that of our traditional induction

Proof of $\forall m \in \mathbb{N}$ $m \geq k$ $P(m)$ with Complete Induction.

Proof:

(i) ***(Base Steps)*** Show that $P(k)$ and $P(k+1)$ are true

(ii) ***(Induction Assumption)*** Assume we can find an $n \in \mathbb{N}$ such that $P(t)$ is true for any $t \in \mathbb{N}$ such that $k \leq t < n$

(iii) (***Prove:*** $\mathbf{P(n)}$) ... thus $P(n)$ is true

Therefore $\forall m \in \mathbb{N}$ such that $m \geq k$ then $P(m)$ is true.

The astute student will note we are really doing nothing different here... as in PMI we said *for any* n so why not up to any $n-1$. But, this really

allows us to do exactly what we have been doing its just that in step (iii) it becomes quite cumbersome to balance $n+1$ everywhere, so this way just lets us use n as well sometimes we can just get some number less than n and it is there we would like to invoke the induction assumption not hitting exactly one number. This range version is much more versatile and it is the method that I personally just always default to.

Example 6.11.4 ***Prove:*** For any $m \in \mathbb{N}$ such that $m \geq 1$ we have f_{3m} is even (every third Fibonacci number is even)

Proof. ***(i) (Base Cases):***
As we are to show this result for any $m \geq 1$, our first base case will be 1!

$$f_{3\cdot 1} = f_2 + f_1 = 1 + 1 = 2$$

and since 1 is an integer and thus $2 = 2 \cdot 1$ is even.
As we are using PCI we need to show our next base case of 2.

$$f_{3\cdot(2)} = f_6 = f_5 + f_4 = 8$$

(see Example 6.11.2, p. 118 for the complete calculation of f_6) and since 4 is an integer and thus $8 = 2 \cdot 4$ is even.
Hence we have established the base cases:

$$P(1) : f_{3\cdot(1)} \text{ is even}$$

and

$$P(2) : f_{3\cdot(2)} \text{ is even}$$

(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$f_{3t} \text{ is even}$$

for any $t \in \mathbb{N}$ such that $1 \leq t < n$
(iii) (***Prove:*** $\mathbf{P(n)}$)
Calculate:

$$\begin{aligned} f_{3n} &= f_{3n-1} + f_{3n-2} \\ &= f_{3n-2} + f_{3n-3} + f_{3n-2} \\ &= 2(f_{3n-2}) + f_{3(n-1)} \end{aligned}$$

Hence, by induction assumption, $f_{3(n-1)}$ is even. Thus by definition of even, we can find an integer m such that $f_{3(n-1)} = 2m$
Calculate:

$$\begin{aligned} f_{3n} &= 2f_{3n-2} + 2m \\ &= 2(f_{3n-2+m}) \end{aligned}$$

Thus by definition of even, f_{3n} is even. Thus by proof by PCI, f_{3n} is even for all $n \in \mathbb{N}$ ■

□

Example 6.11.5 ***Prove:*** For any $m \in \mathbb{N}$ such that $m \geq 1$ we have f_{3m+1} is odd

Proof. ***(i) (Base Case):***
Since, again, we are to show this for any $m \geq 1$, our first base case is 1!

$$f_{3(1)+1} = f_4 = f_3 + f_2 = (f_2 + f_1) + f_2 = (1+1) + 1 = 3$$

Since 1 is an integer and $3 = 1 \cdot (1) + 1$ we have that 3 is odd.
As we are using PCI we need to show our next base case of 2.

$$f_{3\cdot(2)+1} = f_7 = f_6 + f_5 = 13$$

(see Example 6.11.2, p. 118 for the complete calculation of f_7) and since 6 is an integer and thus $13 = 2 \cdot 6 + 1$ is odd.
Hence, we have estableshed the base cases

$$P(1) : f_{3\cdot(1)+1} \text{ is odd}$$

and

$$P(2) : f_{3\cdot(2)+1} \text{ is odd}$$

(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that

$$f_{3t+1} \text{ is odd}$$

for any $t \in \mathbb{N}$ such that $1 \leq t < n$
(iii) (***Prove:*** **P(n)**)
Calculate:

$$\begin{aligned} f_{3n+1} &= f_{3n} + f_{3n-1} \\ &= f_{3n} + f_{3n-2} + f_{3n-3} \\ &= 2(f_{3n}) + f_{3n-2} + f_{3(n-1)} \\ &= 2(f_{3n}) + f_{3(n-1)+1} + f_{3(n-1)} \end{aligned}$$

Note: we know f_{3n} and $f_{3(n-1)}$ are even, because we just proved it. By our induction assumption, $f_{3(n-1)+1}$ is odd. Hence by definition of odd, we can find $l, m, a \in \mathbb{Z}$ such that $f_{3n} = 2l$, $f_{3(n-1)} = 2m$, and $f_{3(n-1)+1} = 2a + 1$.
Calculate:

$$\begin{aligned} f_{3n} + f_{3(n-1)+1} + f_{3(n-1)} &= 2l + 2a + 1 + 2m \\ &= 2(l + a + m) + 1 \end{aligned}$$

Thus by definition of odd, f_{3n+1} is odd. Thus by proof by PCI, f_{3n+1} is odd for all $n \in \mathbb{N}$ ■
□

6.12 Well-Ordering Principle

One of the most important properties of the natural numbers, that will be used constantly in your studies even if it is rarely mentioned and that is:

Well-Ordering Principle (WOP).

Every nonempty subset of $\mathbb{N}$ has a smallest element.

In class when I have introduced this topic in the past it has been greeted

with the dreaded *wEℓL oBvIoUsLy*.

This property is quite unique to the natural numbers, it's not true in the integers, the rationals, the positive rational numbers, the real numbers, nor are the non-negative real numbers.

WOP seems to come up most often with contradiction, specifically assuming some property you to want to be true for the natural numbers is not. This is the negation of a universal statement, and thus you are assuming an existential, one way of interpreting this existential is to say that thus the set of all natural numbers that do not have this property is nonempty. Then WOP gives us a smallest member of this set, and we can quite often contradict by constructing a smaller element, for example.

For our first example and for the rest of this section we will need a couple of assumptions, firstly the following definitions

Definition 6.12.1 Prime Number. We say an integer, n, is **prime** when the only divisors are 1 and n ◊

and of course for the non-primes.

Definition 6.12.2 Composite Integer. We say an integer, n, is **composite** when it is not prime, that is when it has a divisor other than 1 and n. ◊

Note 6.12.3 Besides our usual assumptions we will also assume the properties of inequalities you know and love from your college algebra course as well (I usually skip these proofs in class but include them for reference to WOP in my later classes)

We will also find the next lemma useful for the following proofs.

Lemma 6.12.4 *For all integers a and b with $b > 0$, if $a|b$ then $a \leq b$*

Proof. Let a and b be arbitrary integers with $b > 0$ and assume that $a|b$. By definition of divides we can find an integer q such that $b = aq$. Since we assumed that $b > 0$ we have that both $a > 0$ and $q > 0$. For sake of contradiction assume that $a > b$, hence $0 < a - b$ hence $0 < a - aq = a(1 - q)$.
Since $a > 0$ then $0 < (1 - q)$ hence $0 < q < 1$ thus $q = 0$ and hence $b = a \cdot q = a \cdot 0 = 0$ a contradiction to our assumption that $b > 0$, as specifically $b \neq 0$. ■

Example 6.12.5 ***Prove:*** Every natural number $n > 1$ has a prime factor.

Proof. Choose an arbitrary $n \in \mathbb{N}$, if n is prime then indeed n has a prime factor, namely itself. If n is composite then something other than n and 1 must divide n. Therefore the following set is non-empty:

$$R = \{m \in \mathbb{N} \mid m|n,\ m \neq n, \text{ and } m \neq 1\}$$

By WOP, R has a smallest element, denote this element as $p \in T$.
For the sake of contradiction assume that p is not prime, that is we assume that p is composite. By definition of composite we can find a divisor d such that $d \neq 1$ and $d \neq p$, yet by definition of divides we can find a $k \in \mathbb{Z}$ such that $p = dk$ and we can find a $t \in \mathbb{N}$ such that $n = tp$, thus $n = tdk$, therefore $d \in R$ Yet by Lemma 6.12.4, p. 121 we have that $d \leq p$ yet we assumed $d \neq p$ hence $d < p$ a contradiction to p being the smallest element of R. □ ■

□

We have used the next proposition without proof throughout the text, now we can finally present a proof here.

Proposition 6.12.6 The Division Algorithm. *For all integers a and b, with $a \neq 0$, there exists unique integers q and r such that*

$$b = qa + r$$

with $0 \leq r < |a|$

Proof of the Division Algorithm. Let a and b be integers with $a \neq 0$.
Consider the set:

$$S = \{b - ak \mid k \in \mathbb{Z} \text{ and } b - ak \geq 0\}$$

Notice that if $0 \in S$ then we can find a $t \in \mathbb{Z}$ such that $b - at = 0$ thus $b = at$ and hence t plays the role of our desired q and we can simply set $r = 0$. So we now assume that $0 \notin S$.
Since 0 is not in S, then $b \neq 0$ as if b were zero then $b - a \cdot 0 = 0$. Now if $b > 0$ then $b - a \cdot 0 \in S$ and thus $S \neq \emptyset$, if $b < 0$ and $a > 0$ then $b - a \cdot (2b) > 0$ thus $b - a \cdot (2b) \in S$ and again S is not empty, if $a < 0$ then the same can be said of $b - (-1) \cdot a \cdot (2b)$. Therefore $S \neq \emptyset$ and hence we can use WOP to determine that there must be a smallest element, name this element r. By the definition of S we can find an integer q such that $r = b - aq$. Thus $b = aq + r$ and $r \geq 0$. For the sake of contradiction assume that $r > |a|$, hence $r - a > 0$ when $a > 0$ and $r + a > 0$ when $a > 0$.
Case 1: Assume $a > 0$
Next note that $b - a(q - 1) = b - aq + a = r + a > 0$ thus $b - a(q + 1) \in S$, yet $b - a(q + 1) < b - aq$ a contradiction to r being the smallest member of S, hence $r \leq a = |a|$ as desired.
Case 2: Assume $a < 0$
Now note that $b - a(q - 1) = b - aq + a = r + a > 0$ thus $b - a(q - 1) \in S$, yet $b - a(q - 1) < b - aq$ a contradiction to r being the smallest member of S, hence $r \leq -a = |a|$ as desired. ■

Proposition 6.12.7 The Fundamental Theorem of Arithmetic. *Every natural number greater than 1 is either prime or can be expressed as a product of primes.*

Proof of The Fundamental Theorem of Arithmetic. For this proof we will use PCI
(i) (Base Case):
Our base case is 2 in this example as we are trying to prove the statement for any $m > 1$. So consider $2 \in \mathbb{N}$ by Lemma 6.12.4, p. 121 anything that divides 2 must be less than or equal to 2, and hence it is either 1 or 2, and thus 2 is prime, hence we have established our base case.
(ii) (Induction Assumption):
Assume we can find an $n \in \mathbb{N}$ such that for any $t \in \mathbb{N}$ such that $1 < t < n$ then t is either prime or can be expressed uniquely as a product of primes.
(iii) (***Prove:*** $\mathbf{P(n)}$)
By Example 6.12.5, p. 121 we can find an integer q and a prime number p such that $n = qp$. By Lemma 6.12.4, p. 121 we have that $q < n$. If $q = 1$ then n is prime and we are done, so assume that $q > 1$. Since $1 < q < n$ by our induction assumption we can write q as a product of primes, denote this as $q = \prod_{i=1}^{s} p_i$ for some $s \geq 1$ and each p_i is a prime. Thus $n = (\prod_{i=1}^{s} p_i) \cdot p$ hence we have written n as a product of primes. ■

6.13 Exercises

1. Use Induction to prove that the following hold

   (a) $\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$ for all $m \geq 1$

(b) $\sum_{i=1}^{n}(2i-1)^3 = n^2(2n^2-1)$ for all $m \geq 1$

(c) $\prod_{i=1}^{n}(2i-1) = \frac{(2n)!}{n!2^n}$ for all $m \geq 1$

(d) $\sum_{i=1}^{m}(3i-2) = \frac{m}{2}(3m-1)$ for all $m \geq 1$

(e) $\sum_{i=1}^{m}(2i-1)^3 = m^2(2m^2-1)$ for all $m \geq 1$

(f) $\sum_{i=1}^{m}\frac{i}{(i+1)!} = 1 - \frac{1}{(m+1)!}$

(g) $\sum_{i=0}^{m}3^i = \frac{3^{m+1}-1}{2}$ for all $m \in \mathbb{N}$

(h) $f_1 + f_2 + f_3 + ... + f_m = f_{m+2} - 1$ for all $m \geq 1$

(i) $f_{m+6} = 4f_{m+3} + f_m$ for all $m \geq 1$

(j) f_{3m+2} is odd for all $m \geq 1$

2. Let $\mathscr{A} = \{A_i \mid i \leq m\}$ be an indexed family of sets, prove: $\left(\bigcup_{i=1}^{m} a_i\right)^c = \bigcap_{i=1}^{m} A_i^c$ for all $m \geq 1$

Chapter 7

Relations

This is chapter involves itself with one of most important concepts of all of mathematics. It is the concept of relationship. This concept has already been explored (admittedly very little as I tried my best to avoid it) in this course but has been a major component of your traditional mathematics education.

In this course it has been seen with the little we have done with inequalities and even addition, believe it or not, but what you will hopefully immediately notice is the relations you have the most experience with are functions. Using your the years of intuition when working with the more general concept of relation will serve you very well in this chapter.

7.1 What is a Relation?

A relation at its heart is a simple a way of formalizing sentences like:

Bart is related to Lisa.

Slightly more formal, we will take two sets and define how the elements of these sets are related to each other.

Definition 7.1.1 Relations. Let A and B be sets. R is a **relation** from A to B if and only if R is a subset of $A \times B$ That is,

$$R \subseteq A \times B$$

When R is a relation from A to A we say it is a **relation on** A. $\Diamond$

Relation Notation and Verbage.

For sets A and B, with a relation R from A to B when

$$(a, b) \in R$$

we say:

- a is R-related to b
- a is related via R to b
- a is related to b (when R is understood in the context)

When $(a, b) \in R$ we will write

$$aRb$$

and when $(a, b) \notin R$ we will write

$$a \not R b$$

Note 7.1.2 Since the empty set $\emptyset$, is a subset of any set it is a relation from A to B. As well since any set is a subset of itself, the set $A \times B$ is also a relation from A to B.

At first glance this definition does not seem to match up with our intuition at all, and to add to that the notation may seem very unfamiliar. Our next example hopefully at least motivates the notation.

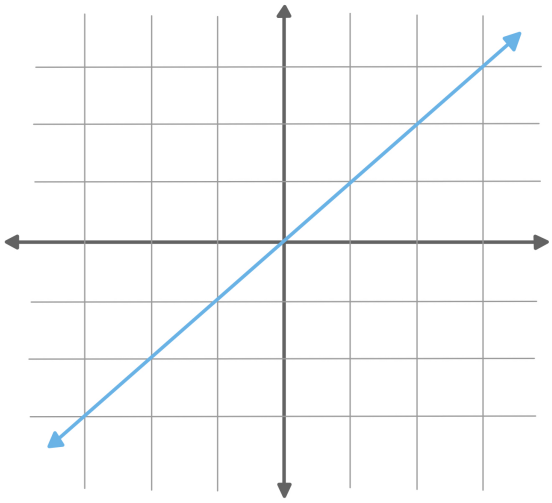
Example 7.1.3 Lets quickly examine a few relations on the real numbers, $\mathbb{R}$

(A) ***Equals:***

$$\{(a, a) \mid a \in \mathbb{R}\}$$

$(a, b) \in$ Equals means $a = b$

This relation can be viewed as the graph of $y = x$

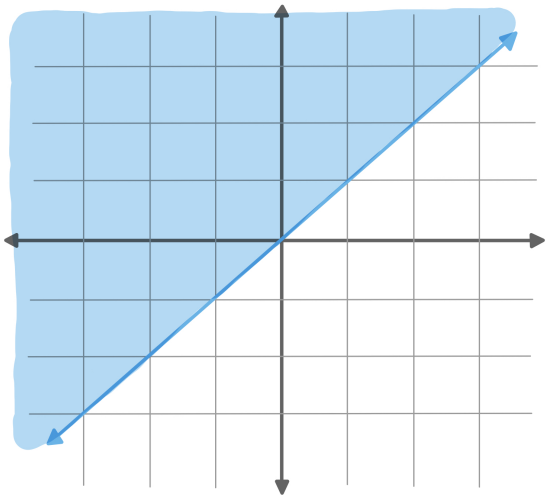


(B) ***Less than:***

$$\{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a < b\}$$

$(a, b) \in$ Less than means $a < b$

This relation can be visualized as the following shaded region



□

While admittedly this is quite a verbose way of explaining something that is already in your lexicon, hopefully this last example helps calm your stomach or at least motivate the notation, I would like to now step back and look at this new concept a little more abstractly.

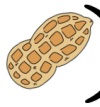
Example 7.1.4 For this example define the following two sets

$$Z = \{ \text{  }, \text{  }, \text{  } \}$$

$$F = \{ \text{  }, \text{  }, \text{  } \}$$

where Z consists of some animals from the zoo, and F is a set of some foods.

We will now define the relation, E as the following subset of $Z \times F$

$$E = \{ (\text{  }, \text{  }), (\text{  }, \text{  }), (\text{  }, \text{  }), (\text{  }, \text{  }) \}$$

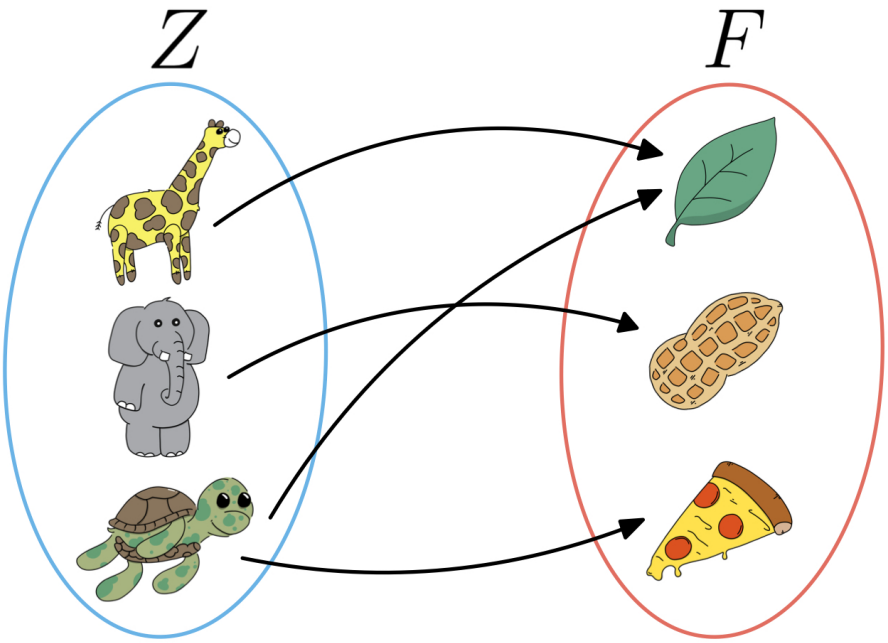
This is the relation of *eats*. Namely, $(a, b) \in E$ means a *eats* b. For example

$$(\text{  }) \in E$$

that is

or it is read/visualized more like:

Next, to motivate the wordage a relation *from* Z to F, we often visualize using what I refer to as the *egg* picture, where we draw an arrow from the element in the set Z to the element in the set F it is related to.



□

For sets A and B a relation from A to B does not need to *use* every element of A nor every element of B, we define the elements it does use.

Definition 7.1.5 Domain. The domain of the relation R from A to B is the set

$$\text{Dom}(R) = \{x \in A \mid \exists y \in B \text{ such that } xRy\}$$

◊

Definition 7.1.6 Range. The range of a relation R is the set

$$\text{Rng}(R) = \{y \in B \mid \exists x \in A \text{ such that } xRy\}$$

◊

Example 7.1.7 In this example, consider the two sets

$$A = \{1, 2, 3, 4, 5\}$$

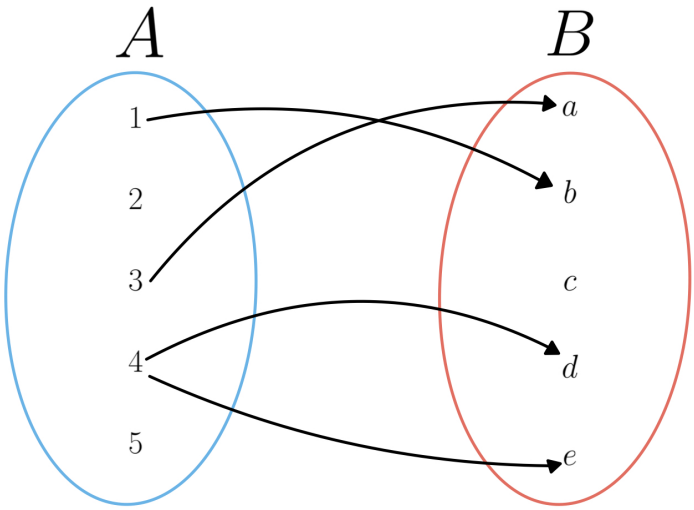
and

$$B = \{a, b, c, d, e\}$$

and define the relation R from A to B defined as

$$R = \{(1, b), (3, a), (4, d), (4, e)\}$$

which can be visualized as:



For this relation we have the following

$$\text{Dom}(R) = \{1, 3, 4\}$$

and

$$\text{Rng}(R) = \{a, b, d, e\}$$

□

7.2 New Relations From Old

This subsection is dedicated to making new relations from old ones. Our first method is by *turning around* the arrows.

Definition 7.2.1 Inverse. If R is a relation from A to B, then the inverse of R is the relation

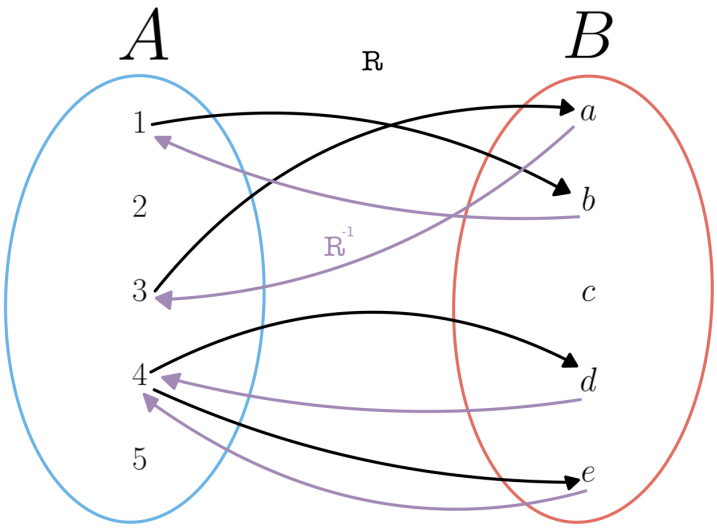
$$R^{-1} = \{(y, x) \mid (x, y) \in R\}$$

◊

Example 7.2.2 We will consider the same sets and relation as in Example 7.1.7, p. 127. The inverse is thus

$$R^{-1} = \{(a, 3), (b, 1), (d, 4), (e, 4)\}$$

which can be visualized as



Notice we have the following domain and range

$$\text{Dom}(R^{-1}) = \{a, b, d, e\}$$

$$\text{Rng}(R^{-1}) = \{1, 3, 4\}$$

□

Proposition 7.2.3 *Let R be a relation from A to B*

(a) $Dom(R^{-1}) = Rng(R)$

(b) $Rng(R^{-1}) = Dom(R)$

Proof of Proposition 7.2.3. We will prove part (a) and leave part (b) as an exercise to the reader
Let R be a relation from A to B.
Prove: $\text{Dom}(R^{-1}) = \text{Rng}(R)$
Don't forget relations are just sets, and to prove equality of sets, you must prove both subsets!
Proof of $\text{Dom}(\mathbf{R^{-1}}) \subseteq \text{Rng}(\mathbf{R^{-1}})$:
Let $a \in \text{dom}(R^{-1})$. Hence by definition of domain, we can find $b \in B$ such that $aR^{-1}b$. Hence, by definition of inverse, bRa. Since $b \in B$, by definition of range, $a \in \text{rng}(R)$.
Proof of $\text{Dom}(\mathbf{R^{-1}}) \supseteq \text{Rng}(\mathbf{R^{-1}})$:
Let $a \in \text{dom}(R^{-1})$. Hence, by definition of domain, we can find $b \in B$ such that $aR^{-1}b$. Hence, by definition of inverse, bRa. Since $b \in B$, by definition of range, $a \in \text{Rng}(R)$. ■

This next construction is one that may be familiar from your college algebra.

Definition 7.2.4 Composite. Let R be a relation from A to B, and let S be a relation from B to C. The composite of R and S is

$$S \circ R = \{(a, c) \mid \exists b \in B \text{ such that } (a, b) \in R \text{ and } (b, c) \in S\}$$

◊

Example 7.2.5 For this example consider again the sets

$$A = \{1, 2, 3, 4, 5\}$$

and

$$B = \{a, b, c, d, e\}$$

but in addition consider the set

$$C = \{\text{leaf}, \text{pizza}, \text{elephant}, \text{turtle}\}$$

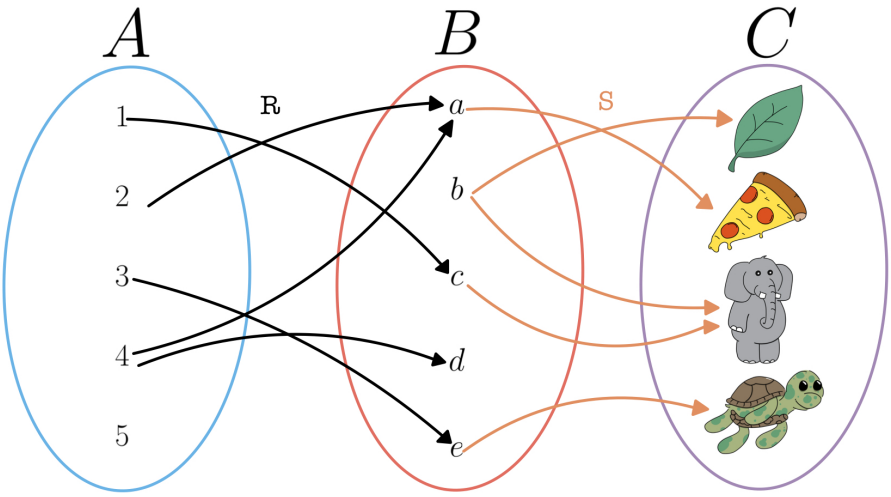
and define the relation R from A to B as

$$R = \{(1, c), (2, a), (3, e), (4, a), (4, d)\}$$

and define the relation S from B to C as

$$S = \{(b, \text{leaf}), (b, \text{elephant}), (c, \text{elephant}), (e, \text{turtle}), (a, \text{pizza})\}$$

Thus we can visulaize the composition as



and the relation is thus defined as

$$S \circ R = \{(4, \text{pizza}), (1, \text{elephant}), (3, \text{turtle}), (2, \text{pizza})\}$$

Notice we have the following domain and range of the composition

$$\text{Dom}(S \circ R) = \{1, 2, 3, 4\}$$

$$\text{Rng}(S \circ R) = \{\text{pizza}, \text{elephant}, \text{turtle}\}$$

□

Lets explore a few examples proving using this new concept of composition.

Example 7.2.6 Consider N and S, relations on $\mathbb{Z}$, defined as follows:

$$N = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 9|(a - b)\}$$

$$S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 6|(a - b)\}$$

Prove: $N \circ S \subseteq \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 3|(a - b)\}$

Proof. As one must do, we assume what we need to assume, namely assume that N and S are relations on $\mathbb{Z}$ defined above.
To begin, choose an arbitrary element $x \in N \circ S$, since N and S are relations on $\mathbb{Z}$ by definition of composite we can find an $a \in \mathbb{Z}$ and a $b \in \mathbb{Z}$ such that $x = (a, b)$, such that we can find an integer f such that $6|(a - f)$ and $9|(f - b)$. By definition of divides we can find an $s \in \mathbb{Z}$ and $t \in \mathbb{Z}$ such that $a - f = 6s$ and $f - b = 9t$. Calculate

$$\begin{aligned} a - b = (a - f) + (f - b) &= 6s + 9t \\ &= 3(2s + 3t) \end{aligned}$$

and since $2s + 3t$ is an integer by the definition of divides we can conclude that $3|(a - b)$, and thus $(a, b) \in \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 3|(a - b)\}$ as desired. ■

□

Definition 7.2.7 Identity Relation. For any set A, the identity relation on A is the set $I_A = \{(a, a)|a \in A\}$ ◊

Proposition 7.2.8 *Let A, B, C and D be sets. Let R be a relation from A to B, S a relation from B to C, and T be a relation from C to D*

(a) $\left(R^{-1}\right)^{-1} = R$

(b) $T \circ (S \circ R) = (T \circ S) \circ R$ *(composition is associative)*

(c) $I_B \circ R = R$ *and* $R \circ I_A = R$

(d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Proof of Proposition 7.2.8. We will prove part (b) and leave the rest as exercises for the reader.
Suppose that $A, B, C,$ and D are sets. Let R be a relation from A to B, S be a relation from B to C, and T be a relation from C to D.
Since we are proving an equality, we will have to prove both subsets.
Proof of $\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R}) \subseteq (\mathbf{T} \circ \mathbf{S}) \circ \mathbf{R}$
Let $a \in T \circ (S \circ R)$, by definition of composition, $T \circ (S \circ R)$ is a relation from A to D, hence by the definition of relation we can find an $x \in A$ and a $y \in B$ such that $a = (x, y)$. Now, as well by definition of composition, $S \circ R$ is a relation from A to C, and since T is a relation from C to D, we can find a $z \in C$ such that $(z, y) \in T$ and $(x, z) \in (S \circ R)$. Again, by the definition of composition, since S is a relation from B to C and R is a relation from A to B we can find $w \in B$ such that $(x, w) \in R$ and $(w, z) \in S$.
Since $(z, y) \in T$, and $(w, z) \in S$ then by definition of composite we have that $(w, y) \in (T \circ S)$. And since $(x, w) \in R$ and $(w, y) \in (T \circ S)$ then by definition of composite we can conclude that $(x, y) \in (T \circ S) \circ R$.
Proof of $\mathbf{T} \circ (\mathbf{S} \circ \mathbf{R}) \supseteq (\mathbf{T} \circ \mathbf{S}) \circ \mathbf{R}$
For this part, we choose an arbitrary element $b \in (T \circ S) \circ R$. Again, by definition of composition $T \circ S$ is a relation from B to D and since R is a relation from A to B, hence $(T \circ S) \circ R$ is a relation from A to D, hence we can find a $s \in A$ and a $t \in D$ such that $b = (s, t)$. As well, by the definition of composite we can find $u \in B$ such that $(s, u) \in R$ and $(u, t) \in T \circ S$. Yet, by definition if composite since T is a relation from C to D and S is a relation from B to C we can find $i \in C$ such that $(u, i) \in S$ and $(i, t) \in T$. Thus, because $(s, u) \in R$ and $(u, i) \in S$ by definition of composite $(s, i) \in S \circ R$. In a similar

fashion as we also have $(i,t) \in T$ we can conclude that $(s,t) \in T \circ (S \circ R)$ as desired.
Since we have shown that both $T \circ (S \circ R) \subseteq (T \circ S) \circ R$ and $T \circ (S \circ R) \supseteq (T \circ S) \circ R$ we can conclude that $T \circ (S \circ R) = (T \circ S) \circ R$. ■

7.3 Equivalence Relations

Equivalence relations show up a lot in your future math courses especially in algebra and number theory. Yet, before we dive into an equivalence relation lets look at the three properties which make it up. First up is the reflexive property.

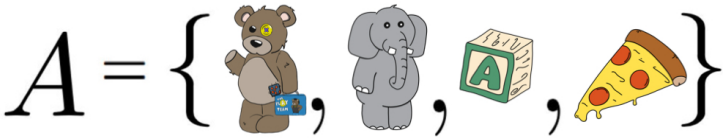
Definition 7.3.1 Reflexive. We say that a relation R on a set A is **reflexive** on A whenever

$$\forall x \in A,\ xRx$$

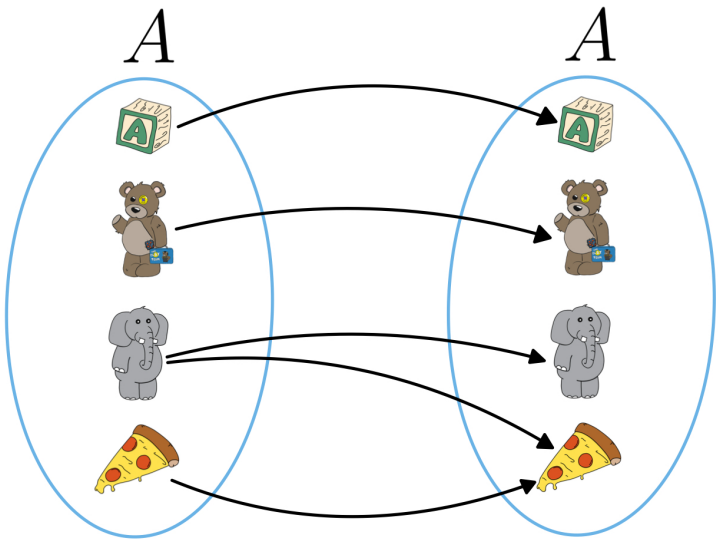
◊

For our first example in this section we will return to our cartoons.

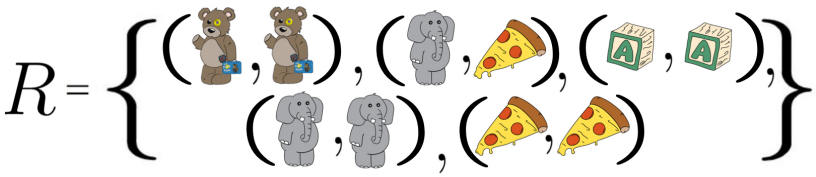
Example 7.3.2 Consider the following set A



and consider the relation R on A defined as



or as a set



notice that for every element of A it is in an ordered pair with itself, and hence R is reflexive. □

Let see a couple of examples of proof involving reflexive.

Example 7.3.3 Consider the relation S on $\mathbb{Z}$ defined as

$$S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 3|(a + 2b)\}$$

Prove: S is reflexive

Proof. To prove this we let $a \in \mathbb{Z}$, to show a is included in an order pair with membership to S amounts to proving an existential.
That is we will need to produce an integer to create an ordered pair with a. Well, that integer is a.
To see this simply note that

$$a + 2a = 3 \cdot (a)$$

and since a is an integer by definition of divides 3 divides $a + 2a$, and hence $(a, a) \in S$.
Since we have chosen a arbitrary we can conclude that S is reflexive as desired. ■
□

Example 7.3.4 Let A be a set, and let R be a relation on A.
Prove: if R is reflexive then $\text{Dom}(R) = A$

Proof. Assume R is reflexive on A. As usual to show equality of sets (don't forget relations are sets!) we will need to break our proof into two parts.
Proof of $\text{Dom}(\mathbf{R}) \subseteq \mathbf{A}$
As usual, let $a \in \text{Dom}(R)$, hence by definition we can find a $b \in A$ such that $(a, b) \in R$, since R is a relation on A we have that $a \in A$.
Proof of $\text{Dom}(\mathbf{R}) \supseteq \mathbf{A}$
This time, let $x \in A$, since we have assumed R is reflexive, by definition $(x, x) \in R$ and hence by definition of domain $x \in \text{Dom}(R)$.
Since we have shown both $\text{Dom}(R) \supseteq A$ and $\text{Dom}(R) \subseteq A$ we have that $\text{Dom}(R) = A$ as desired. ■
□

The next property that defines an equivalence relation is symmetric.

Definition 7.3.5 Symmetric. We say that a relation R on a set A is **symmetric** on A whenever

$$\forall x, y \in A, \text{ if } xRy \text{ then } yRx$$

◊

Example 7.3.6 Consider the set

$$B = \{1, 2, 3, 4, 5, 6\}$$

and the relation T on B defined as

$$T = \{(1, 2), (1, 5), (6, 5), (2, 1), (5, 1), (5, 6)\}$$

This relation is symmetric to see this unlike with reflexive we need not check every element of B we instead check every element of T

$$\text{Since } (1, 2) \in T \text{ we need (and have) } (2, 1) \in T$$
$$\text{Since } (1, 5) \in T \text{ we need (and have) } (5, 1) \in T$$
$$\text{Since } (6, 5) \in T \text{ we need (and have) } (5, 6) \in T$$

now we have exhausted all the elements of T and thus T is indeed symmetric.
□

Lets explore an example of a proof involving the symmetric property next.

Example 7.3.7 Consider the relation R on $\mathbb{Z}$ defined as

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 3|(a + b)\}$$

Prove: R is symmetric

Proof. To prove that R is symmetric we must choose an arbitrary $(a, b) \in R$. By definition of R $3|(a + b)$, by definition of divides we can find an integer k such that $a + b = 3k$ yet since $a + b = b + a$ we have that $b + a = 3k$ and hence $3|(b + a)$ and thus $(b, a) \in R$. Hence R is symmetric. ■

□

Example 7.3.8 ***Prove:*** If S is a symmetric relation on A, and $R \subseteq S$, then $R^{-1} \subseteq S$

Proof. Let R be a relation on the set A. Assume S is a symmetric relation on A and $R \subseteq S$. Let $x \in R^{-1}$. Thus by definition of relation, and definition of inverse, we can find $(p, j) \in A$ such that $x = (p, j)$. Thus, by definition of inverse, $(j, p) \in R$. Thus by our assumption and the definition of subset, $(j, p) \in S$. And, since S is symmetric, $(p, j) \in S$. Since $(p, j) = x$, $x \in S$
Since $x \in R^{-1}$ and $x \in S$, by definition of subset, $R^{-1} \subseteq S$ ■

□

The final property which makes an equivalence relation is transitive.

Definition 7.3.9 Transitive. We say that a relation R on a set A is **transitive** on A whenever

$$\forall x, y, z \in A, \text{ if } xRy \text{ and } yRz, \text{ then } xRz$$

◊

Example 7.3.10 Consider the relation T on $\mathbb{Z}$ defined as

$$T = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 6|(a - b)\}$$

Prove: T is transitive on $\mathbb{Z}$

Proof. To prove that T is transitive we must choose two elements $(a, b) \in T$ and $(b, c) \in T$.
By definition of T both $6|(a-b)$ and $6|(b-c)$. Hence by the definition of divides we can find $s \in \mathbb{Z}$ and $t \in \mathbb{Z}$ such that $a - b = 6s$ and $b - c = 6t$. Calculate:

$$\begin{aligned} a - c = (a - b) + (b - c) &= 6s + 6t \\ &= 6(s + t) \end{aligned}$$

since $s + t$ is an integer we can conclude that $6|(a - c)$ and hence $(a, c) \in T$.
Therefore by the definition of transitive T is transitive. ■

□

Example 7.3.11 ***Prove:*** R is transitive if and only if $R \circ R \subseteq R$

Proof. Let R be a relation on a non-empty set A
Proof of $\mathbf{R}$ is transitive $\implies \mathbf{R} \circ \mathbf{R} \subseteq \mathbf{R}$
Assume R is transitive. Let $(x, y) \in R \circ R$. By definition of composition, we can find $z \in A$ such that $(x, z) \in R$ and $(z, y) \in R$. Since R is transitive, $(x, y) \in R$.
Since $(x, y) \in R \circ R$ and $(x, y) \in R$, by definition of subset, $R \circ R \subset R$.
Proof of $\mathbf{R}$ is transitive $\impliedby \mathbf{R} \circ \mathbf{R} \subseteq \mathbf{R}$
Assume $R \circ R \subseteq R$. Let $(x, y) \in R$ and $(y, z) \in R$. Since $(x, y) \in R$ and $(y, z) \in R$, by definition of composition, $(x, z) \in R \circ R$. Hence by our assumption that $R \circ R \subseteq R$, and definition of subset, $(x, z) \in R$.
Thus, by definition of transitive, R is transitive. ■

□

Proposition 7.3.12 *Let A be a non-empty set. For the power set $\mathscr{P}(A)$, the relation "is a subset of" is reflexive on $\mathscr{P}(A)$, and transitive, but not symmetric.*

Proof of Proposition 7.3.12. ***[Reflexive]***
Let $X \in \mathscr{P}(A)$. (Need To Show: $X \subset X$) Assume $a \in X$. Hence, $a \in X$, thus by definition of subset, $X \subset X$ and hence "subset of" is reflexive.
[Transitive]
Let $X, Y, Z \in \mathscr{P}(A)$ such that $X \subset Y$ and $Y \subset Z$. Let $a \in X$. Thus by definition of subset, since $X \subset Y$, $a \in Y$. Since $Y \subset Z$, and $a \in Y$, $a \in Z$ Thus, by definition of subset, since $a \in X$ and $a \in Z$, $x \subset Z$. Hence "subset of" is transitive.
[NOT Symmetric]
notice $\emptyset \subset A$ but $A \not\subset \emptyset$ as we assumed that A was not empty hence "subset of" is not symmetric. ■

Now we have collected all of the properties which make an equivalence relation, the definition is almost self evident.

Definition 7.3.13 Equivalence Relation. A relation R on a set A is an **equivalence relation** on A if R is reflexive, symmetric, and transitive on A.
◊

Example 7.3.14 Consider the relation E on $\mathbb{Z}$ defined as

$$E = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 5|(a - b)\}$$

Prove: E is an equivalence relation

Proof. The definition of equivalence relation has three properties:

- reflexive
- symmetric
- transitive

thus a proof that a relation is an equivalence relation should be split into three parts.

Proof of Reflexive:

To see that E is reflexive we start with an arbitrary element $a \in \mathbb{Z}$. Now for this relation we can calculate:

$$\begin{aligned} a - a &= 0 \\ &= 5 \cdot 0 \end{aligned}$$

since 0 is an integer $a - a$ is thus divisible by 5, and hence $(a, a) \in E$ as desired. Therefore E is reflexive.

Proof of Symmetric:

To show that E is symmetric we begin by choosing a pair $(b, c) \in \mathbb{Z} \times \mathbb{Z}$ such that $(b, c) \in E$. By the definition of E $5|(b - c)$ thus by definition of divides we can find an integer k so that $b - c = 5k$ and hence $c - b = -5k$ and since $-k$ is an integer by definition of divides 5 divides $c - b$ thus $(c, b) \in E$; therefore E is symmetric.

Proof of Transitive:

To prove E is transitive we begin with two arbitrary elements of E, namely $(d, e) \in E$ and $(e, f) \in E$. By definition of E 5 divides both $d - e$ and $e - f$, thus by definition of divides we can find integers r and s such that $d - e = 5r$ and $e - f = 5s$. Now calculate:

$$\begin{aligned} d - f = (d - e) + (e - f) &= 5r + 5s \\ &= 5(r + s) \end{aligned}$$

siince $r + s$ is an integer we have that $d - f$ is divisible by 5 and thus $(d, f) \in E$ and hence E is transitive.

As we have shown that E is reflexive, symmetric and transitive we have have verified that E is an equivalence relation as desired! ■

□

For the next example we will find the following definition and lemma helpful.

Definition 7.3.15 Parity. We say that two integers have the same **parity** when either both are even or both are odd. ◊

Lemma 7.3.16 *For any integers a and b if $a + b$ is divisible by 2 then a and b have the same parity.*

Proof of Lemma 7.3.16. We will approach this proof exhaustive, using Lemma 4.6.1, p. 52 to break us into cases.

Case 1:* a *is even and* b *is even

In this case we assume that we can find integers k and ℓ so that $a = 2k$ and $b = 2\ell$. Calculate

$$\begin{aligned} a + b &= 2k + 2\ell \\ &= 2(k + \ell) \end{aligned}$$

since $k + \ell$ is an integer we have that $a + b$ is even, hence when a and b are

both even that $a + b$ is even.
Case 2:* a *is odd and* b *is even
In this case we assume that we can find integers s and t so that $a = 2s + 1$ and $b = 2t$. Calculate

$$\begin{aligned} a + b &= (2s + 1) + 2t \\ &= 2(s + t) + 1 \end{aligned}$$

since $s + t$ is an integer we have that $a + b$ is odd. Hence when a is odd and b is even then $a + b$ is odd.
Case 3:* a *is even and* b *is odd
In this case we assume we can find integers r and v so that $a = 2r$ and $b = 2v+1$. Calculate

$$\begin{aligned} a + b &= 2r + (2v + 1) \\ &= 2(r + v) + 1 \end{aligned}$$

since $r + v$ is an integer we have that $a + b$ is odd. Hence with a is even and b is odd $a + b$ is odd
Case 1:* a *is odd and* b *is odd
In this final case we assume we can find integers n and m so that $a = 2n + 1$ and $b = 2m + 1$. Calculate

$$\begin{aligned} a + b &= (2n + 1) + (2m + 1) \\ &= 2n + 2m + 1 + 1 = 2n + 2m + 2 \\ &= 2(n + m + 1) \end{aligned}$$

since $n + m + 1$ is an integer we conclude that $a + b$ is even. Therefore when a is odd and b is odd we have that $a + b$ is even.
Therefore we see that the only time that $a + b$ is even is exactly when a and b have the same parity. ■

Example 7.3.17 Consider the relation R on $\mathbb{Z}$ defined as

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 2|(a + b)\}$$

Prove: R is an equivalence relation

Proof. As we are proving that R is an equivalence relation we should split it into three parts.

Proof of Reflexive:

To show reflexive we start with an arbitrary element $a \in \mathbb{Z}$, then calculate

$$a + a = 2a$$

and since a is an integer we have that $a + a$ divisible by 2 and hence $(a, a) \in R$ and thus R is reflexive.

Proof of Symmetric:

To prove that R is symmetric choose an arbitrary element $(x, y) \in R$, thus by definition of R we have that $2|(x + y)$ hence we can find an integer k such that $x + y = 2k$, yet note that $y + x = x + y = 2k$ hence $y + x$ is divisible by 2 and therefore $(y, x) \in R$ and hence R is symmetric.

Proof of Transitive:

To prove transitive we choose elements of R, namely $(b, c) \in R$ and $(c, d) \in R$. By definition of membership to R we have that $2|(b + c)$ and $2|(c + d)$, that is that both $b + c$ and $c + d$ are even.

By Lemma 7.3.16, p. 136 and Lemma 4.6.1, p. 52 we can break the rest of our proof in to a couple of cases.

Case 1:* c *is even

Assume that c is even, by Lemma 7.3.16, p. 136 since we have that both $b + c$ is even and $c + d$ is even we can conclude that both c and d are even. Hence by the definition of even we can find integers n and m such that $c = 2n$ and $d = 2m$. Calculate

$$\begin{aligned} b + d &= 2n + 2m \\ &= 2(n + m) \end{aligned}$$

since $n + m$ is an integer we have that $2|(b + d)$ thus $(b, d) \in R$ as desired.

Case 1:* c *is odd

Assume that c is odd, by Lemma 7.3.16, p. 136 then both b and d are odd as we have that both $b + c$ and $c + d$ are even. By definition of even we can find two integers s and t such that $b = 2s + 1$ and $d = 2t + 1$. Calculate

$$\begin{aligned} b + d &= (2s + 1) + (2t + 1) \\ &= 2s + 2t + 2 \\ &= 2(s + t + 1) \end{aligned}$$

since $s + t + 1$ is an integer we have that $2|(b + d)$ and thus $(b, d) \in R$ as desired. Hence in both cases we have that R is transitive.

As we have shown that R is reflexive, symmetric and transitive we have have verified that R is an equivalence relation as desired! ■

□

Example 7.3.18 Let A be a set and let both R and S be relations on A.

Prove: if R and S are equivalence relations then $R \cap S$ is an equivalence relation.

Proof. Let A be a set and let both R and S be relations on A and assume both R and S are equivalence relations. To prove that $R \cap S$ is an equivalence relation we should break it down into the three conditions.
Proof of Reflexive:
To prove reflexive, we begin with an arbitrary element $a \in A$. Since R and S are equivalence relations they are in particular reflexive we have that $(a, a) \in R$ and $(a, a) \in S$, hence by definition of intersection $(a, a) \in R \cap S$ thus $R \cap S$ is reflexive.
Proof of Symmetric:
To prove symmetric, we choose an element $(x, y) \in R \cap S$. By definition of intersection both $(x, y) \in R$ and $(x, y) \in S$. Since both R and S are equivalence relations in particular they are both symmetric and hence $(y, x) \in R$ and $(y, x) \in S$, thus by the definition of intersection $(y, x) \in R \cap S$. Therefore $R \cap S$ is symmetric.
Proof of Transitive:
To prove transitive we start with elements $(r, s) \in R \cap S$ and $(s, t) \in R \cap S$, by definition of intersection we have that $(r, s) \in R$, $(r, s) \in S$, $(s, t) \in R$ and $(s, t) \in S$. Since both R and S are equivalence relations, in particular they are transitive we have that $(r, t) \in R$ and $(r, t) \in S$, hence by definition of intersection $(r, t) \in R \cap S$. Therefore $R \cap S$ is transitive.
Hence since we have shown that $R \cap S$ is reflexive, symmetric, and transitive we have that $R \cap S$ is an equivalence relation. ■

□

An equivalence relation has a natural subdivision on the set it is on.

Definition 7.3.19 Equivalence Class. Let R be an equivalence relation on a set A. For $x \in A$ the **equivalence class** of x modulo R is the set

$$\bar{x} := \{y \in A \mid xRy\}$$

Each element of $\bar{x}$ is called a **representative** of this class. ◊

Definition 7.3.20 Modulo. The set

$$A/R = \{\bar{x} \mid x \in A\}$$

of all equivalence classes is called A **modulo** R (A mod R) ◊

Example 7.3.21 Consider the set

$$A = \{0, 1, 2, 3, 4\}$$

and define the relation R on A as follows

$$R = \{(a, b) \in A \times A \mid 3|(a + 2b)\}$$

We claim that this is an equivalence relation of A, yet since we just have a finite set lets just go through and find all the relations, namely

$$R = \{(0, 0), (1, 1), (2, 2), (3, 3), (4, 4), (0, 3), (3, 0), (1, 4), (4, 1)\}$$

We can then go through and check that all the properties of an equivalence relation, notice for example that the following are all members of R (0,0), (1,1), (2,2), (3,3), (4,4) and hence R is reflexive.

To continue note the following are all members of R

$$(0, 0) \text{ and } (0, 0)$$
$$(1, 1) \text{ and } (1, 1)$$

$$(2,2) \text{ and } (2,2)$$
$$(3,3) \text{ and } (3,3)$$
$$(4,4) \text{ and } (4,4)$$
$$(0,3) \text{ and } (3,0)$$
$$(1,4) \text{ and } (4,1)$$

and hence R is symmetric. For transitive we check them all again that all of the following are members of R

$$(0,0),\ (0,3) \text{ and } (0,3)$$
$$(0,3),\ (3,0) \text{ and } (0,0)$$
$$(3,3),\ (3,0) \text{ and } (3,0)$$
$$(0,3),\ (3,3) \text{ and } (0,3)$$
$$(1,1),\ (1,4) \text{ and } (1,4)$$
$$(4,1),\ (1,1) \text{ and } (4,1)$$
$$(4,4),\ (4,1) \text{ and } (4,1)$$
$$(4,1),\ (1,1) \text{ and } (4,1)$$
$$(1,4),\ (4,4) \text{ and } (1,4)$$

Now note the following equivalence classes:

$$\bar{0} = \bar{3} = \{0,3\}$$
$$\bar{1} = \bar{4} = \{1,4\}$$
$$\bar{2} = \{2\}$$

□

Proposition 7.3.22 *Let R be an equivalence relation on a nonempty set A. For all x and y in A,*

a.) $x \in \bar{x}$ and $\bar{x} \subseteq A$

b.) xRy if and only if $\bar{x} = \bar{y}$

c.) x is not related to y if and only if $\bar{x} \cap \bar{y} = \emptyset$

Proof of Proposition 7.3.22. We prove part (a) and part (b), leaving part (c) as an exercise.
Proof of part (a)
Proof of $\mathbf{x \in x}$
Let $x \in A$, since R is an equivalence relation, in particular it is reflexive, thus xRx, hence by definition of $\bar{x}$, $x \in \bar{x}$
Proof of $\mathbf{x \subseteq A}$
Let $\ell \in \bar{x}$. Thus by definition of $\bar{x}$, $xR\ell$. Hence, $(x,l) \in R$. Since R is a relation on A, $R \subseteq A \times A$. Hence by definition of cross product, $\ell \in A$.
Proof of (b) xRy if and only if $\bar{x} = \bar{y}$
Let R be a relation on a non-empty set A
Proof of $\mathbf{xRy \implies x = y}$
Let $(x,y) \in R$, as our objective is to prove equality of sets we should break it into two parts.
Proof of $\mathbf{x \subseteq y}$
Let $a \in \bar{x}$. Thus by definition of equivalence class xRa. Since R is an equivalence relation, it is symmetric, and as we assumed $(x,y) \in R$, we can thus

conclude $(y, x) \in R$. Since R is an equivalence relation, it is also transitive. And since we already concluded $(y, x) \in R$ and $(x, a) \in R$ we can now conclude $(y, a) \in R$.
Thus by definition of equivalence class, $a \in \bar{y}$. Thus by definition of subset, $\bar{x} \subseteq \bar{y}$.
Proof of $\mathbf{x \supseteq y}$
let $a \in \bar{y}$. Thus by definition of equivalence class yRa. Since R is an equivalence relation, it is transitive. And since we already concluded $(x, y) \in R$ and $(y, a) \in R$, we can now conclude $(x, a) \in R$.
Thus by definition of equivalence class, $a \in \bar{y}$. Thus by definition of subset, $\bar{x} = \bar{y}$
Proof of $\mathbf{xRy \iff x = y}$
Let $x \in A$ and $y \in A$ such that $\bar{x} = \bar{y}$. Since R is an equivalence relation, it is reflexive. Hence, xRx. Thus by definition of $\bar{x}$, $x \in \bar{x}$. Since we assumed $\bar{x} = \bar{y}$, in particular $\bar{x} \subseteq \bar{y}$, $x \in \bar{y}$. By definition of $\bar{y}$, yRx. Since R is an equivalence relation, it is symmetric. Since we concluded $(y, x) \in R$, we can conclude $(x, y) \in R$ ■

7.4 Partitions

When I say partition you already have a sense of the word, like wall or a fence, it brings to mind separate areas or groups. We make this concept inside of a set more formal in our following definition.

Definition 7.4.1 Partition. Let A be a non-empty set. $\mathscr{P}$ is a **partition** of A if $\mathscr{P}$ is a set of subsets of A such that:

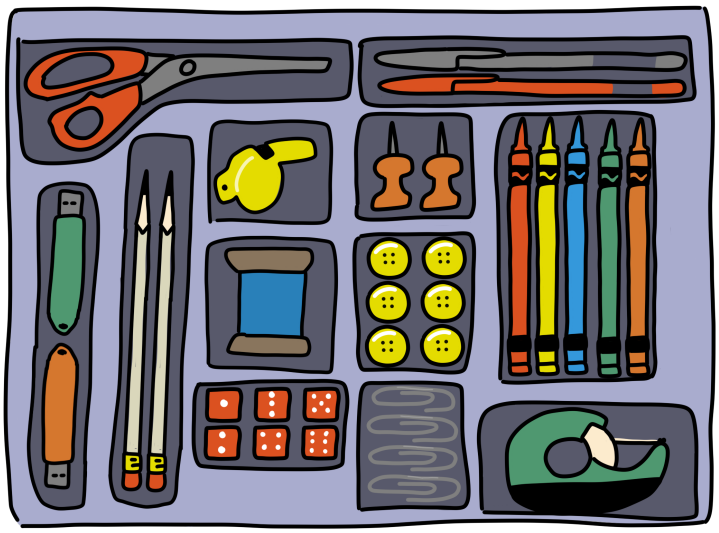
(i) If $X \in \mathscr{P}$, then $X \neq \emptyset$

(ii) If $X \in \mathscr{P}$ and $Y \in \mathscr{P}$, then $X = Y$ or $X \cap Y = \emptyset$

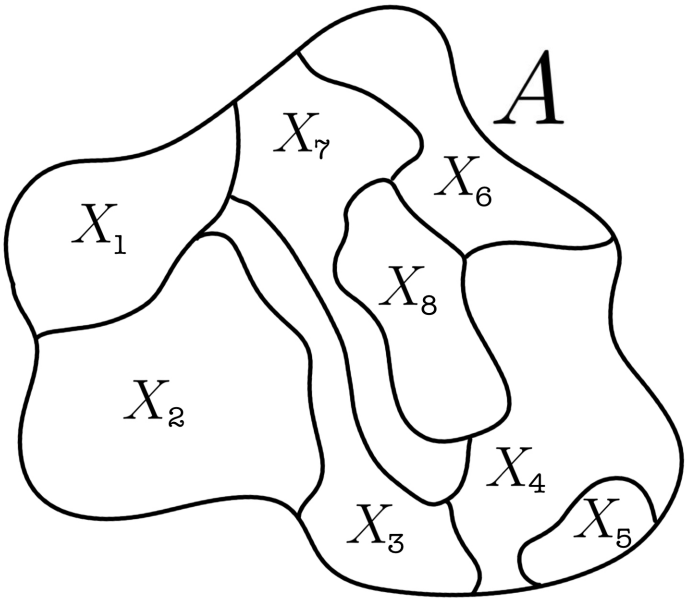
(iii) $\bigcup_{X \in \mathscr{P}} X = A$

◊

This is quite rigorous of a definition but do not loose that this is simply separating things into separate non-overlapping groups somewhat like a drawer organizer.



Sets at their heart have no defining characteristics, so we often draw them as blobs with no discernible shape so as we do not accidentally divine some pattern that does not exist. We then visualize a partition as a sectioning off of this amorphous blob as in the following figure, where we have an arbitrary set A and a family of subsets $\mathscr{X} = \{X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8\}$ which partition A.



Example 7.4.2 Consider the set T containing the following elements

$T =$ 

and consider the family of subsets $\mathscr{S} = \{S_1, S_2, S_3, S_4\}$, where each set is defined as follows

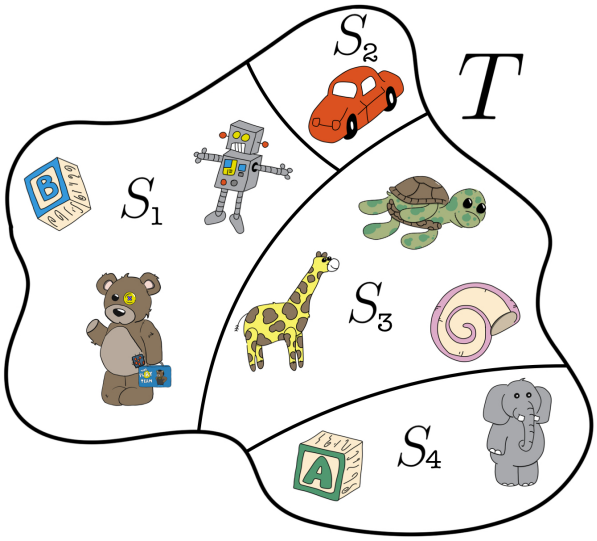
$$S_1 = \{\text{  }, \text{  }, \text{  }\}$$

$$S_2 = \{\text{  }\}$$

$$S_3 = \{\text{  }, \text{  }, \text{  }\}$$

$$S_4 = \{\text{  }, \text{  }\}$$

Notice that all of the subsets are non-empty (condition (i))any two sets that are not the same share no toys (condition (ii)), and that they indeed include all of the toys (condition (iii))



□

Example 7.4.3 Consider the family of set $\mathscr{A} = \{A_n \mid n \in \mathbb{N}\}$ where each set is defined as follows for any $n \in \mathbb{N}$

$$A_n = \{a \in \mathbb{Z} \mid 3|(a - n)\}$$

Prove: $\mathscr{A}$ is a partition of $\mathbb{Z}$.

Proof. There are three conditions to being a partition, so we will split our proof into three parts:
Condition (i)
Let $n \in \mathbb{N}$, notice that $(n-n) = 0 = 3 \cdot 0$ and since 0 is an integer we can conclude that 3 divides $n-n$ and hence $n \in A_n$.
Therefore for any $n \in \mathbb{N}$ we have that $A_n \neq \emptyset$, thus proving that $\mathscr{A}$ satisfies condition (i) of a partition.
Condition (ii)
Let r and s be arbitrary natural numbers, assume that $A_r \cap A_s \neq \emptyset$, and hence we can find at least one mutual element of A_r and A_s, name one of these elements $y \in A_r \cap A_s$. By definition of A_r and A_s we have that both $3|(r-y)$ and $3|(s-y)$. By definition of divides we can find two integers k and m so that $r-y = 3k$ and $s-y = 3m$, hence we can calculate

$$r - s = (r-y) - (s-y) = 3k - 3m = 3(k-m)$$

For a similar calculation,

$$s - r = (s-y) - (r-y) = 3m - 3k = 3(m-k)$$

(If perhaps you have felt lost in this proof so far, we are using the *concluding an or* technique from Section 3.28, p. 44) It is our desire to show equality of these two sets, as usual, breaking our proof in to two more parts
Proof of $\mathbf{A_r \subseteq A_s}$
let $x \in A_r$ by definition of A_r this means that $3|(r-x)$ thus by definition of divides we can find a $w \in \mathbb{Z}$ such that $r - a = 3w$, thus calculate

$$s - x = (r-x) - (r-s) = 3w - 3(k-m) = 3(w-k+m)$$

and since $w-k+m$ is an integer we can conclude that 3 divides $s-x$ hence we have that $x \in A_s$ as desired.
Proof of $\mathbf{A_r \supseteq A_s}$
let $z \in A_s$ by definition of A_s this means that $3|(s-z)$, by definition of divides we can find an integer t so that $s - z = 3t$. Now calculate

$$r - z = (s-z) - (s-r) = 3t - 3(m-k) = 3(t-m+k)$$

since $t-m+k$ is an integer we have that 3 divides $r-z$ and hence $z \in A_r$ as desired.
since we have shown both $A_r \subseteq A_s$ and we have shown $A_r \supseteq A_s$ we can conclude that $A_r = A_s$. Furthermore, this proves that $\mathscr{A}$ satisfies condition (ii) of being a partition.
Condition (iii)
For this last condition we again should show to containments of sets
Proof of $\bigcup_{\mathbf{n}\in\mathbb{N}} \mathbf{A_n} \subseteq \mathbb{Z}$
For this part let $p \in \bigcup_{n\in\mathbb{N}} A_n$, by definition of union over a family, we can find a $b \in \mathbb{N}$ such that $p \in A_b$, yet by definition of A_b we have that $p \in \mathbb{Z}$ as desired. (most texts would call this the obvious direction)
Proof of $\bigcup_{\mathbf{n}\in\mathbb{N}} \mathbf{A_n} \supseteq \mathbb{Z}$
Now, let $q \in \mathbb{Z}$, Calculate $q - q = 0 = 3 \cdot 0$ and since 0 is an integer we have that 3 divides $q-q$, hence $q \in A_q$ therefore $q \in \bigcup_{n\in\mathbb{N}} A_n$ as desired.
Since we have shown both $\bigcup_{n\in\mathbb{N}} A_n \subseteq \mathbb{Z}$ and $\bigcup_{n\in\mathbb{N}} A_n \supseteq \mathbb{Z}$ we can conclude $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{Z}$, thus $\mathscr{A}$ satisfies condition (iii) of being a partition.
Since we have shown the three conditions of being a partition we can conclude that $\mathscr{A}$ is a partition. ■

□

It turns out that this last example is actually a quite apt example of partitions. Partitions turn out not to be something new, they are actually just equivalence relations. We make this comment more precise in the following two propositions.

Proposition 7.4.4 *If R is an equivalence relation on a non-empty set A then A/R is a partition of A.*

Proof of Proposition 7.4.4. Let R be an equivalence relation on a non-empty set A.
There are three conditions to being a partition, so we will split our proof into three parts
Condition (i)
Let $x \in A$, then since R is an equivalence relation, in particular R is reflexive, thus we have xRx thus $x \in \bar{x}$ and hence $\bar{x} \neq \emptyset$, thus A/R satisfies condition (i) of being a partition.
Condition (ii)
let $a \in A$ and $b \in A$, and assume that $\bar{a} \cap \bar{b} \neq \emptyset$, then by Proposition 7.3.22, p. 140 (b) we can conclude that $\bar{a} = \bar{b}$, and hence A/R satisfies condition (ii) of being a partition.
Condition (iii)
We will split this condition into two parts
Proof of $\bigcup_{\mathbf{y \in A}} \mathbf{y} \subseteq \mathbf{A}$
Let $s \in \bigcup_{y \in A} \bar{y}$, hence we can find a $t \in A$ such that $s \in \bar{t}$, by Proposition 7.3.22, p. 140 (a) we have that $\bar{t} \subseteq A$ and hence $s \in A$ as desired.
Proof of $\bigcup_{\mathbf{y \in A}} \mathbf{y} \supseteq \mathbf{A}$
Let $c \in A$, then since R is an equivalence relation, in particular it is reflexive, thus cRc and hence $c \in \bar{c}$ therefore $c \in \bigcup_{y \in A} \bar{y}$ as desired.
Since we have shown that both $\bigcup_{y \in A} \bar{y} \subseteq A$ and $\bigcup_{y \in A} \bar{y} \supseteq A$ we can conclude that $\bigcup_{y \in A} \bar{y} = A$, therefore we have shown that A/R satisfies condition(iii) of being a partition.
Since we have shown the three conditions of being a partition we can conclude that $\mathscr{A}$ is a partition. ■

Proposition 7.4.5 *Let $\mathscr{P}$ be a partition of a nonempty set A. For x and $y \in A$ define xQy if and only if there exists $C \in \mathscr{P}$ such that $x \in C$ and $y \in C$. Then Q is an equivalence relation on A.*

Proof of Proposition 7.4.5. We will prove the three conditions for Q to be an equivalence relation.
[Reflexive]
let $x \in A$. Since $\mathscr{P}$ is a partition, $\bigcup_{X \in \mathscr{P}} X = A$ we have that $x \in \bigcup_{X \in \mathscr{P}} X$. Hence we can find a $C \in \mathscr{P}$ such that $x \in C$. Hence, $(x, x) \in Q$, since $x \in C$ and $x \in C$.
[Symmetric]
Let $(x, y) \in Q$. By definition of Q we can find $D \in \mathscr{P}$ such that $x \in D$ and $y \in D$. Hence, $y \in D$ and $x \in D$. Thus by definition of Q, $(y, x) \in Q$.
[Transitive]

Let $(x, y) \in Q$ and $(y, z) \in Q$. By definition of Q we can find $C_1, C_2 \in \mathscr{P}$ such that $x \in C_1$ and $y \in C_1$, and $y \in C_2$ and $z \in C_2$. Hence, $y \in C_1 \cap C_2$. Hence $C_1 \cap C_2 \neq \emptyset$. Hence by definition of partition, $C_1 = C_2$. Hence $x \in C$ and $z \in C$. Hence by definition of $Q, (x, z) \in Q$.
Since Q satisfies the three conditions of being an equivalence relation it is an equivalence relation as desired. ■

7.5 Functions

Functions are important no matter the field you go into, and you have had a lot of experience with functions up to this point. Let's now formalize the definition of function as a specific type of relation.

Definition 7.5.1 Function. A **function**, or **mapping**, from A to B is a relation f from A to B such that:

(i) The domain of f is A.

(ii) If $(x, y) \in f$ and $(x, z) \in f$ then $y = z$

For a function f we write

$$f : A \to B$$

We *say*

$$"f \text{ is a function from } A \text{ to } B"$$

or

$$"f \text{ maps } A \text{ to } B"$$

The set B is called the **codomain** of f.
In the case where $B = A$, we say that

$$f \text{ is a function on } A"$$

When $(x, y) \in f$, we write $y = f(x)$. ◊

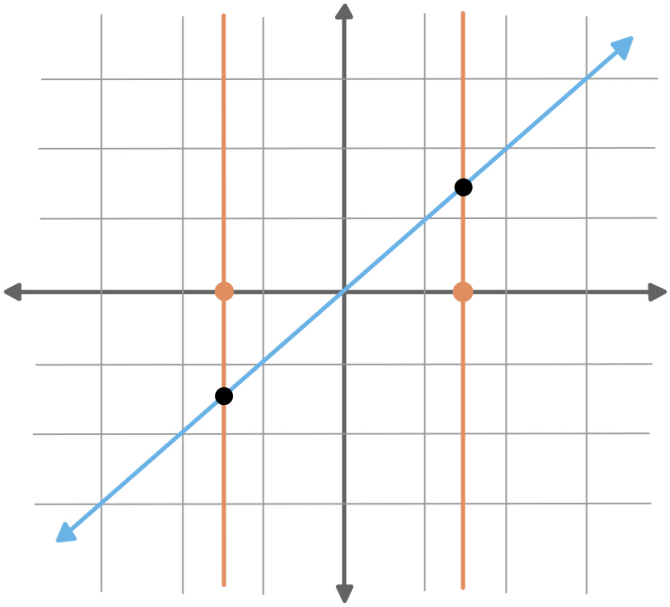
At first glance condition (ii) may look foreign to you, yet in your calculus and college algebra classes you probably just called this the vertical line test, seen in this next example.

Example 7.5.2 We saw that *equals* was a relation at the beginning of this chapter in Example 7.1.3, p. 125, indeed it is also a function. To use it in the our new context of functions, define the function

$$f : \mathbb{R} \to \mathbb{R}$$

as

$$f(x) = x$$



Notice that where we choose to draw a vertical line is the choice of an element of the domain of f, i.e. an element of $\mathbb{R}$, and the condition that the vertical line only hits the graph once is the condition the f(x) has only one output, as is condition (ii) of being a function. □

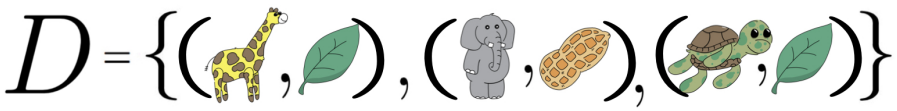
Example 7.5.3 Notice that the *eats* relation from Example 7.1.4, p. 126 is not a function as both

and

So lets consider a slightly different relation, by putting the turtle on a diet,

$$D : Z \to F$$

defined as the following



Now it makes sense to use the *of* notation of functions because for example there is only one way to write the following:

□

Example 7.5.4 Consider the relation f from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$ defined as

$$f = \{((a, b), c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \mid c = 3a + 2b\}$$

Prove: f is a function

Proof. To prove that f is a function we need to show the two conditions of being a function.
Condition (i)
The first condition is an equality of sets, per usual we will split this into two parts
Proof of Dom(**f**) $\subseteq \mathbb{Z} \times \mathbb{Z}$
Let $(a, b) \in \text{Dom}(f)$ by definition of f we have that $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ as desired. (the room chants *obviously!*)
Proof of Dom(**f**) $\supseteq \mathbb{Z} \times \mathbb{Z}$
Let $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, then $((x, y), 3x + 2y) \in f$ by definition of f, as desired.
Since we have shown both $\text{Dom}(f) \subseteq \mathbb{Z} \times \mathbb{Z}$ and $\text{Dom}(f) \supseteq \mathbb{Z} \times \mathbb{Z}$ we can conclude $\text{Dom}(f) = \mathbb{Z} \times \mathbb{Z}$. Therefore we have shown that f satisfies condition (i) of being a function.
Condition (ii)
Assume $((n, m), c) \in f$ and $((n, m), d) \in f$, hence by definition of f we have that $c = 3n + 2m$ and that $m = 3n + 2m$ hence $c = d$ as desired.
Since we have shown both conditions to be a function we can conclude that f is a function. ■
□

The jump from relations to functions can be jarring to students especially with all of the corresponding notations, we take a moment now and attempt to make sense of them.

Functions VS Relations.

Let A and B be sets, and consider a function $f : A \to B$.
At the root a function is just a *relation* and hence $f \subseteq A \times B$
Instead of writing

$$(x, y) \in f$$

or

$$xfy$$

we write

$$f(x) = y,$$

moreover we most often ***don't write*** the y, that is we have

$$x \in A \text{ and } f(x) \in B.$$

To put this context of relations once again (and hopefully not make it too much more convoluted) we have

$$(f, f(x)) \in f$$

and perhaps the most labyrinthine interpretation where f represents the relation f and $f(x)$ is the element of B related to x via f.

$$x \ f \ f(x)$$

The next concepts come up over and over again in algebra, analysis and topology.

Definition 7.5.5 Image. Let $f : A \to B$, and let $X \subseteq A$, The **image** of X (or **image set**) is defined as

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

◊

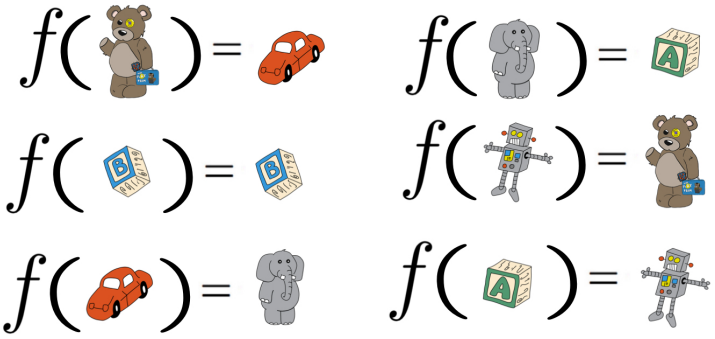
Example 7.5.6 Consider the following set T

$T =$ 

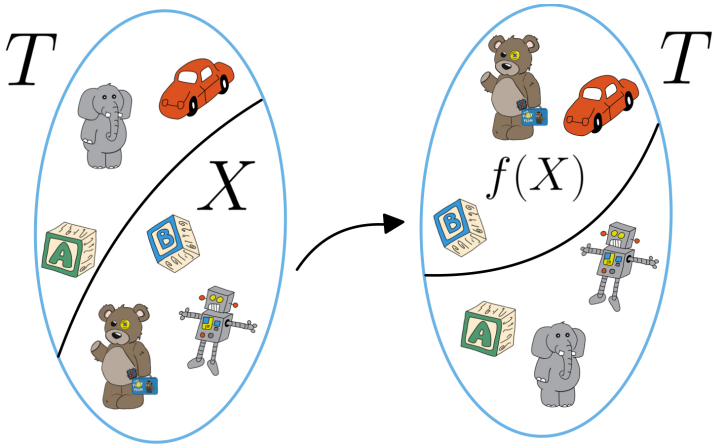
and the subset $X \subseteq T$

$X =$ 

Now define the funciton $f : T \to T$ as follows



Then we can visualize the image of X, $f(X)$, as follows



□

Definition 7.5.7 Inverse Image. Let $f : A \to B$, and let $Y \subseteq B$, The **inverse image** of X (or **inverse image set**) is defined as

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$$

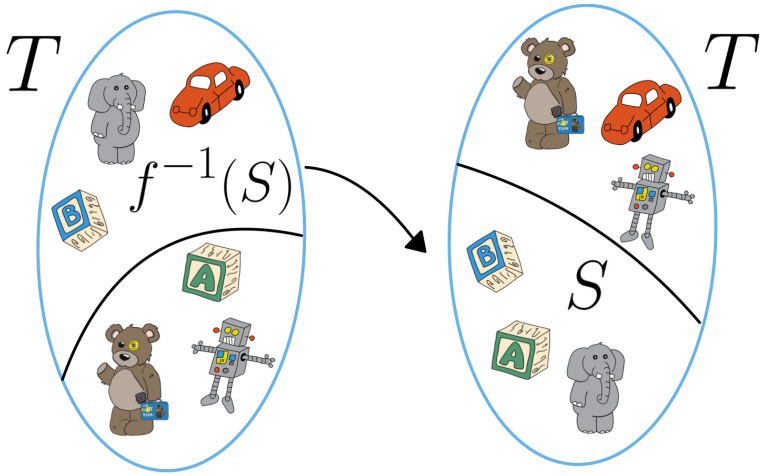
◊

Note 7.5.8 The inverse image should not be confused with the inverse relation.

Example 7.5.9 Consider the same set and function from Example 7.5.6, p. 149. This time define the subset $S \subseteq T$ as

$$S = \{ \text{elephant}, \text{B-block}, \text{A-block} \}$$

We can then visualize the preimage of S, $f^{-1}(S)$, as follows.



□

Proposition 7.5.10 *Let $f : A \to B, C$ and D be subsets of A, and E and F be subsets of B.*

(a) $f(C \cap D) \subseteq f(C) \cap f(D)$

(b) $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$

Proof of Proposition 7.5.10. ***Proof of (a)***
Let $x \in f(C \cap D)$. Thus by definition of image, we can find a $j \in C \cap D$ such that $f(j) = x$. By definition of intersect, $j \in C$ and $j \in D$. Since $j \in C$, by definition of image, $x \in f(C)$ as well. Since $j \in D$, by definition of image, $x \in f(D)$. Thus, by definition of intersection, $x \in f(C) \cap f(D)$.
Proof of (b)
To show equality we should as usual break it into two parts.
Proof of $\mathbf{f^{-1}(E \cap F) \subseteq f^{-1}(E) \cap f^{-1}(F)}$
Let $x \in f^{-1}(E \cap F)$. Thus by definition of inverse image, $f(x) \in E \cap F$. Thus by definition of intersection, $f(x) \in E$ and $f(x) \in F$. By definition of inverse image, $x \in f^{-1}(E)$ and $x \in f^{-1}(F)$. Hence, by definition of intersection, $x \in f^{-1}(E) \cap f^{-1}(F)$.
Proof of $\mathbf{f^{-1}(E \cap F) \supseteq f^{-1}(E) \cap f^{-1}(F)}$
Let $y \in f^{-1}(E) \cap f^{-1}(F)$ hence by definition of intersection $y \in f^{-1}(E)$ and $y \in f^{-1}(F)$. By definition of inverse image we have that both $f(y) \in E$ and $f(y) \in F$ hence by definition of intersection we have that $f(y) \in E \cap F$. Therefore by definition of preimage we have that $y \in f^{-1}(E \cap F)$ as desired.
Since we have shown $f^{-1}(E \cap F) \subseteq f^{-1}(E) \cap f^{-1}(F)$ and $f^{-1}(E \cap F) \supseteq f^{-1}(E) \cap f^{-1}(F)$ we can thus conclude $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$ ■

Let's end this section with a couple more examples of proofs involving these new concepts.

Example 7.5.11 Let $f : A \to B, D \subseteq A$ and $E \subseteq B$
Prove: $f(f^{-1}(E)) \subseteq E$

Proof. Let $x \in f(f^{-1}(E))$. By the definition of image, we can find $y \in f^{-1}(E)$ such that $f(y) = x$. By definition of inverse image, $f(y) \in E$. Thus, since $f(y) = x$ we have that $x \in E$, therefore $f(f^{-1}(E)) \subseteq E$. ■

□

Example 7.5.12 Let $f : A \to B$, and let $X \subseteq A$, $Y \subseteq A$, $U \subseteq B$, and $V \subseteq B$.
Prove: $f^{-1}(U) - f^{-1}(V) = f^{-1}(U - V)$.

Proof. As this is a proof of equality of sets we should break the proof into two pieces.
Proof of $\mathbf{f^{-1}(U) - f^{-1}(V) \subseteq f^{-1}(U - V)}$
Let $x \in f^{-1}(U) - f^{-1}(V)$. By defintion of difference, $x \in f^{-1}(U)$ and $x \notin f^{-1}(V)$. By definition of inverse image, $f(x) \in U$ and $f(x) \notin V$. By definition of difference, $f(x) \in U - V$. Thus, by definition of inverse image, $x \in f^{-1}(U - V)$.
Proof of $\mathbf{f^{-1}(U) - f^{-1}(V) \supseteq f^{-1}(U - V)}$
Let $y \in f^{-1}(U - V)$ by definition of inverse image $f(y) \in U - V$, by definition of difference $f(y) \in U$ and $f(y) \notin V$ hence by definition of inverse image $y \in f^{-1}(U)$ and $y \notin f^{-1}(V)$, thus by definition of difference $y \in f^{-1}(U) - f^{-1}(V)$
Since we have shown both $f^{-1}(U) - f^{-1}(V) \subseteq f^{-1}(U - V)$ and $f^{-1}(U) - f^{-1}(V) \supseteq f^{-1}(U - V)$ we can conclude $f^{-1}(U) - f^{-1}(V) = f^{-1}(U - V)$ ■

□

7.6 Bijections

The concept of something being the same as something else is ubiquitous in mathematics. In this course we have already seen that equals is not as easy as it may of first seemed when dealing with sets. The bijection is how we go about in our combinatorics, algebra, and many other classes to show two objects we are studying are the *same*.

Definition 7.6.1 Surjection. A function $f : A \to B$ is **onto** B, or is a **surjection** means

$$\text{Rng}(f) = B.$$

When f is a surjection, we write

$$f : A \twoheadrightarrow B$$

or

$$f : A \overset{\text{onto}}{\to} B.$$

◊

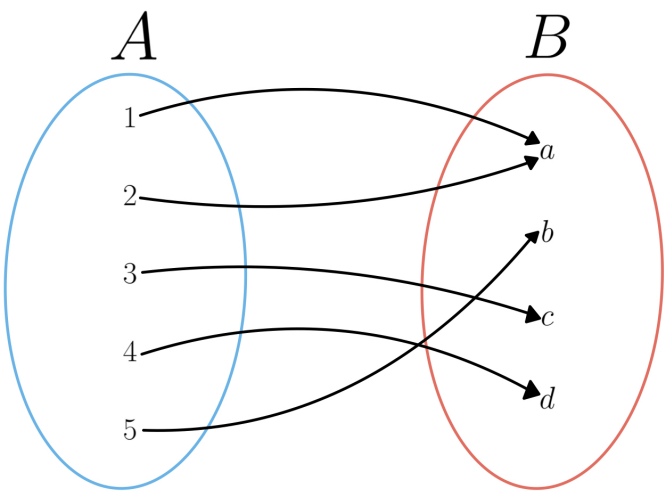
Example 7.6.2 A function that is surjective just needs to hit every element in the codomain. Consider the two sets

$$A = \{1, 2, 3, 4, 5\}$$

and

$$B = \{a, b, c, d, e\}$$

and consider the function $f : A \to B$ defined as



□

Example 7.6.3 Consider the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ from Example 7.5.4, p. 148 defined as

$$f(a, b) = 3a + 2b$$

Prove: f is surjective

Proof. The definition of surjective involves an equality of sets, so we break our proof into two parts.
Proof of Rng(**f**) $\subseteq \mathbb{Z}$
Let $c \in \text{Rng}(f)$ by definition of range we can find an $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(a, b) = c$, yet by definition of f we have that $f(a, b) = 3a + 2b$, since both a and b are integers we can conclude that $3a + 2b$ is an integer and thus $c \in \mathbb{Z}$ as desired.
Proof of Rng(**f**) $\supseteq \mathbb{Z}$
Let $z \in \mathbb{Z}$, by Proposition 6.12.6, p. 121 we can find two integers q and r such that $0 \leq r < 3$ such that $q = 3z + r$. Since $0 \leq r < 3$ we have that $r = 0$ or $r = 1$ or $r = 2$, splitting our proof into 3 cases
Case 1: Assume $r = 0$
In this case since $q \in \mathbb{Z}$ and 0 is also an integer we have that $z = 3q + 2 \cdot 0$ hence $f(q, 0) = z$ and thus $z \in \text{Rng}(f)$ as desired.
Case 2: Assume $r = 1$
For this case note that $r = 1 = 3 - 2$ hence $q + 1$ and -1 are integers we have that $z = 3q + 3 - 2 = 3(q + 1) + (-1) \cdot 2$ hence $f(q + 1, -1) = z$ thus $z \in \text{Rng}(f)$ as desired.
Case 3: Assume $r = 2$
In this case since q and 1 are integers we have that $z = 3q + 2$ hence $f(q, 1) = z$, therefore $z \in \text{Rng}(f)$ as desired.
Because we have shown no matter what r is that $z \in \text{Rng}(f)$ we can conclude that $z \in \text{Rng}(f)$
Since we have shown both $\text{Rng}(f) \subseteq \mathbb{Z}$ and $\text{Rng}(f) \supseteq \mathbb{Z}$ we can conclude $\text{Rng}(f) = \mathbb{Z}$, therefore we have shown that f is surjective. ■

□

Before we jump into our next example, lets shed a little light on composing functions.

Composing Functions.

Once again functions are just relations, thus we have already defined how to compose them.

For example considering three sets A, B, and C and two functions $f : A \to B$ and $g : B \to C$ we can then consider the composition

$$g \circ f : A \to C.$$

When we were dealing with relations we would have taken a pair $(a, c) \in g \circ f$ to only be a member of $g \circ f$ when we could find an element $b \in B$ such that $(a, b) \in f$ and $(b, c) \in g$, with a function this element is self evident, it is $f(a)$ since

$$(a, b) \in f$$

means

$$f(a) = b.$$

Furthermore, since $\mathrm{Dom}(f) = A$ we know we have such a b (another reason that the notation $f(a)$ even makes sense).

That is we interpret the composition of functions as

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

Example 7.6.4 Let $f : A \to B$ and $g : B \to C$ be functions.

Prove: If $g \circ f$ is surjective then g is surjective

Proof. Assume that $g \circ f$ is surjective. To prove that g is surjective we need to show an equality of sets, so break it into the usual parts.
Proof of $\mathrm{Rng}(\mathbf{g}) \subseteq \mathbf{C}$
Let $y \in \mathrm{Rng}(g)$ by definition of range we can find an $x \in B$ such that $g(x) = y$ hence by definition of g we have that $g(x) \in C$ as desired.
Proof of $\mathrm{Rng}(\mathbf{g}) \supseteq \mathbf{C}$
Let $c \in C$, since we have assumed that $g \circ f$ is surjective, in particular $C \subseteq \mathrm{Rng}(g \circ f)$ we have that $c \in \mathrm{Rng}(g \circ f)$ thus by definition of range we can find a $a \in A$ such that $g \circ f(a) = c$, that is $g(f(a)) = c$, and by definition of f we have that $f(a) \in B$, hence we have that $c \in \mathrm{Rng}(g)$.
Since we have shown both $\mathrm{Rng}(g) \subseteq C$ and $\mathrm{Rng}(g) \supseteq C$ we can conclude that $\mathrm{Rng}(g) = C$, hence we have shown that g is surjective. ■

□

Definition 7.6.5 Injection. A function $f : A \to B$ is **one-to-one**, or is an **injection**, means

whenever $f(x) = f(y)$ then $x = y$.

We write this as

$$f : A \hookrightarrow B,$$

or

$$f : A \overset{1\text{-}1}{\to} B.$$

◊

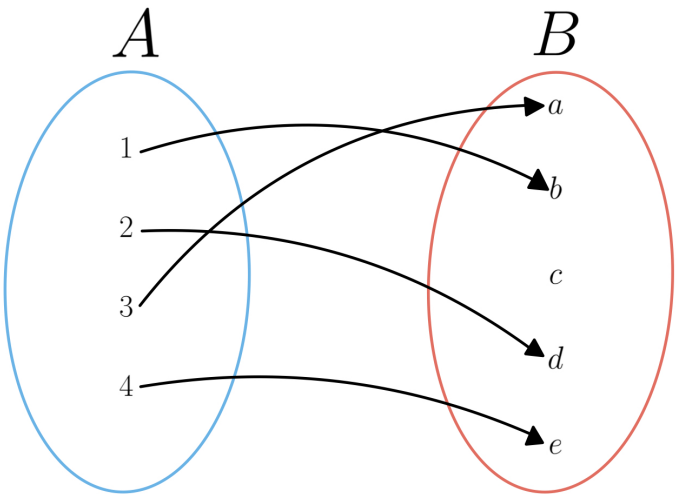
Example 7.6.6 A function that is injective just needs that no two inputs hit the same output. Consider, again, the two sets

$$A = \{1, 2, 3, 4\}$$

and

$$B = \{a, b, c, d, e\}$$

and consider this time the function $f : A \to B$ defined as



□

Example 7.6.7 Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined for any $a \in \mathbb{Z}$ as

$$f(a) = a + 5$$

Prove: f is an injective function.

Proof. We leave the task of proving that f is indeed a function to the reader, and we prove that f is injective.
Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $f(x) = f(y)$ by definition of f this means $x + 5 = y + 5$, subtracting five on both sides of the equation gives us $x = y$ as desired. ■

□

Notice that the function from Example 7.6.3, p. 152 is ***not*** one-to-one since $6 = f(2, 0) = f(0, 3)$ yet $(2, 0) \neq (0, 3)$.

Example 7.6.8 ***Prove:*** If $f : A \to B$ is one-to-one and $g : B \to C$ is one-to-one, then $g \circ f$ is one-to-one.

Proof. Assume $f : A \hookrightarrow B$ and $g : B \hookrightarrow C$. Let $x \in A$ and $y \in A$ such that $g \circ f(x) = g \circ f(y)$.
By definition of function we can have that $f(x) \in B$ $f(y) \in B$.
By assumption that $g \circ f(x) = g \circ f(y)$, that is $g(f(x)) = g(f(y))$. By our assumption that g is one-to-one, $f(x) = f(y)$. Thus, by our assumption that f is one-to-one, $x = y$. Hence $f \circ g$ is one-to-one ■

□

Proposition 7.6.9 *f^{-1} is a function from Rng(f) to A if and only if f is one-to-one.*

Proof of Proposition 7.6.9. As we are to prove a biconditional we will split the proof into two parts.
Proof of **f** is one-to-one $\implies$ $\mathbf{f^{-1}} : \mathrm{Rng}(\mathbf{f}) \to \mathbf{A}$
Assume f is one-to-one. We have defined the inverse of a relation in Definition 7.2.1, p. 128, so what we want to show is that f^{-1} is a function. To show a relation is a function we need to show that it satisfies both conditions to being a function.

Proof of Condition (i):
This first condition Definition 7.5.1, p. 146 is the equality of sets, namely $\text{Dom}(f^{-1}) = \text{Rng}(f)$ this was proven in Proposition 7.2.3, p. 129.
Proof of Condition (ii)
Let $x \in B$, $y \in A$ and $z \in A$ such that $f^{-1}(x) = y$ and $f^{-1}(x) = z$. By definition of inverse, $f(y) = x$ and $f(z) = x$. Thus, by our assumption, $y = z$ as desired.
Proof of $\mathbf{f^{-1} : \text{Rng}(f) \to A} \implies \mathbf{f}$ is one-to-one
Let $x \in A$ and $y \in A$ such that $f(x) = f(y)$. Name this element $w = f(x) = f(y)$. By definition of inverse, $f^{-1}(w) = x$ and $f^{-1}(w) = y$. Thus, by our assumption that f^{-1} is a function by condition (i) of being a function we have, $x = y$ as desired. ■

Now we have set up all the pieces we need to define a bijection.

Definition 7.6.10 Bijection. A function $f : A \to B$ is a **one-to-one correspondence**, or a **bijection** means
f is one-to-one and onto B.
We write this as

$$f : A \xrightarrow{\sim} B$$

◊

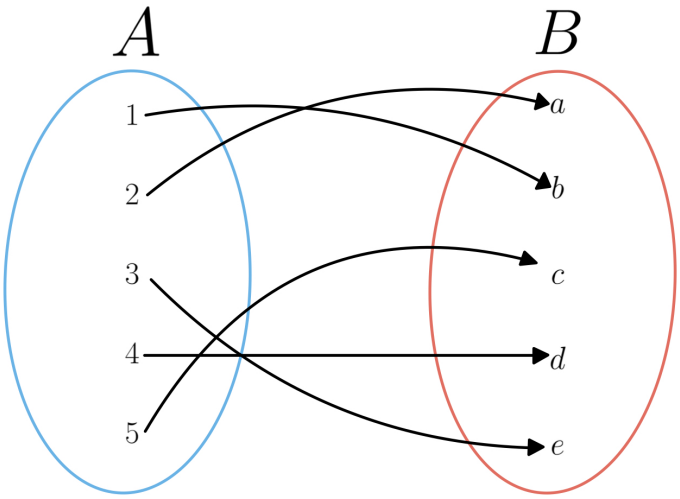
Example 7.6.11 A function that is bijective needs that no two inputs hit the same output, as well as to reach every element of the codomain. Consider, again, the two sets

$$A = \{1, 2, 3, 4, 5\}$$

and

$$B = \{a, b, c, d, e\}$$

and consider this time the function $f : A \to B$ defined as



□

Example 7.6.12 Consider the function $g : \mathbb{Z} \to \mathbb{Z}$ defined for any $a \in \mathbb{Z}$ as

$$g(a) = a - 2$$

Prove: g is a bijection.

Proof. To show this function is a bijection we will need to show it is injective and surjective.
Proof of one-to-one:
Let x and y be two arbitrary integers, such that $g(x) = g(y)$ by definition of g we have that $g(x) = x - 2$ and $g(y) = y - 2$ therefore $x - 2 = y - 2$, adding two to both sides of the equations leaves us with $x = y$ as desired.
Proof of onto:
To show our desired equality of sets we split into two parts.
Proof of $\text{Rng}(\mathbf{g}) \subseteq \mathbb{Z}$
Let $b \in \text{Rng}(g)$, by definition of range we can find an integer a such that $g(a) = b$ by the definition of g we have that $g(a) = a - 2$, since both a and 2 are integers we have that $a - 2$ is an integer and hence $b \in \mathbb{Z}$ as desired.
Proof of $\text{Rng}(\mathbf{g}) \supseteq \mathbb{Z}$
Let $m \in \mathbb{Z}$, note to show that we have membership of $\text{Rng}(g)$ we need to produce an integer so that g maps this new integer to m. This is an existential, and the way we produce this element in unimportant to the proof. Notice that since m and 2 are integers we have that $m + 2$ is an integer, and notice that $g(m + 2) = m + 2 - 2 = m$ and hence by definition of range we have that $m \in \text{Rng}(g)$ as desired.
Because we have shown that $\text{Rng}(g) \subseteq \mathbb{Z}$ and $\text{Rng}(g) \supseteq \mathbb{Z}$ we can conclude that $\text{Rng}(g) = \mathbb{Z}$, therefore we have that g is onto as desired.
Since we have shown that g is both one-to-one and onto we have that g is a bijection. ■

□

Proposition 7.6.13 *If $f : A \to B$ is a bijection, and $g : B \to C$ is a bijection, then $g \circ f : A \to C$ is a bijection.*

Proof of Proposition 7.6.13. Assume f is a bijection from A to B and g is a bijection from B to C.
[Proof of one-to-one]
Let $x \in A$ and $y \in A$ such that $g \circ f(x) = g \circ f(y)$, hence $g(f(x)) = g(f(y))$
By our assumption g is a bijection, in particular one-to-one, this implies $f(x) = f(y)$. Since f is a bijection, in particular one-to-one, $x = y$, therefore $g \circ f$ is one-to-one as desired.
[Proof of Onto]
Proof of $\text{Rng}(\mathbf{g} \circ \mathbf{f}) \subseteq \mathbf{C}$
Let $y \in \text{Rng}(g \circ f)$. By definition of range, $y \in C$. Thus, $\text{Rng}(g \circ f) \subseteq C$.
Proof of $\text{Rng}(\mathbf{g} \circ \mathbf{f}) \supseteq \mathbf{C}$
Let $y \in C$. Thus by our assumption that g is a bijection, specifically surjective, we can find $w \in B$ such that $g(w) = y$, and since f is a bijection, specifically surjective.
Thus by assumption that f is a bijection, specifically surjective, we can find $x \in A$ such that $f(x) = w$. Thus by definition of composition, $g \circ f(x) = y$. Hence, $y \in \text{Rng}(g \circ f)$. Thus $C \subset \text{Rng}(g \circ f)$.
Since we have shown that both $\text{Rng}(g \circ f) \subseteq C$ and $\text{Rng}(g \circ f) \supseteq C$ we can conclude $\text{Rng}(g \circ f) = C$ so that we can conclude that $g \circ f$ is onto as desired.
Thus, $g \circ f : A \to C$ is a bijection. ■

7.7 Exercises

1) $\text{Rng}(R^{-1}) = \text{Dom}(R)$

2) $I_B \circ R - R$ and $R \circ I_A = R$

3) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

4) R is a reflexive relation on A if and only if $I_A \subset R$.

5) R is symmetric if and only if $R = R^{-1}$.

6) Suppose that R and S are equivalence relations on a set A. Prove that $R \cap S$ is an equivalence relation on A.

7) Prove that if R is a symmetric, transitive relation on A, and the domain of R is A, then R is reflexive on A.

8) Let R be a relation on the set A. Prove that $R \cup R^{-1}$ is symmetric.

9) If $f : A \to B$ is onto B and $g : B \to C$ is onto C, then $g \circ f$ is onto C.

10) Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is one-to-one, then f is one-to-one.

11) Let $F : A \to B$ and $G : B \to A$. If F is one-to-one and onto B, then $G = F^{1}$ if and only if $G \circ F = I_A$ or $F \circ G = I_B$.

12) $f(C \cup D) - f(C) \cup f(D)$

13) $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$

14) $f^{-1}(\bigcup_{\beta \in \Gamma} E_\beta) = \bigcup_{\beta \in \Gamma} f^{-1}(E_\beta)$

15) Prove that $f(a, b) = 5a + 3b$ defines a surjective function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$ but not injective.

Index

Colophon

This book was authored in PreTeXt.