Everything You Always Wanted To Know About Mathematics*

(*But didn't even know to ask)

A Guided Journey Into the World of Abstract Mathematics and the Writing of Proofs

Brendan W. Sullivan

bwsulliv@andrew.cmu.edu

with Professor John Mackey

Department of Mathematical Sciences
Carnegie Mellon University
Pittsburgh, PA

May 10, 2013

This work is submitted in partial fulfillment of the requirements for the degree of Doctor of Arts in Mathematical Sciences.

Contents

Part I

Learning to Think Mathematically

Chapter 1

What Is Mathematics?

1.1 Truths and Proofs

How do you know whether something is true or not? Surely, you've been told that the angles of a triangle add to $180°$, for example, but how do you *know* for sure? What if you met an alien who had never studied basic geometry? How could you *convince* him/her/it that this fact is true? In a way, this is what mathematics is all about: devising new statements, deciding somehow whether they are true or false, and explaining these findings to other people (or aliens, as the case may be). Unfortunately, it seems like many people think mathematicians spend their days multiplying large numbers together; in actuality, though, mathematics is a far more creative and writing-based discipline than its widely-perceived role as ever-more-complicated arithmetic. One aim of this book is to convince you of this fact, but that's merely a bonus. This book's main goals are to show you what mathematical thinking, problem-solving, and proof-writing are really all about, to show you how to do those things, and to show you how much fun they really are!

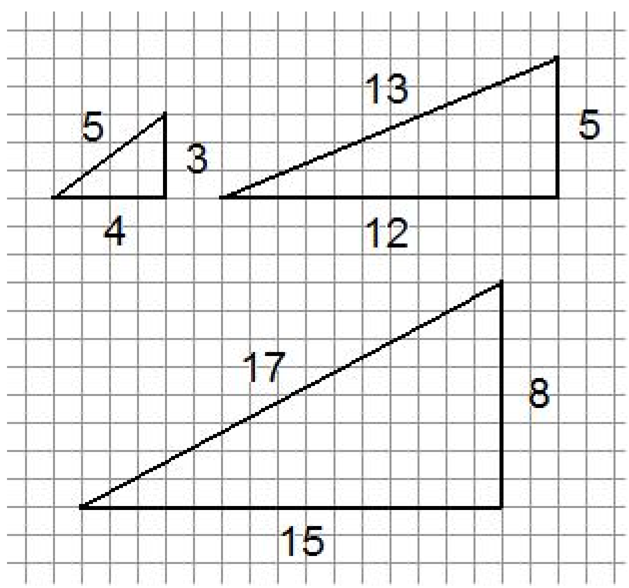
As a side note, you might even wonder "What does it mean for something to be true?" A full discussion of this question would delve into philosophy, psychology, and maybe linguistics, and we don't really want to get into that. The main idea in the context of mathematics, though, is that **something is true only if we can *show* it to be true *always***. We know $1 + 1 = 2$ always and forever. It doesn't matter if it's midnight or noon, we can rest assured that equation will hold true. (Have you ever thought about how to show such a fact, though? It's actually quite difficult! A book called the *Principia Mathematica* does this from "first principles" and it takes the authors many, many pages to even get to $1 + 1 = 2$!) This is quite different from, perhaps, other sciences. If we conduct a physical experiment 10 times and the same result occurs, do we know that this will *always* happen? What if we do the experiment a million times? A billion? At what point have we actually *proven* anything? In mathematics, repeated experimentation is not a viable proof! We would need to find an argument that shows why such a phenomenon would *always* occur. As an example, there is a famous open problem in mathematics called the *Goldbach Conjecture*. It is unknown, as of now, whether it is true or not, even though it has been verified by computer simulations up until a value of roughly 10^{18}. That's a *huge* number, but it is still not enough to know whether the conjecture is True or False. Do you see the difference? We mathematicians like to *prove* facts, and checking a bunch of values but not *all* of them does *not* constitute a proof.

1.1.1 Triangle Tangle

We've introduced the idea of a **proof** by talking about what we hope proofs to accomplish, and why we would care so much about them. You might wonder, then, how one can *define* a proof. This is actually a difficult idea to address! To approach this idea, we are going to present several different mathematical arguments. We want you to read along with them, and think about whether they are convincing. Do they *prove* something? Are they correct? Are they understandable? How do they make you feel? Think about them on your own and develop some opinions, and then read along with our discussion.

The mathematical arguments we will present here are all about triangles. Specifically, they concern the **Pythagorean Theorem.**

Theorem 1.1.1 (The Pythagorean Theorem)**.** *If a right triangle has base lengths a, b and hypotenuse length c, then these values satisfy $a^2 + b^2 = c^2$.*



How do we know this? It's a very useful fact, one that you've probably used many times in your mathematics classes (and in life, without even realizing).

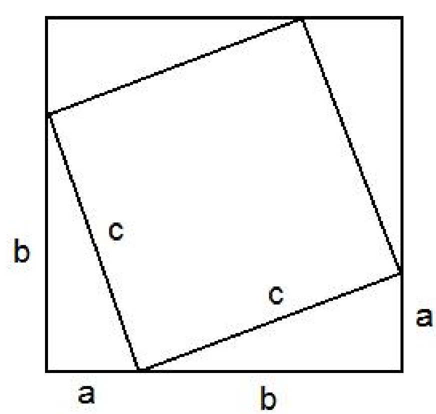
Have you ever wondered why it's true? How would you explain it to a skeptical friend? This is what a **mathematical proof** attempts to accomplish: a clear and concise explanation of a fact. The reasoning behind requiring a proof makes a lot of sense, too, and is twofold: it's a relief to know that what we thought was true is, indeed, true and it's nice to not have to go through the explanation of the fact every time we'd like to use it. After proving the Pythagorean Theorem (satisfactorily), we merely need to refer to the theorem by name whenever a relevant situation arises; we've already done the proof, so there's no need to prove it again.

Now, what exactly constitutes a proof? How do we know that an explanation is sufficiently clear and concise? Answering this question is, in general, rather difficult and is part of the reason why mathematics can be viewed as an art as much as it is a science. We deal with cold, hard facts, yes, but being able to reason with these facts and satisfactorily explain them to others is an art form in itself.

Examples of "Proofs"

Let's look at some sample "proofs" and see whether they work well enough. (We say "proof" for now until we come up with a more precise definition for it, later on.) Here's the first one:

"Proof" 1. Draw a square with side length $a + b$. Inside this square, draw four copies of the right triangle, forming a square with side length c inside the larger square.



The area of the larger square can be computed in two ways: by applying the area formula to the larger square or by adding the area of the smaller square to the area of the four triangles. Thus, it must be true that

$$(a + b)^2 = c^2 + 4 \cdot \frac{ab}{2} = c^2 + 2ab$$

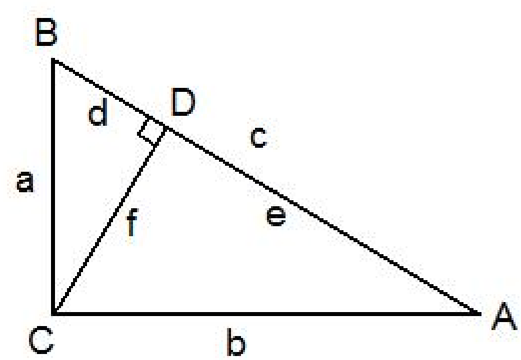
Expanding the expression on the left and canceling a common term on both sides yields

$$a^2 + \cancel{2ab} + b^2 = c^2 + \cancel{2ab}$$

Therefore, $a^2 + b^2 = c^2$ is true. $\square$

Are you convinced? Did each step make sense? Maybe you're not sure yet, so let's look at another "proof" of the theorem.

"Proof" 2. Suppose the Pythagorean Theorem is true and draw the right triangle with the altitude from the vertex corresponding to the right angle. Label the points and lengths as in the diagram below:



Since the Pythagorean Theorem is true, we can apply it to all three of the right triangles in the diagram, namely ABC, BCD, ACD. This tells us (defining $e = c - d$)

$$a^2 = d^2 + f^2$$
$$b^2 = f^2 + e^2$$
$$c^2 = a^2 + b^2$$

Adding the first two equations together and replacing this sum in the third equation, we get

$$c^2 = d^2 + e^2 + 2f^2$$

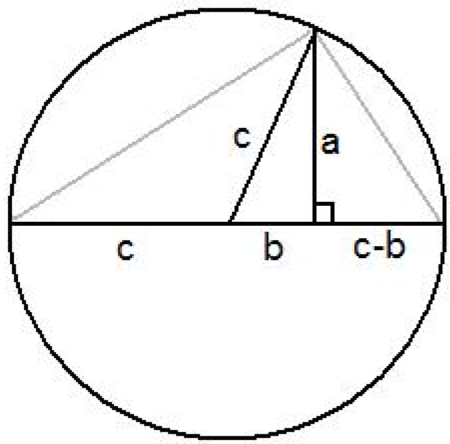
Notice that angles $\angle ABC$ and $\angle ACD$ are equal, because they are both complementary to angle $\angle CAB$, so we know triangles $\triangle CDB$ and $\triangle ADC$ are *similar triangles*. (We are now assuming some familiarity with plane geometry.) This tells us $\frac{e}{f} = \frac{f}{d}$, and thus $f^2 = ed$. We can use this to replace f^2 in the line above and factor, as follows:

$$c^2 = d^2 + e^2 + 2de = (d + e)^2$$

Taking the square root of both sides (and knowing c, d, e are all positive numbers) tells us $c = d + e$, which is true by the definition of the lengths d and e. Therefore, our assumption that the Pythagorean Theorem is true was valid. □

What about this proof? Was it convincing? Was it clear? Let's examine one more "proof" before we decide what a constitutes a "correct" or "good" proof.

"Proof" 3. Observe that



so $\frac{a}{c+b} = \frac{c-b}{a}$ and thus $a^2 + b^2 = c^2$. □

Did that make any sense to you? Finally, here's one last "proof" to consider.

"Proof" 4. The Pythagorean Theorem must be true, otherwise my teachers have been lying to me. □

Discussion

Before reading on, we encourage you to think about these four "proofs" and even discuss them with another student or a friend. What do you think constitutes a "correct" proof? Is clarity and ease of reading important? Does it affect the "correctness" of a proof?

From a historical perspective, mathematical proof-writing has evolved over the years and there is a good, general consensus as to what constitutes a "correct" proof:

- It is important that every *step* in the proof, every logical inference and claim, is *valid*, mathematically speaking.
- It is also important that the proof-writer makes (reasonably) clear why a statement follows from the previous work or from outside knowledge.

What's nice about the *truth* requirement is that mathematics has been built up so that we can read through an argument and verify each claim as True or False. What's difficult to define is *clear* writing. In a way, it is much like Supreme Court Justice Potter Stewart's famous definition of obscenity: "I know it when I see it".

Given these four arguments for comparison, let's assess them for clarity and correctness:

Clarity:

- "Proofs" 1 and 2 are fairly well explained. There are clear statements about what the writer is doing and why. They indicate where any equations come from, and even include some pictures to illustrate their ideas for the reader.

  Notice that "proof 1" does rely on some basic prior knowledge, like the algebraic manipulation of variables and formulae for the area of a triangle and square, but this is fine.

  Likewise, "Proof 2" relies on some understanding of similar triangles and what this means about the lengths of their sides. At least the proof-writers pointed this out, so an interested reader could look up some relevant ideas. If they didn't say this, a reader might be confused and have no idea how to figure out what they're missing!

- "Proof" 3 is very poorly worded! It offers no explanation whatsoever. This makes it quite difficult to determine whether their claims are actually correct. Yes, a picture is included, but there is no indication of *why* they chose to draw a circle around the triangle, or why the stated equations follow from the diagram.

- "Proof" 4 is a grammatically correct English sentence, but it doesn't *explain* anything!

Already, we can see that "Proof" 4 is certainly ont a viable candidate for being a good and proper *proof*. "Proofs" 1 and 2 are still in the running, since they are at least written clearly. "Proof" 3, as it is written now, would probably not be a good candidate; however, maybe it does contain correct ideas that just require better explanations. Perhaps it could be rewritten as a good and proper *proof*.

Let's analayze the logical correctness of these four arguments:

Correctness:

- "Proof" 1 mostly good. The formulae for the areas of the square and triangles are correctly applied, and the algebraic manipulation thereof is correct. But how do we know that the process they described—putting four copies of the given triangle inside a larger square—creates a square with side length c on the inside? They merely say it *does* so without really saying *why*. Other than this omission, though, this proof is both well-written and correct.

(Can you prove that fact, that the shape inside is actually a square? Just look at its angles: can you show why they are all *right* angles?)

- Unfortunately, "Proof" 2 is completely invalid! Every logical step that it makes does follow from the previous one. For instance, assuming we have the triangles set up this way, we can correctly deduce that ΔCDB and ΔADC are similar triangles. However, why is it that we can *assume* the theorem is True right at the beginning? Isn't that what we are trying to accomplish in the proof, overall? This is a crucial flaw. **Assuming a fact and deducing something True from it does *not* allow us to conclude the original assumption was valid.**

  If this method were valid, we could "prove" just about anything we wanted! Here's an example: What do you think of the following "proof" that $0 = 1$?

  "Proof". Assume $0 = 1$. Then, by the symmetric property of $=$, it is also true that $1 = 0$. Adding these two equations tells us $1 = 1$, which is True. Therefore, $0 = 1$ was a valid assumption, so it must be True. $\square$

  Do you see the similarity between this and "Proof" 2 above? The same sort of flawed reasoning was used: we assumed one fact, did some work to get to something else we know to be True, and then said that the assumed fact must be True, as well.

- Regarding "Proof" 3, most mathematicians would say it is a "bad proof", despite the fact that everything it appears to claim is correct. We say "appears" because, without any words to explain what's going on, we don't actually know what the proof-writer is trying to say! However, we will say that the kernel of a perfectly good proof is contained therein.

  From the diagram, you can show that the stated equation, $\frac{a}{c+b} = \frac{c-b}{a}$, must follow. (Hint: Use similar triangles!) From there, it is a simple manipulation to deduce that $a^2 + b^2 = c^2$.

  Can you write some sentences to go along with the diagram that would turn this into a proper proof?

- Lastly, just about every reasonably logical person (we hope!) would say that "Proof" 4 is not even close to being a proof, however convenient it might be to make such statements.

This discussion shows that "Proof" 1 is actually a good proof. Amongst all four, it is the most clearly-written, and the one that is logically correct. We can refer to it now as a **proof**. "Proof" 2 is outright incorrect, despite how clearly it is presented. "Proof" 3 contains correct ideas, but is not presented clearly. "Proof" 4 is so far from a proof that we don't even want to discuss it.

Question

Before moving on to other topics, we'll leave you with a question: if we give you three positive numbers a, b, c that satisfy $a^2 + b^2 = c^2$, is it necessarily true that there is a right triangle with side lengths a, b and hypotenuse length c? If so, how could you go about constructing it? If not, why not?

1.1.2 Prime Time

While we're on the topic of proofs, let's look at another proof, for a different theorem. As a reminder (or brief introduction), let's talk about *prime numbers.*

Definition, Examples, and Uses

Definition 1.1.2. *A positive integer p that is larger than 1 is called a* **prime** *number if the only positive divisors of p are* 1 *and p. A non-prime positive integer is called a* **composite** *number.*

Prime numbers have shown to be incredibly important in all branches of mathematics, not just the study of integers and their properties, which is known as **number theory**. One of the most famous **conjectures** (a guess at a theorem that has been neither proven nor disproven thus far) in all of mathematics is the *Riemann Hypothesis.* Its conclusion has been shown to be closely related to the distribution of prime numbers throughout the integers. Many books have been written on this topic. Also, most modern cryptography schemes are based on multiplying huge prime numbers together, relying on the fact that it's quite difficult to undo this process and figure out the two huge prime factors, given their product. So now you know: every time you buy a song on iTunes with your credit card, some computer just multiplied two large prime numbers!

The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ (remember, 1 does not fit our definition). How many prime numbers are there? How far apart are they? Is there a pattern? Answering questions like these can be interesting and fun, but also difficult (and sometimes, impossible!). Here, we'll answer one of the questions: are there an infinite number of prime numbers?

Theorem and Proof

Theorem 1.1.3 (Infinitude of the Primes)**.** *There are infinitely-many prime numbers.*

"Proof". Assume instead that there are only finitely-many prime numbers, and list them in ascending order: $p_1, p_2, p_3, \ldots, p_k$, so that p_k is the largest of these prime numbers. Define the new number

$$N = (p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_k) + 1$$

It must be true that N is divisible by some prime number. However, it cannot be divisible by p_1 or p_2 or $\ldots$ or p_k, because that would leave a remainder of 1, based on how we defined N. Thus, N is divisible by some other prime number that is *not* in the list.

If N itself is composite (i.e. not prime), then we have found some new prime $p < N$ that is not in the list of *all* primes we presumably had. If N itself is prime, then we have a new prime $N > p_k$, so p_k is not actually the largest prime number. Either way, we have a new prime guaranteed to not be in the given list of k primes. Therefore, there must be infinitely-many prime numbers. □

What do you think of this "proof"? Are you convinced? It feels a little different from the other arguments we've seen so far, doesn't it? Try explaining to a classmate how this one differs from "Proof 1" of the Pythagorean Theorem from the previous section. We will reveal this, though: this "proof" here is actually a fully correct *proof*, sans quotation marks!

1.1.3 Irrational Irreverence

Let's talk about a different type of number, now: **rational** numbers. You might know rational numbers as "fractions" or "quotients" or "ratios".

Definition and Examples

Here is a precise definition of *rational* numbers:

Definition 1.1.4. *A real number r is a* **rational** *number if and only if it can be expressed as a ratio of two integers $r = \frac{a}{b}$, where a and b are both integers (and $b \neq 0$).*

A real number that is not rational is called **irrational**.

Nothing about this definition says that there has to be only one such representation of a rational number; it merely requires that a rational number have at least one such a representation. For instance, 1.5 is a rational number because $1.5 = \frac{3}{2} = \frac{12}{8} = \frac{30}{20}$ and so on. A real number that is not rational is called an **irrational** number, and that's the entire definition: *not* rational, i.e. there is no such representation of the number as a ratio of integers. You may know that $\sqrt{2}$ is an irrational number, but how do you *prove* such a thing? Try it for yourself. We will actually reexamine this question later on (see Example 4.9.4). Other irrational numbers you may know already include e, π, φ and $\sqrt{n}$ where n is any positive integer that is not a perfect square.

Questions

Given this definition of rational/irrational, we might wonder how we can combine irrational numbers to produce a rational number. Try to answer the following questions on your own. If your answer is "yes", try to find an example, and if your answer is "no", try to explain why the desired situation is not possible.

(1) Are there irrational numbers a and b such that $a \cdot b$ is a rational number?

(2) Are there irrational numbers a and b such that $a + b$ is a rational number?

(3) Are there irrational numbers a and b such that a^b is a rational number?

Did you find any examples? It turns out that the answer to all three questions is "yes"! The first two are not too hard to figure out, but the third one is a little trickier.

Here, we'll work through a proof that says the answer to the third is "yes". The interesting part about it, though, is that we won't actually come up with definitive numbers a and b that make a^b a rational number; we'll just narrow it down to two possible choices and show that one of those choices *must* work. Sounds interesting, right? Let's try it.

Proof. We know $\sqrt{2}$ is an irrational number. Consider the number $x = \sqrt{2}^{\sqrt{2}}$. There are two possibilities to consider:

- If x is rational, then we can choose $a = \sqrt{2}$ and $b = \sqrt{2}$ and have our answer.

- However, if x is irrational, then we can choose $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ because then

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$$

  and 2 is a rational number.

In either case, we can find irrational numbers a and b such that a^b is a rational number. Thus, such a pair of numbers must exist. $\square$

How do you feel about this proof? Is it convincing? It answers the third question above with a definitive "yes", but it does not tell us *which* pair a, b is actually the correct one, merely that one of the pairs will work. (It turns out that $\sqrt{2}^{\sqrt{2}}$ is also irrational, but that fact takes a lot more work to prove.)

There are plenty of other concrete examples that answer this question, though. Can you come up with any? (Hint: try using the $\log_{10}$ function...)

1.2 Exposition Exhibition

1.2.1 Simply Symbols

Mathematics is a Language

Despite appearances (and some densely-written textbooks), mathematics is not just a collection of symbols that we push around on paper. The English language is based on a fixed group of symbols (the 26 letters of the alphabet plus common punctuation like the period and comma and parenthesis) but we put these symbols together in a specific way, while following some standard and agreed-upon conventions, to craft meaningful words, phrases, sentences, paragraphs, and so on; in essence, English, like any language, is a way to convey meaning via a collection of symbols and a collection of rules governing those symbols. The same concept applies to the *language of mathematics*: there is a collection of symbols and a set of rules that we apply to those symbols.

One difference is that the collection of symbols we use in mathematics can be rather large, depending on which branch of mathematics currently being discussed. A big part of the structural versatility of mathematics is that we can always create and define new symbols to use. Oftentimes, this is even done to make things shorter and easier to read.

Another main difference between mathematics and other languages is that we choose carefully how to *define* our words and the concepts they represent. Frequently, most of the debates mathematicians have revolve around definitions. This may be surprising to you; perhaps it would make more sense to think that mathematicians debate over proofs and conjectures, or maybe it's a novel idea that mathematicians even debate at all! Choosing the right definitions and terms for a newly-discovered concept is a crucial component of mathematical discovery and exposition since it helps the discoverer/inventor explain his/her ideas to other, interested people. (Without this process, there is no advancement in mathematics, just a bunch of isolated people trying to discover truths on their own.)

The situation is similar with spoken languages, but not as extreme, it seems. For instance, if you said to your friend, "I'm hungry", or "I'm feeling a bit peckish", or "Oh my god, I'm starving", they hear essentially the same message and would respond roughly the same way in each case. In mathematics, though, our definitions are far more precise and don't incorporate the types of nuances that spoken language permits. Of course, there are benefits and disadvantages to both philosophies, but in mathematics we strive for precision whenever possible, so we like our definitions to be exact and unwavering. That said, though, we have control over what those definitions are! This is why debates over definitions are so prevalent in the mathematical world: choosing the right definitions for concepts at hand can make future work with those concepts much easier and more convenient.

Choosing Definitions Properly

As a concrete example, let's return to Definition 1.1.2 of a *prime number* that we saw in the previous subsection. It said:

Definition. *A positive integer p that is larger than 1 is called a* **prime** *number if the only positive divisors of p are* 1 *and p. A non-prime positive integer is called a* **composite** *number.*

There doesn't seem to be anything questionable about this definition, does there? Perhaps you would have worded it differently or been more concise or used a different variable letter or what have you, but the ultimate message would be the same: a prime number is a certain type of number that has a certain property. However you choose to write out what that specific type of number is (a positive integer larger than 1) and what that property is (having no positive divisors except itself and 1), you obtain an equivalent definition.

There are some subtle questions behind this definition, though: Why is it that particular type of number? Why is it that particular property—only being divisible by 1 and itself—that we care so much about? What if the definition was slightly different? Would things really change that much? We'll address these questions with another question: What do you think of the following alternative definition of a prime number?

Definition 1.2.1. *An integer p that is less than -1 or greater than 1 is called a* prime *number if the only positive divisors of p are* 1 *and p.*

Do you notice the subtle difference? All of the numbers that fit the previous definition of "prime" still fit this one, but now so do negative numbers! Specifically, given any number p that is prime under the old definition, $-p$ is now prime under the new definition. Is this a reasonable idea? What's wrong with having negative prime numbers?

How about this third definition of prime numbers?

Definition 1.2.2. *A positive integer p is called a* prime *number if the only positive divisors of p are* 1 *and p.*

(Remember that 0 is neither positive nor negative, by convention.) Now, the negative numbers are out of bounds, but 1 fits this definition. Is this reasonable? The only positive divisors of 1 are 1 and ... itself, right?

This is where a debate could arise: perhaps you don't mind allowing 1 to be a prime number, but your friend is vehemently against it. Well, without solid reasons either way, there's no way to say that either of you is *wrong*, really; you just made different choices of terminology, and neither of them change the inherent property that the only positive divisors of 1 are 1 and itself. As a similar idea, consider this: whether you call them sandals or thongs or flip-flops, the fact remains that those types of shoes are appropriate footwear at the beach.

With historical hindsight and new desires in mind, though, oftentimes one particular definition is shown to be more appropriate. In the future, we will look at **prime factorizations**, a way of writing every (positive) integer as a product of only prime numbers. For instance, $15 = 3 \cdot 5$ and $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$ and $142857 = 3^3 \cdot 11 \cdot 13 \cdot 37$ are all prime factorizations.

There is a special property about these factorizations, too: in general, a prime factorization of a positive integer is **unique**! That is, there is one and *only* one way to write a positive integer as a product of prime numbers (since we think of different orderings of the factors as the same thing, so $105 = 3 \cdot 5 \cdot 7$ and $105 = 7 \cdot 3 \cdot 5$ are the same factorization). This is something we will *prove* rigorously using the first definition we gave above. What if we use the second definition, or the third? Is this property of uniqueness still true? Why do you think this uniqueness property is so important? Ultimately, the lesson here is that definitions should be driven by both logic and usefulness, and this can change over time and stir some debate.

Mathematicians Study Patterns

Another benefit of establishing clear and precise definitions is the knowledge and understanding you gain as a thinker; establishing logical foundations can be helpful in the future. A major aspect of how human beings learn involves identifying patterns through everyday experience and then associating ideas, concepts, words and events with those patterns. Then, one can use those patterns to predict and theorize about abstract ideas, concepts and events.

For instance, it has been studied and shown that human babies initially lack, but develop over time, the concept of *object permanence*. If you show a child a colorful toy that they smile at and enjoy, and then hide it under a cardboard box, the child doesn't quite understand that the toy still exists but is just out of sight. He/she will act as if the object is no longer in existence. At some point, though, we learn that this isn't true and that objects that are outside our realm of vision are still existent. How exactly does this happen? Well, perhaps we recognize the pattern of many such occurrences where an object "disappears" and then we find it again later.

Better examples can be found in the natural sciences, and they illustrate an extra facet of pattern recognition and abstract thinking that is of utmost importantance, particularly in mathematics and the sciences. One can imagine that Neanderthals somehow knew that any time they picked up a rock and held it at arm's length and then let go, the rock would fall to the ground. This probably happened over and over and so they "understood" that this phenomenon is a necessary product of nature. After enough occurrences, it was likely understood that this would always happen, or, at least, any instance in which it didn't happen would cause great confusion and fear. (It is this type of emotional response which might serve to explain how the infrequent but powerful occurrences of, say, volcanic eruptions led ancient civilizations to blame such events on "angry gods").

None of these observations of events brought these prehistoric human beings any closer to understanding *why* the rock would always fall to the ground, or being able to *explain* why it would necessarily happen every time. It would be many milennia before people even began to think to ask why and how this phenomenon occurred, and even longer before Isaac Newton finally proposed a model that sought to explain the behavior of gravity (the name given to this type of phenomenon, eventually). And even now, some say, we still haven't figured out precisely how it works. (Go online and Google "loop quantum gravity" and try to understand that, if you're curious).

It's this abstractive leap in thinking—from observations of a pattern to an epistemological understanding of that pattern—that characterizes a truly inquisitive and intellectual thinker, a true **scientist**, in the best sense of the word. Whom would you consider the better entomologist: the voracious reader who has memorized and can list all of the currently-known species of beetle in the world, or the laboratory scientist who has examined a variety of species and can take a new specimen and classify it as a beetle or non-beetle? This is somewhat of a leading question, but the main point is this: it is far more beneficial to *understand* a definition and the motivations behind it than it is to simply know a bunch of *instances* that satisfy a certain definition.

This is, arguably, even more important in mathematics. Can you imagine a mathematician who didn't know what a prime number was but could merely list the first 100 prime numbers from memory and was content with that? Of course not! Part of the beauty, versatility, and appeal of the study of mathematics is that we examine patterns and phenomena and then choose how to make the appropriate definitions associated with those patterns. We then use our newfound understanding of those patterns to make rigorously precise predictions about other patterns and phenomena. Thoroughly understanding a definition or concept increases the predictive power, and is far more effective than merely knowing examples of that definition/concept.

1.2.2 Write Right

Another interesting aspect of mathematics is that, as much as it is a language unto itself, we rely on an external language to convey the mathematical thoughts and insights we have. Try rewriting any of the definitions and proofs we've looked at before without using any words. It's tough, isn't it? Accordingly, we want the written language we use to convey mathematical ideas to follow the same types of standards we apply to the mathematical "sentences" we write: we want them to be *precise*, *logical*, and *clear*.

Now, deciding on a precise, logical, and clear definition for each of these three words is a difficult task, in itself. However, we can all agree that it would be ideal for a proof to be:

- **precise:** no individual statement should be untrue or interpretable in multiple ways that would make the truth debatable;

- **logical:** each step should follow from previous steps with proper motivation and explanation; and,

- **clear:** steps should be connected and described with proper English grammar and usage, helping the reader to see what's going on.

Let's examine a few "proofs" that disregard these standards and somehow fail to fit the definition of *proof* that we have so far.

Bad "Proof" #1

First, we have a "proof" that 1=2, so we know there must be something wrong with this one. Can you find the error? Which standard does it violate? Precision, logic, or clarity?

"Proof". Suppose we have two real numbers x and y, and consider the following chain of equalities:

$$\begin{aligned}
x &= y \\
x^2 &= xy && \text{multiply both sides by } x \\
x^2 - y^2 &= xy - y^2 && \text{subtract } y^2 \text{ from both sides} \\
(x+y)(x-y) &= y(x-y) && \text{factor both sides} \\
x + y &= y && \text{cancel } (x-y) \text{ from both sides} \\
y + y &= y && \text{remembering } x = y\text{, from the first line} \\
2y &= y \\
2 &= 1 && \text{divide both sides by } y
\end{aligned}$$

□

The issue here is *precision*. After factoring in line four, it seems convenient and wise to divide by the common factor $(x - y)$ to obtain line five; however, line one tells us that $x = y$ so $x-y = 0$, and **division by zero is not allowed**! Working with the variables x and y was just a way to throw you off the scent and disguise the division by zero. (While we're on the topic, why is division by zero not allowed? Can you think of a reasonable explanation? Think about it in terms of multiplication.)

Bad "Proof" #2

Here's another proof of a similar "fact", namely that $0 = 36$.

"Proof". Consider the equation $x^2 + y^2 = 25$. Rearranging to isolate x tells us

$$x = \sqrt{25 - y^2}$$

and then adding 3 to both sides and squaring yields

$$(x+3)^2 = \left(3 + \sqrt{25 - y^2}\right)^2$$

Notice that $x = -3$ and $y = 4$ is a solution to the original equation, so the final equation should be true, as well. Plugging in these values for x and y tells us

$$0 = (-3+3)^2 = \left(3 + \sqrt{25-16}\right)^2 = (3+3)^2 = 36$$

Therefore, $0 = 36$. □

What happened here? Can you spot the illogical step? Perhaps it would help if we rewrote the steps of the proof using the specific values of the variables

x and y that we chose towards the end:

$$\begin{aligned}(-3)^2 + 4^2 &= 25 \\ -3 &= \sqrt{25 - 4^2} \\ (-3+3)^2 &= \left(3 + \sqrt{25 - 4^2}\right)^2 \\ 0 &= 36\end{aligned}$$

It's obvious now, isn't it? There's an issue with applying the square root operation to both sides of an equation, and it's dependent on the fact that $(-x)^2 = x^2$.

When we are looking to solve an equation like $z^2 = x^2$, we have to remember there are two roots of this equation: $z = -x$ and $z = x$. Accordingly, starting from an equation and squaring both sides is a completely logical step (the truth of the resulting equations *follows* from the truth of the original equation), but working the other way is an illogical step (the truth of the squared equation does not *necessarily* tell us that the square-rooted equation is also true). This is an issue with **conditional statements** or **logical implications**, an idea we will discuss in detail later on (in Section 4.5.3). For now, we can summarize this idea with the following line:

If $a = b$ then $a^2 = b^2$, but if $a^2 = b^2$ then $a = b$ or $a = -b$.

This shows why moving from $x^2 + y^2 = 25$ to $x = \sqrt{25 - y^2}$ in the "proof" above is an illogical step: we are immediately assuming one particular choice for the square root when there are two possible options. What would have happened if we had chosen the negative square root there? Try rewriting the proof with the second step reading $-x = \sqrt{25 - y^2}$, instead, and then use the same values for x and y at the end. What happens? What if you use $x = 3$ and $y = -4$ instead? Or $x = -5$ and $y = 0$? Can you describe how to determine when we should use the positive root x and when we should use the negative root $-x$?

Mathematics Uses the "Inclusive Or"

Since this word just arose, let's mention the use of *or* in the sentence above. When we say "$a = b$ or $a = -b$", we mean that *at least* one of the two statements must be true, possibly both. Now, if both $a \neq 0$ and $b \neq 0$, then only one of the concluding statements can be true; that is, in that context, only one of the roots (positive or negative) will be the correct one and not both. If $b = 0$, though, then both of the concluding statements say the same thing, $a = 0$, so it would be illogical to dictate that *or* means only one of the statements can be true and doesn't allow both of them to be true, simultaneously. In other situations, this distinction makes a more marked difference.

For instance, if you order a sandwich at a restaurant and the waiter asks, "Do you want fries or potato salad on the side?", it is understood that you can choose one of those options, but not both. This is an example of the **exclusive *or*** since it excludes you from choosing both options. Alternatively, if you forgot to bring a writing implement to class and are looking for any old way to take notes and ask your friend, “Do you have a pencil or pen I can borrow?”, it is understood that you really don’t care which one of the two options is provided, as long as at least one is available. Maybe your friend has both, and any one of them will do. This is an example of the **inclusive *or***, and this is the interpretation that is assumed in all mathematical examples.

Unclear Arguments

The last two bad “proofs” failed because of issues with precision and logical correctness. The third condition we require of a good proof is that it be *clear*: we want the writing to explain what the proof-writer accomplishes in each step and why that accomplishment is relevant. In other words, we don’t want the reader to stop at any point and ask, “What does that sentence mean?” or “Where did that come from?” or similar questions born from confusion. If it helps, think about writing a proof in terms of explaining it to your friend in your class, or the grader who will be reading your homework assignment, or a family member of similar intelligence. Reread your own writing and try to anticipate any questions that might arise or any clarifications that might be asked of you, and then address those issues by rewriting.

There are several ways that a proof could fail this condition and come across as unclear. For one, the words and sentences might fail to properly explain the steps and motivations of the proof, and this could actually be because there are too many words (obscuring the proof by overburdening the reader) or because there are too few words (not giving the reader enough information to work with) or because the words chosen are confusing (not properly explaining the proof). These are issues with the *language* of the proof.

Mathematically, any number of issues could arise, in terms of clarity. Perhaps the proof-writer suddenly introduces a variable without stating what type of number it is (an integer, a real number, etc.) or skips a few steps of arithmetic/algebra or uses new notation without defining what it means first or ... None of these acts is technically wrong or illogical, but they can certainly cause confusion for a reader. Can you think of any other ways that a proof can be unclear? Try to think of a language-based one and a mathematical one.

Bad “Proof” #3

Let’s state a simple fact about a polynomial function and then examine a “proof” about that fact. Read the argument carefully and try to pinpoint some sentences or mathematical steps that are *unclear*.

Fact: Consider the polynomial function $f(x) = x^4 - 8x^2 + 16$. This function satisfies $f(x) \geq 0$ for any value of x.

“Proof”. No matter what the value of x is that we plug into the function f of x we can write the value that the function puts out by factoring the polynomial,

like this:

$$f(x) = x^4 - 8x^2 + 16 = (x-2)^2(x+2)^2$$

Now, any number z must be less than -2, or greater than 2, or strictly between -2 and 2, or equal to one of them. When $z > 2$ then $z - 2$ and $z + 2$ are both greater than 0 so $f(z) > 0$. When $z < -2$ then both terms are negative and a negative squared is positive so $f(z) > 0$, too. When $-2 < x < 2$, a similar thing happens, and when $x = 2$ or $x = -2$ one of the terms is 0 so $f = 0$. Therefore, what we were trying to prove has to be true. □

What is there to criticize in this proof? First of all, is it correct? Is it precise? Logical? Clear? Where is it unclear? Try to identify the statements, both linguistic and mathematical, that are even slightly unclear, and try to amend them appropriately. Without pointing out any of the individual errors, we offer below a much better, *clearer* proof of the fact above.

Proof. We begin by factoring the function $f(x)$ by considering it as a quadratic function in the variable x^2

$$f(x) = (x^2)^2 - 8x^2 + 16 = (x^2-4)^2$$

Next, we can factor $x^2 - 4 = (x+2)(x-2)$ and rewrite the original function as

$$f(x) = \big((x+2)(x-2)\big)^2 = (x+2)^2(x-2)^2$$

Now, for any real number x, $(x+2)^2 \geq 0$ and $(x-2)^2 \geq 0$, since a squared quantity is always nonnegative. A product of two nonnegative terms is also nonnegative, so $f(x) = (x+2)^2(x-2)^2 \geq 0$, for any value of x. □

What are the differences between the first "proof" and this second proof? Does your rewritten proof look like this second one, as well?

One of the critiques of the first "proof" is that it does not fully explain the situation where $-2 < x < 2$; rather, it merely says that something "similar" happens and does not actually carry out any of the details. This is a common situation in mathematics (where some steps of a proof are "left to the reader") and it is a convenient technique that can sometimes avoid tedious arithmetic/algebra and make reading a proof easier, faster, and more enjoyable. However, it should be used sparingly and with caution. It is important, as a proof-writer, to make sure that those steps do work, even if you are not going to present them in your proof; you should consider providing the reader with a short summary or hint as to how those steps would actually work. Also, a proof-writer should try not to use this technique on steps that are crucial to the ultimate result of the proof.

In this particular case, the actual steps of factoring are skipped completely and the analysis of the case where $-2 < x < 2$ is only mentioned in passing, yet these are essential components of the proof! It is such a short proof, anyway, that showing these steps does not represent a great sacrifice in brevity or clarity. Again, this brings up the point of proof-writing as an art, as much as a science:

choosing when to leave some of the verification of details to the reader can be tricky. In this particular instance, showing all of the steps is important.

That being said, though, the second proof we showed here is much clearer. Moreover, it completely avoids the case analysis that appears in the first "proof"! There was an issue of clarity with one of the cases in the first "proof", but rather than simply expound the details in the amended version, we opted to scrap that technique altogether and use a shorter, more direct proof. Now, this is not to say that the technique of the first proof is incorrect. Were we to fill in the gaps of the argument of the first "proof", we would obtain a completely correct proof. However, some of the steps in that technique are redundant. Notice that the cases where $-2 < x < 2$ and where $x > 2$ are actually identical, in a sense: the factors satisfy $(x-2)^2 > 0$ and $(x+2)^2 > 0$ in both cases. In fact, this is true of the first case, where $x < -2$, as well! So why separate this argument into three separate cases when the same ultimate observation is applied to all three of them? In this case, it is best to combine them into one (also using the knowledge that when $x = 2$ or $x = -2$, one of the factors is 0). Again, using that expanded technique is certainly not incorrect; rather, it just adds some unnecessary length to the proof.

We mentioned the term "case" and the phrase "case analysis" in the above paragraphs without properly defining or explaining what we mean. For now, we want to postpone a discussion of these terms until we thoroughly discuss logic in Chapter 4. If you're itching for immediate gratification regarding this issue, though, you can skip ahead to Section 1.4.4 and check out the "Hungarian friends" problem, which contains some intricate case analyses.

1.2.3 Pick Logic

We have used the word "logical", and its associated forms, quite frequently, already, without fully explaining what we mean by it. We realize this seems to go against the precision and clarity that we have been so strongly advocating thus far, but we also have to admit that, unfortunately, it is extremely difficult to provide a thorough definition of *logic*.

Games

If you're looking for a decent heuristic understanding of logic, try thinking about it in terms of "logic puzzles" like Sudoku or Kakuro. These puzzles/games are built around very specific rules that are established and agreed upon from the very beginning, and then the solver is presented with a starting board and expected to apply those rules in a rigorous manner until the puzzle is solved. For instance, in Sudoku, remembering the conditions that each digit from 1 through 9 must appear exactly once in every row, column, and 3×3 box allows the solver to systematically place more and more numbers in the grid, continually narrowing down the large number of potential "solutions" to find the unique answer that the starting grid of numbers yields. An important aspect of this solving process is that at no time is it necessary (or wise, at that) to *guess*;

every step should be guided by a rational choice given the current situation and the established rules of the puzzle, and within that framework, the puzzle is guaranteed to be solvable (given enough time, of course).

Mathematical logic is a little different, in some respects, but the essence is the same: there are established rules of how to play the game and every move should be guided by those rules and current knowledge, and nothing else. This is what we mean when we say that writing mathematical proofs should be governed by *logic*: every step, from one truth to another, should follow the agreed-upon rules and only reference those rules or already-proven facts. The "game" or "puzzle" that we're playing in a proof (and in mathematics, in general) is not as clear-cut as a Sudoku puzzle. Even more confusing, though, is the idea that sometimes we start playing an unwinnable game and don't realize it!

This idea of an "unwinnable game" is an astounding, surprising, and downright powerful conclusion of the work of mathematician Kurt Gödel, a 20th century Austrian logician. His *Incompleteness Theorems* address an inherent problem with strong logical systems: there can be True statements that aren't *provable* within that system. We are unable to provide a thoroughly detailed explanation of some terms here (namely, *logical system* and *provable*), but hopefully you see that there is something weird going on here. How could this be possible? If something is True in mathematics, can't we somehow show that it is true? How else would we know that it is true?

Some Mathematical History

To begin to address these natural questions, let's step a little further back in time and discuss the beginnings of logic as a full-fledged branch of mathematics. One thing to keep in mind throughout this discussion is that we can't completely address every topic that comes up, and that this may feel dissatisfying, and we understand that. Part of the beauty of mathematics is that learning about any one topic brings up so many other questions and concepts to think about, and these can be addressed, as well, with more mathematics. Context is important, though, and for the context of this book, we just don't have the time and space to address all of these tangentially-related topics. We are not trying to hide anything from you or sweep some issues under the rug; rather, we're just dealing with the reality of making sure we're not forcing you to read 10,000 pages on the entire history of mathematics just to get our point across!

You will probably study many of the people that we mention below (and the work they did) further along in your mathematical careers. At that point, you'll have a deeper understanding and appreciation for the subject built by hands-on experience with the material, and you'll be better-equipped to tackle the issues therein. For now, we are merely introducing these people out of interest. Mathematics has a rich and interesting history, and it helps to be aware of it! Here, we will try to present a concise yet meaningful interpretation of logic—its history, motivations, and meaning—that fits with the current context.

The mathematicians and philosophers in the mid- to late-19th century who first studied the ideas that would evolve into modern logic were interested in many of the same issues we are trying to investigate here: How do we know something is True? How can we express that truth? What types of "somethings" can we even declare to be True or not? Breaking down mathematical language to its very roots, these mathematicians studied ways to combine a fixed set of symbols in very specific ways to create more complicated statements, but in the grand scheme of things, these statements were still rather simple. This is not meant to be a knock against their efforts; one must start somewhere, after all, and these people were working from the ground up.

One of the first major efforts was to investigate the foundations of arithmetic, or the study of the **natural numbers** $(1, 2, 3, 4, \dots)$. Much like Euclid sought to study geometry by establishing a short list of accepted truths, or **axioms**, and then derive truths from these given assumptions, Italian mathematician Giuseppe Peano established a set of axioms for the natural numbers, while others approached the topic from a slightly different viewpoint. Meanwhile, this newfound appreciation for being rigorous and decisive about truths and proving those truths led David Hilbert and others to bring up some issues with Euclid's axioms, specifically the parallel postulate.

This work on geometry and arithmetic naturally led into further, intricate study of other areas of mathematics and fervent attepmts to axiomatize fields like analysis of the real numbers. Karl Weierstrass, in studying this topic, produced some mind-blowing examples of functions with strange properties. For instance, try to define a continuous function that is not differentiable anywhere. (If you're unfamiliar with these terms from calculus, don't worry about it; suffice it to say, it's difficult.) Finally, Richard Dedekind was able to establish a rigorous, logical definition of the real numbers, derived entirely from the natural numbers, and not dependent on some vague, physical notion that a continuum of numbers must exist.

Later on, this study branched off slightly into the study of **sets**, or collections of objects. The groundwork for much of this area was laid by Georg Cantor towards the end of the 19th century. He was the first to truly study the theory of infinite sets, establishing the controversial idea that there are different "sizes" of infinity. That is, he showed that some infinite sets are strictly bigger than other infinite sets. This idea was so controversial at the time, that he was hated by many other mathematicians! Nowadays, we realize Cantor was right. (This also gives you a flavor of what we'll discuss later in Section 7.6. Take this as an intriguing example: the set of odd integers and the set of even integers are the same size, sure, but they are both also the same size as the set of *all* integers. However, the set of all real numbers is *strictly* bigger!)

Indeed, some mathematicians were quite shocked by Cantor's discoveries, and even the great Bernhard Riemann thought the development of set theory would be the scourge of mathematics (at first, anyway). This was not the case, though, and it has flourished since then, with many mathematicians working on ways to represent all of mathematics in just the right way and understand the "foundations" of mathematics. In a way, you can think of set theory as the study of the basic objects that all mathematicians are working with, ultimately, in a way similar to the fact that all of chemistry is done by appropriately combining elements of the periodic table in more and more complicated ways.

A further development from these topics was the study of symbolic logic, which is a bit more concrete than the abstract ideas we've mentioned so far, and whose basic ideas we will be studying frequently in the beginning chapters of this book. This area covers how we can combine mathematical equations and symbols with language-based symbols and connectors to make meaningful mathematical statements that are able to be confirmed as true via a proof. This is an incredibly important component of mathematics, in general, and this book, in particular. Individual viewpoints are certainly more nuanced and specific than this, but, in general, most mathematicians are of the mindset that there are many mathematical truths out there waiting to be discovered and we spend our time learning about the truths we have already uncovered with the hopes of exposing even more of those truths. It's like a giant archaelogical dig, whereby studying the bones and artifacts we've already unearthed will help us to predict what kinds of other treasures we will find and where, which tells us where to look and how to dig once we get there. In a way, logic is that process that is abstracted from the digging by one step: logic is the study of the digging process. It tells us how we can actually take our mathematical knowledge and learn from it and combine it with other knowledge to prove further truths from that.

Now, this is not a precise analogy, mind you, and the study of abstract logic is far more complicated and intricate. For our purposes, in this book, though, this is a sufficiently reasonable way to think of logic. We will learn about some of the first principles and basic operations of symbolic logic and apply this knowledge to our study of writing proofs. It will help us to actually understand what a proof even *is*, it will help guide the construction of proofs that we want to write, it will allow us to critique proofs that may be incorrect, and it will ultimately help us understand just how mathematics works, as a whole.

Applications of Logic: Theoretical Computer Science

One very important application of the ideas and results of logic is in the development and study of computer science, particularly theoretical computer science and computability theory. This particular branch of mathematics was initially motivated by one of David Hilbert's Twenty-Three Problems: this was a list of famously unsolved conjectures in the world of mathematics at the time of their publishing, in 1900. Problem number ten dealt with solving **Diophantine Equations**, which are equations of the form

$$a_1x_1^{p_1} + a_2x_2^{p_2} + a_3x_3^{p_3} + \cdots + a_nx_n^{p_n} = c$$

where $a_1, a_2, \ldots, a_n$ and c are fixed, given constants, $p_1, \ldots, p_n$ are fixed natural numbers, and $x_1, x_2, \ldots, x_n$ are variables that are left to be determined so that they make the equation true.

Given an equation like this, one might wonder whether there are any solutions at all and, if so, just how many there are. Furthermore, if we're given that the fixed constants a_i and c are all rational numbers, we might wonder whether we can ensure that there is a solution where all of the variables x_i are also rational numbers. Some theoretical results have been established regarding this particular problem, but Hilbert's tenth problem, as stated in 1900, asked whether there was "a process according to which it can be determined in a finite number of operations" whether there is a solution to a given equation where all of the variables x_i are rational numbers. They didn't have a proper notion or definition of this term at the time, but what Hilbert was asking for was an **algorithm** that would take in the values of the constants a_i and c and output True or False depending on whether there exists a solution with the desired property. An important part of his question was that this "process" takes a finite number of steps before outputting an answer.

A student at Cambridge in the United Kingdom by the name of Alan Turing began working on this problem years later by thinking of a physical machine that would be executing the steps required to output an answer to the posed problem. Some subsequent publications of his described his invention, what we now call a *Turing Machine*, which is an interesting theoretical device that could be used to answer some problems in formal logic, but also represents many of the ideas that go into building modern computers. We say it's a *theoretical device* because the nature of its definition ensures that it is not physically feasible to build and operate, but it handles some theoretical problems quite well, including the aforementioned tenth problem of Hilbert. More specifically, this machine gave rise to a proper definition for what we mean when we say that something is computable, or able to be determined in a finite number of steps, and this helped to establish a proper notion of an **algorithm**. It would be unfair of us to discuss these topics without also mentioning Alonzo Church, who was working on similar problems at the same time as Turing. Their names, together, are placed on the *Church-Turing thesis* which relates the work of the Turing machine to the more theoretical, formal logic-based notion of computability.

What Will *We* Do with Logic?

While all of these topics in set theory and logic are inherently interesting and immensely important to mathematics, in general, we simply don't have enough time and space to discuss them in detail. Instead, let's focus a bit more on the notions of logic that we'll be using in writing and critiquing mathematical proofs.

We will consider: (1) what kinds of "things" we can actually state and prove, (2) how we can combine "things" that we know to be true to produce more complex truths, and (3) how we can explain how we arrived at the conclusion that those "things" are, indeed, True. For lack of a better term, we say "things" since we don't yet have a formal definition of **mathematical statement**, which is really the type of "thing" that we will be proving. In essence, a mathematical statement is a combination of symbols and sentences from the languages of mathematics and English (in this book, at least) that can be verified as either True or False, but not both or neither. A proof, then, amounts to arranging a sequence of steps and explanations that use true mathematical statements and sentences to connect these truths together and yield the desired truth of a specific statement at the end. Our study of logic will deal with just how we can combine those steps and guarantee that our proof leads to the correct assesment of truth at the end.

More specifically, we will examine what a mathematical statement really is and how we can combine them to produce more complicated statements. The words *and* and *or* will be particularly important there, since those two words allow us to combine two mathematical statements together in new and meaningful ways. We will also look at **conditional** mathematical statements, which are statements of the form "If A, then B" or "A implies B". These are really the bread and butter of mathematical statements and a majority of important mathematical theorems are of this form. These statements involve making some *assumptions* or *hypotheses* (contained in the statement A), and using those assumed truths to derive a *conclusion* (contained in the statement B). Look back at the statement of the Pythagorean Theorem in Section 1.1.1 and notice how it is in the form of a conditional statement. (Could it be written another way? Try writing the statement of the theorem in a non-conditional form and think about whether it is an inherently different statement in that form. Find another famous mathematical theorem that is in the form of a conditional statement and try doing the same change of format.)

Another important idea in mathematics, and one that will show up all the time in proof-writing, is the concept of a **variable**. Sometimes we want to talk about a type of mathematical object in generality without assigning it a specific value and this is accomplished by introducing a variable. You have likely seen this happen all the time in your previous study of mathematics, and we've even done it already in this book. Look again at the Pythagorean Theorem statement in Section 1.1.1. What do the letters a, b, c represent? Well, we didn't state it explicitly, but we know that these are positive real numbers that represent the lengths of the three sides of a right triangle. What triangle? We didn't mention a specific one or point to a specific drawing or anything like that, but you knew all along what we were talking about. Moreover, the proofs we examined didn't depend on what those values actually are, merely that they are positive real numbers with certain properties. This is incredibly useful and important and, in a way, it saves time since we don't have to individually consider *all* possible right triangles in the universe (of which there are infinitely-many!) and can reduce the whole idea into one compact statement and proof.

One thing we can do with variables is **quantify** them. This involves making claims about whether a statement is true for *any* potential value of a variable, or maybe for just *one* specific value. For instance, in the Pythagorean Theorem, we couldn't claim that $a^2 + b^2 = c^2$ for any positive real numbers a, b, c; we had to impose extra assumptions on the variables to obtain the result we did. This is an example of **universal** quantification: "For *all* numbers a, b, c with this property and that property, we can guarantee that ..." Similarly, we can quantify **existentially**: "There *exists* a number n with this property."

Can you think of a theorem/fact that we have examined so far that uses existential quantification? Look again at the proof that there are irrational numbers a and b such that a^b is rational. Notice that this claim we proved is of the existence type: we claimed that *there are* two such numbers with the desired properties, and we then proceeded to show that there must, indeed, be those numbers. Now, the interesting part of that proof was that it was *nonconstructive*; that is, we were able to prove our claim without saying what the numbers a and b actually are, explicitly. We narrowed it down to two choices but never made a claim as to which one is the correct choice, merely that one of the pairs *must* work.

1.2.4 Obvious Obfuscation

As a preview of these logical concepts that we'll be examining in mathematical detail later on, let's take some real-world, language-based examples of these ideas.

Conditional Statements

First, let's investigate **conditional statements**. Mathematical theorems frequently take the form of a conditional statement, but these types of statements also appear in everyday language all the time, sometimes implicitly (which can only add to the confusion). For instance, people talk sometimes about what they would do with their lottery winnings, saying something like

> If I win the lottery, then I will buy a new car.

The idea is that the second part of the statement, after the "then", is dependent on the first part of the statement, which is associated with the "if". When the conditions outlined in the "if" part are satisfied, the actions outlined in the "then" part are guaranteed to take place.

The part of a conditional statement associated with the "if" is known as the **hypothesis** (or sometimes, more formally, the **antecedent**). The part associated with the "then" is known as the **conclusion** (or, more formally, the **consequent**).

Sometimes the conclusion of the conditional is more subtle, or the verb tenses in the sentence are such that it doesn't even include the word "if". Take the following quote from the film *Top Gun*, for example:

> It's classified. I could tell you, but then I'd have to kill you.

The idea here is that the first part, "I could tell you", is a hypothesis in disguise. The sentence *"If I told you, I would have to kill you"* would have the same logical meaning as the actual film quote; however it doesn't convey the same forceful, dramatic connotations. It's quite common to actually not include the word "then" in the conclusion of a conditional statement; while reading the sentence, you might even add the word in your mind without realizing. Take the following lyrics from a song by the band The Barenaked Ladies, say:

> If I had \$1,000,000, we wouldn't have to walk to the store.
> If I had \$1,000,000, we'd take a limousine 'cause it costs more.

Both lines are conditional statements, but neither includes the word "then"; it is understood to be part of the sentence.

Compare these examples to the following sentence and see what's different:

> I carry an umbrella only if it is raining.

The idea here is that the speaker would hate to carry an umbrella around for no good reason, preferring to make sure it would be of use. Does this sentence have the same meaning as the following, similar sentence?

> If I am carrying an umbrella, it is raining.

In modern language usage, the notion of conditional can be a little fuzzy. The first sentence could be interpreted to mean that sometimes it might be raining but the speaker forgets to bring an umbrella, say. The second sentence is a clear assertion of a conditional statement: seeing me walking around with an umbrella lets you necessarily deduce this is because it's raining. In mathematics, we associate these two sentences and say they have the same logical meaning.

This motivates the meaning of the phrase "only if" and, subsequently, the phrase "if and only if". Consider the following two sentences:

> I will buy a new car if I win the lottery.
> I will buy a new car *only if* I win the lottery.

The first one says that winning the lottery guarantees I will buy a new car, whereas the second one says that the act of buying a new car guarantees that it is because I just won the lottery. If both of these sentences are true, then the events "winning the lottery" and "buying a new car" are equivalent, in a sense, because the occurrence of each one *necessarily guarantees* the occurrence of the other.

Accordingly, mathematical definitions commonly use the phrase **"if and only if"**. For example, we might write "An integer is even if and only if it is divisible by 2." This indicates that knowing a number has that property allows us to call it "even", and knowing a number is even allows us to conclude the divisibility property. (Sometimes, though, a definition will just use *if*, with the *only if* part left unstated but understood. You may have noticed that we did this with the definition of prime numbers in Section 1.1.2.)

Creating More Conditional Statements from Others

Starting with a conditional statement, we can modify it slightly to produce three other conditional statements with the same content but different structure. Continuing to use the "lottery/car" example, let's consider the following four versions of the original sentence:

1. If I win the lottery, then I will buy a new car.
2. If I bought a new car, then I won the lottery.
3. If I don't win the lottery, then I won't buy a new car.

4. If I didn't buy a new car, then I didn't win the lottery.

How do these sentences compare? Do any of them have the same logical meaning as each other? Are all of them True, necessarily, assuming the truth of the first one? We would argue that, in this case, sentence two could be False, even if the first sentence is True. Perhaps I got a hefty raise at work or inherited some money and decided to buy a new car. What about sentences three and four, though? Can they be associated with the others somehow? We will leave this for you to discuss and explore on your own. It might be interesting to ask the same questions of some of the other conditional statements we've looked at and see if your answers are different, too.

One final example of a conditional statement we'll mention comes from a joke by standup comedian Demetri Martin.

> I went into a clothing store and a lady came up to me and said, "If you need anything, I'm Jill." I've never met anyone with a conditional identity before. "What if I don't need anything! Who are you?"

This should give you a flavor for the ways that conditional statements in modern language can be imprecise or subtle, and sometimes open to interpretation. In mathematics, we want these types of statements to be rigorous, well-defined, and unambiguous. This is something we will investigate further later on in Section 4.5.3. For now, though, it might help to think of these types of statements in the rigorous way in which a computer algorithm would interpret an `if` ... `then` statement. When the conditions of the `if` part are satisfied, the subroutine is executed, and they are ignored otherwise. Likewise, a `while` loop is merely a sequence of `if` ... `then` statements condensed into one, concise form.

Quantifiers

Next, let's examine some examples of **quantifiers**. We will use quantifiers when there is an unknown variable meant to be an object drawn from a collection of possible values or representations. For instance, when we quantified the variables a, b, c in the statement of the Pythagorean Theorem, they were drawn from the collection of real numbers that represent the side lengths of right triangles. For a non-mathematical example, consider the following sentence:

> Every person is loved by someone.

What are the variables here? How are they quantified? Be careful because, yes, there are in fact two quantifications in this sentence, one for each of two separate variables. In both cases, the variables represent a member of the collection of all people in the world, and the first variable is quantified universally while the second one is quantified existentially. That may sound confusing, so let's try rewriting the sentence more verbosely:

> For every person x in the world, there exists another person y with the property that person y loves person x.

Do you see how this has the same logical meaning as the first sentence? Surely, this one is unnecessarily wordy and precise for a conversation, but we present it here to show you the underlying variables and quantifiers. The key phrases for the quantifiers are *"for every"* (universal) and *"there exists"* (existential).

The Order of Quantification Matters!

Now, let's look at a similar sentence as the last example:

> Someone is loved by every person.

This sentence is quite similar to the one above; it has all of the same words, even! What did the change in word order do to the logical meaning of the sentence? Well, there are still two variables and two quantifiers, one universal and one existential, but the order in which those quantifiers are applied has been switched. The verbose version of this sentence reads:

> There exists a person x with the property that, for every person y in the world, person y loves person x.

This has a completely different meaning from the first sentence! The first one seemed believable but this one is almost outlandish. This should give you an idea of how important it is to keep the order of quantification straight so that you are actually saying what you mean to be saying.

Nested Quantifiers

The following examples illustrate how our brains can sometimes process quantifiers in language-based sentences fairly quickly and easily, even when the interconnectedness might make it difficult to understand. When quantifiers follow one after the other, we call them *nested*.

The ability to analyze and udnerstand such sentences might depend on the context of the sentence and the message it is trying to convey. If the message makes sense and we believe it, it can be easier to grasp. The best example we know of this phenomenon is embodied by the following quote, attributed to the great presidential orator Abraham Lincoln:

> You can fool some of the people all of the time, and all of the people some of the time, but you can not fool all of the people all of the time.

There are quantifiers all over the place here! We are talking about the collection of all people and the collection of instances in which certain people are fooled, and quantifying on those collections. Try to write this sentence with a few different wordings to see if it can sound any "simpler" or more concise.

Could there be another way to phrase the sentence that would remove some (or all) of the quantifiers without altering the meaning?

Finally, out of personal interest and to inject a bit of humor, we'll mention a similar quote that comes from Bob Dylan's song "Talkin' World War III Blues", from his 1963 album *The Freewheelin' Bob Dylan*:

> Half of the people can be part right all of the time
> Some of the people can be all right part of the time
> But all of the people can't be all right all of the time
> I think Abraham Lincoln said that

We will discuss these topics in greater detail later on, where we will examine their mathematical motivations, meanings, and uses. For now, we can't stress enough how important these issues are in writing proofs. Stringing together a bunch of sentences with no way of knowing how they're connected is not a proof, but a properly-structured series of logical statements and implications is exactly what we're looking for.

1.3 Review, Redo, Renew

Thus far, we have sought to motivate and explain mathematical reasoning and proof-writing from a logical standpoint but, along the way, we have used some mathematical concepts and techniques with which you may or may not be familiar. It is important, of course, to think logically and rationally when doing mathematics, but this is only part of the bigger picture. We have tried to explain how to organize mathematical ideas and structure them in a meaningful way that can convince others of a specific fact, but those ideas must contain some mathematical concepts related to that fact!

For instance, we couldn't have looked at any of the proofs of the Pythagorean Theorem without having a rudimentary understanding of geometry: what a triangle is, some basic properties of triangles and lines and angles, etc. What else did we assume the reader would understand? Many of the steps involved arithmetic, like manipulating multiple equations by multiplying through by the same factor or subtracting two equations, and so on. Those ideas may be second-nature to you now, but at some point you had to learn these things and see why and how they actually worked so that you could safely and appropriately use them in the future.

Look back over some of the other proofs we looked at in the previous sections. What mathematical ideas did we use? Try to write down a few and think about when and how you learned about them. Try to write down some specific facts that we may have used without explicitly saying so and think about why we would do that. Also, try to find a few instances where we made a claim but didn't necessarily fully explain why it must be True, and try to do that. For instance, in "Proof 1" of the Pythagorean Theorem, we drew four identical triangles inside a square and then said that the figure inside would also be a square. Is this really True? How can we be so sure? Try to prove it!

Presumed Knowledge

The main point is that we can't actually write proofs without imbuing them with some meaningful mathematical content. Accordingly, one of the main goals of this book is to share some interesting mathematical facts with you. Sometimes, this involves working with objects you already know about and have seen before (like triangles or prime numbers) and trying to do new things with them. Other times, we may be introducing you to completely new mathematical objects (like equivalence relations or binomial coefficients) and working with those. What we'd like to do now is discuss some mathematical objects and concepts that we will use rather frequently and that you might have seen before. We aren't necessarily assuming that you've seen all of these, but none of these ideas are too hard to learn/relearn quickly, and they will be quite useful throughout the remainder of this book, and the remainder of your mathematical life, as well! We've included a handful of problems for you to work on to give you some practice, both throughout this section and at the end of it.

1.3.1 Quick Arithmetic

We won't be expecting you to multiply six digit numbers in your head or anything like that, but being able to manipulate "small" numbers via addition, subtraction and multiplication is an important skill. Sure, calculators and computing programs can be helpful, but we hope that it isn't necessary to run off to `Maple` or `Mathematica` or your `TI-89` whenever we need to add a couple of four digit numbers, say. Technology provides us with many conveniences in the form of accuracy and time-efficiency but when we rely on these devices too heavily, we diminish our ability to verify those answers we get (in the event of a typo or missed keystroke, for instance) and when we use them too frequently, we may not actually save any time at all!

We encourage you to continually try to perform any arithmetic steps we face either in your head or on a piece of scrap paper. It will be fairly infrequent that any problems/puzzles involve arithmetic with "large" numbers and even when they do, there may be a special trick that can reduce the problem to something easier. For instance, try to work on the following series of problems and see what you notice.

Problem 1.3.1. For each of the following multiplications, try to identify the final digit of the resulting number. If your answer is "0" then try to identify how *many* zeroes are at the end of the resulting number.

1. $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$
2. $1 \cdot 2 \cdot 3 \cdot \dots \cdot 10$
3. $1 \cdot 2 \cdot 3 \cdot \dots \cdot 25$
4. $1 \cdot 2 \cdot 3 \cdot \dots \cdot 100$
5. $1 \cdot 2 \cdot 3 \cdot \dots \cdot 1000$

6. $1 \cdot 2 \cdot 3 \cdot \cdots \cdot 10000$
7. $1 \cdot 2 \cdot 3 \cdot \cdots \cdot 10^9$

Try to write down a few sentences that would explain to a friend the procedure you used above. That is, given any number n, explain how to identify the number of zeroes at the end of the number resulting from multiplying $1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$

What did you notice? Did you use your calculator for the first few? Surely that would work, or you could even do the first two or three by hand, but how did that help you later on? How did that help you to explain your procedure? Certainly, you needed to find a more general way of figuring out how to tackle this problem, and resorting to a calculator or computer might help you in some cases, but it won't provide you with any insight into the answer.

If you haven't figured out a general procedure, we'll give you this:

Hint: Think about how many multiples of 2 and how many multiples of 5 appear in the multiplication. Try to pair them together. (Why would you want to do that?)

1.3.2 Algebra Abracadabra

The term **algebra** has a couple of meanings in the mathematical world with some different nuances to each. Usually, the term brings to mind manipulating equations with variables and trying to find a numerical solution for them. This is probably how you handled word problems in a high school algebra class. More generally, though, **abstract algebra** is a branch of mathematics that studies certain mathematical structures that have specific properties, oftentimes having no relation to integers or real numbers.

Much of the groundwork for this field was laid by mathematicians before the 19th century who were seeking roots of polynomial equations where the variables were raised to the third or fourth or even higher powers. For a quadratic equation (containing a variable raised to the second power), you probably remember the formula for finding a root of the equation (i.e. a value for the variable that will make the expression evaluate to zero); this is the famous *Quadratic Formula*.

Did you also know there is a procedure for finding the root of an expression involving a variable that is cubed? Or even raised to the fourth power? Interestingly enough, the mathematicians working on this general problem discovered that there are *no* such procedures possible for higher powers! A lot of the concepts and structures they were working with developed into some inherently interesting mathematics, and people have been studying those objects ever since, eventually branching off and working with the underlying properties of those objects, stripping away the numerical context of finding roots of equations. This is usually what a mathematician means when he/she says "algebra".

In this particular context, though, we will be using "algebra" in the sense that you're likely thinking of it: manipulating multiple equations and variables to obtain numerical values for the variables that make the expressions evaluate to numbers that satisfy all of the equations involved. There is actually a rich and wonderful theory behind solving systems of linear equations, but this type of in-depth study is better suited for a course on matrix algebra (also called linear algebra). For now, we'll look at a couple of handy tricks and then let you practice them.

Solving Systems of Linear Equations

A system of linear equations is just a collection of equations involving a certain number of variables (all raised to the first power, hence *linear*) multiplied by coefficients and added together, and set equal to some constants. There are specific conditions on the coefficients and constants that guarantee whether or not a solution exists (and whether there are infinitely many or just one, in fact) but we won't get into those specific details. Suffice it to say that the systems of equations we will have to handle in this book will have unique solutions, and this means that the number of equations we have will be the same as the number of variables involved. Knowing that ahead of time, how do we manipulate a system of equations to find that unique solution?

In practice, the most time-efficient way of solving a system depends on the coefficients and constants, as well, and perhaps spotting a particular way of applying the methods we are about to explain. That said, simply following these methods will always work in a short amount of time, anyway, so don't be too concerned with finding the absolute shortest method in any given case.

Method 1: The first method involves a system of two equations and two unknowns. In this case, we can use one of the equations to express one variable in terms of the other, then substitute this into the second equation, yielding one equation and one unknown. From that, we can find a specific value for one variable, and substitute this back into the first equation to find a specific value for the other variable, thereby obtaining the solution we wanted. Let's see this process in action with a particular example. Consider the system of equations below:

$$\begin{aligned} 7x + 4y &= -2 \\ -2x + 3y &= 13 \end{aligned}$$

Following the method we just described, we would rearrange the first equation to write y in terms of x

$$y = \frac{1}{4}(-2 - 7x)$$

then substitute this into the second equation

$$-2x + 3 \cdot \frac{1}{4}(-2 - 7x) = 13$$

and solve that new equation for x:

$$\begin{aligned} -2x - \frac{3}{2} - \frac{21}{4}x &= 13 \\ -\frac{29}{4}x &= \frac{29}{2} \\ x &= -2 \end{aligned}$$

Then, we would use this value in the first equation and solve for y:

$$\begin{aligned} 7 \cdot (-2) + 4y &= -2 \\ 4y &= -2 + 14 = 12 \\ y &= 3 \end{aligned}$$

Therefore, the solution we sought is $(x, y) = (-2, 3)$.

What if we had used the value of x we found in the second equation instead of the first? Well, it would produce the same value of y, but maybe the arithmetic would have been slightly quicker. Or, what if we had done it the other way around, and expressed x in terms of y, solved for y, then went back and solved for x? Again, we would have found the same solution, but perhaps the numbers would work out more "nicely" and save us a few seconds of scratch work. This is what we mean by not worrying about finding the most "efficient" method. Sure, there are multiple ways to approach this system of equations, but they ultimately stem from the same method (substitute and solve) and yield the same solution.

Method 2: An alternative way to handle a system of two equations and two unknowns is to multiply both equations through by particular values and then add them together, choosing those multipliers appropriately so that one of the variables is eliminated. Using the example from above, we could multiply the first equation by 2 and the second equation by 7, making the coefficient of x in both equations equal yet opposite; then, adding the equations reduces the system to one equation and one unknown, just y. Observe:

$$\begin{aligned} 2 \cdot \big(7x + 4y &= -2\big) \\ 7 \cdot \big(-2x + 3y &= 13\big) \\ 14x + (-14x) + 8y + 21y &= -4 + 91 \\ 29y &= 87 \\ y &= 3 \end{aligned}$$

From there, we can substitute this value into the first or second equation and solve for x.

You can use either of these approaches to handle any system of two equations and two unknowns. Perhaps one would be slightly quicker than the other, depending on the numbers involved, but you won't be saving more than a minute either way, so we encourage you to just choose one and work through it.

Method 3: It can sometimes be convenient to interpret these systems of equations graphically; this is not usually an efficient way of identifying a specific solution to the system, but it can give an indication of whether a solution exists and a rough estimate of the magnitude of the values of the solution.

With two unknowns, we can interpret an equation like $ax + by = c$ in terms of a line in the plane by rearranging: $y = -\frac{a}{b}x + \frac{c}{b}$. This is the line with slope $-\frac{a}{b}$ and y-intercept $\frac{c}{b}$. Given two such equations, we can draw two lines in the plane and locate the point of intersection visually. The (x, y) coordinates of that point are precisely the solution we would find by solving the system of equations as we described above.

This visual method also applies to a system of three equations and three unknowns, but this requires drawing lines in three-dimensional space. This can be difficult to do in practice, but is technically achievable. These same concepts also apply to larger numbers of equations and unknowns, but drawing "lines" in four or more dimensions is impossible for us human beings to visualize!

More than two variables: Reduce! The next part of this method builds upon the first by taking a system of more than two equations (and unknowns) and continually reducing it to smaller systems, eventually obtaining a system of two equations and two unknowns, where we can apply the first part of the method. We will illustrate the method by considering a system of three equations and three unknowns, like the one below:

$$\begin{aligned} 6x - 3y + z &= -1 \\ -3x + 4y - 2z &= 12 \\ 5x + y + 8z &= 6 \end{aligned}$$

The first goal is to eliminate one of the three variables. In essence, this can be done in one of two ways, much like the method for two equations and two unknowns. Let's say we're going to try to eliminate z from the system; we can try to express z in terms of x and y and substitute somehow, or we can multiply some equations and add them together to cancel the coefficients of z. The only difference here is that, whichever option we choose, we need to do it twice. Let's use the first equation to write

$$z = -6x + 3y - 1$$

After substituting this expression for z into both the second and third equations, we will have a system of two equations and two unknowns.

One way to think about this is that we need information from all three equations to ultimately arrive at an answer, and in reducing the system to two equations, we need to somehow retain information from all three of the original equations. The expression we have for z came from the first equation, so we need to subtitute it into the other two to retain all of the information we need.

Compare this to the following sequence of steps: rearrange the first equation to isolate z and substitute this into the second equation, then rearrange the second equation to isolate z and substitute this into the first equation. What happens? The intuition is that we have somehow "lost" information from the third equation and, yes, we will obtain a system of two equations and two unknowns, but it will have insufficient information to yield a unique solution for x and y. If you actually perform the steps we just described (try doing this to check our work), you obtain the following "system" of two equations after minimal simplification:

$$\begin{aligned} 9x - 2y &= 10 \\ \frac{9}{2}x - y &= 5 \end{aligned}$$

These are really the same equation! Accordingly, we wouldn't actually be able to solve them for unique values of x and y.

Let's return to where we were and substitute the expression for z above into the second and third equations

$$\begin{aligned} -3x + 4y - 2 \cdot (-6x + 3y - 1) &= 12 \\ 5x + y + 8 \cdot (-6x + 3y - 1) &= 6 \end{aligned}$$

and then simplify

$$\begin{aligned} 9x - 2y &= 10 \\ -43x + 25y &= 14 \end{aligned}$$

Applying one of the methods from the first problem will give us the solution $(x, y) = (2, 4)$. Having *both* of these values in hand, we can now return to any one of the original three equations and solve for z; better yet, we can just use the isolated expression for z we found already from the first equation:

$$z = -6x + 3y - 1 = -6 \cdot (2) + 3 \cdot 4 - 1 = -12 + 12 - 1 = -1$$

More than two variables: Reduce another way! Another way to reduce a system from three equations to two equations is related to the "multiply and add" method from before, but we still have to be careful about ensuring that we retain information from all three equations. Using the same system of three equations from above, we might notice that after multiplying the first equation by 8 and the second equation by 4, the coefficient of z in all three equations is either ± 8. This allows us to add/subtract the equations in a convenient way to reduce the system to two equations and two unknowns. Specifically, let's do the multiplication we just mentioned

$$\begin{aligned} 48x - 24y + 8z &= -8 \\ -12x + 16y - 8z &= 48 \\ 5x + y + 8z &= 6 \end{aligned}$$

and then add the first equation to the second

$$\begin{aligned} (48x - 12x) + (-24y + 16y) + (8z - 8z) &= -8 + 48 \\ 36x - 8y &= 40 \end{aligned}$$

and the second equation to the third

$$\begin{aligned}(-12x + 5x) + (16y + y) + (-8z + 8z) &= 48 + 6 \\ -7x + 17y &= 54\end{aligned}$$

This produces two equations involving only x and y; furthermore, we have combined information from all three original equations to produce these, so we can be assured that we haven't "lost" anything. Solving this new system

$$\begin{aligned}36x - 8y &= 40 \\ -7x + 17y &= 54\end{aligned}$$

via any of the previous methods we discussed produces the solution $(x, y) = (2, 4)$. Substituting these values into any of the three original equations and solving for z produces the ultimate answer we sought.

We could have performed similar steps to eliminate y from the system of three equations, too; for instance, we could add 4 times the first equation to three times the second, and subtract 4 times the third equation from the second. Any of these methods would produce the same ultimate answer, but some of them may shorten the arithmetic steps or involve "nicer" numbers (i.e. fewer fractions, smaller multiplications, what have you). Solving a system with more equations amounts to the same general procedure: multiply the equations and add to eliminate one variable from the system and continue doing this until there are only two equations and two unknowns; then, solve for the values of those two variables and work backwards, substituting those values to solve for the values of the variables that had been eliminated.

Algebra Practice

Problem 1.3.2. Solve the following system of equations for (x, y, z):

$$\begin{aligned}x + y + z &= 15 \\ 2x - y + z &= 8 \\ x - 2y - z &= -2\end{aligned}$$

Now, solve this similar system for (x, y, z):

$$\begin{aligned}x + y + z &= 15 \\ 2x - y + z &= 9 \\ x - 2y - z &= -2\end{aligned}$$

Compare the changes in the values of x, y, and z between the two systems.

Which variable changed the most? The least? What is the ratio of these changes?

How large/small can you make this ratio by changing the constant on the right-hand side of the second equation of the system?

Problem 1.3.3. A father, mother and son were sitting in a restaurant eating dinner, when they were approached by another family consisting of a father, mother and son. This second family was struck by their resemblance to the first family, so the second father asked the first, "How old are the three of you? I'm guessing we are all about the same age". The first father happened to be a mathematician and did not feel like giving away his family member's ages so easily, and thus "revealed" them to the others in a tricky way. He said, "Well, our current ages combine to make 72, and I happen to be six times as old as my son. However, in the future when I am just twice his age, our combined age will be twice our current combined age. How old do *you* think we are?"

How old are the three family members?

1.3.3 Polynomnomnomials

Sometimes we will need to work with variables that are squared or cubed or raised to even higher powers. In general, a **polynomial** is the term we use for a function that has one or more variables raised to integer powers, multiplied by coefficients, and added together. Here are some examples of polynomials:

$$x^2 - 7x + 1, \quad 7p^6 + 5p^4 + 3p^2 + 2p, \quad \frac{1}{2}z^2 + 9y^2z - 2y + z^3y^2 - 7z$$

These types of functions are quite common and popular in mathematics, partly due to their convenient properties and partly due to their prevalence in nature. We will see them appear throughout this book. For now, though, let's focus on polynomials that only have *one input variable*.

Roots of Polynomials

Sometimes, we will define a polynomial function in the context of a puzzle and wonder whether there are any values for the input variable that make the ouput value 0. These input values are called **roots** of the polynomial.

One way to identify roots of a polnyomial is to **factor** it into linear terms; that is, we try to express the function as a series of multiplications instead of additions, since we can declare that (at least) one of the factors must be 0 to achieve a 0 value. The motivation behind this technique relies on the following fact:

> **Fact**: If a and b are real numbers and $ab = 0$, then $a = 0$ or $b = 0$ (or possibly both).

Example 1.3.4. Let's see a specific example. Let's try to factor the following polynomial:

$$p(x) = x^2 + 6x + 8$$

(It is common notation to define polynomials as $p(x)$, where p stands for polynomial, x is the input variable, and $p(x)$ is the output value corresponding to the input value x. This doesn't have to be the case, though.)

You might notice that

$$p(x) = x^2 + 6x + 8 = (x + 4) \cdot (x + 2) = (x + 4)(x + 2)$$

(It is also fairly common to drop the $\cdot$ when there are factors separated by parentheses, so we will adopt that convention from here on out, as well.)

The reason this factorization works is because we are applying the distributive property multiple times, in reverse. If we were to expand the factorization we just found, explicitly showing every step, it would look like:

$$\begin{aligned} p(x) &= (x + 4)(x + 2) \\ &= x(x + 2) + 4(x + 2) \\ &= (x^2 + 2x) + (4x + 8) \\ &= x^2 + 2x + 4x + 8 = x^2 + 6x + 8 \end{aligned}$$

All we really did to write down the factorization was to notice that the terms $+4$ and $+2$ have product $+8$, which is the constant term, and they have sum $+6$, which is the coefficient on the x term. Knowing how the subsequent expansion of those factors would work out allows us to write down that factorization without really checking it.

Factoring Quadratics

Let's take what we did with that specific example and try to generalize to any quadratic function. If we want to factor a quadratic polynomial like

$$p(x) = x^2 + bx + c$$

we seek values r and s so that $r \cdot s = c$ and $r + s = b$. Usually, we can do this "by inspection", or by just staring at these two equations and thinking for a minute to come up with the appropriate values. (That's what we did with the last example!)

What do we do if the coefficient of the x^2 is not 1 but some other number a? Well, notice that if we can factor the polynomial $\frac{p(x)}{a} = x^2 + \frac{b}{a}x + \frac{c}{a}$, then we can find a factorization of the original polynomial $p(x)$, as well, by just multiplying by a. This won't affect our ability to find roots of the polynomial (our original goal), because we're assuming $a \neq 0$ (otherwise we didn't really have a quadratic polynomial to begin with and wouldn't need to factor it). Once we've found this factorization, it's easy to identify the roots of $p(x)$; since we want to figure out when $p(x) = 0$, we can just use the factorization and the fact we mentioned above to conclude that

$$\begin{aligned} 0 = p(x) = (x + r)(x + s) \quad &\text{implies} \quad x + r = 0 \text{ or } x + s = 0 \\ &\text{which implies} \quad x = -r \text{ or } x = -s \end{aligned}$$

That is, the roots must be $-r$ and $-s$.

What if we have a polynomial of the form $p(x) = x^2 - a^2$? This particular type of function is known as a **difference of squares**, and has a quick factorzation trick. This is a quadratic polynomial so, following the method from above, we would seek values r, s such that $rs = -a^2$ and $r + s = 0$ (since there is no x term in $p(x)$). The second constraint tells us $r = -s$ and using this in the first constraint tells us $r^2 = a^2$. Thus, using $r = a$ and $s = -a$ achieves the factorization $p(x) = (x - a)(x + a)$ and so the roots are $\pm a$. (Notice that using $r = -a$ and $s = a$ also satisfies both constraints, yet it actually yields the same factorization of $p(x)$.)

Similar tricks can sometimes be applied to polynomials of higher **degree** (recall that "degree" means the highest power of the input variable). For instance, the following polynomial has degree 4

$$p(x) = 4x^4 - x^2 - 3$$

but we can factor it easily if we define $y = x^2$ and write it as a quadratic polynomial

$$p(y) = 4y^2 - y - 3 = (4y + 3)(y - 1)$$

Notice that you can think about the factorizations of the coefficients of the y^2, y, and constant terms to jump right to the factorization we found, or you can follow the division trick we mentioned. Here, we would want to factor $\frac{p(y)}{4} = y^2 - \frac{1}{4}y - \frac{3}{4}$, so we need $rs = -\frac{3}{4}$ and $r + s = -\frac{1}{4}$; using $r = -1$ and $s = +\frac{3}{4}$ works, so we obtain the factorization

$$\frac{p(x)}{4} = (y + (-1))\left(y + \frac{3}{4}\right)$$

which can be simplified as

$$p(x) = 4(y - 1)\left(y + \frac{3}{4}\right) = (y - 1)(4y + 3)$$

which is exactly what we had before.

A Root Yields A Factor

Of course, this trick of identifying roots can work in reverse, too: if we can easily spot a root of a polynomial, that can help us in identifying one of the factors. As an example, look at the cubic polynomial below and see if you can find a root "by inspection"; that is, see if you can find an input value for x that will make $p(x)$ evaluate to zero:

$$p(x) = x^3 - 3x + 2$$

If you haven't spotted it yet, you might want to try plugging in some "easy values", like the first few integers (both positive and negative) to see what happens. If you do so, you'll find that $p(1) = 1 - 3 + 2 = 0$. Accordingly, we know that a factorization of the polynomial p should include the factor $(x-1)$, since this corresponds to the root $x = 1$. Knowing this, we want to divide $p(x)$ by the factor $(x-1)$ so that we can further factor that quotient and identify all of the roots of p.

Polynomial "Division"

How do we divide polynomials, though? We seek another polynomial $q(x)$ so that $p(x) = q(x) \cdot (x-1)$, or in other words, we need to find $\frac{p(x)}{x-1}$. One way to identify such a function is by using the same principles of **long division** that you learned all about in middle school when you were dividing integers. The same concepts apply to polynomial functions! Think back to how long division works, and try working through some basic examples— like $22 \div 7$, say—to refresh your memory about how it works.

Now, let's try to apply those same principles to polynomials. Here's an example of the idea of long division applied to $\frac{x^3-3x+2}{x-1}$:

$$
\begin{array}{r|rrrr}
 & x^2 & +x & -2 & \\
\hline
x-1 & x^3 & & -3x & +2 \\
 & -x^3 & +x^2 & & \\
\cline{2-3}
 & & x^2 & -3x & \\
 & & -x^2 & +x & \\
\cline{3-4}
 & & & -2x & +2 \\
 & & & 2x & -2 \\
\cline{4-5}
 & & & & 0
\end{array}
$$

In each iteration of the method, we try to find the largest "factor" that can "go into" the larger term. In this case, these are just multiples of powers of x; we identify the largest power of x that can "go into" the current term in question. Since the dividend has x^3 and the divisor has x, we write x^2 above the division line. Then, we multiply $(x-1)$ by x^2, write this below the dividend, and subtract to find the remainder.

We repeat the same process until we have a constant term above the division line (i.e. a multiple of x^0) and see the remainder. Since the remainder here is 0, we know that we have a factorization with no remainder. We can then factor the resultant quadratic by noticing that $r = 2$ and $s = -1$ satisfy $r + s = 1$ and $rs = -2$, so we can finally write

$$p(x) = (x-1)(x-1)(x+2) = (x-1)^2(x+2)$$

Accordingly, the roots of $p(x)$ are $x = 1$ and $x = -2$. For this function, the degree of the polynomial is 3 but the function has only 2 roots. Does this strike you as odd? Can you think of a polynomial of degree 3 that has only 1 root? How about a polynomial of degree 3 with no roots? What about 4 roots, or 5 or more? Are any of these possible? Why or why not? What if we were working with a polynomial of degree 4? Of degree n? What can you say for sure about the number of roots a polynomial has, relative to its degree?

Expanding Factors

Sometimes, when working on a puzzle, we start from a factorization of a polynomial and want to expand the factors completely so we can identify the coefficient of a particular term. How can we quickly and easily multiply polynomials together? In essence, we are trying to apply the distributive law over and over without having to write out all of the steps (although that thorough, step-by-step procedure is guaranteed to work, so if you are unsure of your answer, it is always a good idea to go back and check each step thoroughly).

One particular instance where we can reduce the number of steps involved is when we need to expand a factorization like $(a+b)^n$, where a and b represent any constant or variable and n is an integer. In this specific situation, there is a convenient way to identify the coefficients of the expanded polynomial, and those values come from **Pascal's Triangle**.

This is an arrangement of rows of integers into a triangular shape, where each row corresponds to a particular value of n in such an expansion. The trick to generate Pascal's Triangle is to write the first two rows as all 1s, and the outside "legs" of the triangle as all 1s. In the interior of the triangle, any entry is filled in by finding the sum of the two entries immediately above that entry, to the left and to the right. Try generating the first few rows of the triangle yourself and compare to the one below to make sure you've done the procedure correctly.

$n=0$:					1				
$n=1$:				1		1			
$n=2$:			1		2		1		
$n=3$:		1		3		3		1	
$n=4$:	1		4		6		4		1

We've written the n values on the left side to indicate the correspondence with the original problem of expanding $(a+b)^n$. In general, any term of the expansion will be some coefficient (taken from the triangle) times $a^k b^{n-k}$ for some value of k between 0 and n; that is to say, in every term of the expansion, the sum of the powers of a and b in that term must be n. The numbers in any given row of the triangle are written in an order corresponding to decreasing powers of a, so that the first 1 is the coefficient of a^n, the next number is the coefficient of $a^{n-1}b$, and so on.

If we were faced with expanding $(a+b)^2$, we would read the $n=2$ row of Pascal's Triangle and see that the coefficients should be $1, 2, 1$, and that these are the coefficients for a^2, ab, b^2, respectively. Thus,

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

which we could have also accomplished fairly easily by just expanding by hand. What if we were faced with expanding $\left(x^2+2\right)^4$, say? This isn't done as quickly by hand, so let's see what happens if we use Pascal's Triangle. The $n=4$ row tells us the coefficients of $a^4, a^3b, a^2b^2, ab^3, b^4$ are $1, 4, 6, 4, 1$, respectively, where $a = x^2$ and $b = 2$. Thus, we can write

$$\begin{aligned}
\left(x^2+2\right)^4 &= 1 \cdot \left(x^2\right)^4 + 4 \cdot \left(x^2\right)^3 \cdot 2 + 6 \cdot \left(x^2\right)^2 \cdot (2)^2 \\
&\quad + 4 \cdot x^2 \cdot (2)^3 + 1 \cdot (2)^4 \\
&= x^8 + 4 \cdot x^6 \cdot 2 + 6 \cdot x^4 \cdot 4 + 4 \cdot x^2 \cdot 8 + 16 \\
&= x^8 + 8x^6 + 24x^4 + 32x^2 + 16
\end{aligned}$$

Try performing this expansion step-by-step and compare, too. There are actually some very interesting properties of Pascal's Triangle that are deeply rooted in some other mathematical concepts, and these properties are particularly useful in the field of **combinatorics**. We will, in fact, examine many of these properties in greater detail later on! For example, you might wonder *why* it is the case that this procedure—adding the two entries above—yields entries that correspond to expanding factors like this. We will prove that it works when we discuss the **Binomial Theorem** and its related ideas! (See Section 8.4.4 if you're curious.)

Completing the Square

There is one more polynomial-related trick we need to mention before deriving an important result. Sometimes, it is useful to rewrite a polynomial as a squared term plus a constant term, so that we can separate the variables and constants in a convenient way. This amounts to adding and subtracting a particular term so that, overall, we have added 0 to the polynomial, but the term is chosen in a way that lets us rewrite the terms of the polynomial conveniently. This process is known as **completing the square**, in the sense that we add a term to create a squared factor, and complete the polynomial by subtracting a corresponding amount.

Let's try this procedure with an example and then attempt to generalize. Start with the following polynomial:

$$p(x) = x^2 + 8x + 9$$

A factorization isn't immediately apparent here, so let's try to complete the square. We want to see a term like $(x + a)^2$, where we know the coefficient of x is 1 since the polynomial has $1 \cdot x^2$. Expanding a term like that gives $x^2+2ax+a^2$. Since we need $8x$ to appear, we should use $a = 4$. This expansion gives $x^2 + 8x + 16$, but we really want to see $+9$ as the constant term, so let's add and subtract 7 from the original polynomial:

$$p(x) = x^2 + 8x + 9 + 7 - 7 = (x^2 + 8x + 16) - 7 = (x + 4)^2 - 7$$

Does this look familiar? Precisely, it's a difference of squares, and we know how to factor that:

$$\begin{aligned} p(x) &= x^2 + 8x + 9 = (x+4)^2 - 7 = (x+4)^2 - \left(\sqrt{7}\right)^2 \\ &= \left(x + 4 + \sqrt{7}\right)\left(x + 4 - \sqrt{7}\right) \end{aligned}$$

Accordingly, the roots of this polynomial are $x = -4 - \sqrt{7}$ and $x = -4 + \sqrt{7}$.

Let's generalize! Suppose we start with a quadratic polynomial of the form

$$p(x) = ax^2 + bx + c$$

and, to complete the square, we want to add and subtract a particular term. How did we find that term before? Well, the expansion of a term like $(rx+s)^2$ yields $r^2x^2 + 2rsx + s^2$, and to match these coefficients with the coefficients of the original polynomial, we see that we need $r^2 = a$, so we should use $r = \sqrt{a}$. (Notice that this requires $a \geq 0$, of course! What should we do if $a < 0$?) Then, to have $2rs = b$, we need $s = \frac{b}{2r} = \frac{b}{2\sqrt{a}}$. Then, when this is expanded we have added on $s^2 = \frac{b^2}{4a}$, so we should subtract that from the polynomial.

These steps are performed below, with some extra algebraic cleanup, of sorts, to make the terms look "nicer":

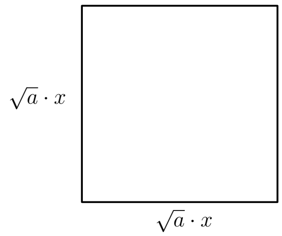
$$\begin{aligned} p(x) &= ax^2 + bx + c = ax^2 + bx + \frac{b^2}{4a} + c - \frac{b^2}{4a} \\ &= \left(\sqrt{a}x + \frac{b}{2\sqrt{a}}\right)^2 + \left(c - \frac{b^2}{4a}\right) \\ &= \left(\sqrt{a} \cdot \left(x + \frac{b}{2a}\right)\right)^2 + \left(c - \frac{b^2}{4a}\right) \\ &= a\left(x + \frac{b}{2a}\right)^2 + \left(c - \frac{b^2}{4a}\right) \end{aligned}$$

This now tells us how to complete the square, given any quadratic polynomial!

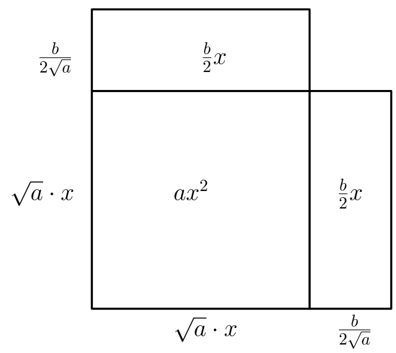
Visualizing Completing the Square

Here's a helpful way to remember how to do this process. It's based on a visual representation of the areas of squares and rectangles.

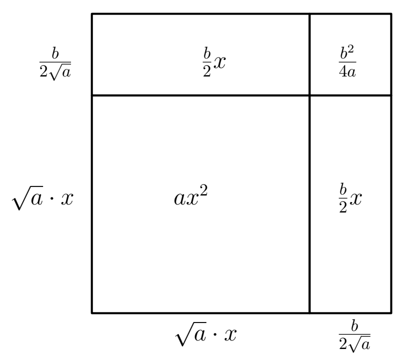
Let's suppose that $a, b > 0$ so that we can geometrically interpret $ax^2 + bx$ as the area of a rectangle. Specifically, let's take the ax^2 term to be the area of a square. This means each side has length $\sqrt{a} \cdot x$:



How might we represent the bx term? We want to build this square into a larger square; this is what completing the square means. So, we should build some rectangles around this square that will help us proceed towards that goal. Let's split the area contributed by the bx term into two rectangles, each with area $\frac{b}{2}x$. Since we must have one side with length $\sqrt{a} \cdot x$, and we want the total area to be $\frac{b}{2}x$, then we see that we need the other length to be $\frac{b}{2\sqrt{a}}$:



What do we need to add to make this a square? We see that there is just a tiny square piece left to fill in the upper-right corner. Each side is length $\frac{b}{2\sqrt{a}}$, so its area—the term we need to add on—is $\frac{b^2}{4a}$.



Look at that! This is the same term we produced above with our algebraic derivation. By adding that on, we were able to factor the terms as a perfect square. We just needed to make sure to subtract it off, as well, so that the net change to the original expression is zero.

This is a helpful trick to keep in mind. It can remind you about both the motivating process for completing the square, as well as how to achieve it. One thing you should ponder, though: Why is it that this visual representation works? We had to assume $a, b > 0$ to be able to draw these diagrams, so why is it that the general formula works no matter what a and b are?

The Quadratic Formula

Let's returning to the question of identifying the roots of a polynomial. Specifically, let's recall the **quadratic formula**. You may have memorized this formula as a way to "solve quadratic equations" but do you know *why* it actually works? Let's try to figure it out! In general, we start with a quadratic polynomial of the form

$$p(x) = ax^2 + bx + c$$

where $a \neq 0$ (otherwise, it's not actually quadratic), and we want to identify the values of x such that $p(x) = 0$. (Did you try to answer our questions above about how many roots this type of polynomial can have? Keep those concepts in mind throughout the following derivation.) We can't hope to factor the polynomial into linear factors too easily, so let's take advantage of the process we used above: completing the square. The benefit of that procedure is that we can set $p(x) = 0$ and rearrange the terms after completing the square to solve for x. Observe:

$$0 = p(x) = ax^2 + bx + c = a\left(x + \frac{b}{2a}\right)^2 + \left(c - \frac{b^2}{4a}\right)$$

simplifies to:

$$\frac{b^2}{4a} - c = a\left(x + \frac{b}{2a}\right)^2$$

Now, we want to to start "undoing" the processes here to solve for x, and this would require taking the square root of boths sides. But what if $\frac{b^2}{4a} - c < 0$? We couldn't take that square root at all! Or what if $\frac{b^2}{4a} - c = 0$? Is that a problem? Do we have anything to worry about when $\frac{b^2}{4a} - c > 0$? These are issues that are related to the questions we had before about the possible number of roots a polynomial can have. You may have deduced (correctly) that a quadratic polynomial can have *at most* two roots, but here we have uncovered the possibility (and reasons why) that a quadratic polynomial may have one or zero roots!

- In the case where $\frac{b^2}{4a} - c < 0$, then *no* value of x can possibly satisfy the last line in the derivation above. Therefore, there would be no roots of $p(x)$ in the set of real numbers.

- In the case where $\frac{b^2}{4a} - c = 0$, then taking the square root of both sides of the last line above is perfectly valid, but it will produce *exactly one* value of x:

$$\begin{aligned}\frac{b^2}{4a} - c = 0 &= a\left(x + \frac{b}{2a}\right)^2 \\ 0 &= x + \frac{b}{2a} \\ x &= -\frac{b}{2a}\end{aligned}$$

The remaining case is when $\frac{b^2}{4a} - c > 0$. Here, we can expect *two* roots of $p(x)$ because taking the square root of both sides introduces two possible solutions. In general, when we have a situation like $s^2 = t$, we can say that the only possible solutions are $s = \sqrt{t}$ and $s = -\sqrt{t}$ but we must consider both (we usually write this as $s = \pm\sqrt{t}$). Solving for x in that case yields

$$\begin{aligned}\frac{b^2}{4a} - c &= a\left(x + \frac{b}{2a}\right)^2 \\ \pm\sqrt{\frac{b^2 - 4ac}{4a}} &= \sqrt{a}\left(x + \frac{b}{2a}\right) = \sqrt{a}x + \frac{b}{2\sqrt{a}} \\ -\frac{b}{2\sqrt{a}} \pm \frac{\sqrt{b^2 - 4ac}}{\sqrt{4a}} &= \sqrt{a}x \\ -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{\sqrt{4a^2}} &= x\end{aligned}$$

Now, we need to be careful about the square root observation we made before. In general, $\sqrt{4a^2} = \pm 2a$, but we already know that the fractional term involving that square root already has an associated ± 1 factor, so this factor won't change that. Therefore, we can conclude

$$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Voilà, the quadratic formula!

Remember that the final steps of the derivation were carried out under the assumption that $\frac{b^2}{4a} - c > 0$. Does this formula still apply when $\frac{b^2}{4a} - c = 0$? Could we have performed the same steps as we did immediately above while operating under that assumption? Why or why not?

Problems

Problem 1.3.5. Find all possible values of a so that $x - a$ is a factor of $x^2 + 2ax - 3$.

Problem 1.3.6. Find all possible values of b so that $x^3 + b$ is divisible by $x + b$ with no remainder.

Problem 1.3.7. Factor $x^n - 1$ for any natural number n.

Problem 1.3.8. Determine the value of x defined by

$$x = \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \cdots}}}}$$

Hint: try to express the infinitely-nested square roots by using x, itself.

Problem 1.3.9. Use completing the square to prove that the sum of a positive number n and its reciprocal is always greater than or equal to 2, and that the only number that makes the sum equal to 2 is $n = 1$.

Hint: take the sum, add and subtract 2, and rearrange.

Problem 1.3.10. How can we find the roots of a quartic polynomial of the form $ax^4 + bx^2 + c$?

1.3.4 Let's Talk About Sets

We've mentioned some particular types of numbers already, but we want to specifically define the sets of numbers we will be working with in the future. Each of these collections of numbers is represented by a particular letter in the `blackboard bold` font. The **natural numbers** (also known as whole numbers or counting numbers) are so-called because they feel "natural" to say as we start counting objects. We can write

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$$

(There is a more specific and technical definition that we will explain later on.) We use $\mathbb{N}$ to stand for "natural".

Using $\mathbb{N}$, we can define a related collection of numbers: the set of all **integers**, which combines the natural numbers, 0, and the negative natural numbers. We can write

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

The letter $\mathbb{Z}$ comes from the German word *Zahlen*, meaning "number".

From this set, we can define the collection of **rational numbers**. These numbers can be represented as a ratio of integers, but they don't seem to have a natural "listing" like the sets $\mathbb{N}$ and $\mathbb{Z}$, so we can't write this set in the way that we did above. For this, we use a very common set notation, as follows:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$$

We read this as:

> "The set of rational numbers is the set of all numbers of the form $\frac{a}{b}$, where a and b are both integers and b is nonzero."

This conveys the necessary information that a rational number is a fraction, where the numerator and denominator are integers (but the denominator can't be 0 because division by 0 is disallowed). The reason we use the letter $\mathbb{Q}$ for the rational numbers is because $\mathbb{R}$ was already reserved for the *real* numbers and $\mathbb{Q}$ was the next previous letter available. Also, $\mathbb{Q}$ contains all of the *quotients* of integers, so that makes sense, too!

The **real numbers** $\mathbb{R}$ have a very technical definition that we, unfortunately, cannot delve into completely in this book. (That just goes to show how difficult it is to mathematically define that set!) For now, one way to think of the real numbers is via a **number line**. The real numbers are all numbers that lie on the line, while the numbers of $\mathbb{N}, \mathbb{Z}$ and $\mathbb{Q}$ are specific numbers that lie on the line, but they don't comprise the entirety of the line. In a way, $\mathbb{R}$ is the "completion" of $\mathbb{Q}$, in the sense of "filling in the gaps" between rational numbers.

1.3.5 Notation Station

A popular and convenient way of writing sums and products is to use a shortened notation that collects many terms or factors into one common form. For instance, what if we wanted to talk about the sum of the first 500 natural numbers? It would be tedious to write out all 500 terms of the sum, so it is common to write something like $1 + 2 + 3 + \cdots + 499 + 500$. (We've already used ellipses like this, in fact. Did you understand what we meant?) This is popular and does get the point across, but some mathematicians take offense to the unnecessary use of ellipses in the middle. We put off talking about this issue until now because it's often the case that **notation** can be difficult to learn and comprehend. Rather than bombard you with new symbols right away, we appealed to our intuitive understanding of what "..." accomplish.

Now, that we've brought it up, let's see how to avoid using ellipses. To write the sum we mentioned above, we would use the following notation:

$$1 + 2 + 3 + \cdots + 499 + 500 = \sum_{i=1}^{500} i$$

The large sigma $\sum$ comes from the Greek letter corresponding to S, for "sum", and the **index** i tells us to find the values of the individual terms of the sum. Writing $i = 1$ below and 500 above the $\sum$ sign means that we let i assume all of the natural number values between 1 and 500 (inclusive). Using those values, we substitute into the general expression for the term, which is just i, in this case. Accordingly, we find that the terms are $1, 2, 3, \ldots, 500$, as desired. Try to find a few other ways of writing this sum by altering the expression for the general term and/or the values of the index. What if we wanted to find the sum of the first 500 even natural numbers? What about all of the even natural numbers up to (and including) 500? Try to write those sums in the notation style above.

Related to this is the $\prod$ notation. If we wanted to look at the product of the first 500 natural numbers, we would follow the same conventions of identifying values for the index and the general term:

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot 499 \cdot 500 = \prod_{i=1}^{500} i$$

The large pi $\prod$ comes from the Greek letter corresponding to P, for "product". Again, try expressing this in a different way by changing the general term and/or index values. What if we wanted to find the product of the first 500 *even* natural numbers? What about all of the even natural numbers *up to* (and including) 500? Try to write those products in the notation style above.

Problems

Problem 1.3.11. Write an English sentence that describes what the following equation means:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Problem 1.3.12. Express, in appropriate notation, the sum and product of the first n powers of 2, starting with $2^0 = 1$. Can you prove a formula for the sum? The product?

Problem 1.3.13. Consider the sum of all the odd numbers between 17 and 33 (inclusive). Write this sum in summation notation where the index starts at 0. Now try writing it where the index starts at 1. Now try writing it where the index starts at 8, and again with 9. Which of these feels "more natural"? Why?

1.4 Quizzical Puzzicles

Let's put into action some of the principles we have discussed so far. Specifically, let's examine some interesting mathematical puzzles and explain how to go about solving them. None of these involves knowing anything beyond basic algebra and arithmetic, but this does not mean they are "basic" or "easy", since they all involve critical thinking skills and keen insight to solve and understand. Along the way, we will be employing some logical ideas we have brought up already. We might have to work with polynomial functions, or solve some equations algebraically. We might have to think careful about order and flow of our arguments, making sure everything follows from previous knowledge or deductions. Overall, we should also be thinking about what constitutes a good and valid *proof* of the facts we discover!

1.4.1 Funny Money

Problem Statement

This classic puzzle is contained in a story about some friends paying for a shared hotel room:

> Three friends are on a road trip and stop at a hotel late one night looking for a room to catch up on some rest. The clerk on duty says that there is only one room vacant for that night and it costs \$30 for the three of them, if they want to squeeze in together. The friends decide they are desperate for sleep and agree to split the room amongst them, each placing a \$10 bill on the counter to pay up front. The clerk thanks them, hands them the key, and they head off to grab their bags from the car. Meanwhile, another clerk shows up to start his shift and realizes that the previous clerk had made an error and overcharged the three friends for their room: it should have only been \$25. He takes a \$5 bill from the register, hands it to the bellhop on duty and says, "Bring this to Room #29. The guests there were overcharged." The bellhop nods and heads off to their room. When the three friends answer the door, they are surprised and happy to discover they earned a refund. To split the money fairly, one friend makes change with five \$1 bills and then each friend takes \$1, giving the remaining \$2 to the bellhop as a friendly tip. The bellhop thanks them kindly and heads back to work.
>
> Now, each of the three friends contributed \$9 to the room, plus a \$2 tip, making a total of \$29. But they originally gave the clerk \$30... What happened to the missing dollar?!

Think carefully about this before turning the page and reading our solution.

Solution: Keeping Careful Track of the Money

Did you figure it out? Did you realize there is really nothing "missing"? This puzzle is intended to confuse the reader and mislead them into searching for something that isn't really there. The numbers involved are chosen so that the "missing sum" of \$1 is so small that the reader believes that something mysterious happened, but careful and logical analysis of the events should lead you to realize that the question at the end is not really a fair one; it is based on a misinterpretation of the situation, and trying to ignore its reasoning is the key to figuring out the solution to this puzzle. When the numbers are changed greatly so that the final discrepancy is of a much larger value, the reader no longer has that emotional investment to seek out that "missing dollar".

First, let's analyze what actually happened in this particular case. The key is careful interpretation of where the money actually goes. It helps to forget about the individual people involved and think of two distinct entities: the group of friends, who we'll call F, and the clerk/bellhop combo from the hotel, who we'll call H. Now, let's replay the steps of the story and describe where the money comes from and goes to at each step:

(1) F arrives and gives \$30 to H (original cost of room)

(2) H gives \$5 back to F (refund for overcharge)

(3) F gives \$2 back to H (tip to bellhop)

(4) Net change: F gave \$30-\$5+\$2=\$27 to H

It makes more sense now, doesn't it? The refund was \$5, so the room actually cost \$25 and it doesn't make sense to say that the three friends each paid \$9 for it, plus the tip to the bellhop. That \$27 contribution from the three of them *includes* the tip. The question after the story implies that the we should be *adding* the tip to the friends' contribution but, really, it is part of their contribution. By grouping the friends together and the bellhop/clerk together, we can actually track down how the money changes hands.

Generalizing: Changing The Numbers

Let's change the problem in the way that we mentioned above; specifically, let's try to change the numbers of the problem to remove that emotional attachment to the "missing dollar" and make the discrepancy much larger. To begin, we will define some variables to represent the dollar amounts used in each of the steps outlined above. We could try to approach this problem by "testing out" specific values for these dollar amounts and seeing what happens but it will be more efficient to essentially "try everything at once" by introducing variables and substituting specific values for them later on.

We will let $3n$ represent the original cost of the hotel room (the amount paid by the three friends when they first arrived), for some value of n. We choose this because we want the cost to be evenly split by the friends. Next, we want to define a variable to represent the refund they receive. Knowing that they will want to split this amount evenly amongst the three of them and have some leftover to tip the bellhop, let's say that the refund is of the form $3r + 2$. The variable r represents how much each friend individually receives back from the hotel, and the 2 represents the tip for the bellhop. Now, let's restate the puzzle with these variables instead of the original values.

> Three friends are on a road trip and stop at a hotel late one night looking for a room to catch up on some rest. The clerk on duty says that there is only one room vacant for that night and it costs $\$3n$ for the three of them, if they want to squeeze in together. The friends decide they are desparate for sleep and agree to split the room amongst them, each placing $\$n$ on the counter to pay up front. The clerk thanks them, hands them the key, and they head off to grab their bags from the car. Meanwhile, another clerk shows up to start his shift and realizes that the previous clerk had made an error and overcharged the three friends for their room: it should have only been $\$3n - (3r + 2)$. He takes $\$3r + 2$ from the register, hands it to the bellhop on duty and says, "Bring this to Room #29. The guests there were overcharged." The bellhop nods and heads off to their room. When the three friends answer the door, they are surprised and happy to discover they earned a refund. To split the money fairly, each friend takes $\$r$, giving the remaining \$2 to the bellhop as a friendly tip. The bellhop thanks them kindly and heads back to work.
>
> Now, each of the three friends contributed $\$n-r$ to the room, plus a \$2 tip, making a total of $\$3(n - r) + 2$. But they originally gave the clerk $\$3n\ldots$ What happened to the missing $\$3n - [3(n - r) + 2] = \$3r - 2$?!

Do you see what happened now? The discrepancy occurs, as we explained before, because the question considers *adding* the \$2 tip to the refunded cost of the room and comparing that to the original cost of $\$3n$. The actual comparison should be between the refunded contribution of the friends, which is $\$3(n-r) = \$3n - 3r$, and the sum of the refunded cost of the room and the tip, which is $\$3n - (3r + 2) + 2 = \$3n - 3r$. No discrepancy there!

Generalizing: Questions For You

In the original statement of the puzzle, the values were $n = 10$ and $r = 1$, so that the "missing amount" was magically $\$3r - 2 = \$1$. If we had chosen larger values—say $n = 100$ and $r = 10$—then the \$300 room actually should have cost \$268, the bellhop would bring the friends \$32, they would each take \$10, he would keep \$2, and the discrepancy becomes \$28. Would anyone actually believe that \$28 went missing in those transactions? What if we use even larger values of n and r? How large can you make the discrepancy? How small? Given a desired discrepancy, in dollars, can you find values for n and r that achieve that value? How many ways are there to do that?

Lessons From This Puzzle

Logic and rational thinking are important when solving a puzzle because it is sometimes easy to be misled by emotions. Had we stated the puzzle originally as the "missing $28 problem", would you have reacted the same way? Would you have been as temporarily confused before trying to backtrack and discover what really happened?

1.4.2 Gauss in the House

Problem Statement

There is a popular anecdote among mathematicians that may or may not be apocryphal, but some of us would like to believe that it is true, because it features one of the greatest mathematicians/physicists of all time, Carl Friedrich Gauss. He worked in the late 1700s and early- to mid-1800s and proved some fundamental and powerful results in a broad range of areas. He studied number theory, and complex analysis, and optics, and geometry, and astronomy, and so much more! Read the story below, think about what you would have done in that situation—as a young child and now—and then read on for a discussion.

> It was early in the morning in an elementary school classroom, and the students were acting noisy and rowdy, much to the dismay of the teacher, who was feeling quite sick and tired, literally, and quite sick and tired of their behavior. He needed a way to occupy them for a while so that he could relax at his desk and recuperate. He bellowed out to the room and told them to take out their slates and chalk. After asking a few more times, everyone had obliged. He then told them to add together all of the numbers from 1 to 100, and that the first person to do so would earn the privelege of being the teacher's helper for the day. He returned to his desk and sat down, relieved that they would be occupied for quite some time performing large sums. After only a minute, though, one boy walked up to the desk and showed the teacher his slate with the answer. The teacher was astounded and had to spend a few minutes performing the arithmetic himself to check the answer, but in the end, the little boy was correct, and he had accomplished this feat so quickly. How did he do it?

Think carefully about this before turning the page and reading our solution. Remember, this story "happened" in the days before calculators, so you should not be using anything more than your brain and a pencil and paper.

Solution: Reducing Computations

Perhaps you figured this one out. There are actually a number of ways to approach this problem that are slightly different, but they mostly amount to the same insight: trying to reduce the number of computations required.

To naively go through and add each of the 100 numbers to the previously obtained sum would require 99 additions, with ever larger numbers involved. Certainly, the trick here is not to just do these additions faster than the others, it is to be more efficient with the computations that are required. Remember that multiplication can be viewed as repeated addition of one number with itself, so perhaps we can reduce all of these additions to one multiplication, provided we find the right number to add to itself over and over.

Another important fact to remember is that addition is **associative** and **commutative**, meaning we can perform the additions in any order and be assured that we obtain the same answer. Specifically, we can add all the numbers from 100 down to 1 and get the same result for the sum, call it S. Let's write down this fact in a convenient way here:

$$\begin{array}{ccccccccccccccc} 1 & + & 2 & + & 3 & + & \cdots & + & 98 & + & 99 & + & 100 & = & S \\ 100 & + & 99 & + & 98 & + & \cdots & + & 3 & + & 2 & + & 1 & = & S \\ \hline 101 & + & 101 & + & 101 & + & \cdots & + & 101 & + & 101 & + & 101 & = & 2S \end{array}$$

Notice that we have written down the desired sum in two different ways, added those two sums entry by entry, and obtained an expression for $2S$, twice the desired sum. That new expression can be written as a multiplication because there are 100 terms, each of which is the number 101. Thus,

$$2S = 101 \cdot 100 \quad \text{and therefore,} \quad S = 101 \cdot 50 = 5050$$

This is much faster than performing 99 additions, and in fact, if we think carefully, we may be able to do the entire process in our heads!

Alternate Solution: Pairing Terms

Now, a very similar way of seeing this problem is to skip adding the two lines we wrote above and just pair off the numbers in the original sum, as follows:

$$\begin{aligned} S &= 1 + 2 + 3 + \cdots + 98 + 99 + 100 \\ &= (1 + 100) + (2 + 99) + (3 + 98) + \cdots + (49 + 52) + (50 + 51) \\ &= 101 + 101 + \cdots + 101 = 50 \cdot 101 = 5050 \end{aligned}$$

This approach is essentially equivalent to the one we described above; it still takes advantage of the associative property of addition to convert the sum into a multiplication, it just skips over the intermediate steps where we found an expression for $2S$ and then divided by two.

Generalizing: Even n

What if the teacher had asked his students to add the numbers from 1 to 1000? Would they have protested? Would Gauss have been able to find the answer just as quickly? What would you do? We're not sure about the first two questions, but we think that you could handle this sum just as easily. The only thing different here is that the number of pairs we create will be 500 (instead of 50), and each of those pairs will sum to 1001 (instead of 101), so the result will be

$$1 + 2 + 3 + \cdots + 998 + 999 + 1000 = 1001 \cdot 500 = 500500$$

Does it look like there's a pattern there? Do you think you could say what the sum of all of the numbers from 1 to 1 million is right away without doing the multiplication?

Generalizing: Odd n

What if the teacher had asked for the sum of the first 99 numbers instead? Would the pairing process still work? Let's see:

$$\begin{aligned} S &= 1 + 2 + 3 + \cdots + 97 + 98 + 99 \\ &= (1 + 99) + (2 + 98) + (3 + 97) + \cdots + (48 + 52) + (49 + 51) + 50 \\ &= (49 \cdot 100) + 50 = 4950 \end{aligned}$$

Notice that we had an *odd* number of terms in total, so we couldn't pair off every number, and had to add 50 to the result of the multiplication. Could we have paired the numbers in a different way?

$$\begin{aligned} S &= 1 + 2 + 3 + \cdots + 97 + 98 + 99 \\ &= (1 + 98) + (2 + 97) + (3 + 96) + \cdots + (48 + 51) + (49 + 50) + 99 \\ &= (49 \cdot 99) + 99 = 50 \cdot 99 = 4950 \end{aligned}$$

This *seems* more similar to the result of the original puzzle, because we ultimately performed *one* multiplication. This may seem like a strange coincidence now, but try to follow the steps above with some other odd sums. What is the sum of the first 7 integers? The first 29? The first 999? The first 999999?

Generalizing: Any n

Let's step back from the individual cases that we have examined here and try to solve the problem in a more general sense. Let's pretened that the teacher had presented the students with the following problem:

> Find a formula for the sum of the first n numbers. I want a *specific* formula so that if someone tells me what n is, I can find an answer quickly by plugging in that particular value.

The caveat in the second sentence rules out a solution of the form given by our investigations above. We have already come up with some simple *algorithms* for finding a solution to this problem, but we have now been asked to find a *forumla* that will produce a solution. How do we begin to approach this? Well, based on some observations we made above, it would make sense to tackle this puzzle by handling the cases where n is even and where n is odd separately. We saw that the pairing worked out slightly differently in those cases, so let's investigate one and then the other. In each case, we are looking for a formula for $S(n)$, the sum represented by $1+2+3+\cdots+(n-2)+(n-1)+n$. We are using this new notation $S(n)$ to indicate that the sum *depends* on that particular value of n.

If n is even, we know that we can pair off every number and have no terms leftover:

$$\begin{aligned}
S(n) &= 1+2+3+\cdots+\left(\frac{n}{2}-1\right)+\frac{n}{2}+\left(\frac{n}{2}+1\right)+\cdots \\
&\qquad +(n-2)+(n-1)+n \\
&= (1+n)+(2+(n-1))+(3+(n-2))+\cdots \\
&\qquad +\left(\left(\frac{n}{2}-1\right)+\left(\frac{n}{2}+2\right)\right)+\left(\left(\frac{n}{2}\right)+\left(\frac{n}{2}+1\right)\right) \\
&= (n+1)\cdot\frac{n}{2}=\frac{n^2+n}{2}
\end{aligned}$$

Try this formula with some of the even values of n we examined above (like 100, 1000, 1000000, etc.) It works, doesn't it? Note that the reason we can write terms involving $\frac{n}{2}$ and be assured they are part of the sum is that n is *even*, so $\frac{n}{2}$ is also a whole number.

Okay, now what happens if n is odd? We know that we won't be able to pair off every number, so we need to be clever about what we do here. Remember our approach with summing the first 99 numbers? By leaving off the last term of the sum, we could pair off all of the other terms with no leftover, and futhermore, each of those pairs summed to the *same value* as that last number. Let's try using that approach here:

$$\begin{aligned}
S(n) &= 1+2+3+\cdots+\left(\frac{n-1}{2}-1\right)+\frac{n-1}{2}+\left(\frac{n-1}{2}+1\right)+\cdots \\
&\qquad +(n-2)+(n-1)+n \\
&= (1+(n-1))+(2+(n-2))+\cdots+\left(\left(\frac{n-1}{2}\right)+\left(\frac{n-1}{2}+1\right)\right)+n \\
&= n+n+\cdots+\left(\frac{2n-2}{2}+1\right)+n=(n+n+\cdots+n)+n
\end{aligned}$$

This has shown that each of the pairs of terms sums to n, the final number that we removed before the pairing process. Now, let's think carefully about how *many* pairs we had. Notice that we can number them by looking at the first number of the pair: the first pair was $(1, n-1)$, the second pair was $(2, n-2)$, and so on, and the first number in the last pair was $\frac{n-1}{2}$. Therefore, we had exactly that many pairs: $\frac{n-1}{2}$. (Remember that n is odd, so we can rest assured that $n-1$ is even, so $\frac{n-1}{2}$ is a whole number. We haven't been mentioning that every time, so be sure to go back over what we've done so far and convince yourself that every step and every term we write is valid.) To those pairs, we tacked on a final number, n, so we can write the multiplication for the sum as follows:

$$S(n) = \left(\frac{n-1}{2} + 1\right) \cdot n = \left(\frac{n-1}{2} + \frac{2}{2}\right) \cdot n = \frac{n+1}{2} \cdot n = \frac{n^2+n}{2}$$

Wow, this is the exact same formula we found in the case where n is even! Did this surprise you? It's not obvious at all that we should end up with the same formula, even with the similarity of the approaches to the problem. What does this suggest to you? A mathematician would see such a "coincidence" and wonder whether there is a much *simpler* and *direct* route to this result; that is, is there a way we could approach this puzzle that would answer *both* odd and even cases simulatenously? Since we obtained the same answer, there might be a way to do it. Think about this for a minute before reading on.

Generalizing: Any n, *without* separate cases

It turns out that we already hinted at this other method in our previous discussion of this puzzle. Remember when we wrote the sum forwards on one line and backwards on another line and added them together? Well, when we treated the odd/even cases here, we decided to avoid that method because it seemed to add a couple of extra steps; the "pairing terms" process seemed slightly quicker so we followed that method. What if we went back and reexamined the "add the sum twice" method? We'd find something like this:

$$\begin{array}{ccccccccccc} 1 & + & 2 & + & \cdots & + & (n-1) & + & n & = & S(n) \\ n & + & (n-1) & + & \cdots & + & 2 & + & 1 & = & S(n) \\ \hline (n+1) & + & (n+1) & + & \cdots & + & (n+1) & + & (n+1) & = & 2S(n) \end{array}$$

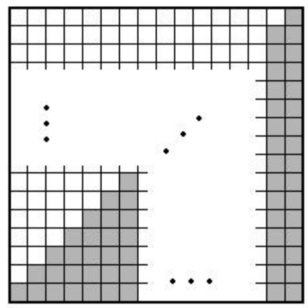
In this case, we have n terms in the sum on the third line, and each term is $(n+1)$. Thus,

$$(n+1) \cdot n = 2S(n) \quad \text{and therefore,} \quad S(n) = \frac{1}{2}(n+1) \cdot n = \frac{n^2+n}{2}$$

This is the formula we have obtained already, and we found it here in a way that didn't depend on whether n is odd or even! (Look back at the steps we just performed and verify for yourself that the odd/even property of n is really irrelevant.)

Alternate Solution: Visual Diagram

Before we wrap up this puzzle, we want to mention a geometric approach to the solution. We will relate the sum $S(n)$ to the area of a square and find a way to draw the individual terms of the sum $(1, 2, 3, \ldots, n-1, n)$ as portions of the square's area. Specifically, let's consider an $n \times n$ square and draw the sum's terms as rectangles with increasing height, each with width one unit. See the picture below:



Now, asking for a formula that yields the sum $S(n)$ is equivalent to asking what *area* is covered by all of the rectangles we have drawn inside this square. Trying to add up the individual areas is just restating the puzzle, so we need to think of a way to relate this area to the total area of the square. To do this, let's think about what is left over; that is, how can we describe the area of the square that is *not* covered by the rectangles? Look at the area strictly above the first 1×1 rectangle: it is also a rectangle, with dimensions $(n-1) \times 1$.

Look at the area above the 2×1 rectangle: it is a $(n-2) \times 1$ rectangle. This pattern continues! Eventually, we have a 1×1 rectangle above the $(n-1) \times 1$ rectangle and then no area above the last $n \times 1$ rectangle. What is the total area of all of those rectangles? Well, it looks a lot like the sum $S(n)$ we are considering, but it is just missing the final term, n. Now, we can add up the areas of all the rectangles by relating them to $S(n)$ and then to the square's area:

$$n^2 = S(n) + (S(n) - n) = 2S(n) - n$$

Therefore,

$$S(n) = \frac{n^2 + n}{2}$$

the same formula we had before!

Lessons From This Puzzle

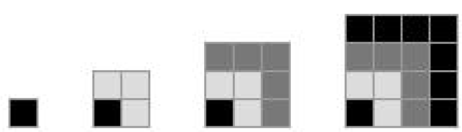
Sometimes there are several completely reasonable ways to approach a puzzle and obtain a solution. Some of them might come to mind first but take longer to execute, some might be trickier to find but lead to a solution much more easily, or some might just go nowhere at all! It's often hard to tell beforehand what's going to happen with any particular approach, so just start trying to work through the puzzle and see what happens, keeping track of what you've tried and what happened so that you can reassess that approach later. This is a fact we need to keep in mind as we advance in our mathematical careers. We can't always know exactly what to do right away. We are bound to get stuck sometimes, or try roads that end up being dead ends. This shouldn't be discouraging; it's just the way it is!

As a subpuzzle, try redoing the "paired terms" for the odd n case, but instead of leaving off the last term of the sum, try separating the middle term and pairing the numbers from the outside in. Does this give you the same result? Does it seem any easier/faster/different than the approach we used? Alternatively, what if we had handled the even n case by saying that $n = 2k$ for some number k? What would we do for odd n? Does this notation change the procedure at all? Does it make it any easier to handle? Now, can you think of any completely different methods to attack this puzzle?

1.4.3 Some Other Sums

Summing Odd Numbers: Observing a Pattern

While we're on the topic of evaluating sums of integers, let's look at some related problems. First, we will look at an interesting geometric way of interpreting sums of *odd* integers: let's represent 1 as a 1×1 block, and then each successively larger odd integer as a right-angled corner of 1×1 blocks that fits perfectly around the previous such figure. Why would we do this? Well, since these are all odd numbers, successive terms differ in size by two, and lengthening the sides of our corner pieces by one each time allows us to snugly fit the corners around each other and build successively larger squares!



Does this pattern continue? If we believe that it does, how could we prove such a thing? What does this geometric pattern mean in terms of the numerical sums? This is a good question to answer first, because as pretty as the geometric pattern is, it's difficult to work with and manipulate and, ultimately, *prove* decidedly. In essence, pointing to the first few terms of the pattern and saying, "Look, it works!" does *not* constitute an official, mathematical proof, so we must find a better way of formulating this problem. This is not to downplay the meaningfulness and beauty of the pattern we noticed; it is quite interesting that it works out that way and it did provide us with some valuable insight into what might be going on, mathematically, but at the end of the day, that's all it can do for us.

Summing Odd Numbers: Proving Our Findings

Let's try to write the sums represented by the figures above in numerical terms. The corner pieces are made from 1×1 blocks, and there are two more blocks in each corner than the previous one, so each square figure that we saw is represented by a sum like

$$1 \quad \text{or} \quad 1+3 \quad \text{or} \quad 1+3+5 \quad \text{or} \quad 1+3+5+7$$

and so on. What we notice from these terms is that, indeed, they sum to square numbers:

$$1 = 1^2 \qquad 1+3 = 4 = 2^2 \qquad 1+3+5 = 9 = 3^2 \qquad 1+3+5+7 = 16 = 4^2$$

This is really the pattern that we want to prove; it is equivalent to the geometric pattern we noticed before, but now it is written in terms we can manipulate. Let's think about how can we do this, now. Is this pattern similar to anything we've seen before? Have we proved any results about sums of integers? Of course! Look back at the previous puzzle; we proved (in a few ways, in fact) that

$$1 + 2 + 3 + \cdots + (n-1) + n = \frac{n^2+n}{2}$$

How might this be useful in this puzzle? The sum formula we proved involves *all* consecutive integers from 1 to n, but for the current desired formula, we only want to consider consecutive *odd* integers.

Before, we used the function $S(n)$ to represent the sum of the first n natural numbers, so let's define a function $T(n)$ to represent the sum of the first n odd natural numbers. Now, we need to identify the terms of that sum first, and then relate those to $S(n)$ somehow. Below, we have written out the sums for $n = 1, 2, 3$ and 4. Can you find a way to identify the largest term in the sum and express that in terms of n?

$$n = 1: \quad 1, \quad n = 2: \quad 1+3, \quad n = 3: \quad 1+3+5, \quad n = 4: \quad 1+3+5+7$$

Notice that the last term of the sum is always $2n-1$. This is related to a general fact, that any *even* integer can be represented as $2k$, for some particular integer k, and any *odd* integer can be represented as $2n-1$, for some particular integer n. (We can also express an odd integer as $2n+1$ for some integer, as well, right? In this context, it is more convenient to use the $2n-1$ form, though.) Accordingly, we want to find a formula for the sum of the first n odd natural numbers, given by

$$T(n) = 1 + 3 + 5 + 7 + \cdots + (2n-3) + (2n-1)$$

Can we relate this sum to $S(n)$ or something similar? Well, notice that the sum

$$S(2n) = 1 + 2 + 3 + \cdots + (2n-3) + (2n-2) + (2n-1) + 2n$$

contains *all* of the natural numbers from 1 to $2n$, whereas $T(n)$ only contains the odd natural numbers in that range. Perhaps it would make sense to subtract those two sums and try to find an expression for the sum of the leftover terms:

$$\begin{aligned} S(2n) - T(n) &= \big(1 + 2 + 3 + \cdots + (2n-1) + 2n\big) \\ &\qquad - \big(1 + 3 + 5 + \cdots + (2n-3) + (2n-1)\big) \\ &= 2 + 4 + 6 + \cdots + (2n-2) + 2n \end{aligned}$$

These terms are all of the *even* natural numbers from 2 to $2n$. How can we find a formula for this sum? Do we need to do any extra work, or can we apply a previously-proven result? Well, since all of the terms are *even*, we can divide everything by 2 and write

$$\begin{aligned} \frac{1}{2}\left(S(2n) - T(n)\right) &= \frac{1}{2}\big(2 + 4 + 6 + \cdots + (2n-2) + 2n\big) \\ &= 1 + 2 + 3 + \cdots + (n-1) + n = S(n) \end{aligned}$$

and we can be assured that all of the terms in the sum on the far right are, indeed, integers. Not only that, they are *all* of the consecutive integers from 1 to n, and we have a formula for that sum! Now, *everything is written in terms of formulas we already know*, namely $S(n)$ and $S(2n)$, and the one formula that we are seeking, namely $T(n)$. The last step now is to rearrange the equation to isolate $T(n)$ and then substitute what we know about the formulas involving S:

$$\begin{aligned} \frac{1}{2}\left(S(2n) - T(n)\right) &= S(n) \\ S(2n) - T(n) &= 2S(n) \\ S(2n) - 2S(n) &= T(n) \\ \frac{(2n)^2 + 2n}{2} - \frac{2 \cdot (n^2 + n)}{2} &= T(n) \\ \frac{4n^2 + 2n - 2n^2 - 2n}{2} &= T(n) \\ \frac{2n^2}{2} &= T(n) \\ n^2 &= T(n) \end{aligned}$$

This looks rather nice, doesn't it? Despite having to muddle through some algebraic steps, we arrived at one of the conclusions we were hoping to prove: that the sum of consecutive odd integers is a perfect square. Not only that, we have managed to prove precisely how that square number is related to the number of terms in the sum. Specifically, a concise way of summarizing the result that we just proved is to say that "the sum of the first n odd integers is n^2."

Alternate Solution: An Inductive Argument

Could we have proven this in a different way? What if we had not yet proven the result from the previous section, or if we hadn't thought to use it in that way? Could we have somehow taken advantage of the geometric structure of the sums that we noticed at first?

Let's go back and think about this in a slightly different way. Specifically, let's see why adding one more term to a sum produces another square number. Suppose we knew already that one of the sums produced a square number; we know this is true for the first sum ($1 = 1^2$), but let's assume that this happens for some arbitrary number of terms, n. That is, let's *assume* that

$$1 + 3 + 5 + \cdots + (2n-3) + (2n-1) = n^2$$

for some value of n. Given this as a fact, what can we subsequently deduce about the next sum? When we add one more term to the sum, we add on the next odd integer, $2n + 1$, so let's see how this affects the value of the sum:

$$1 + 3 + 5 + \cdots + (2n-3) + (2n-1) + (2n+1) = n^2 + 2n + 1 = (n+1)^2$$

This seems to confirm our belief, doesn't it? Knowing that one sum behaves in the way we expect it to ("if the sum of the first n odd integers is $n^2 \ldots$") allows us to deduce that the next sum must *also* behave in the same way ("…then the sum of the first $n + 1$ odd integers is $(n + 1)^2$"). Does this also prove the result? What do you think? Does it feel strange to essentially assume our result to prove something further about it? Is that really what we did?

This proof strategy, using one form of the result to prove something about a "subsequent" form of the result is called **mathematical induction**. (In general, the meaning of the term "subsequent" depends on the context; here, it meanis the next sum with one more term.) We will examine this strategy in more detail in the next chapter. For now, we will point out that this is a perfectly sound strategy, but it is highly dependent on the fact that the *first* sum behaves appropriately: $1 = 1^2$. That way, the work we did allows us to deduce that the second sum behaves that way ($1 + 3 = 2^2$), which then alllows us to deduce that the third sum behaves that way ($1+3+5 = 3^2$), and so on… What if we had only been able to prove that second part, but the first sum didn't work out in the way that we wanted? Would we stil be able to prove the result? What does this tell you about the induction strategy, in general? We will address some of these issues in more generality later on.

Generalizing: Arithmetic Series

One final sum problem we want to mention is strongly related to the two that we've seen so far and, in fact, if we had proven this next result first, we wouldn't have had to do anything more to prove the first two! In that sense, this next result is *stronger* than the first two: the truth of this result *implies* the truth of the first two. (This is a common notion in mathematical terminology, to label results as *stronger* or *weaker* than others.)

For this result, we want to examine a general **arithmetic series**. This phrase means that we're adding a sequence of numbers where the difference in value between successive terms is a fixed value. Another way of thinking about this is that each term is obtained from the previous one by adding on a fixed constant. Notice that the sums we've examined in the last two puzzles were arithmetic series: in the first sum, each term differed by 1 (or, we added 1 to each term to get the next term), and in the second sum, each term differed by 2 (or, we added 2 to each term to get the next term).

How can we represent a general arithmetic series? Knowing that successive terms must differ by a fixed constant, let's assign that value a variable, say c, for constant. Now, there must be a first term in the sum, as well, so let's assign that value a variable, say a, since it's the first letter. We just need one more variable to tell us how *many* terms there are in the sum, so we will use k, since we've used that variable before with the same meaning. Now, we can represent the entire sum with just these three variables:

$$A(a, c, k) = a + (a + c) + (a + 2c) + (a + 3c) + \cdots + (a + (k-2)c) + (a + (k-1)c)$$

We can use the fact that each pair of successive terms differ by c to express the second term using the first term, a, and we can use this to express the third term, and so on, by continually adding c. We wanted k terms in total so, thinking of the first term as $a + 0 \cdot k$, the final term will be what we obtain after adding c to the first term $k - 1$ times (there are k numbers from 0 to $k - 1$, inclusive). Notice, as well, that we introduced the notation $A(a, c, k)$ to mean "the sum of the arithmetic series with first term a, constant difference c, and k terms". Now, how can we figure out this sum?

Let's employ a strategy that worked before: in the first sum puzzle, we wrote the terms of the sum forwards and backwards and added them together. This allowed us to create many pairs of terms that all had the same sum, reducing the sum to a multiplication. What happens when we do that here? We see that

$$\begin{array}{ccccccc} a & + & (a+c) & + \cdots + & (a+(k-1)c) & = & A(a,c,k) \\ (a+(k-1)c) & + & (a+(k-2)c) & + \cdots + & a & = & A(a,c,k) \\ \hline (2a+(k-1)c) & + & (2a+(k-1)c) & + \cdots + & (2a+(k-1)c) & = & 2A(a,c,k) \end{array}$$

Again, we find that each pair of terms has the same sum, and in this case that sum is $2a+(k-1)c$. How many such pairs are there? There are exactly k terms, of course! (That's why we chose to use that variable, even.) Representing the sum as a a multiplication, we can now deduce that

$$2A(a, c, k) = k \cdot (2a + (k-1)c)$$

and therefore,

$$A(a, c, k) = \frac{k}{2} \cdot (2a + (k-1)c)$$

Does this look like what you expected for a result? Did you have any expectations? It sometimes helps to try to "guess" what might happen, and then see if and how the results match up with your intuitions.

Applying the General to the Specific

We mentioned before that the sums we examined previously were both arithmetic series, so does this formula yield the correct value for those sums? In the first puzzle, the values of the variables were $a = 1$, $c = 1$, and $k = n$; plugging in those values yields

$$A(1, 1, n) = \frac{n}{2} \cdot (2 + (n-1)) = \frac{n}{2} \cdot (n+1) = \frac{n^2+n}{2}$$

which is, indeed, what we derived. What about the second sum? What were the values of the variables? Is the formula correct? We will leave it to you to verify that result.

Another Representation

As a final comment for this puzzle, we want to discuss one other way of representing the formula we just derived. Look at the term in the parentheses and write it slightly differently: $a+(a+(k-1)c)$. Do those terms look particularly interesting? Well, they are the first and last terms of the sum, respectively. This gives us a different way of stating the sum formula we derived: $A(a, c, k) = \frac{k}{2}(a + b)$, where a is the first term of the sum and b is the final term. This version of the formula can be more convenient, and lets us verify some sums more quickly.

For instance, if we told you to find the sum of an arithmetic series with first term 12 and last term 110 and 14 terms in total, you wouldn't have to bother figuring out the constand difference c; instead, you could simply find the sum: $\frac{14}{2} \cdot (12 + 110) = 854$. Much faster, right? What is the value of c for that arithmetic series? Is there an easy way to find c, given a and b and k?

Lessons From This Puzzle

It can be helpful to be aware of previous results, since they can make other proofs shorter and easier. Sometimes, it's difficult to recognize when a particular result would be useful or, even if you recognize its use, it may be difficult to figure out how to apply it. In this case, we recognized that we had proven a sum formula before, so it made sense to at least try to figure out how it might be useful in proving a different sum formula. However, there was a completely different way to prove the formula for the sums of odd integers that didn't depend on our previous result. That hints at a more general result, and a curious mathematician would try to explore the problem in more generality, which we did by looking at an arbitrary arithmetic series. In the end, though, we used multiple strategies for the first two sum formulas, and applied just one of those to the general series problem. Could we have used the strategies in other settings? Could we prove the first sum formula by induction, as well? Could we prove the second sum formula using the forwards/backwards writing technique? Try to use those strategies and see what happens. It may seem strange or unnecessary to you, because we already have the results, but seeing how different techniques work in different settings is a valuable lesson. In mathematics, it is often as hard (or harder, even) to figure out which strategy to use in a proof as it is to figure out the result to be proven. With that in mind, it's helpful to practice particular strategies to develop an intuition for when they will work and when we need to try something else.

1.4.4 Friend Trends

Problem Statement

This puzzle is based on the following anecdote concerning a Hungarian sociologist and his observations of circles of friends among children.

> "In the 1950s, a Hungarian sociologist S. Szalai studied friendship relationships between children. He observed that in any group of around 20 children, he was able to find four children who were mutual friends, or four children such that no two of them were friends. Before drawing any sociological conclusions, Szalai consulted three eminent mathematicians in Hungary at that time: Erdos, Turan and Sos. A brief discussion revealed that indeed this is a mathematical phenomenon rather than a sociological one. For any symmetric relation R on at least 18 elements, there is a subset S of 4 elements such that R contains either all pairs in S or none of them. This fact is a special case of Ramsey's theorem proved in 1930, the foundation of Ramsey theory which developed later into a rich area of combinatorics."
>
> (Quoted from lecture notes by MIT Prof. Jacob Fox.)

The puzzle we now present follows the same idea but with some smaller numbers. Specifically, we are interested in investigating the smallest size of a group of people that *necessitates* a subgroup of three people that are all mutually friends or all mutually enemies.

> Assume that amongst a group of people, any two of them are either friends or enemies, and that these are the only possible relationships (i.e. no acquaintances or frenemies or anything like that). Take a group of four people and try to assign a designation of friend/enemy to each pair so that there are *no* groups of three people that are all friends or all enemies. Can you do this with a group of five people? How about six? Seven? Ten? Twenty? Try to identify a cutoff number for the size of the group where you can be *guaranteed* to find a subgroup of three people that are all friends or all enemies.

Think carefully about this before turning the page and reading our solution.

Representing The Problem Effectively

Did you figure it out? This is a very tricky puzzle, so don't feel bad if you struggled with finding a solution. In fact, we think that investigating this puzzle is just as important as actually finding an answer, because there are several ways to approach this puzzle and it's always interesting to see how different people interpret the puzzle.

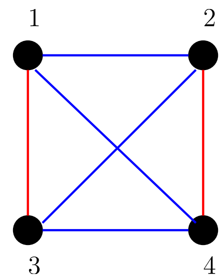
Let's start by discussing how to even write down/draw/talk about this situation. For any of the questions posed by this puzzle, we are meant to consider a group of people with a certain size and think about the relationship between any two people in the group. To tackle this puzzle, we will need a way to represent all of these relationships in an efficient and easily-interpretable way, so that we can verify the desired property about the subgroups of size three. Specifically, we want to easily identify whether or not there are any subgroups of size three that are *homogeneous*, in the sense that the three people are *all* friends or *all* enemies. From now on, we will refer to this as the **"homegeneity property"**.

How could we do this? How could we represent the people and their relatinships? We could number the people in the group, then write out a list of all pairs of numbers and label each pair with F (friend) or E (enemy). Let's try doing that for a group of four people:

$$12F \quad 13E \quad 14F \quad 23F \quad 24E \quad 34F$$

Does this friend/enemy group satisfy the homogeneity property? It's not so easy to verify, is it? For one, the numbering makes it difficult to find subgroups of size three, and to verify the property, we need to check *all* such subgroups to make sure they are not EEE or FFF. Perhaps we should find a better way of *representing* the information of the puzzle before attempting a solution. Can you think of a more visually pleasing way of representing whether two people are friends or enemies, for all possible pairs in the group? Specifically, we would like to have a relatively efficient way of looking for subgroups of size three and recognizing whether they are all friends or all enemies.

Let's try representing each person in the group as a single dot and connecting two people with a type of line dependent on whether those two are friends or enemies. For example, let's connect two people that are friends with a blue line and two people that are enemies with a red line (and remember that any two people are either friends or enemies and nothing else, so each pair of dots must have some colored line between them). For example, the following diagram depicts the relationships we assigned in the line above, with the other notation:



Now, what would we be looking for to verify the homogeneity property? We want three dots (three people) so that all of the lines between them are either blue (all friends) or red (all enemies). That's right—we're looking for **monochromatic triangles**! (Note: we want the vertices of the triangle to be one of the original dots we drew; that is, we don't want a vertex to be a place where two lines cross. Also, *monochromatic* comes from the Greek words *monos* and *khroma*, meaning "one" and "color", respectively.) This representation is much easier to interpret visually and makes checking for a solution much faster.

Based on the diagram above, we have addressed the question regarding four people: we have found a particular arrangement of friends and enemies so that there are no subgroups of size three that are either all friends or all enemies. That is, there are no subgroups of size three with the homogeneity property. This shows that such a situation can be achieved with four people, so we are not *guaranteed* to have a group with the homogeneity property amongst four people.

Can you find another such arrangement? How can you be sure that it's a *different* arrangement than the one we've already seen? How many different arrangements are there that satisfy the homogeneity property? Now, try drawing an arrangment that *does* have a subgroup of size three with the homogeneity property. What does that look like? How many of these arrangements are there?

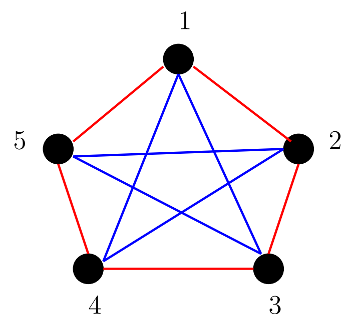
Restating the Problem for $n = 5$

Let's move on and think about a group of five people. Our diagram changes because we have five dots now, and this means there are more lines to draw. Still, we are looking to fill in all of the connections with a blue or red line and make sure there are no monochromatic triangles. Is this possible? (Hint: try arranging the dots into a regular pentagon shape and then filling in the lines.) Try to draw this a few times and see if any of your arrangements work. It may also help to draw in a few lines randomly and then guide your choices from there on out by making sure that you don't create any triangles when you add a new line.

Did you figure it out? Turn the page to see how we did it …

Solution for $n = 5$

Here is our arrangment of red/blue lines amongst five dots that completely avoids the homogeneity property:



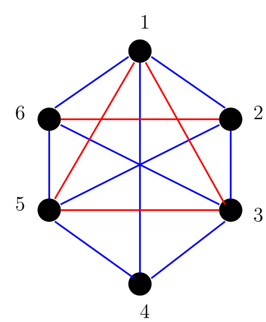
Notice the elegant symmetry of the figure: all of the red lines are on the outside of the pentagon, and all of the blue lines are in the interior of the shape. The reason this works is that any triangle using three dots as vertices must use either two outside lines and one inside line, or two inside lines and one outside line. (Think about that: why couldn't we use three inside lines or three outside lines to make a triangle?) This *guarantees* that any triangle we draw will use two differently-colored lines, so this figure does *not* have the homogeneity property! Of course, we could look at all possible triangles inside the diagram and make sure none of them use one color. How many such triangles are there? How quickly could you check all of them by hand? Is it easier to do that, or to notice the inside/outside property that we mentioned above?

Perhaps you found a solution that doesn't look like the drawing we have. How can you tell whether it's actually a different figure? How many blue and red lines are there in your diagram? In ours? Try redrawing your figure by moving the dots around but maintaining the relationships between the dots (i.e. the color of line drawn between any two of them). Can you make your figure look like ours? What do you think this says about the number of solutions to this puzzle?

What about $n = 6$?

Okay, now we're ready to think about what happens when we have six people. In terms of the dots and lines, we're looking to draw all possible connections between six dots with either blue or red lines and ensure that there are no triangles with the same line type. Before you start drawing, try to think about the solutions to this puzzle when we were working with four and five dots. What did those solutions look like? What was the number of lines that we had to fill in? How many will we have to draw this time? Can we try to make this figure look like the solution for five dots? It sometimes helps to think about how a solution to a current puzzle might be similar to previous work. Now, try to draw this figure and see what happens.

Did it work? Why not? Where did you run into trouble? How many lines could you draw before you were *forced* to make a monochromatic triangle? That is, how many lines could you fit into the figure before the next one you drew would make a monochromatic triangle, no matter whether it was blue or red? These are just tangential questions, in a way, to solving this particular puzzle, but they're worth thinking about because they're interesting in their own right and they may guide us toward a solution for this puzzle or a generalization thereof. For illustration's sake, here is one of our attempts at trying to assing red and blue lines in a diagram. Why did we stop here? How many more lines need to be added? Can we add any of them?

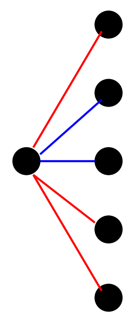


The situation we face now is interesting because it's of the opposite nature to the kind of situations we faced before. With four and five dots, we wanted to show that it was *possible* to arrange all of the lines to make no monochromatic triangles. To show that, we just had to do it! Exhibiting a *particular* figure with the desired property was sufficient to show that it was possible to achieve the property we wanted. With six dots, though, it seems like it is *not* possible to arrange the lines so that there are no monochromatic triangles. How can we prove that this is a fact? It is tempting to say that we should just look at all possible arrangements of the lines and argue that there is *at least* one monochromatic triangle in every single one of them. Is this feasible? How many arrangements of the lines are there? How could we easily find a monochromatic triangle in any given diagram? Remember how we did this with the figure with five dots? We noticed that any triangle would have to use at least one line from the outside and at least one line from the inside, which guarantees right away that any triangle has two types of lines. Could we do the same thing here, and identify some property that *guarantees* a triangle?

The issue is that there are *too many* possible arrangments of the lines in the diagram with six dots for us to check all of them by hand! There are 15 lines to be drawn, each of which could be either blue or red, so it seems like there are 2^{15} possible arrangements. This is a big number! (In actuality, there are slightly fewer possibilities because some of them are equivalent in some sense; more technically, they are called "*isomorphic*".)

Solution: Working with an *Arbitrary* Diagram

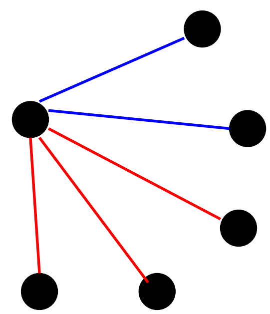
We need to be more clever with our argument so that we can prove a property about *any* diagram without drawing a particular one. That is, we need to find some fact, some property that is true of all of the possible diagrams with six dots, that will still allow us to deduce that there must be a triangle. One way to approach this is to think about drawing the lines in one small section of the diagram. Specifically, let's take any of the six dots and consider the five lines coming out from that dot. For example, we might have something like this:



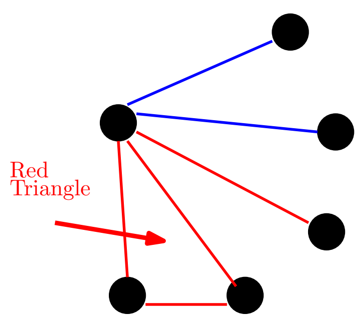
How many are blue and how many are red? This is partially a trick question: we're not really considering any *particular* diagram (like the one above) but rather trying to find a fact about all possible diagrams. Thus, we can't answer that question too specifically. Pretend we are prsented with an **arbitrary** diagram, and we have to make an argument that will work no matter what that diagram was.

Here's what we *can* say: There must be at least three blue lines *or* at least three red lines. Do you see why this is true? The only way this *wouldn't* be true is if there were two (or fewer) blue lines *and* two (or fewer) red lines leaving this particular dot, for a total of four (or fewer) lines. We know that all possible connections must be drawn, though, so there should be five! (This argument is an example of a concept known as the **Pigeonhole Principle**. The idea is that we can't place five objects, of two different colors, into two different boxes without putting three objects of one color into one box. This is an incredibly useful strategy with these types of problems, and we will examine the principle in much greater detail later on in Section 8.6.)

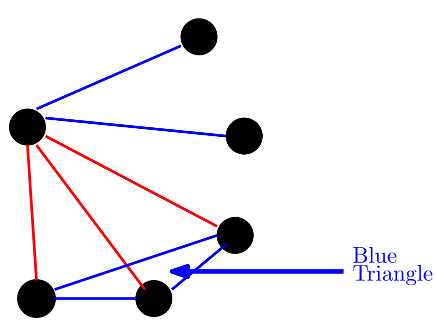
So where do we stand? We started with *any* of the figures with six dots and all lines filled in, and focused on one particular dot; coming out from this dot, there must be three blue lines *or* three red lines. It could be either color, so we can't just assume it's red and follow an argument that way; we can do that, but we have to come back to this point afterwards and see what would change if the three lines were blue. So let's do that: let's examine all of the figures where there are three red lines exiting this particular dot. Where can we go from there? We haven't yet assumed anything about the other lines in the figure, so let's look at what those could be. Examine the picture below to see what line colors we have assumed exist so far:



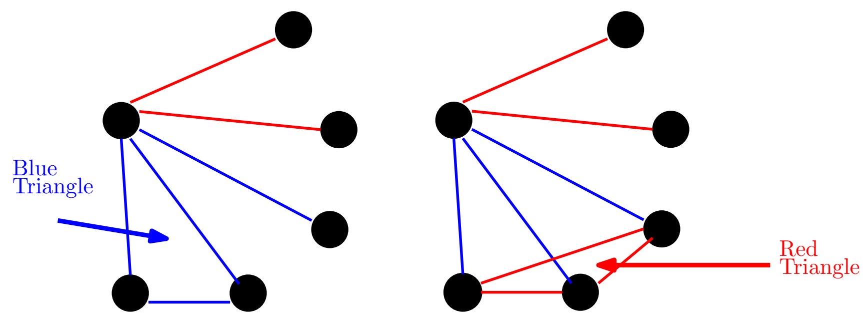
Now, what lines could be added to this diagram that would avoid making a triangle of one color amongst three dots? We can't necessarily make any assumptions about the lines coming out from the two dots that are isolated in the picture, so let's focus on the three dots on the bottom. What color could the lines among those be? Well, if any of them are red, that would form a monochromatic triangle between the two endpoints of that line and the original dot we focused on! That would be a problem.



Okay, the only way to avoid that is to make all of those lines blue. But that would make a blue triangle among those three dots! Wow, it looks like we *cannot avoid* making a monochromatic triangle no matter what we do!



Let's go back to our Pigeonhole argument and reassess the situation. What if the three lines of the same type that were guaranteed by the argument were blue instead of red? Well, nothing would really change, right? We would still be stuck, in terms of adding new lines among the three dots on the bottom of the figure:



If we include any blue lines, that forms a monochromatic triangle with the original dot, and if we make all of them red, that forms a monchromatic triangle there! In this sense, the two arguments we followed after the Pigeonhole argument were *identical*; if we were to replace every instance of the word "blue" with "red" and vice versa, we would have the same argument. Sometimes, mathematicians will use this situation to shorten a proof and just say that "without loss of generality, the three lines are red." This is usually taken to mean that if we were to make the other choice instead (i.e. if the lines were blue) then the further argument would have an identical structure, mathematically, so we can save space and time by not writing the same words over again. This is so common, in fact, that you might sometimes see this phrase, "without loss of generality", abbreviated as **WOLOG** or **WLOG**.

Solution: Summarizing Our Results

What have we accomplished so far? We produced *specific* diagrams that showed we could arrange the lines among four and five dots so that we can avoid a monochromatic triangle, and we argued that *any* diagram of lines with six dots *must* have a monochromatic triangle. In terms of the friends/enemies formulation of the puzzle, this means that any group of six people must have a subgroup of three people that are all friends or all enemies.

Notice how helpful it was to recast the puzzle into this dots/lines formulation; it allowed us to completely forget about the social context of the problem (which can be distracting, in a way) and let us simplify our terminology and notation (we went from labeling pairs of people as "friends" or "enemies" to simply drawing one line between two dots). This is a very useful strategy: extracting the inherent *structure* of a puzzle—the underworkings, the relationships between the elements, how they interact, etc.—and rewriting everything in terms of just those parts. This can make the puzzle easier to understand and tackle, and it can guide us into devising better notation. What if we had continued to solve this puzzle with the $13F, 23E, \dots$ notation? That may have eventually worked, but it would have been much harder!

One of this puzzle's original questions was to identify a cutoff number so that any larger group of people would necessarily have this subgroup property. Do you think we have accomplished that? Have we identified a cutoff? Could six be that number? Why or why not? In any group of seven people, there's a smaller group of six people, and then our work above proves that there must be three mutual friends/enemies among that group! Certainly, this works for any group of people of size larger than six, so this must be that precise cutoff point we were looking for. This is an analogous result to the one mentioned in the original statement of the puzzle, where the Hungarian sociologist noticed this phenomenon for subgroups of size four. That problem is much more difficult to solve, so we handled a smaller, simpler case here. Both of these results are related to a larger class of problems known as **Ramsey Theory**. This branch of combinatorics and graph theory works with identifying these kind of "cutoff points" where, as the size of some structure (like a group of people) grows and grows, there is eventually a point where we can be *guaranteed* to find a subgroup with a certain property (three mutual friends/enemies). What was at first thought to be a sociological phenomenon turned out to be a rigorous mathematical fact. How about that!

Generalizing: Questions for You

Let's pose some interesting and related questions before moving on. What if we had been looking for homogeneous groups of a different size, like four or five or twelve? Certainly, we would have to have a larger group of people, overall, to guarantee finding such a subgroup. Can we always do this? That is, given any desired subgroup size, can we identify a cutoff point in the way that we did here? Can you figure out how to prove that such a cutoff point *must* exist, even without finding the particular number? Furthermore, what if we allowed for a third possibility: friend, enemy, unacquainted. Could we answer similar questions about homogeneous groups? These are all questions related to Ramsey Theory and some of them are quite difficult to answer and took mathematicians many years to address. Many of these kinds of simply-stated questions are still open, unsolved problems! Don't be discouraged if you don't make any progress on these questions. We believe that even attempting to answer them and thinking about the issues therein is meaningful and beneficial enough, in itself.

Lessons From This Puzzle

This puzzle brought up several difficulties. First, we had to find a way to interpret the puzzle in a meaningful way so that we could even address the questions it asked, and this involved coming up with appropriate *notation* to represent the elements of the puzzle. This is an important part of mathematical problem-solving, particularly for a puzzle like this that doesn't incorporate the notation and visualization as part of the problem statement.

Second, to identify six as the group cutoff size, we had to somehow prove that something *is not* possible, but the number of possible configurations to examine was way too large to examine each one individually. This happens frequently, particularly in problems related to computer science and algorithms. To address this, we had to employ a strategy far more clever than mere brute force, and it's not always clear what strategy that should be. Here, we essentially started to try to fill in the lines as if it was going to work out, and then realized that we reached a point that was impossible to fix. Proving that something is possible can amount to just showing an example of that phenomenon (which we did with the groups of size four and five), but proving something is *impossible* can be much trickier and require some context-dependent ingenuity.

Lastly, we saw that it can be interesting to think of questions closely-related to the puzzle at hand that simply tweak one or more of the conditions of the problem. What if we look for larger subgroups? What if we allow for more types of lines? How does this change the results? Exploring the boundaries of puzzles by changing the conditions like this can lead to new mathematical discoveries and techniques, and keeps mathematicians actively searching for new knowledge and ways of sharing that knowledge.

1.4.5 The Full Monty Hall

Problem Statement

This puzzle involves only basic probability and arithmetic, yet it has continually stumped some very smart people over the years. In fact, a debate erupted in 1990 when Marilyn vos Savant published the puzzle and her solution in her column in *Parade* magazine, with many people (mathematicians included) writing her letters to agree or disagree with her (correct, we should say) answer. Let's see what you think!

> Suppose you're on a game show and you're given the choice of three doors. Behind one door is a car; behind the others, goats. The car and the goats were placed randomly behind the doors before the show. The rules of the game show are as follows: After you have chosen a door, the door remains closed for the time being. The game show host, Monty Hall, who knows what is behind the doors, now has to open one of the two remaining doors, and the door he opens must have a goat behind it. If both remaining doors have goats behind them, he chooses one at random. After Monty Hall opens a door with a goat, he will ask you to decide whether you want to stay with your first choice or to switch to the last remaining door. Imagine that you chose Door 1 and the host opens Door 3, which has a goat. He then asks you "Do you want to switch to Door Number 2?" Is it to your advantage to change your choice?

Of course, we are assuming that you would prefer to win a car over a goat, and that you want to maximize the chances of winning that one car. Also, we should mention that this puzzle takes its name from the host (Monty Hall) of a TV game show called *Let's Make a Deal*.

So what do you think? Imagine yourself standing on the stage in front of a TV audience, when Monty Hall asks you, "Do you want to switch to the other door?" What do you do?

Think carefully about this before turning the page and reading our solution.

Solution: *Always* Switch

We'll state the answer right away because it might shock you: you should definitely switch your choice! Reasoning this out and obtaining this solution is the tricky and confusing part, and establishing the right way to interpret the puzzle is part of what has confused solvers for so long.

Analyzing an Incorrect Argument

Let's start by showing you an *incorrect* "solution" that claims switching is irrelevant. Imagine you and your friend heard this puzzle, and he/she gave you this explanation. How would you respond? Would you agree? Why? If not, how would you tell them they're wrong? What is wrong with their explanation?

> Well, after I pick a door and Monty Hall shows me a goat behind another door, then there are only two doors that are unopened. One of them has a goat and the other one has a car, so there's a 50/50 chance that the car is behind my door and a 50/50 chance that the car is behind the other door. Therefore, it doesn't matter whether I switch or not, so I might as well stick with the choice I already made.

Are you convinced by this? Let's try to figure out what's wrong with this argument. The main question we need to address to solve this puzzle involves figuring out two numbers: the probability of winning the car by sticking with our first choice, and the probability of winning the car by switching to the other door. We need to identify these two values and compare them; only *then* can we definitively address the question of the puzzle.

Now, the argument above seems to address both of these probabilities by saying they are both 50%, but there is a problem with how the arguer interprets the situation. What do you think the chances are of winning the car by staying with the first choice? In essence, this is equivalent to not even having Monty Hall show us another door with a goat behind it. If we are going to stay with our first choice of a door, we might as well not even see a goat behind a different door since that doesn't *affect* the object behind the door we originally chose. Let's restate this idea to reiterate its importance:

> Since there are three doors, the chances of picking the right one first is $\frac{1}{3}$, and seeing a goat behind another door *doesn't change that fact.*

This is the problem with the above argument and, in fact, one of the most common mistakes made in "solving" this puzzle.

The next step is to figure out the probability of winning the car *after* switching and compare this to $\frac{1}{3}$. There are several ways to accomplish this, in fact. One concise way is to reason that switching results in success (winning the car) whenever we first choose a door that happens to have a goat. In those cases, the two unchosen doors conceal a goat and a car, in some order, and the game show host is forced to show us the goat; thus, the car is concealed behind the remaining door, and switching results in a win. Since we will choose a door with a goat behind it $\frac{2}{3}$ of the time, we conclude that switching results in a win $\frac{2}{3}$ of the time.

Enumerating the Possibilities

These explanations might seem unsatisfactory to you, so let's try to actually enumerate (explicitly count) the possible arrangements of the goats and the car behind the doors and write down what happens if we switch in each case. The first thing to notice is that the numbering of the doors is *irrelevant* since all choices are made randomly; that is, whether the car lies behind the door with "#1" printed on it, or "#2" or "#3", the results will be the same: we still have a $\frac{1}{3}$ chance of identifying that door with the car. Accordingly, we can assume WOLOG (remember that this acronym means "without loss of generality") that the car lies behind Door #1 and the goats stand behind Doors #2 and #3. Of course, this is our imposition on the problem, and we can't say that the game-player knows this (otherwise he/she would pick Door #1 every time!). With this arrangement in mind, let's examine all 3 choices we could make at the beginning, and see what switching or staying would accomplish in each case:

Door #1	Door #2	Door #3
Car	Goat	Goat

Our choice	Host shows	Result of switching	Result of staying
Door #1	Door #2 or Door #3	Goat	Car
Door #2	Door #3	Car	Goat
Door #3	Door #2	Car	Goat

One important observation is that when we initially choose the door with the car, the host could choose either of the remaining doors to show us a goat, and he makes that choice *randomly*. For either choice, though, we lose by switching and win by staying. Still, those situations only occur $\frac{1}{3}$ of the time, i.e. after we chose the door with the car behind it, initially. Since each of the rows of the table above is equally likely, we can conclude that $\frac{2}{3}$ of the time we win by switching, while $\frac{1}{3}$ of the time we win by staying.

Does this puzzle make more sense now? Try posing this puzzle to some of your friends and family and gauge their reactions. How many produced the correct answer? How many could correctly explain it? How many erroneously said "it doesn't matter"? How many had already heard the puzzle before?

Generalizing to Many Doors and Cars

Let's look at a generalization of this game show situation and try to prove whether or not switching is also a good idea there. Specifically, let's say there are n doors and m cars in total, so there are $n - m$ goats. To analyze this, we need to specify that $m \leq n - 2$. Think about why this is necessary:

- If $m = n$ were true, then we always win all the time, whether we switch or not. Hence, there's nothing to prove in this case.
- If $m = n-1$ were true, then whenever we happen to choose the door with the *only* goat behind it at first, the host is *unable* to show us a door with a goat. Hence, the game is ruined and the question of switching is moot.

Now, with these variables in place, here are the new rules of the game: We choose one of the n doors. The host identifies all *other* doors that conceal a goat and randomly chooses one of those doors and opens it. We then have the option to stick with our original choice or switch to *any* of the other doors, of our choosing. What is the strategy now? Should we switch? Should we stay? Does the answer depend on m and n at all? How?

We will approach this modified puzzle in much the same way as the first approach to the version above. We can't possibly enumerate all situations in this version because m and n are unknown variables. Instead, we need to apply logical reasoning to deduce the probabilities associated with winning when staying and when switching. The first key observation is exactly the same as one we made before: the probability of winning when *staying* is exactly the probability of choosing a door concealing a car at first. When we choose a door with a car behind it first, no matter what other door the host reveals, staying on our current choice results in a win. Furthermore, when we chose a door concealing a goat at first, staying results in a loss. Thus, the only way to win while sticking with our first choice is by choosing one of the m doors with a car behind it out of the n total doors. This probability is precisely $\frac{m}{n}$.

To identify the probability of winning after *switching*, we need to think carefully about the probabilities associated with each step. Notice that since $m \geq 2$ is a possibility, it may be that we chose a door with a car at first, switched our choice, and *still won*. With that in mind, we should examine two different cases, here: (a) what happens when we choose a door with a goat first, and (b) what happens when we choose a door with a car first. Each case will leave a different number of options for the host and, subsequently, a different number of ways for us to switch and win, so we should handle them separately.

(a) Let's say we first chose a door with a goat. There are now $n - m - 1$ doors remaining that conceal goats, and the host randomly picks one of those to open. From our perspective, switching leaves us with $n-2$ options (we can't switch to the opened door or our first choice), m of which are cars. Thus, the probability of winning after switching, in this *particular* case, is $\frac{m}{n-2}$.

Since there were $n - m$ goats originally, this case occurs with a probability of $\frac{n-m}{n}$. Therefore, the contribution of this case to the total chances of winning after switching is

$$\frac{n-m}{n} \cdot \frac{m}{n-2} = \frac{nm-m^2}{n(n-2)}$$

(Think about why we *multiplied* these probabilities together. Why did we need to do that at all? Why didn't we add them together? What will we do to combine this probability with the probability associated with the next case?)

(b) Next, let's say we first chose a door with a car. There are now $n-m$ doors remaining that conceal goats, and the host randomly picks one of those to open. From our perspective, switching leaves us with $n-2$ options, $m-1$ of which are cars. Thus, the probability of winning after switching, in this *particular* case, is $\frac{m-1}{n-2}$.

Since there were m cars originally, this case occurs with a probability of $\frac{m}{n}$. Therefore, the contribution of this case to the total chances of winning after switching is

$$\frac{m-1}{n-2} \cdot \frac{m}{n} = \frac{m^2-m}{n(n-2)}$$

Since these two cases occur separately (i.e. they both can't occur simultaneously) we should add these probabilities together. This will tell us the totaly probability of winning a car after switching from our original choice to another random door:

$$\begin{aligned} \frac{nm-m^2}{n(n-2)} + \frac{m^2-m}{n(n-2)} &= \frac{nm-m^2+m^2-m}{n(n-2)} \\ &= \frac{nm-m}{n(n-2)} \\ &= \frac{m(n-1)}{n(n-2)} \\ &= \frac{m}{n} \cdot \frac{n-1}{n-2} \end{aligned}$$

Now, there's a reason we chose to write the fraction the way we did here. We want to compare this probability to the chances of winning after staying with our first choice of door, which was $\frac{m}{n}$. We see that the probability of winning after switching is, in fact, a multiple of that other probability, and the factor $\frac{n-1}{n-2} > 1$ because $n-1 > n-2$. Written in inequality form:

$$\frac{m}{n} < \frac{m}{n} \cdot \underbrace{\frac{n-1}{n-2}}_{>1}$$

Therefore, the chances of winning after switching are *strictly better* (i.e. not equal to, always better) than the chances of winning after staying. We should always switch to another random door!

Applying the General to the Specific

The original version of this puzzle is the specific case where $n=3$ and $m=1$, so we can check that our result makes sense. The formulas we derived tell us the chances of winning after switching are $\frac{1}{3}$, as we found previously, and the chances of winning after staying are $\frac{1(3-1)}{3(1)} = \frac{2}{3}$, as we found previously. Neat!

Generalizing: Questions for You

What happens for other values of m and n? Can you make the "always switch" strategy significantly better than the "always stay" strategy? That is, how large of a difference can we get between the probability of winning associated with the two strategies? How small can we make it? Is it possible to make them equal?

Another modified version of this puzzle is based on the host opening more than 1 door, revealing multiple goats. Specifically, suppose there are n total doors, m of which have cars, and that, after your first choice, the host randomly identifies p doors with goats and opens all of those, after which you may choose to switch to any of the remaining $n - p - 1$ doors, or stick with your first pick. What is the best strategy in this game? What sorts of conditions do you need to impose on m, n and p to ensure we can even play the game at all? Should you always switch, or does it depend on p? How large/small can we make the difference in the chances of winning for the "always switch" and "always stay" strategies?

Lessons From This Puzzle

Intuition and quick decisions are sometimes helpful in *guiding* us to a solution, but it is always important to check those snap judgments to make sure they are based on sound, rational arguments. In this puzzle, saying that the chances were "50/50" maybe made sense at first, but after thinking about it more carefully and reassessing the situation, we realized there was a flaw in the argument. Specifically, that flaw had to do with interpreting the puzzle correctly and following the steps of the game show in the appropriate order. It was best to assess the probabilities in the order in which they occur as the game is played, rather than starting from an ending position and looking backwards.

In general, puzzles involving probability are quite tricky and require careful analysis, so it's important to keep that in mind. A larger lesson here, as well, is that oftentimes the most simply stated puzzles are the trickiest to figure out. Never be fooled into thinking that a puzzle will be easy to solve because the statement is short or easy to understand!

For more information about the Monty Hall problem and the psychology involved, check out this link to the following paper: Krauss, Stefan and Wang, X. T. (2003). "The Psychology of the Monty Hall Problem: Discovering Psychological Mechanisms for Solving a Tenacious Brain Teaser", *Journal of Experimental Psychology*: General 132(1).

1.5 It's Wise To Exercise

We'll conclude this chapter with a handful of exercises that incorporate some of the ideas we've discussed so far, or give you a chance to practice your previous knowledge, or just keep you on your mental toes. Attempt as many as you can, and discuss potential solutions with some friends to see what they think. At the end of the day, though, just think of this as a way to keep your brain muscles limber!

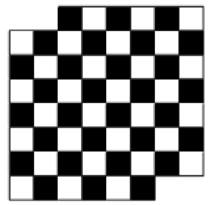
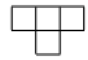
Problem 1.5.1. A fly is resting on the front of a train that is hurtling forward at 60 kilometers per hour. On the same track, 300 kilometers straight ahead, another train is hurtling towards the first train at 60 kilometers per hour. At that moment, when the trains are 300 km apart, the fly takes off at 90 km per hour. He continually flies back and forth between the trains, flying just above the track and instantaneously turning around when he reaches a train. What is the total distance traveled by the fly before the two trains crash together, squishing the fly between them in the process? How did you figure this out? Try to generalize the situation to when one train travels at a km/hr, the other at b km/hr, and the fly at c km/hr.

Problem 1.5.2. A government mint is commissioned to produce gold coins. The mint has 20 machines, each of which is producing coins weighing 5 grams apiece. One day, the foreman of the mint notices that some coins are light, and after assessing the machines, he finds that one of them is making 4 gram coins, while the other 19 machines are working perfectly. He decides to use the situation to his advantage and identify the smartest employee, to be promoted next. He tells the workers that exactly one machine is producing coins that are 4 grams, and that they need to determine which machine is broken. You, as an employee, are allowed to take one, and *only* one, reading on a scale. You can place any number of coins from any machines, of your choosing, but you must pool them together and will only see the total weight of all the coins, as a number in grams. How do you do this so that you can determine precisely which machine is the broken one?

Problem 1.5.3. In a game of chess, the Queen is allowed to move vertically, horizontally, or diagonally, in any direction, for any number of spaces. Try to place 8 Queens on a standard 8×8 chessboard so that *none* of the Queens is attacking any of the others (that is, no Queen can make one move and capture another one immediately). Exhibit a way to do this or show that it is not possible. If you found a way, how many different ways do you think there are to do so? If you showed it isn't possible, find a smaller number of Queens to place so that it is possible. What is the maximum number of Queens you can possibly place on the board in this way?

Problem 1.5.4. Start with a standard 8×8 chessboard and remove 2 squares at opposite corners, say the top-right and bottom-left. Can you cover *all* of the remaining squares with 2×1 dominos so that none of the dominos *overlap*? (Note: this is known as a *tiling* of the board.) Why or why not? What about in the general case, with an $n \times n$ board? Does your answer depend on n at all? How so?

Problem 1.5.5. Consider a standard 8×8 chessboard, with two adjacent squares removed from each corner. (See picture.) Can you tile this board with T-shaped tetrominoes? (See picture.) If so, how? If not, why not?

What about in the general case, with an $n \times n$ board? Does your answer depend on n at all? How so?

Problem 1.5.6. Given a real number x, we let $\lfloor x \rfloor$ denote the largest integer smaller than (or equal to) x and we let $\lceil x \rceil$ denote the smallest integer greater than (or equal to) x. For instance, $\lfloor 6.02 \rfloor = 6$ and $\lfloor 6.99999 \rfloor = 6$ and $\lfloor 6 \rfloor = 6$ and $\lfloor -6.5 \rfloor = -7$.

Determine a more specific and concise representation for the value of the following expressions, whenever possible. (You might have to find a few different expressions, depending on x.)

1. $\lfloor x \rfloor + \lfloor 1 - x \rfloor$
2. $\lceil x \rceil + \lceil 1 - x \rceil$
3. $\lfloor x \rfloor + \lceil x \rceil$
4. $\frac{\lfloor x \rfloor}{x}$
5. $\lfloor x^2 \rfloor - \lfloor x \rfloor^2$
6. $\lceil x^2 \rceil - \lceil x \rceil^2$

Problem 1.5.7. Find three natural numbers a, b, c so that no subset has a sum that is divisible by 3. That is, find a, b, c so that none of the following sums is divisible by 3: $a, b, c, a+b, a+c, b+c, a+b+c$. Is this possible? Why or why not?

Try to do the same thing with 4 numbers: find a, b, c, d so that no subset has a sum that is divisible by 4. Is this possible? Why or why not?

Try to generalize. Can you say anything about finding n natural numbers so that no subset has a sum divisible by n?

Problem 1.5.8. Recall the way that we solved the *Friend Trends* problem, by working with dots and colored lines. For this problem, we want to address a similar situation where we have a certain number of dots and need to draw all possible lines so that any two dots are connected by exactly one line, but in this case we don't care about the color, so we can say all lines are drawn in black, say. Can you draw this figure with 3 dots so that none of the lines cross? What about with 4 dots? Or 5? Or 6? Why or why not? Try to explain why any of those figures are impossible to achieve. If you can't achieve 0 crossings, what is the minimum number you could possibly achieve?

Problem 1.5.9. Let's use the same assumptions from the *Friend Trends* problem: any two people are either friends or enemies, and there are no other relationships. Take a group of n people and assume that no person has more than k friends. We want to separate the n people into some number of clubs so that each person is in exactly one club. How many clubs do we need, in total, so that we can distribute the n people so that nobody is in a club with a friend? Given the relationships between all the people (i.e. given two people, we know whether they are friends or enemies) and that number of clubs, how would we go about separating the people to achieve this property?

Problem 1.5.10. Draw a circle. Place 3 dots along the circumference of the circle. We want to color the sections between the dots (each section gets exactly one color) so that no dot is touched by two sections of the same color. How many colors do we need? What about if we place 4 dots around the circumference of the circle? Or 5? Try to generalize to n dots. What can you say about the number of colors required?

Problem 1.5.11. Suppose you have a drawer full of socks. It contains 2 pairs of blue socks, 3 pairs of red socks, and 4 pairs of green socks. (Also assume that left and right socks are indistinguishable.) One morning, you are in a great rush and start grabbing socks randomly, one at a time, and holding on to all of them until you have a pair. How many socks do you need to take out of the drawer to *guarantee* that you have a pair on your hands?

How does your answer change if we had twice as many pairs, of each color, as before? What if we had 3 pairs of socks in each of red, green, blue, yellow and brown? What if we had n pairs of socks in each of m colors?

Problem 1.5.12. A group of four friends find themselves on one side of a bridge late at night while walking home. The bridge is old and rickety and unsafe to cross as a group. They only have one flashlight between them and the light is only strong enough to light the way for two friends at a time. Each friend has a different level of comfort with the bridge, so they will cross at different speeds. One friend will take 5 minutes to cross, one will take 10, one will take 15, and one will take 20. If two friends cross together, they cross at the pace of the *slower* friend. How long will it take all 4 friends to get across the bridge? Can you find the method that produces the absolute shortest time?

Problem 1.5.13. Consider the usual denominations of coins for the American dollar: pennies (1 cent), nickels (5 cents), dimes (10 cents), and quarters (25 cents). What coins would you need to carry around in your pocket to *guarantee* that you can pay any price between 0 cents and 100 cents with exact change? Are there several possible sets of coins that would achieve this? What is the smallest total value of coins with this property? Are there several possible sets of coins with this same minimum total value?

Problem 1.5.14. Let a, b, c be real numbers, with $a \neq 0$. What is wrong with the following "spoof" that $-\frac{b}{2a}$ is a solution to the equation $ax^2 + bx + c = 0$, if anything?

"Spoof": Let x and y be solutions to the equation. Subtracting $ay^2+by+c=0$

from $ax^2+bx+c=0$ yields $a(x+y)(x-y)+b(x-y)=0$. Hence, $a(x+y)+b=0$, and so $x+y=-\frac{b}{a}$. Since x and y were *any* solutions, we may repeat this computation with $x=y$. Thus, $2x=-\frac{b}{a}$, and therefore $x=-\frac{b}{2a}$ is a solution. "□"

Problem 1.5.15. Explain why $(-1)(-1)=1$. Pretend you are writing for a fellow classmate of similar intelligence who is skeptical of this fact and needs to be convinced. It is *not enough* to just say "Because it is!" Try to come up with a helpful *geometric* or *physical* explanation, some kind of memorable argument.

Problem 1.5.16. For each of the following proposed equations, identify all of the real numbers that satisfy them:

(1) $|x-2|=|x-3|$

(2) $|2x-1|=|2x-3|$

(3) $|2x-2|=|3x-3|$

(4) $|x+1|=|x-5|$

(5) $|x-1|+|x-2|=|x-3|$

Problem 1.5.17. **The First Rule Of Logic Club Is . . . :** To join Logic Club, you must decide to *always* tell the truth or *always* lie. Members of Logic Club know who lies and who soothsays. I do not belong to Logic Club, but I encounter three members on the street who make the following statements:

- Jack: "All three of us are liars."
- Tyler: "Exactly two of us are liars."
- Chuck: "Jack and Tyler are liars."

Who should I believe, if anyone?

Problem 1.5.18. Solve $\sqrt{x-1}=x-3$ for all real values of x that satisfy the equation. Explain your work, and try to indicate why your answer/s is/are the *only* answer/s.

Problem 1.5.19. You have two strings of fuse. Each will burn for exactly one hour. The fuses are not necessarily identical, though, and do not burn at a constant rate. All you have with you is a lighter and these two fuses. Can you measure exactly 45 minutes? If so, explain how. If not, explain why.

Problem 1.5.20. This problem is a variation of a standard puzzle, a form of which first appeared in the Saturday Evening Post way back in 1926!

Three friends pitched in and bought a big bag of M&M candies. They brought the box back to their apartment and decided to wait and share the bag the next day at a party.

During the night, the first friend woke up and felt like having a snack. He decided to just eat his share of the candies now and not have any the next day. He opened the bag, divided the M&Ms into three equal piles, but realized there was one left over. He figured that one extra couldn't hurt, and ate his share and the extra, then put the rest back in the bag.

Later in the night, the second friend did the exact same thing. He woke up feeling hungry, divded what was left in the bag into three piles, and ate his share plus the extra one that was left over.

Even later in the night, the third friend did the exact same thing, including the extra M&M left over.

The next day at their party, the friends split the bag of remaining candies into three *equal* shares and enjoyed them. (No one acknowledged what they had all done, of course).

How many M&Ms were in the bag to begin with? What is the smallest possible number?

Problem 1.5.21. Given a list of real numbers, their *arithmetic mean* is defined to be their sum divided by the number of terms, and their *geometric mean* is defined to be their product raised to the power of one over the number of terms. That is, supposing we have $x_1, x_2, \ldots, x_n$ that are real numbers, then the arithmetic mean is

$$\frac{x_1 + x_2 + \cdots + x_n}{n}$$

and the geometric mean is

$$\sqrt[n]{x_1 \cdot x_2 \cdots x_n}$$

(Note: The n-th root of a number is the same as that number raised to the power of $\frac{1}{n}$.)

Can you identify two numbers so that the arithemtic and geometric means are *equal*? Can you identify two numbers so that the arithmetic mean is strictly greater than the geometric mean? How about the other way around?

Repeat this with three numbers, four numbers, etc. Can you identify a general pattern?

Problem 1.5.22. Consider the variable equation $6x + 15y = 93$. We want to find some *integral* solutions; that is, we want to find values of x and y that are both *integers* (natural numbers, zero, and negative natural numbers) that satisfy the equation.

1. Find a solution where both x and y are positive integers. Decribe, with a few sentences, how you came up with this solution.

2. Find a solution where one of the values, x or y, is positive and the other is negative. Again, describe how you came up with this solution.

3. How many solutions do you think there are? Try to write down a characterization of all possible solutions, or describe how you might find them all.

Problem 1.5.23. A **magic square** is an $n \times n$ array that contains each of the numbers from 1 to n^2 exactly once and has the property that every row and column (and both of the main diagonals) sums to the same number.

For example, here is a 3×3 magic square:

8	1	6
3	5	7
4	9	2

Notice that the so-called **magic sum** of each row/column/diagonal is 15 in this case.

Can you find a formula for what the magic sum of an $n \times n$ magic square must be?

(*Hint:* There is a result we discovered in this chapter that will be useful.)

Problem 1.5.24. How many whole numbers less than or equal to 1000 have a 1 as at least one of their digits? For instance, we want to count 1 and 12 and 511 once each.

Problem 1.5.25. We have several piles of koala bears. In an attempt to disperse them, we remove exactly one koala bear from each pile and place all of those koalas into one new pile. For example, if we started with koala piles of sizes 1, 4, and 4, we would then end up with koala piles of sizes 3, 3, and 3; or, if we started with piles of size 3 and 4, we would end up with piles of size 2 and 3 and 2.

It **is** possible that we do this operation *exactly once* and end up with the *exact same pile sizes* as we started with (the order of them is irrelevant; only the *sizes* matter).

Identify all the collections of piles that have this property and explain why they are the only ones.

Hint: An example of a starting situation with this property is when we have just one pile of size 1. We do the operation and again obtain one pile of size 1. Bingo.

Hint 2: Be sure to also explain why your situations are the *only* ones that work. How can we be sure you didn't miss some answers?

1.6 Lookahead

This introductory chapter is meant to get you thinking about what **mathematics** is, how we **solve problems**, and what it means to write a **proof**. Throughout the rest of the book, we will be discussing all three of these ideas in more and more detail. In doing so, we will explore several different areas of the mathematical universe. We have an overarching plan for our journey, so don't think that we are just stumbling randomly through the forest. Our major goals are to (a) formalize some of the intuitive ideas we have about mathematical objects, (2) see many examples of good proofs and develop the ability to create and write good proofs, (3) develop problem-solving skills and the ability to apply mathematical knowledge, and (4) cultivate an appreciation for both the art and science of mathematics.

Scan the table of contents at the beginning of the book to get a sense for where our journey is headed. The phrases and terminology might be foreign to you now, but by the end of the book, we will all be speaking the same language: **mathematics**.

Chapter 2

Mathematical Induction: "And so on . . ."

2.1 Introduction

This chapter marks our first big step toward investigating mathematical proofs more throughly and learning to construct our own. It is also an introduction to the first significant **proof technique** we will see. As we describe below, this chapter is meant to be an appetizer, a first taste, of what **mathematical induction** is and how to use it. A couple of chapters from now, we will we be able to rigorously define induction and *prove* that this technique is mathematically valid. That's right, we'll actually prove how and why it works! For now, though, we'll continue our investigation of some interesting mathematical puzzles, with these particular problems hand-picked by us for their use of inductive techniques.

2.1.1 Objectives

The following short sections in this introduction will show you how this chapter fits into the scheme of the book. They will describe how our previous work will be helpful, they will motivate why we would care to investigate the topics that appear in this chapter, and they will tell you our goals and what you should keep in mind while reading along to achieve those goals. Right now, we will summarize the main objectives of this chapter for you via a series of statements. These describe the skills and knowledge you should have gained by the conclusion of this chapter. The following sections will reiterate these ideas in more detail, but this will provide you with a brief list for future reference. When you finish working through this chapter, return to this list and see if you understand all of these objectives. Do you see why we outlined them here as being important? Can you define all the terminology we use? Can you apply the techniques we describe?

By the end of this chapter, you should be able to . . .

- Define what an inductive argument is, as well as classify a presented argument as an inductive one or not.
- Decide when to use an inductive argument, depending on the structure of the problem you are solving.
- Heuristically describe mathematical induction via an analogy.
- Identify and describe different kinds of inductive arguments by comparing and contrasting them, as well as identify the underlying structures of the corresponding problems that would yield these similarities and differences.

2.1.2 Segue from previous chapter

As in the previous chapter, we won't assume any familiarity with more advanced mathematics beyond basic algebra and arithmetic, and perhaps some visual, geometric intuition. We will, however, make use of summation and product notation fairly often, so if you feel like your notational skills are, go back and review Section 1.3.5.

2.1.3 Motivation

Look back at the Puzzle in Section 1.4.3, where we proved that the sum of the first n odd natural numbers is exactly n^2. We first observed this pattern geometrically, by arranging the terms of the sums (odd integers) as successively larger "corner pieces" of a square. The first way we proved the result, though, didn't seem to depend on that observation and merely utilized a previous result (about sums of even *and* odd integers) in an *algebraic* way; that is, we did some tricky manipulation of some equations (mutliplying and subtracting and what have you) and then–voilà!–out popped the result we expected. What did you think about that approach? Did it feel satisfying? In a way, it didn't quite match the geometric interpretation we had, at first, so it might be surprising that it worked out so nicely. (Perhaps there is a *different* geometric interpretation of this approach. Can you find one?)

Our second approach was to model that initial geometric observation. We transformed visual pieces into algebraic pieces; specifically, a sum was related to the area of a square, and the terms of the sum were related to particular pieces of that square. We established a *correspondence* between different intepretations of the same problem, finding a way to relate one to the other so that we could work with either interpretation and know that we were proving something about the overall result. The benefit of the visual interpretation is that it allowed us to take advantage of a general proof strategy known as **mathematical induction**, or sometimes just **induction**, for short. (The word *induction* has some non-mathematical meanings, as well, such as in electromagnetism or in philosophical arguments, but within the context of this book, when we say *induction*, we mean *mathematical induction.*) What exactly is induction? How does it work? When can we use this strategy? How do we adapt the strategy to a particular puzzle? Are there variations of the strategy that are more useful in certain situations? These are all questions that we hope to answer in this chapter.

The first topic we'd like to address is a question that we didn't just ask in the last paragraph, namely, "*Why* induction? *Why* bother with it?" Based on that puzzle in Section 1.4.3, it would seem that mathematical induction isn't entirely necessary since there might be other ways of proving something, instead of by induction. Depending on the context, this very well may be true, but the point we'd like to make clear from the beginning is that *induction is incredibly useful!* There are many situations where a proof by induction is the most concise and clear approach, and it is a well-known general strategy that can be applied in a variety of such situations. Furthermore, applying induction to a problem requires there to be a certain *structure* to the problem, a dependence of one "part" of the result on a "previous part". (The "parts" and the "dependence" will depend on the context, of course.) Recognizing that induction applies, and actually going through the subsequent proof process, will usually *teach* us something about the inherent structure of the problem. This is true even when induction fails! Perhaps there's a particular part of a problem that "ruins" the induction process, and identifying that particular part can be helpful and insightful.

We hope to motivate these points through some illustrative examples first, after which we will provide a reasonably thorough *definition* of mathematical induction that will show how the method works, in generality. (A completely *rigorous* definition will have to be put off until a little bit later, after we have defined and investigated some relevant concepts, like set theory and logical statements and implications. For now, though, the definition we give will suffice to work on some interesting puzzles and allow us to discuss induction as a general proof strategy.)

2.1.4 Goals and Warnings for the Reader

Do keep in mind that we are still building towards our goal of mathematical rigor, or as much as is possible within the scope and timing of this book and course. Some of the claims we make in this Chapter will be clarified and technically proven later on, once we have properly discussed the natural numbers and some basic mathematical logic. All in due time!

That said, this chapter is still very important, since we are continuing to introduce you to the process of solving mathematical problems, applying our existing knowledge and techniques to discover new facts and explain them to others. In addition, mathematical induction is a fundamental proof technique that will likely appear in every other mathematics course you take! This is because of its usefulness and the prevalence of inductive properties throughout the mathematical world.

2.2 Examples and Discussion

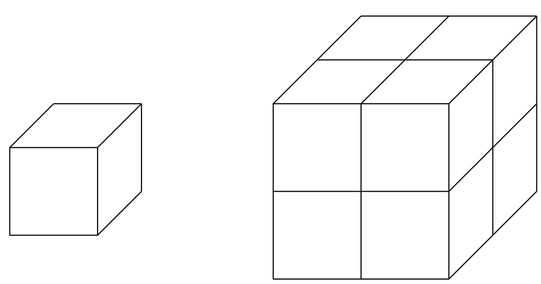
2.2.1 Turning Cubes Into Bigger Cubes

To motivate the overall method of mathematical induction, let's examine a geometric puzzle and solve it together. This example has been chosen carefully to illustrate how **mathematical induction** is relevant when a puzzle has a particular type of structure; specifically, some truth or fact or observation *depends* or *relies* or can be *derived* from a "previous" fact. This dependence on a previous case (or cases) is what makes a process *inductive*, and when we observe this phenomenon, applying *induction* is almost always a good idea.

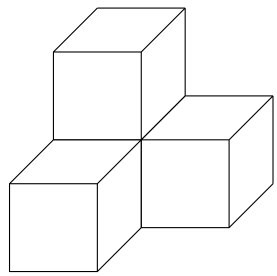
1-Cube into a 2-Cube

Let's examine cubic numbers and, specifically, let's try to describe a cubic number *in terms of* the previous cubic number. Imagine a $1 \times 1 \times 1$ cube, just one building block. How can we build the "next biggest" cube, of size $2 \times 2 \times 2$, by adding $1 \times 1 \times 1$ building blocks? How many do we need to add? Arithmetically, we know the answer: $2^3 = 8$ and $1^3 = 1$, so we need to add 7 blocks to have the correct volume. Okay, that's a specific answer, but it doesn't quite tell us *how* to arrange those 7 blocks to make a cube, nor does it give us any insight into how to answer this question for *larger* cubes. Ultimately, we would like to say how many blocks are required to build a $100 \times 100 \times 100$ cube into a $101 \times 101 \times 101$ cube without having to perform a lot of tedious arithmetic; that is, we are hoping to eventually find an answer to the question: given an $n \times n \times n$ cube, how many blocks must we add to build it into a $(n+1) \times (n+1) \times (n+1)$ cube? With that in mind, let's think carefully about this initial case and try to answer it with a general argument.

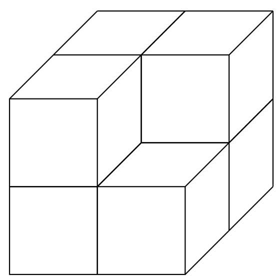
Given that single building block, and knowing we have to add 7 blocks to it, let's try to identify exactly where those 7 blocks should be placed to make a $2 \times 2 \times 2$ cube. (For simplicity, we will refer to a cube of size $n \times n \times n$ as an n-cube, for any value of n. We will only need to use values of n that are *natural numbers*, i.e. non-negative whole numbers, in this example.) Look at the pictures of the 1-cube and 2-cube below and try to come up with an explanation of constructing one from the other.



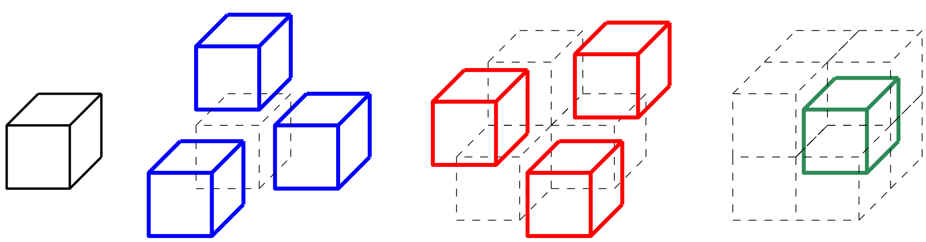
Here's one reasonable explanation that we want to use because it will guide us in the general explanation of building an $(n+1)$-cube from an n-cube, and because it is a mathematically *elegant* and simple explanation. Start with the 1-cube positioned as it is above and "enlarge" the 3 exposed faces by the appropriate amount, in this case by one block. This accounts for 3 of the 7 blocks, thus far: $2^3 = 1^3 + 3 + \_\_\_$. Where are there "holes" now?



The blocks we just added have created "gaps" between each pair of them, and each of those "gaps" can be filled with one block. This accounts for 3 more of the 7 total blocks: $2^3 = 1^3 + 3 + 3 + \_\_\_$. Now what?



There is just one block left to be filled, and it's the very top corner. Adding this block completes the 2-cube and tells us how to mathematically describe our construction process with the following picture and equation:

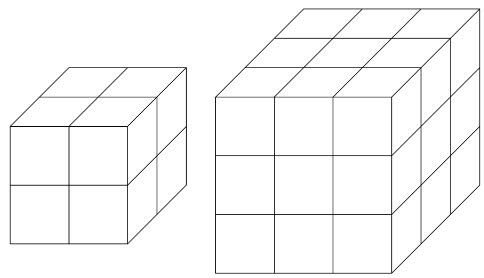


$$2^3 = 1 + {\color{blue}3} + {\color{red}3} + {\color{green}1}$$

2-Cube into a 3-Cube

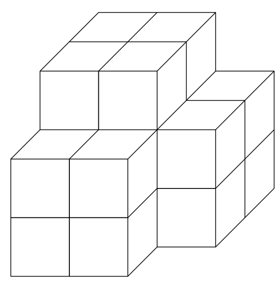
Okay, we might now have a better idea of how to describe this process in general, but let's examine another case or two just to make sure we have the full idea.

Let's start with a 2-cube and construct a 3-cube from it. (You can even try this out by hand if you happen to own various sizes of Rubik's Cubes!) We can follow a process similar to the steps we used in the previous case and just change the numbers appropriately. Starting with a similar picture



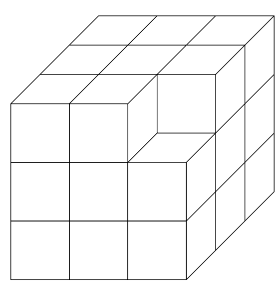
we see that we need to "enlarge" the three exposed faces of the 2-cube but, in this case, the amount by which we need to enlarge them is *different* than before (with the 1-cube) since we are working with a larger initial cube. Specifically, each face must be enlarged by a 2×2 *square* of blocks (whereas, in the previous case, we added a 1×1 square of blocks). Thus, an equation to account for this addition is

$$3^3 = 2^3 + 3 \cdot 2^2 + \underline{\quad}$$

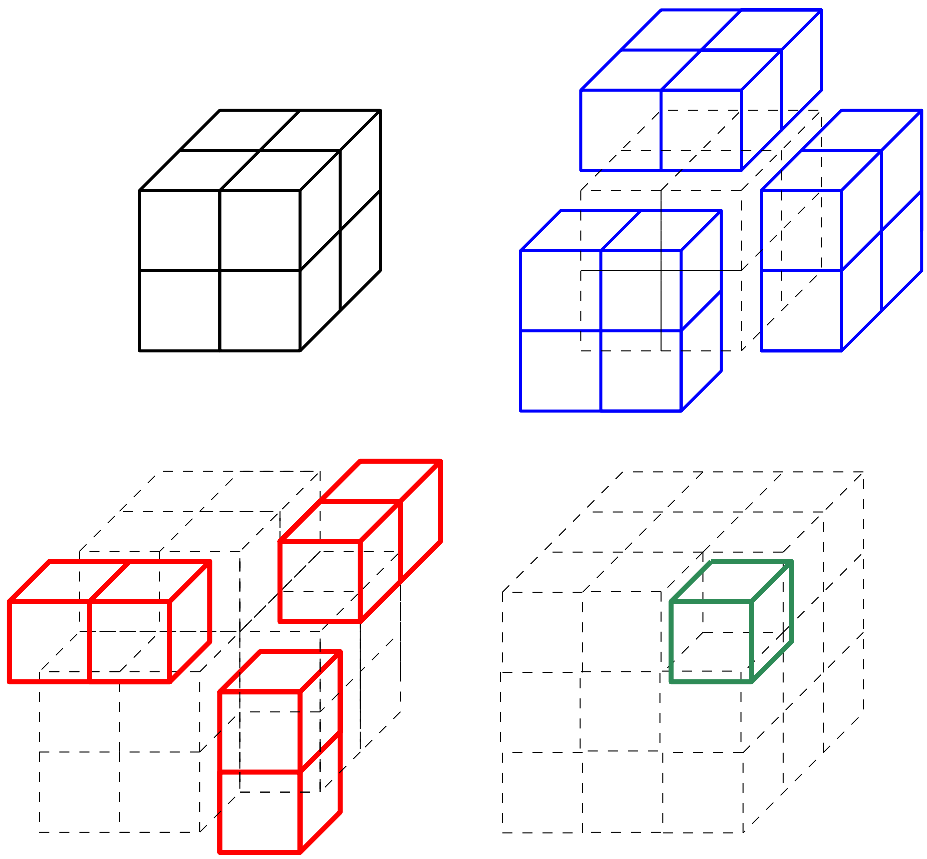


After we do this, we see that we need to fill in the gaps between those enlarged faces with 2×1 of blocks (whereas, in the previous case, we added 1×1 rows of blocks). An equation to account for the additions thus far is

$$3^3 = 2^3 + 3 \cdot 2^2 + 3 \cdot 2 + \underline{\quad}$$



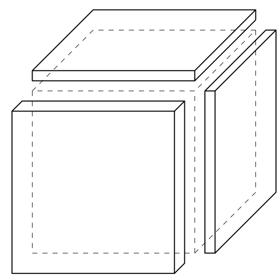
After we do this, we see that there is only the top corner left to fill in. Accordingly, we can depict our construction process and its corresponding equation:



$$3^3 = 2^3 + 3 \cdot 2^2 + 3 \cdot 2 + 1$$

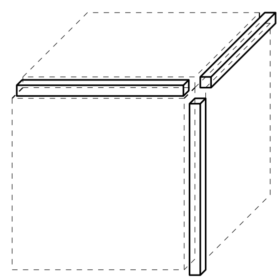
n-Cube into an $(n+1)$-Cube

Do you see now how this process will generalize? What if we started with an n-cube? How could we construct an $(n+1)$-cube? Let's follow the same steps we used in the previous two cases. First, we would enlarge the three exposed faces by adding three *squares* of blocks. How big is each square? Well, we want each square to be the same size as the exposed faces, so they will be $n \times n$ squares, accounting for n^2 blocks for each face:



$$(n+1)^3 = n^3 + 3n^2 + \_\_\_$$

Next, we would fill in the gaps between these enlarged faces with rows of blocks. How long are those rows? Well, they each lie along the edges of the squares of blocks we just added, so they will each be of size $n \times 1$, accounting for n blocks for each gap:



$$(n+1)^3 = n^3 + 3n^2 + 3n + \_\_\_$$

Finally, there will only be the top corner left to fill in! Therefore,

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1$$

"Wait a minute!" you might say, abruptly. "We already knew that, right?" In a way, yes; the equation above is an algebraic identity that we can also easily see by just expanding the product on the left and collecting terms:

$$\begin{aligned}(n+1)^3 &= (n+1) \cdot (n+1)^2 \\ &= (n+1) \cdot (n^2 + 2n + 1) \\ &= (n^3 + 2n^2 + n) + (n^2 + 2n + 1) \\ &= n^3 + 3n^2 + 3n + 1\end{aligned}$$

So what have we really accomplished? Well, the main point behind deriving this identity in this geometric and visual way is that it exhibits how this identity represents some kind of *inductive* process. We sought to explain how to derive one "fact" (a cubic number, $(n + 1)^3$) from a previously known "fact" (the next smallest cubic number, n^3) and properly explained how to do just that. Compare this to one of the methods we used to investigate the fact that the sums of odd integers yield perfect squares, too. That observation also belies an inductive process and, although we didn't describe it as such at the time, we encourage you to think about that now. Look back at our discussion and try to write out how you could write $(n+1)^2$ in terms of n^2 by looking at squares of blocks. Does it look anything like an "obvious" algebraic identity? (If you're feeling ambitious, think about what happens with writing $(n+1)^4$ in terms of n^4. Is there any geometric intuition behind this? What about higher powers?)

The benefit of the method we've used is that we now know how to describe cubic numbers in terms of smaller cubic numbers, *all the way down to* 1; that is, any time we see a cubic number in an expression, we know precisely how to write that value in terms of a smaller cubic number and some leftover terms. Furthermore, each of those expressions and leftover terms have an inherent *structure* to them that depends on the cubic number in question. Thus, by iteratively replacing any cubic number, like $(n+1)^3$, with an expression like the one we derived above, and continuing until we can't replace any more, should produce an equation that has some built in *symmetry*. This idea is best illustrated by actually doing it, so let's see what happens. Let's start with the expression we derived, for some arbitrary value of n,

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1$$

and then recognize that we now know a similar expression

$$n^3 = (n-1)^3 + 3(n-1)^2 + 3(n-1) + 1$$

We proved that this equation holds when we gave a general argument for the expression above for n^3, since that only relied on the fact that $n \geq 1$. We can follow the same logical steps, throughout replacing n with $n-1$, and end up with the second expression above, for $(n-1)^3$. (Does this keep going, for *any* value of n? Think about this for a minute. Does our argument make any sense when $n \leq 0$? Would it make physical sense to talk about, say, constructing a $(-2) \times (-2) \times (-2)$ cube from a different cube?)

Therefore, we can replace the n^3 term in the line above

$$\begin{array}{rcccccccc} (n+1)^3 = & & \cancel{n^3} & + & 3n^2 & + & 3n & + & 1 \\ & + & (n-1)^3 & + & 3(n-1)^2 & + & 3(n-1) & + & 1 \end{array}$$

This is also an algebraic identity, but it's certainly not one that we would easily think to write down just by expanding the product on the left-hand side and grouping terms. Here, we are taking advantage of the *structure* of our result to apply it over and over and obtain new expressions that we wouldn't have otherwise thought to write down. Let's continue with this substitution process and see where it takes us! Next, we replace $(n-1)^3$ with the corresponding expression and find

$$\begin{array}{rcccccccc} (n+1)^3 = & & & & 3n^2 & + & 3n & + & 1 \\ & & \cancel{(n-1)^3} & + & 3(n-1)^2 & + & 3(n-1) & + & 1 \\ & + & (n-2)^3 & + & 3(n-2)^2 & + & 3(n-2) & + & 1 \end{array}$$

Perhaps you see where this is going? We can do this subsitution process over and over, and the columns that we've arranged above will continue to grow, showing us that there is something deep and mathematically symmetric going on here. But where does this process stop? We want to write down a concise version of this iterative process and be able to explain all of the terms that arise, so we need to know where it ends. Remember the very first step in our investigation of the cubic numbers? We figured out how to write $2^3 = 1^3 + 3 + 3 + 1$. Since this was our *first* step in *building* this inductive process, it should be the *last* step we apply when building backwards, as we are now. Accordingly, we can write

$$\begin{array}{rcccccccc}
(n+1)^3 = & & & & 3n^2 & + & 3n & + & 1 \\
 & & & + & 3(n-1)^2 & + & 3(n-1) & + & 1 \\
 & & & + & 3(n-2)^2 & + & 3(n-2) & + & 1 \\
 & & & + & 3(n-3)^2 & + & 3(n-3) & + & 1 \\
 & & & & \vdots & + & \vdots & + & \vdots \\
 & & & + & 3 \cdot 2^2 & + & 3 \cdot 2 & + & 1 \\
 & + & 1^3 & + & 3 \cdot 1^2 & + & 3 \cdot 1 & + & 1
\end{array}$$

This is *definitely* an identity we wouldn't have come up with off the top of our heads! In addition to being relatively pretty-looking on the page like this, it also allows us to apply some of our previous knowledge and simplify the expression. To see how we can do that, let's apply summation notation to the columns above and collect a bunch of terms into some simple expressions:

$$(n+1)^3 = 1^3 + 3 \cdot \sum_{k=1}^{n} k^2 + 3 \cdot \sum_{k=1}^{n} k + \sum_{k=1}^{n} 1$$

In the last chapter, we saw a couple of different proofs that told us

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Let's use that fact in the line above, and also simplify the term on the far right, to write

$$(n+1)^3 = 1 + 3 \cdot \sum_{k=1}^{n} k^2 + \frac{3n(n+1)}{2} + n$$

What does this tell us? What have we accomplished after all this algebraic manipulation? Well, we previously proved a result about the sum of the first n natural numbers, so a natural question to ask after that is: What is the sum of the first n natural numbers *squared*? How could we begin to answer that? That's a trick question, because *we already have*! Let's do one or two more algebraic steps with the equation above by isolating the summation term and then dividing:

$$(n+1)^3 - 1 - n - \frac{3n(n+1)}{2} = 3 \cdot \sum_{k=1}^{n} k^2$$
$$\frac{1}{3}(n+1)^3 - \frac{1}{3}(n+1) - \frac{n(n+1)}{2} = \sum_{k=1}^{n} k^2$$

This is what we've accomplished: we've derived a formula for the sum of the first n square natural numbers! Of course, the expression on the left in the line above isn't particularly nice looking and we could perform some further simplification, and we will leave it to you to verify that this yields the expression below:

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

"And so on" is not rigorous!

There are a couple of "morals" that we'd like to point out, based on all of this work. The first moral is that generalizing an argument is a good method for discovering new and interesting mathematical ideas and results. Did you think about how this puzzle is related to the sums of odd natural numbers? If not, we encourage you strongly to try that now, as well as think about generalizing this even further to four or five dimensional "cubes" and so on. In addition to giving you some other interesting results, it will also be incredibly instructive for learning to think abstractly and apply inductive processes. The second moral is more like an admission: we have *not* technically *proven* the formula above for the sum of the first n square natural numbers. It seems like our derivation is valid and tells us the "correct answer" but there is a glaring issue: ellipses! In expanding the equation for $(n+1)^3$ and obtaining those columns of terms that we collected into particular sums, writing $\vdots$ in the middle of those columns was helpful in guiding our intuition, but *this is not a mathematically rigorous technique*. How do we *know* that all of the terms in the middle are exactly what we'd expect them to be? How can we be so sure that all of our pictures of cubes translate perfectly into the mathematical expressions we wrote down? What do we really mean by "and keep going all the way down to 1"?

As an example, consider this:

$$1, 2, 3, 4, \ldots, 100$$

What is that list of numbers? You probably interpreted it as "all the natural numbers between 1 and 100, inclusive". That seems reasonable. But what if we *actually* meant this list?

$$1, 2, 3, 4, 7, 10, 11, 12, 14, \ldots, 100$$

Why, of course, we meant the list of natural numbers from 1 to 100 that don't have an "i" in their English spelling! Wasn't it obvious?

The point is this: when talking with a friend, and *verbalizing* some ideas, it might be okay to write "$1, 2, 3, \ldots, 100$" and ensure that whoever is listening knows *exactly* what you mean. In general, though, we can't assume that a reader would just naturally *intuit* whatever we were trying to convey; we should be as *explicit* and *rigorous* as possible.

It may seem to you now like we're nit-picking, but the larger point is that there is a mathematical way of making this argument more *precise*, so that it constitutes a completely valid *proof*. Everything we have done so far is useful in guiding our intuition, but we will have to do a little more work to be sure our arguments are completely convincing. There are a few other concepts required to make this type of argument rigorous, in general, and we will investigate those in the next chapter and return to this subject immediately after that. However, in the meantime, let's examine one more example to practice this intuitive argument style and recognizing when induction is an applicable technique.

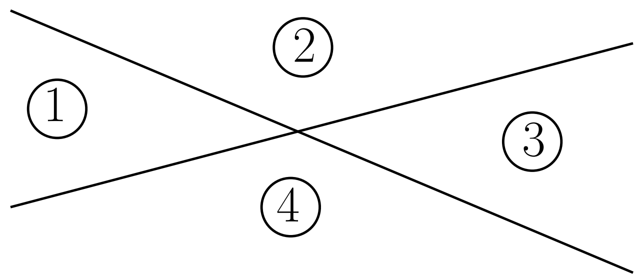
2.2.2 Lines On The Plane

Take a clean sheet of paper and a pen and a ruler. How many regions are on your sheet? Just one, right? Draw a line all the way across the paper. Now there are two regions. Draw another straight line that intersects your first line. How many regions are there? You should count four in total. Draw a third line that intersects both of the first two, but *not* at the point where the first two intersect. (That is, there should be three intersection points, in total.) How many regions are there? Can you predict the answer before counting? What happens when there are 4 lines? Or 5? Or 100? How do we approach this puzzle and, ultimately, solve it? Let's give a more formal statement to be sure we're thinking the same way:

Consider n lines on an infinite plane (two-dimensional surface) such that no two lines are *parallel* and no more than two lines *intersect* at one point. How many distinct regions do the lines create?

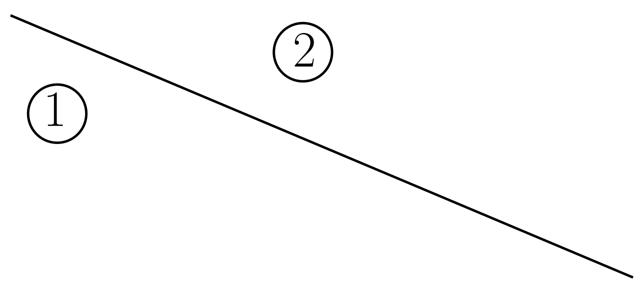
We can draw a few examples by hand when n is small (up to, say, $n = 5$ is reasonable), and let's use this to guide our intuition into making a general argument for an *arbitrary* value of n. (Notice that this strategy is very similar to what we did in the previous puzzle: identify a pattern with small cases, identify the relevant components of those cases that can generalize, then abstract to an aribtrary case.) Specifically, we want to attempt to identify how the number of regions in one drawing *depends* on the number of regions in a drawing with fewer lines. What happens when we draw a new line? Can we determine how this changes the already existing regions? Can we somehow count how many regions this creates? Do some investigation of this puzzle on your own before reading on. If you figure out some results, compare your work to the steps we follow below.

Let's start with a small case, say $n = 2$. We know one line divides a plane into 2 regions; what happens when we add a second line? We know we get 4 regions, because we can just look and count them:

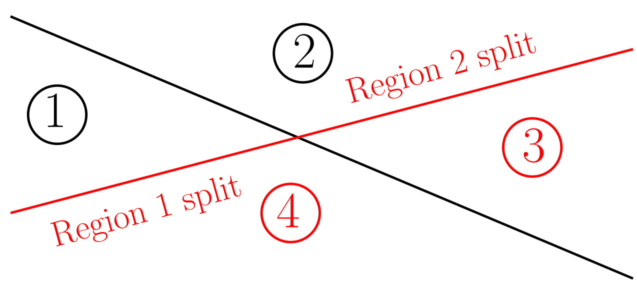


However, we are only looking at *one specific case* of two intersecting lines. How do we know that we will *always* find four regions, no matter how we draw those two lines appropriately? That is, can we describe *how* this happens in a way that somehow incorporates the fact that the number of liens is $n = 2$? Think about it!

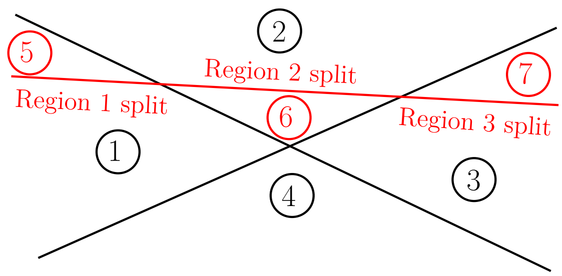
Here's our approach. Notice that each of the already existing regions is split into two when we add a second line, and that this is true *no matter how you choose to draw the lines*; as long as we make sure the two lines aren't parallel, they will always behave this way. That is, if we take one line that splits the plane into two regions,



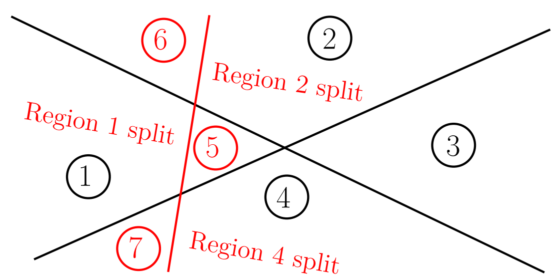
then adding a new line will split each of those existing regions in two. This adds two new regions to the whole plane, giving four regions in total:



What about when $n = 3$? In this case, we want to think about adding a third line to a diagram with two lines and four regions. We want to make an argument that doesn't depend on a *particular* arrangement of the lines, so eventually the only facts we should use are that no lines are *parallel* and any point of *intersection* only lies on two lines (not three or more). For now, though, it helps to look at a particular arrangement of lines so that we are talking about the same diagram; we can use our observations of this specific diagram to guide our general argument. Let's start with a two-line diagram, on the left below, and add a third line, but let's choose the third line so that all of the intersection points are "nearby" or within the scope of the diagram, so that we don't have to rescale the picture:

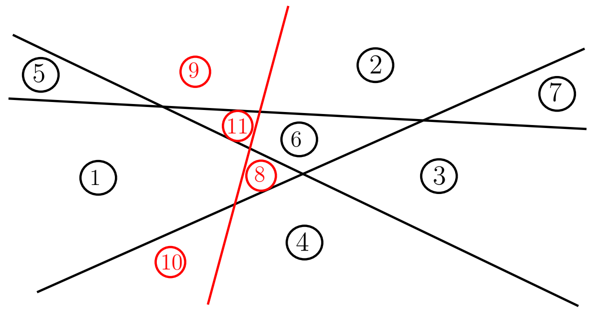


We certainly have 7 regions now, but we made the third line a separate color so that we can identify where the "new" regions appear: one region (the lower quadrant, Region 4) remains unchanged, but the three other regions are split in two and each of those "splits" adds 1 to our count (where there was 1 region, now there are 2). What if we had placed the line differently?



The same phenomenon occurs, where one quadrant remains untouched but the other three are split in two. (How do we know there aren't any other regions not depicted within the scale of our diagram? This is not as easy a question to answer as you might think at first blush, and it's worth thinking about.) Experiment with other arrangements of the three lines and try to convince yourself that this always happens; also, think about *why* this is the case and *how* we could explain that this must happen. Before giving a general explanation, though, let's examine another small case.

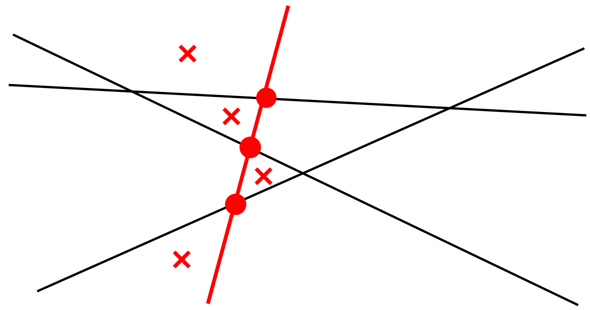
When $n = 4$, we start with three lines and 7 regions and add a fourth line that is not parallel to any of the existing lines and doesn't pass through any existing intersection points. Again, we will want to make an argument that isn't tied to a specific arrangement of the lines, but looking at the following specific diagram will help guide our intuition into making that argument:



Notice that three of the original regions remain unchanged (Regions 3 and 5 and 7), and the other four are split in two. Do you notice a pattern here? It seems like for every n we've examined, adding the n-th line leaves exactly $n-1$ regions unchanged while the rest are split in two. Let's try to explain why this happens. Remember that we're trying to identify how many regions appear when we draw n lines, so let's assign that value a "name" so we can refer to it; let's say $R(n)$ represents the number of regions created by drawing n lines on the plane so that no two lines are parallel and no intersection point belongs to more than two lines. In these examples we've considered for small values of n, we've looked at what *changes* when we add a new line; that is, we've figured out what $R(n)$ is by already knowing $R(n-1)$. Let's try to adapt our observations so that they apply to any *arbitrary* value of n.

Assume that we know $R(n)$ already. (Why can we do this? Do we know any particular value of $R(n)$ for sure, for some specific n? Which? How?) Say we have an *arbitrary* diagram of n lines on the plane that satisfy the two conditions given in the puzzle statement above. How many regions do these lines create? Yes, exactly $R(n)$. Now, what happens when we add the $(n+1)$-th line? What can we say *for sure* about this line and how it alters the diagram? Well, the only information we really have is that (a) this new line is not parallel to any of the existing n lines and (b) this new line does not intersect any of the already existing intersection points. Now, condition (a) tells us that this new line must intersect *all* of the exisiting n lines; parallel lines don't intersect, and non-parallel lines must intersect somewhere. Thus, we must create n new intersection points on the diagram. Can any of those intersection points coincide with any existing intersection points? No! This is precisely what condition (b) tells us. These two pieces of information together tell us that, no matter how we draw this new line, as long as it satisfies the requirements of the puzzle, we *must* be able to identify n "special" points along that line. Those special points are precisely the points where the new line intersects an existing line.

We'd now like to take these special points and use them to identify new regions in the diagram. Look back to the cases we examined above: identify the new intersection points and see if you can associate them with new regions. Perhaps it would help to label those intersections with a large dot and mark the new regions with an X to make them all stand out. We'll show you one example below, where $n=4$. What do you notice? Can you use these dots to help identify how many new regions are created with the addition of that n-th line? Think about this for a minute and then read on.



Exactly! Between any two of the new intersection points, we have a line *segment* that splits a region in two! All that remains is to identify how many new such segments we've created. Since each one corresponds to exactly *one* existing region split in two, this will tell us exactly how many new regions we've created. We've already figured out that this $(n+1)$-th line creates n new intersection points. Think about how these points are arranged on the line. Any two "consecutive" points create a segment, but the extreme points also create infinite segments (that coninue past those extreme points forever). How many are there in total? Exactly $n+1$. (Look at the diagram above, for $n = 3$. We see that there are 3 new intersection points and 4 new segments, with two of them being infinite rays.) This means there are $n+1$ line segments that split regions in two, so we have created exactly $n+1$ new regions! This allows us to say that

$$R(n+1) = R(n) + n + 1$$

Phew, what an observation! It took a bit of playing around with examples and making some geometric arguments, but here we are. We've identified some *inductive structure* to this puzzle; we've found how one case depends on another one. That is, we've found how $R(n+1)$ depends on $R(n)$. This hasn't *completely* solved the puzzle, but we are now much closer. All that remains is to replace $R(n)$ with a similar expression, and continually do this until we reach a value we know, $R(1) = 2$. Observe:

$$\begin{array}{rlccccccc}
R(n+1) = & & & & & & \cancel{R(n)} & + & n+1 \\
= & & & & \cancel{R(n-1)} & + & n & + & n+1 \\
= & & \cancel{R(n-2)} & + & (n-1) & + & n & + & n+1 \\
\vdots & & & & & & & & \\
= & & \cancel{R(2)}+3 & + & \cdots & + & n & + & n+1 \\
= & R(1)+2 \quad + & 3 & + & \cdots & + & n & + & n+1
\end{array}$$

Since we know $R(1) = 2$, we can say

$$R(n+1) = 2 + (2 + 3 + \cdots + n + (n+1)) = 2 + \left(\sum_{k=1}^{n+1} k\right) - 1 = 1 + \sum_{k=1}^{n+1} k$$

and this is a sum we have investigated before! (Also notice that we had to subract 1 because of the missing first term of the sum in parentheses.) Recall that $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, and to represent the sum we have in the equation above, we just replace n with $n+1$. Therefore,

$$R(n+1) = 1 + \frac{(n+1)(n+2)}{2}$$

One final simplification we would like to make is to replace $n+1$ with n throughout the equation, because it makes more sense to have an expression for $R(n)$ (For what values of n is this valid?)

$$R(n) = 1 + \frac{n(n+1)}{2}$$

Finally, we have arrived at an answer to the originally-posed puzzle! In so doing, we employed an *inductive* technique: we explained how one "fact", namely the value of $R(n+1)$, *depends* on the value of a "previous fact", namely $R(n)$, and used these iterative dependencies to work backwards until we reached a particular, *known* value, namely $R(1)$.

We want to point out, again, that the derivation we followed and the observations we made in this section have guided our intuition into an answer, but this has not *rigorously proven* anything. The issue is with the "$\cdots$", which is not a concrete, "officially" mathematical way of capturing the inductive process underlying our technique. Furthermore, our method with the "lines in the plane" problem had us *starting* with a diagram of $n-1$ lines and *building* a new diagram with n lines; is this okay? Why does this actually tell us anything about an *arbitrary* diagram of n lines? Do all such diagrams come from a smaller diagram with one fewer line?

We will, in the next two chapters, learn the necessary tools to fully describe a *rigorous* way of doing what we have done so far, and in the chapter after that, we will employ those tools to make **mathematical induction** officially rigorous. For now, though, we want to give a heuristic definition of induction and continue to examine interesting puzzles and observations that rely on inductive techniques. Practicing with these types of puzzles–learning when to recognize an inductive process, how to work with it, how to use that structure to solve a problem, and so on–will be extremely helpful in the future, and we have no need to delve into technical mathematical detail. (At least, not just yet!)

2.2.3 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What properties characterize an *inductive* process?

(2) How did we prove that $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ is correct? How was our method inductive? (Reread Section 1.4.2 if you forget!)

(3) Why can we take the sum formula mentioned in the previous question and "replace" n with $n+1$ and know that it still holds true? Can we also replace n with $n-1$?

(4) Work through the algebraic steps to obtain our final expression for the sum of the first n squares; that is, verify that

$$\frac{1}{3}(n+1)^3 - \frac{1}{3}(n+1) - \frac{n(n+1)}{2} = \frac{1}{6}n(n+1)(2n+1)$$

(5) Try to recall the argument that adding the $(n+1)$-th line on the plane created *exactly* $n+1$ new regions. Can you work through the argument for a friend and convince him/her that it is valid?

(6) To find the sum of the first n squares, why couldn't we just square the formula for the sum of the first n numbers? Why is that wrong?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Draw 5 lines on the plane (that satisfy the two conditions of the puzzle) and verify that there are 16 regions. Can you also verify that 6 lines yield 22 regions?

(2) Come up with another description of a sequence that goes $1, 2, 3, 4, \dots, 100$ that is *not* simply all of the numbers from 1 to 100. (Recall the example we gave: all the numbers from 1 to 100 with no "i" in their English spelling.)

(3) Come up with an algebraic expression that relates $(n+1)^4$ to n^4, like we did with cubes.

(**Challenge:** Can you come up with a *geometric* interpretation for the expression you just derived?)

(4) **Challenge:** Let's bump the "lines in the plane" puzzle up one dimension! Think about having n planes in three-dimensional space. How many regions are created? Assume that no two planes are parallel, and no three of them intersect in one line. (Think about how these two conditions are directly analogous to the specified conditions for the "lines" puzzle.)

2.3 Defining Induction

To properly motivate the forthcoming definition of **mathematical induction** as a proof technique, we want to emphasize that the above examples used some intuitive notions of the structure of the puzzle to develop a "solution", where we use quotation marks around *solution* to indicate that we haven't officially proven it yet. In that sense, we ask the following question: What if we had been *given* the formula that we derived and asked to verify it? What if we had not gone through any intuitive steps to derive the formula and someone just told us that it is correct? How could we check their claim? The reason we ask this is because we are really facing that situation now, except the person telling us the formula is ... the very same intuitive argument *we* discovered above!

Pretend you have a skeptical friend who says, "Hey, I heard about this formula for the sum of the first n natural numbers squared. Somebody told me that they add up to $\frac{1}{6}n(n+1)(2n+1)$. I checked the first two natural numbers, and it worked, so it's gotta be right. Pass it on!" Being a logical thinker, but also a good friend, you nod along and say, "I did hear that, but let's make *sure* it's correct for *every* number." How would you proceed? Your friend is right that the first few values "work out" nicely:

$$\begin{aligned} 1^2 &= 1 = \frac{1}{6}(1)(2)(3) \\ 1^2+2^2 &= 5 = \frac{1}{6}(2)(3)(5) \\ 1^2+2^2+3^2 &= 14 = \frac{1}{6}(3)(4)(7) \\ 1^2+2^2+3^2+4^2 &= 30 = \frac{1}{6}(4)(5)(9) \end{aligned}$$

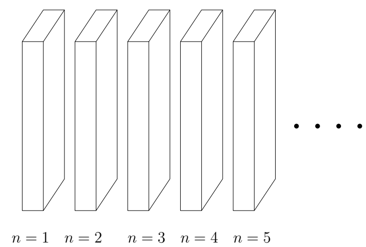
and so on. We could even check, by hand, a large value of n, if we wanted to:

$$1^2+2^2+3^2+4^2+5^2+6^2+7^2+8^2+9^2+10^2 = 385 = \frac{1}{6}(10)(11)(21)$$

Remember, though, that this formula is claimed to be valid for *any* value of n. Checking individual results by hand would take forever, because there are an *infinite* number of natural numbers. No matter how many individual values of n we check, there will always be larger values, and how do we *know* that the formula doesn't break down for some large value? We need a far more *efficient* procedure, mathematically and temporally speaking, to somehow verify the formula for all values of n in just a few steps. We have an idea in mind, of course (it's the upcoming rigorous version of mathematical induction), and here we will explain how the procedure works, in a broad sense.

2.3.1 The Domino Analogy

Pretend that we have a set of dominoes. This is a special set of dominoes because we have an infinite number of them (!) and we can imagine anything we want written on them, instead of the standard array of dots. Let's also pretend that they are set up in an infinite line along an infinite tabletop, and we are viewing the dominos from the side and we can see a label under each one so that we know where we are in the line:



For this particular example, to verify the formula

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

we will imagine a particular "fact" written on each domino. Specifically, we will imagine that the 1st domino has the expression

$$\sum_{k=1}^{1} k^2 = \frac{1}{6}(1)(2)(3)$$

written on it, and the 2nd domino has the expression

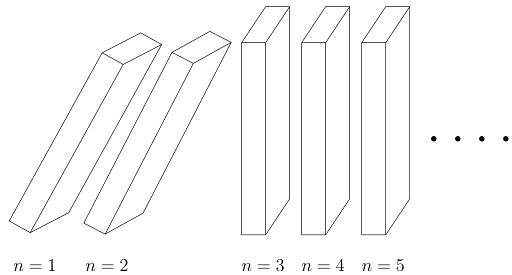
$$\sum_{k=1}^{2} k^2 = \frac{1}{6}(2)(3)(5)$$

written on it. In general, we imagine that the n-th domino in the infinite line has the following "fact" written on it:

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

Since we're dealing with dominos that are meant to fall into each other and knock each other over, let's pretend that whenever a domino falls, that means the corresponding "fact" written on it *is a true statement*. This is how we will relate our physical interpretation of the dominos to the mathematical interpretation of the validity of the formula we derived.

We did check the sum for $n = 1$ by hand: $1^2 = \frac{1}{6}(1)(2)(3)$. Thus, the fact written on the first domino is a true statement, so we know that the first domino will, indeed, fall over. We also checked the sum for $n = 2$ by hand, so we know that the second domino will fall over:



However, continuing like this brings us back to the same problem as before: we don't want to check *every individual* domino to make sure it falls. We would really like to encapsulate our physical notion of the line of dominos—namely, that when a domino falls it will topple into the next one and knock that over, and so on—and somehow relate the "facts" that are written on adjacent dominos.

Let's look at this situation for the first two dominos. Knowing that Domino 1 falls, can we guarantee that Domino 2 falls without rewriting all of the terms of the sum? How are the statements written on the two dominos related? Each statement is a sum of squared natural numbers, and the one on the second domino has exactly one more term. Thus, knowing *already* that Domino 1 has fallen, we can use the *true statement* written on Domino 1 to *verify* the truth of the statement written on Domino 2:

$$\sum_{k=1}^{2} k^2 = 1^2 + 2^2 = 1 + 2^2 = 5 = \frac{1}{6}(2)(3)(5)$$

Now, this may seem a little silly because the only "work" we have saved is not having to "do the arithmetic" to write $1^2 = 1$. Let's use this procedure on a case with larger numbers so we can more convincingly illustrate the benefit of this method. Let's *assume* that Domino 10 has fallen. (In case you are worried about this assumption, we wrote the full sum a few paragraphs ago and you can verify it there.) This means we *know* that

$$\sum_{k=1}^{10} k^2 = \frac{1}{6}(10)(11)(21) = 385$$

is a *true statement*. Let's use this to verify the statement written on Domino 11, which is

$$\sum_{k=1}^{11} k^2 = \frac{1}{6}(11)(12)(23)$$

The sum written on Domino 11 has 11 terms, and the first 10 are exactly the sum written on Domino 10! Since we know something about that sum, let's just separate that 11th term from the sum and apply our knowledge of the other terms:

$$\begin{aligned}\sum_{k=1}^{11} k^2 &= \left(1^2 + 2^2 + \cdots + 10^2\right) + 11^2 \\ &= \left(\sum_{k=1}^{10} k^2\right) + 11^2 \\ &= 385 + 121 \\ &= 506 \\ &= \frac{1}{6}3036 = \frac{1}{6}(11)(12)(23)\end{aligned}$$

Look at all of the effort we saved! Why bother reading the first 10 terms of the sum if we know something about them already?

Now, imagine if we could do this procedure for *all* values of n, *simultaneously*! That is, imagine that we could prove that any time Domino n falls, we are *guaranteed* that Domino $(n+1)$ falls. What would this tell us? Well, think about the infinite line of dominos again. We *know* Domino 1 will fall, because we checked that value by hand. Then, because we verified the "Domino n knocks over Domino $(n+1)$" step for *all* values of n, we know Domino 1 will fall into Domino 2, which in turn falls into Domino 3, which in turns falls into Domino 4, which ... The entire line of dominos will fall! In essence, we could collapse the whole line of dominos falling down into just *two* steps:

(a) Make sure the first domino topples;

(b) Make sure every domino knocks over the one immediately after it in line.

With only these two steps, we can *guarantee* every domino falls and, therefore, *prove* that all of the facts written on them are true. This will prove that the formula we derived is valid for *every* natural number n.

We have already accomplished step (a), so now we have to complete step (b). We have done this for specific cases in the previous paragraphs (Domino 1 topples Domino 2, and Domino 10 topples Domino 11), so let's try to follow along with the steps of those cases and generalize to an arbitrary value of n. We *assume*, for some *specific but arbitrary* value of n, that Domino n falls, which tells us that the equation

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

is a *true statement*. Now, we want to relate this to the statement written on Domino $(n+1)$ and apply the knowledge given in the equation above. Let's do what we did before and write a sum of $n+1$ terms as a sum of n terms plus the last term:

$$\sum_{k=1}^{n+1} k^2 = 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 = \left(\sum_{k=1}^{n} k^2\right) + (n+1)^2$$

Next, we can apply our assumption that Domino n has fallen (which tells us that the fact written on it is true) and write

$$\sum_{k=1}^{n+1} k^2 = \frac{1}{6}n(n+1)(2n+1) + (n+1)^2$$

Is this the same as the fact written on Domino $(n+1)$? Let's look at what that is, first, and then compare. The "fact" on Domino $(n+1)$ is similar to the fact on Domino n, except everywhere we see "n" we replace it with "$n+1$":

$$\sum_{k=1}^{n+1} k^2 = \frac{1}{6}(n+1)((n+1)+1)(2(n+1)+1) = \frac{1}{6}(n+1)(n+2)(2n+3)$$

It is not clear yet whether the expression we have derived thus far is actually equal to this. We could attempt to simplify the expression we've derived and factor it to make it "look like" this new expression, but it might be easier to just expand both expressions and compare all the terms. (This is motivated by the general idea that expanding a factored polynomial is far easier than recognizing a polynomial can be factored.) For the first expression, we get

$$\begin{aligned}
\frac{1}{6}n(n+1)(2n+1) + (n+1)^2 &= \frac{1}{6}n(2n^2+3n+1) + (n^2+2n+1) \\
&= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n + n^2 + 2n + 1 \\
&= \frac{1}{3}n^3 + \frac{3}{2}n^2 + \frac{13}{6}n + 1
\end{aligned}$$

and for the second expression, we get

$$\begin{aligned}
\frac{1}{6}(n+1)(n+2)(2n+3) &= \frac{1}{6}(n+1)(2n^2+7n+6) \\
&= \frac{1}{6}\left[(2n^3+7n^2+6n) + (2n^2+7n+6)\right] \\
&= \frac{1}{3}n^3 + \frac{3}{2}n^2 + \frac{13}{6}n + 1
\end{aligned}$$

Look at that; they're identical! Also, notice how much easier this was than trying to rearrange one of the expressions and "morph" it into the other. We proved they were identical by manipulating them both and finding the same expression, ultimately. Now, let's look back and assess what we have accomplished:

1. We likened proving the validity of the formula

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

for *all* values of n to knocking over an infinite line of dominos.

2. We verified that Domino 1 will fall by checking the formula corresponding to that case by hand.
3. We proved that Domino n will fall into Domino $(n+1)$ and knock it over by *assuming* the fact written on Domino n is true and using that knowledge to show that the fact written on Domino $(n+1)$ must also be true.
4. This guarantees that *all* dominos will fall, so the formula is true for all values of n!

Are you convinced by this technique? Do you think we've *rigorously proven* that the formula is valid for all natural numbers n? What if there were a value of n for which the formula didn't hold? What would that mean in terms of our domino scheme?

Remember that this domino analogy is a good intuitive guide for how induction works, but it is not built on mathematically rigorous foundations. That will be the goal of the next couple of chapters. For now, let's revisit the other example we've examined in this section: lines in the plane. Again, the use of *ellipses* in our derivation of the formula $R(n)$ is troublesome and we want to avoid it. Let's try to follow along with the domino scheme in the context of this puzzle.

Imagine that we have defined the expression $R(n)$ to represent the number of distinct regions in the plane created by n lines, where no two lines are parallel and no three intersect at one point. Also, imagine that on Domino n we have written the "fact" that "$R(n) = 1 + \frac{n(n+1)}{2}$". Can we follow the same steps as above and verify that all the dominos will fall?

First, we need to check that Domino 1 does, indeed fall. This amounts to verifying the statement: "$R(1) = 1 + \frac{1(2)}{2} = 1 + 1 = 2$". Is this a true statement? Yes, of course, we saw this before; one line divides the plane into two regions. Second, we need to prove that Domino n will topple into Domino $(n+1)$ for any *arbitrary* value of n. That is, let's *assume* that "$R(n) = 1 + \frac{n(n+1)}{2}$" is a *true* statement for some value of n and *show* that "$R(n+1) = 1 + \frac{(n+1)(n+2)}{2}$" must also be a true statement. How can we do this? Well, let's follow along with the argument we used before to relate $R(n+1)$ to $R(n)$. By considering the geometric consequences of adding an extra line to *any* diagram with n lines (that also fit our rules about the lines) we proved that $R(n+1) = R(n) + n + 1$. Using this knowledge *and* our assumption about Domino n falling, we can say that

$$R(n+1) = R(n) + n + 1 = 1 + \frac{n(n+1)}{2} + n + 1$$

Is this the same expression as what is written on Domino $(n+1)$? Again, let's simplify *both* expressions to verify they are the same. We have

$$1 + \frac{n(n+1)}{2} + n + 1 = 2 + n + \frac{n^2+n}{2} = \frac{1}{2}n^2 + \frac{3}{2}n + 2$$

and

$$1 + \frac{(n+1)(n+2)}{2} = 1 + \frac{n^2+3n+2}{2} = \frac{1}{2}n^2 + \frac{3}{2}n + 2$$

Look at that; they're identical! Thus, we have shown that Domino n is *guaranteed* to fall into Domino $(n+1)$, for *any* value of n. Accordingly, we can declare that *all* dominos will fall!

Think about the differences between what we have done with this "domino technique" and what we did before to derive the expressions we just proved. Did we use any ellipses in this section? Why is it better to prove a formula this way? Could we have used the domino induction technique to *derive* the formulas themselves?

2.3.2 Other Analogies

The Domino Analogy is quite popular, but it's not the only description of how induction works. Depending on what you read, or who you talk to, you might learn of a different analogy, or some other kind of description altogether. Here, we'll describe a couple that we've heard of before. It will help solidify your understanding of induction (at least as far as we've developed it) to think about how these analogies are all *equivalent*, fundamentally.

Mojo the Magical, Mathematical Monkey

Imagine an infinite ladder, heading straight upwards into the sky. There are infinitely-many rungs on this ladder, numbered in order: 1, 2, 3, and so on going upwards. Our friend Mojo happens to be standing next to this ladder. He is an intelligent monkey, very interested in mathematics but also a little bit magical, because he can actually climb up this infinite ladder!

If Mojo makes it to a certain rung on the ladder, that means the fact corresponding to that number is True. How can we make sure he climbs up the entire ladder? It would be inefficient to check each rung individually. Imagine that: we would have to stand on the ground and make sure he got to Rung 1, then we would have to look up a bit and make sure he got to Rung 2, and then Rung 3, and so on . . . Instead, let's just confirm two details with Mojo before he starts climbing. Is he going to start climbing? That is, is he going to make it to Rung 1? If so, great! Also, are the rungs close enough together so that he can *always* reach the next one, no matter where he is? If so, even greater! These are exactly like the conditions established in our Domino Analogy. To ensure that Mojo gets to *every* rung, we just need to know he gets to the first one and that he can always get to the next one.

Doug the Induction Duck

Meet Doug. He's a duck. He also loves bread, and he's going to go searching through everyone's yards to find more bread. These yards are all along Induction Street in Math Town, where the houses are numbered 1, 2, 3, and so on, all in a row.

Doug starts in the yard of house #1, looking for bread. He doesn't find any, so he's still hungry. Where else can he look? The house next door, #2, has a backyard, too! Doug heads that way, his tummy rumbling. He doesn't find any bread there, either, so he has to keep looking. He already knows house #1 has no bread, so the only place to go is next door to house #3. We think you see where this is going ...

If we were keeping track of Doug's progress, we might wonder whether he eventually gets to *every* yard. Let's say we also knew ahead of time that *nobody* has any bread. This means that whenever he's in someone's yard, he will definitely go to the next house, still searching for a meal. This means that he will definitely get to every house! That is, no matter which house we live in, no matter how large the number on our front door might be, at some point we will see Doug wandering around our backyard. (Unfortunately, he will go hungry all this time, though! Poor Doug.)

2.3.3 Summary

Let's reconsider what we've accomplished with the two example puzzles we've seen thus far, and the analogies we've given. In our initial consideration of each puzzle, we identified some aspect of the *structure* of the puzzle where a "fact" depended on a "previous fact". In the case of the cubic numbers, we found a way to express $(n+1)^3$ in *terms* of n^3; in the case of the lines in the plane, we described how many regions were added when an extra line was added to a diagram with n lines. From these observations, we applied this encapsulated knowledge over and over until we arrived at a "fact" that we knew, for a "small" value of n (in both cases, here, $n = 1$). This allowed us to derive a formula or equation or expression for a general fact that should hold for *any* value of n.

This work was interesting and essential for deriving these expressions, but it was *not enough* to *prove* the validity of the expressions. In doing the work described above, we identified the presence of an inductive process and utilized its structure to derive the expressions in question. This was beneficial in two ways, really; we actually found the expressions we wanted to prove and, by recognizing the inductive behavior of the puzzle, we realized that proving the expressions by *mathematical induction* would be prudent and efficient.

For the actual "proof by induction", we followed two main steps. First, we identified a "starting value" for which we could check the formula/equation by hand. Second, we *assumed* that one particular value of n made the corresponding formula hold true, and then used this knowledge to show that the corresponding formula for the value $n + 1$ must also hold true. Between those two steps, we could rest assured that "all dominos will fall" and, therefore, the formulas would hold true for all relevant values of n.

One Concern: What's at the "top" of the ladder?

You might be worried about something, and we'll try to anticipate your question here. (We only bring this up because it's a not uncommon observation to make. If you *weren't* thinking about this, try to imagine where the idea would come from.) You might say, "Hey now, I think I see how Mojo is climbing the ladder, but how can he actually get *all the way to the top*? It's an infinite ladder, right? And he never gets there . . . right?"

In a way, you would be right. Since this magical ladder really does go on *forever*, then there is truly no *end* to it and Mojo will never get "there". However, that isn't the point; we don't care about any "end" of the ladder (and not just because there *isn't* one). We just need to know that Mojo actually gets to *every possible* rung. He doesn't have to surpass all of them and stand at the top of the ladder, looking down at where he came from. That wasn't the goal!

Think of it this way: pretend you have a vested interest in some particular fact that we're proving. Let's say it's Fact #18,458,789,572,311,000,574,003. (Some huge number. It doesn't matter, really.) Its corresponding rung is waaayyyyyy up there on the ladder, and all you care about is whether or not Mojo gets there on his journey. Does he? . . . You bet he does! It might take a long time (how many steps will it take?), but in this magical world of monkeys and ladders, who cares about time anyway! You know that he'll eventually get there, and that makes you happy. Now, just imagine that for each fact, there's somebody out there in that magical world that cares about only that fact. Surely, everyone will be happy with the knowledge that Mojo will get to their rung on his journey. Nobody cares about whether he gets to the top; that isn't their concern. Meanwhile, out here in our regular, non-magical world, we are extremely happy with the fact that everyone in *that* world will eventually be happy. That entire infinite process of ladder-climbing was condensed into just two steps, and with only those two steps, we can rest assured that every rung on that ladder will be touched. Every numbered fact is true.

Think about this in terms of the Domino Analogy, as well. Do we care whether or not there is some "ending point" of the line of dominoes, so that they all fall into a wall somewhere? Of course not; the line goes on forever. Every domino will eventually fall over, and we don't even care how "long" that takes. Likewise, we know Doug will get to everyone's yard; we don't care "when" he gets to any *individual* yard, just that he gets to *all* of them.

2.3.4 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) How are the Domino, Mojo, and Doug analogies all *equivalent*? Can you come up with some "function" that describes their relationship, that converts one analogy into another?

(2) Find a friend who hasn't studied mathematical induction before, and try to describe it. Do you find yourself using one of the analogies? Was it helpful?

(3) Why is it the case that our work with the cubes didn't *prove* the summation formula? Why did we still need to go through all that work?

(4) Think about the Domino Analogy. Is it a problem that the line of dominoes goes on forever? Does this mean that there are some dominoes that will never fall down? Try to describe what this means in terms of the analogy.

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Work through the inductive steps to prove the formula

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

(2) Work through the inductive steps to prove the formula

$$\sum_{k=1}^{n} (2k-1) = n^2$$

(3) Work through the inductive steps to prove the formula

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

(4) Suppose we have a series of facts that are indexed by natural numbers. Let's use the expression "$P(n)$" to represent the n-th fact.

(a) If we want to prove *every* instance is True, for every natural number n, how can we do this?

(b) What if we want to prove that only every *even* value of n makes a True statement? Can we do this? Can you come up with a modification of one of the analogies we gave that would describe your method?

(c) What if we want to prove that only every value of n greater than or equal to 4 makes a True statement? Can we do this? Can you come up with a modification of one of the analogies we gave that would describe your method?

2.4 Two More (Different) Examples

This short section serves a few purposes. For one, we don't want you to get the idea, right away, that induction is all about proving a *numerical formula* with numbers and polynomials. Induction is so much more useful than that! One of the following examples, in particular, will be about proving some abstract property is true for any "size" of the given situation. You will see how it still falls under the umbrella of "induction", but you will also notice how it is different from the previous examples. Furthermore, these examples will illustrate that sometimes we need to know "more information" to knock over some dominoes. In the previous examples, we only needed to know that Domino n fell to *guarantee* that Domino $n+1$ will fall. Here, though, we might have to know about several previous dominoes. After these two examples, we will summarize how this differs from the domino definition given above, and preview a broader definition of the technique of induction, as it applies to these examples.

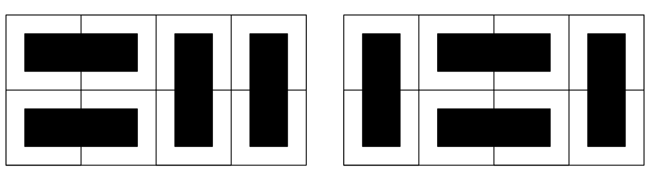
2.4.1 Dominos and Tilings

This next example is a little more complicated than the first two. We will still end up proving a certain numerical *formula*, but the problem is decidedly more visual than just manipulating algebraic expressions. Furthermore, we'll notice an interesting "kink" in the starting steps, where we have to solve a couple of "small cases" before being able to generalize our approach. This will be our first consideration of how the technique of induction can be generalized and adapted to other situations.

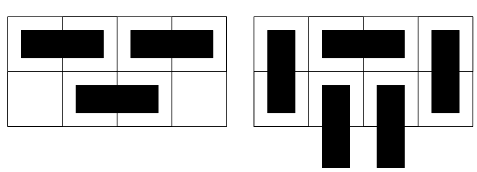
The question we want to answer is nicely stated as follows:

> Given a $2 \times n$ array of squares, how many different ways can we tile the array with dominoes? A *tiling* must have every square covered by one–and *only* one–domino.

For example, the following are proper tilings

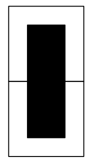


whereas the following are *not* proper tilings

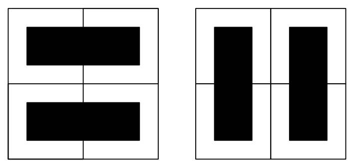


As before, let's examine the first few cases–where $n = 1, 2, 3$, and so on–and see if we notice any patterns. Try working with the problem yourself, before reading on, even!

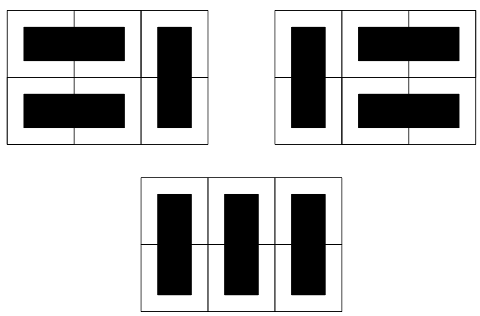
When $n = 1$, we have an array that is exactly the shape of one domino, so surely there is only one way to do this. Let's use the notation $T(n)$ to represent the number of tilings on a $2 \times n$ array. Thus, $T(1) = 1$.



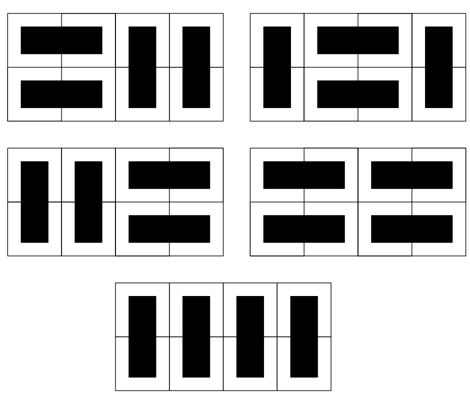
When $n = 2$, we have a 2×2 array. Since the orientation of the array matters, we have each of the following distinct tilings. Thus, $T(2) = 2$.



What about when $n = 3$? Again, we can enumerate these tilings by hand and be sure that we aren't missing any. We see that $T(3) = 3$.

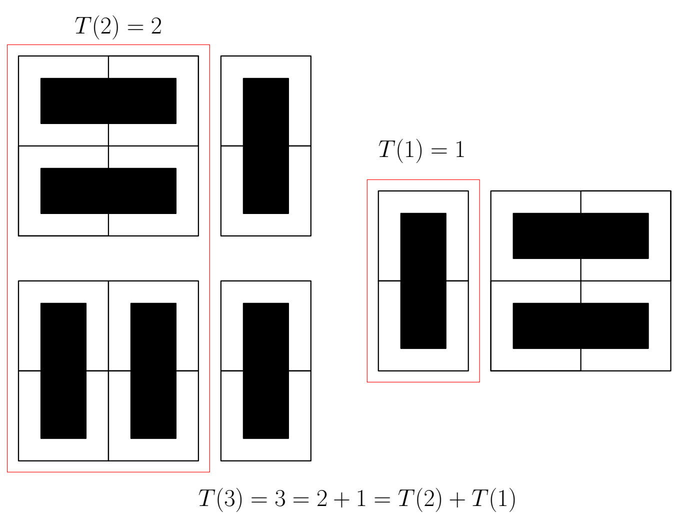


Okay, one more case, when $n = 4$. We see that $T(4) = 5$.

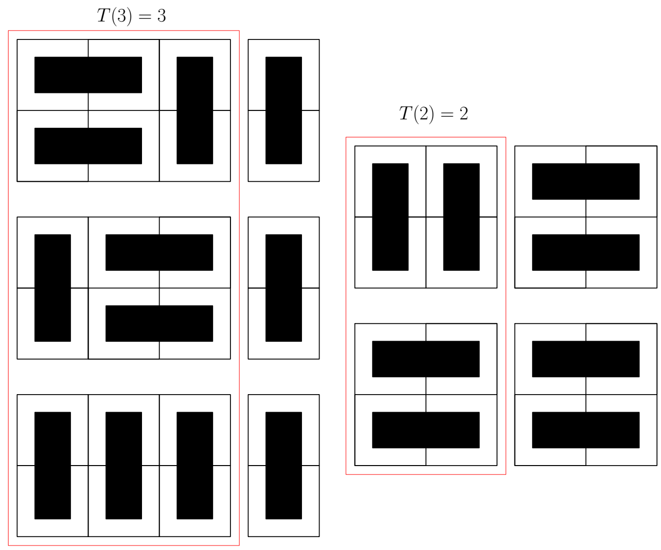


Can we start to find a pattern now? Writing out larger arrays will just be tiresome! Let's think about how we could have used the fact that $T(1) = 1$ to deduce something about $T(2) \ldots$ Well, wait a minute $\ldots$ We couldn't, right? There was something fundamentally different about those two cases. Specifically, because dominoes are 2×1 in size, the fact that we only added one row to the array didn't help us.

Alright, let's consider $n = 3$, then. Could we use the fact that $T(2) = 2$ at all? In this case, yes! Knowing there were two tilings of the 2×2 array, we could immediately build two tilings of the 2×3 array without much thought. Specifically, we can just *append a vertical domino* to each of those previous tilings. But we know now that $T(3) = 3$. Where did the third tiling come from? Look at that tiling again and how it compares to the other two. In that third tiling, the dominoes on the right side are horizontal, as opposed to the vertical one in the other two tilings. If we remove those two parallel, horizontal dominoes, we are left with precisely the situation when $n = 1$. Put another way, we can build a tiling of a 2×3 array by *appending a square of two horizontal dominoes* to the right side. In total, then, we have described all of the tilings of a 2×3 board in terms of boards of smaller sizes, namely 2×2 and 2×1:



Now you might see how the pattern develops! Let's show you what happens when $n = 4$, how we can construct *all* of the tillings that make up $T(4)$ by appending a vertical domino to each of the tilings that make up $T(3)$, or by appending two horizontal dominoes to each of the tilings that make up $T(2)$:



$T(4) = 5 = 3 + 2 = T(3) + T(2)$

Notice, as well, that no tiling for the 2×4 array was produced *twice* in this way. (Think carefully about why this is true. How can we characterize the two types of tilings in a way that will guarantee they don't coincide at all?) With this information, we can immediately conclude that $T(4) = T(3) + T(2)$.

Furthermore, we can generalize this argument; nothing was special about $n = 4$, right? For any particular n, we can just consider all possible tilings, and look at what happens on the *far right-hand side* of the array: either we have one vertical domino (which means the tiling came from a $2 \times (n-1)$ array) or two horizontal dominoes (which means the tiling came from a $2 \times (n-2)$ array). With confidence in this argument, we can conclude that

$$T(n) = T(n-1) + T(n-2)$$

for all of the values of n for which this expression makes sense. What values are those? Remember that we had to identify $T(1)$ and $T(2)$ separately; this argument doesn't apply to those values. Accordingly, we have to add the restriction $n \geq 3$ for the equation above to hold true.

With this information, we can then easily figure out $T(n)$ for any value of n, given enough time. We could write a computer program fairly easily, even. It was this *inductive* argument, though—the pattern that we noticed and our thorough description of why it occurs—that allowed us to make the conclusion in the first place. In this case, too, it just so happens that the value of every term, $T(n)$, depends on the value of *two* previous terms, $T(n-1)$ and $T(n-2)$. This did *not* happen in our previous examples in this chapter, and it hints at something deeper going on here. Do you see how our previous definition of induction, and the domino analogy, doesn't exactly apply here anymore? How might you try to amend our analogy to explain this kind of situation? Think about these issues for a bit and then read on. We'll talk about them more in-depth after the next example.

By the way, did you notice something interesting about our solution to this example? Do you know any other sequences of numbers that behave similarly? Think about it ...

2.4.2 Winning Strategies

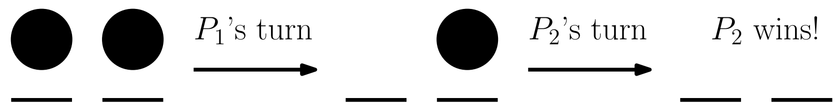
This example will be our first induction puzzle that *doesn't* prove a numerical formula! It might seem strange to think about that, but it's true, as you'll see. This is actually more common in mathematics than you might think, too: a problem or mathematical object might have some underlying inductive structure without depending on something algebraic or arithmetic.

In fact, we will be discussing a *game*. It's a game in the usual sense—there are rules to be followed by two players and there is a clear winner and loser—but it's also a game in the mathematical sense, where we can formulate the rules and playing situations using mathematical notation and discuss formal *strategies* in an abstract way. We can even *solve* the game. This is very different than say, the game of baseball.

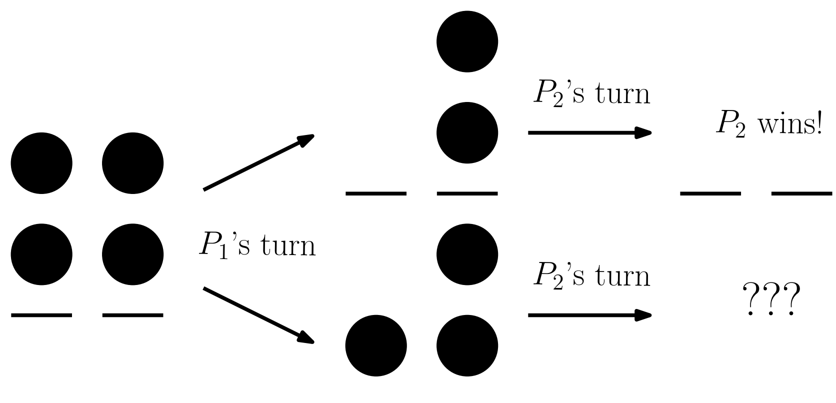
Let's discuss the rules for this game, which we shall call "Takeaway", for now. There are two players, called P_1 and P_2. The player P_1 goes first every time. The players start with two piles of stones in the middle of a table, each pile containing exactly n stones, where n is some natural number. (To distinguish the different versions of the game, we will say the players are "playing T_n" when there are n stones per pile.) On each player's move, they are allowed to remove *any* number of stones from *either* pile. It is illegal, though, to remove stones from both piles at once. The player who removes the *final* stone from the piles is the *winner*.

Try playing Takeaway with some friends. Use pennies or candies or penny candy as stones. Try it for different values of n. Try switching roles so you are P_1 and then P_2. Try to come up with a winning *strategy*, a method of playing that maximizes your chances of winning. Try to make a conjecture for what happens for different values of n. Who is "supposed" to win? Can you *prove* your claim? Seriously, play around with this game and attempt to prove something before reading on for our analysis thereof. You might be surprised by what you can accomplish!

As with the other examples, let's use some small values of n to figure out what's really going on, then try to generalize. When $n = 1$, this game is rather silly. P_1 must empty one pile of its only stone, then P_2 gets the only remaining stone in the other pile. Thus, P_2 wins. (Notice that it doesn't matter which of the two piles P_1 picks from, P_2 will always get the other one. We might say that P_1 picks the pile on the left "without loss of generality" because it doesn't matter either way; the situations are equivalent, so we might as well say it's the left pile to have something concrete to say. We will explore this idea of "without loss of generality" later on when we discuss mathematical logic, too.)



When $n = 2$, we now have a few cases that might appear. Think about P_1's possible moves. Again, they might act on either the left or right pile, but because they're ultimately identical and we can switch the two piles, let's just say (without loss of generality) that P_1 removes some stones from the left pile. How many? It could be one or two stones. Let's examine each case separately.

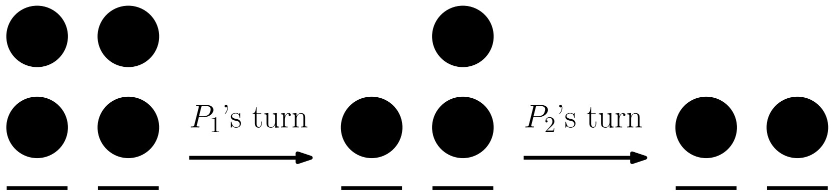


If P_1 removes both stones, how should P_2 react? Duh, they should take the other pile, so P_1 probably shouldn't have made that move in the first place. However, P_1 might not be thinking straight or something and, besides, we need to consider all possible situations here to fully analyze this game. Thus, in this case (the top line in the above diagram) P_2 wins. Okay, that's the easy situation.

What if P_1 removes just one stone from the left pile (the bottom line above)? How should P_2 react? We now have some options:

- If P_2 removes the other stone from the left pile ... well, P_1 takes the other pile and P_1 wins.
- If P_2 removes both stones from the right pile ... well, P_1 takes the last stone from the left pile and P_1 wins.

- However, if P_2 removes just one stone from the right pile ...



Now we have exactly the same situation presented by T_1, which we already analyzed! It is, again, P_1's move first, so we know what will happen: P_2 wins no matter what. If you are player P_2, this is obviously the best move: you win *no matter how* P_1 *responds*!

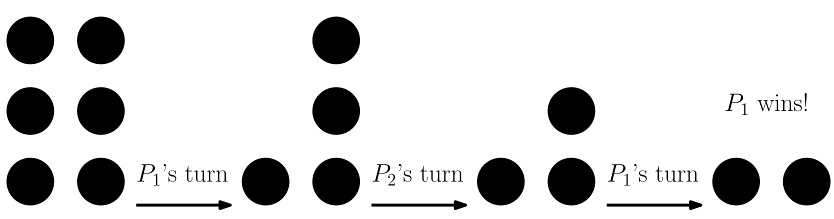
Stepping back for a second, let's think about what this has shown: no matter what P_1 does first (remove one or two stones from either pile), there is *some possible response* that P_2 can make that will *guarantee* a win for P_2, regardless of P_1's subsequent response. Wow, P_2 is sitting pretty! Let's see if this happens for other values of n.

When $n = 3$, we will again assume (without loss of generality) that player P_1 acted on the left pile. They could remove one, two, or three stones:

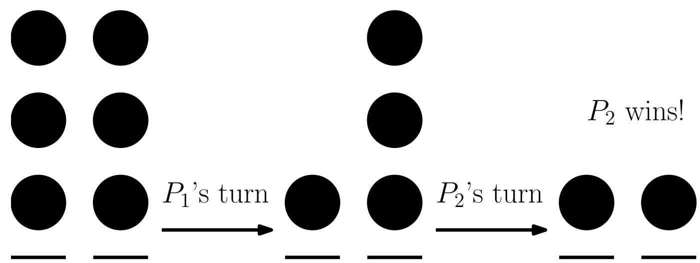
- If P_1 removes all three, P_2 responds by taking the other pile completely and wins.

- If P_2 removes two stones ... well, what should player P_2 do?

Finishing off that left pile is stupid (because P_1 can take the whole right pile and win), and pulling the entire right pile is similarly stupid (because P_1 can take the whole left pile and win), so something in between is required. Now, if P_2 removes just one stone from the right pile, notice that P_1 can respond with the same action; this leaves exactly one stone in both piles, but the roles reversed. With P_2 going first in such a situation, they are now bound to lose, per our previous analysis. Bad move, P_2!



Let's try again. If P_2 removes two stones from the right pile instead ... look at that! We now have exactly one stone in each pile, with P_1 up first, so we know P_1 is going to lose. P_2 strikes again!



Think about the case where $n = 4$ for a minute, and you'll find the exact same analysis occurring. You'll another possibility to consider: player P_1 can remove one, or two, or three, or four stones from the left pile. Whatever they do, though, you'll find that P_2 can just *mimic that action* on the other pile, reducing the whole game to a previous, *smaller* version of the game, where P_2 was shown to be guaranteed a win! It looks like P_2 is in the driver's seat the whole time, since they can respond to whatever P_1 does, making an identical move on the other pile. No matter what P_1 does, there is always a response for P_2 that means they win, regardless of P_1's subsequent moves. In this sense, we say "P_2 has a winning strategy". There is a clear and describable method for P_2 to assess the game situation and choose a specific move to *guarantee a win.*

How might we prove this? How does this even fit into this chapter on induction? It might be hard to see, at the moment. What are we really even proving here? What are the dominoes or rungs in our analogy for this problem? In wrapping your brain around this example, you should hopefully realize the following: induction is *not* about algebraic formulas all the time; induction represents some kind of "building-up" structure, where larger situations depend on smaller ones; we have to prove some initial fact, and then argue how an arbitrary, larger fact can be reduced so that it depends on a previous fact. This is really what the dominoes analogy is meant to accomplish. It just so happens that this analogy is particularly illustrative for certain induction problems (but not all) and is visualizable and memorable. It does not perfectly apply to *all* situations, though.

Read back through these four examples from this chapter and think about how they are similar and how they are different. Try to come up with a more precise, mathematical description of mathematical induction using some better terminology, perhaps of your own invention. (By this, we mean something better than our intuitive analogy. You'd be surprised at how well you might be able to describe induction without really knowing what you "ought" to say, and you'll actually learn a lot, in the process!) In due time, we will have a rigorous statement to make, and prove, about mathematical induction and its various forms. In the meantime, we need to take a trip through some other areas of mathematics to build up the necessary language, notation, and knowledge to come back and tackle this problem. Before we go, though, we should mention a few useful applications of mathematical induction.

2.4.3 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) How are these two examples *inductive*? In what ways are they similar to the previous examples, with the cubes and lines? In what ways are they different?

(2) With the domino tilings, how *many* previous values did we need to know to compute $T(n)$?

(3) What is the difference between writing $T(n) = T(n-1) + T(n-2)$ and $T(n+2) = T(n+1) + T(n)$?

(4) What is the winning strategy in the Takeaway game? Try playing with a friend who doesn't know the game, and use that strategy as player P_2. How frustrated do they get every time you win? Do they start to catch on?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) What is $T(5)$? Can you draw all of those tilings?

(2) Work through the possibilities for takeaway with two piles of 4 stones. Can you make sure that player P_2 always has a winning move?

(3) **Challenge:** What happens if you play Takeaway with *three* piles of equal sizes? Can you find a winning strategy for either player? Try playing with a friend and see what happens!

(4) Look up the *Fibonacci numbers*. How are they related to the sequence of numbers $T(n)$ we found in the domino tiling example?

2.5 Applications

2.5.1 Recursive Programming

The concepts behind mathematical induction are employed heavily in computer science, as well. Think back to how we first derived the formula for $\sum_{k=1}^{n} k^2$.

Once we had a way to represent a cubic number in terms of a smaller cube and some leftover terms, we repeated this subsitution process over and over until we arrived at the "simplest" case, namely, the one that we first observed when starting the problem: $2^3 = 1+3+3+1$. Recursive programming takes advantage of this technique: to solve a "large" problem, identify how the problem depends on "smaller" cases, and reduce the problem until one reaches a simple, known case.

A classical example of this type of technique is seen in writing code to compute the *factorial* function, $n!$, which is defined as the product of the first n natural numbers:

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$$

This is a simple definition that we, as humans, intuitively understand, but telling a computer how to perform this product doesn't work quite the same way. (Try it! How do you say "and just keep going until you reach n" in computer code?) A more efficient way to program the function, and one that models the mathematically inductive definition, in fact, is to have one program *recursively call itself* until it reaches that "simple" case. With the factorial function, that case is $1! = 1$. For any other value of n, we can simply apply the knowledge that

$$n! = (n-1)! \cdot n$$

over and over to compute $n!$. Consider the following *pseudocode* that represents this idea:

```
 factorial(n):

if n = 1
   return 1
else
   return n * factorial(n-1)
end
```

We know that $1! = 1$, so if the program is asked to compute that, the correct value is returned right away. For any larger value of n, the program refers to *itself* and says, "Go back and compute $(n-1)!$ for me, then I'll add a factor of n at the end, and we'll know the answer." To compute $(n-1)!$, the program asks, again, if the input is 1; if not, it calls itself and says, "Go back and compute $(n-2)!$ for me, then I'll add a factor of $n-1$ at the end." This process continues until the program returns $1! = 1$. From there, it knows how to find $2! = 1 \times 2$, and then $3! = 2! \times 3$, and so on, until $n! = (n-1)! \times n$.

Another example involving recursive programming arises with the *Fibonacci numbers*. You may have seen this sequence of numbers before in a mathematics course. (In fact, we even mentioned them in the last section, with the domino tilings!) You also might have heard about how they appear in nature in some interesting and strange ways. (The sequence was first "discovered" by the Italian mathematician Leonardo of Pisa while studying the growth of rabbit populations.) The first two numbers in the sequence are specified to be 1, and any number in the sequence is defined as the sum of the previous two. That is, if we say $F(n)$ represents the n-th Fibonacci number, then

$$F(1) = 1 \quad \text{and} \quad F(2) = 1 \quad \text{and} \quad F(n) = F(n-1) + F(n-2) \text{ for every } n \geq 3$$

Now, what is $F(5)$? Or $F(100)$? Or $F(10000)$? This can be handled quite easily by a recursive program. The idea is the same: if the program refers to either one of the "simple cases", i.e. $F(1)$ or $F(2)$, then it will know to return the correct value of 1 immediately. Otherwise, it will call itself to compute the previous two numbers and then add those together. Look at the pseudocode below and think about how it works. What would happen if we used this program to compute $F(10)$? How would it figure out the answer?

```
Fibonacci(n):

if n = 1 or n = 2
   return 1
else
   return Fibonacci(n-1) + Fibonacci(n-2)
end
```

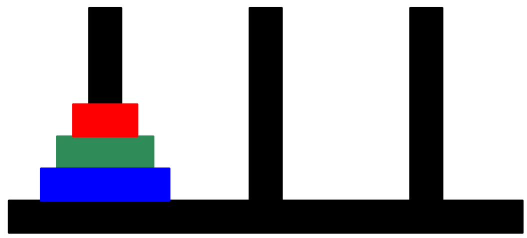
This follows the same idea as the `factorial` program above (let the program call itself to compute values for "smaller" cases of the function until we reach a known value) but there's something a little deeper going on here. If we were to input $n = 10$ into the program, it would recognize that it does not know the output value yet, and it will call itself to compute `Fibonacci(9)` and `Fibonacci(8)`. In each of those calls to the program, it would again recognize the value is as yet unknown. Thus, it would call upon itself again to compute `Fibonacci(8)` and `Fibonacci(7)`, but also `Fibonacci(7)` and `Fibonacci(6)`. That's right, the program calls itself multiple times with the *same input value*. To compute $F(9)$, we need to know $F(8)$ and $F(7)$, but meanwhile, to compute $F(8)$, we also need to know $F(7)$ and $F(6)$. In this way, we end up calling the program `Fibonacci` many times.

Try to compare the programs `Fibonacci` and `factorial`, especially in regards to the inductive processes we have been investigating in this chapter. Do they use similar ideas? How do they relate to the "domino" analogy of mathematical induction that we outlined? Think of the "fact" written on Domino n as being the computation of the correct value of $n!$ or $F(n)$. How does the analogy work in each case? Will all the dominos fall? Keep these questions in mind as you read on. There is some very powerful mathematics underlying all of these ideas.

2.5.2 The Tower of Hanoi

Let's take a short break and play a game. Well, it's not exactly a break because this is, in a sense, an *inductive* game, so it's completely relevant. But it is a game, nevertheless! The *Tower of Hanoi* is a very popular puzzle, partly because it involves such simple equipment and rules. Solving it is another matter, though!

Imagine that we have three vertical rods and three disks of three different sizes (colored blue, green, and red) stacked upon each other like so:



The goal is to move all three disks to another rod (either the middle or the right one, it doesn't matter) by following these rules:

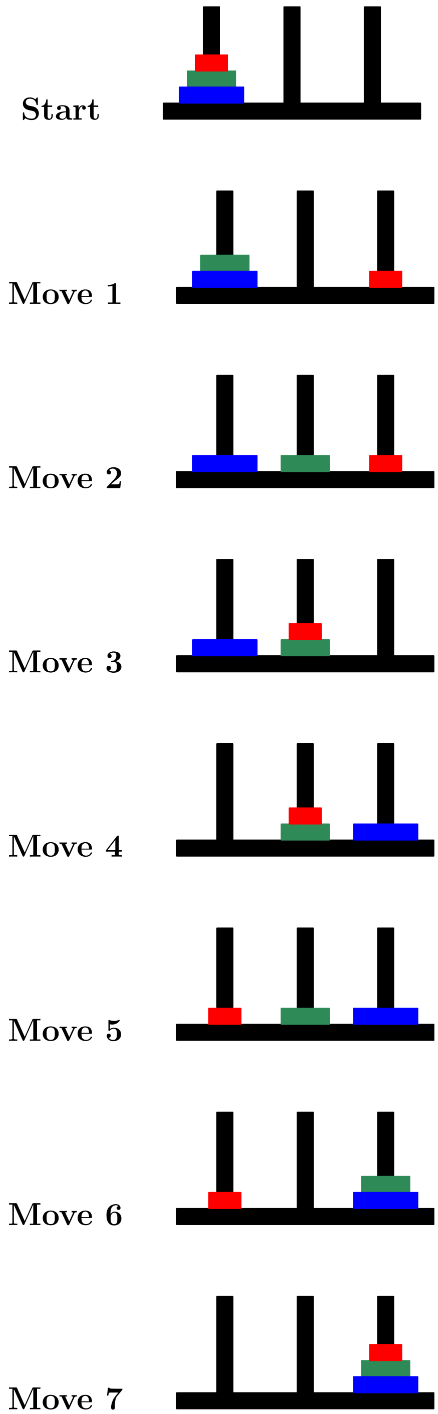
1. A single move consists of moving one (and *only* one) disk from the top of the stack on any rod and moving it to the top of the stack on another rod.

2. A disk cannot be placed on top of a smaller disk.

That's it! Two simple rules, but a difficult game to play. Try modeling the game with a few coins or playing cards or whatever you have handy. (You can even buy Tower of Hanoi sets at some games stores.) Can you solve it? How many moves did it take you? Is your solution the "best" one? Why or why not?

We mentioned that this is an *inductive* game, so let's explore that idea now. We want to consider how many *moves* it takes to solve the puzzle (where one *move* accounts for moving one disk from one rod to another) and, more specifically, identify the *smallest possible number of moves* it would take to solve the puzzle. To solve the puzzle with three disks, we could keep moving the smallest disk back and forth between two rods and generate 100 moves, if we wanted to, and then solve it, but that's certainly not the best way to do it, right? Let's say we found a way to solve the puzzle in a certain number of moves; how could we show that the number of moves we used is the *smallest possible* number of moves?

To address this question, we want to break down the method of solving the puzzle *recursively*. In doing so, we are actually going to answer a far more general question: What is the smallest number of moves required to solve the Tower of Hanoi puzzle with n disks on 3 rods? We posed the puzzle above with just 3 disks to give you a concrete version to think about and work with, but we can answer this more general question by thinking carefully. To make sure we are on the same page, we will show you how we solved the version with 3 disks:


Start
Move 1
Move 2
Move 3
Move 4
Move 5
Move 6
Move 7

Notice that the largest disk is essentially "irrelevant" for most of the solution. Since we are allowed to place any other disk on top of it, all we need to do is "uncover" that disk by moving the other disks onto a different rod, move the largest disk to the only empty rod, then move the other disks on top of the large one. In essence, we perform the same procedure (shifting the two smaller disks from one rod to another) twice and, in between those, we move the large disk from one rod to another. If the largest disk hadn't been there at all, what we actually did was solve the version of the puzzle with 2 disks, but twice! (Think carefully about this and make sure you see why this is true. Follow along with the moves in the diagrams above and pretend the large, blue disk isn't there.)

This shows that the way to solve the 3-disk puzzle involves two iterations of solving the 2-disk puzzle, with one extra move in between (moving the largest disk). This indicates a *recursive* procedure to solve the puzzle, in general. To optimally solve the n-disk puzzle, we would simply follow the procedure to optimally solve the $(n-1)$-disk puzzle, use one move to shift the largest, n-th disk, then solve the $(n-1)$-disk puzzle again.

Now that we have some insight into *how* to optimally solve the puzzle, let's identify how many *moves* that procedure requires. Recognizing that solving this puzzle uses a *recursive* algorithm, we realize that *proving* anything about the optimal solution will require *induction*. Accordingly, we would need to identify a "starting point" for our line of dominos, and it should correspond to the "smallest" or "simplest" version of the puzzle. For the Tower of Hanoi, this is the 1-disk puzzle. Of course, this is hardly a "puzzle" because we can solve it in one move, by simply shifting the only disk from one rod to any other rod. If we let $M(n)$ represent the number of *moves* required to optimally solve the n-disk puzzle, then we've just identified $M(1) = 1$. To identify $M(2)$, we can use our observation from the previous paragraph and say that

$$\underbrace{M(2)}_{\text{solve 2-disk}} = \underbrace{M(1)}_{\text{solve 1-disk}} + \underbrace{1}_{\text{shift largest disk}} + \underbrace{M(1)}_{\text{solve 1-disk}} = 1 + 1 + 1 = 3$$

and then it must be that

$$M(3) = M(2) + 1 + M(2) = 3 + 1 + 3 = 7$$

and

$$M(4) = M(3) + 1 + M(3) = 7 + 1 + 7 = 15$$

and so on. Do you notice a pattern yet? Each of these numbers is one less than a power of 2, and specifically, we notice that $M(n) = 2^n - 1$, for each of the cases we have seen thus far. It's important to point out that observing this pattern doesn't *prove* the pattern; just because it works for the first 4 cases does not mean the trend will continue, but that's exactly what an induction proof would accomplish. Also, recognizing that pattern and "observing" that $M(n) = 2^n - 1$ is a non-trivial matter, itself. We happened to know the answer and had no problem identifying the formula for you. You should probably try, on your own, to "solve" the following relationship

$$M(n) = 2M(n-1) + 1 \quad \text{and} \quad M(1) = 1$$

and see if you can derive the formula $M(n) = 2^n - 1$. The reason such a formula is *nicer* than the above relationship is that, now, $M(n)$ depends only on n, and not on previous terms (like $M(n-1)$, for example). This relationship and others like it are known as *recurrence relations*, and they can be rather difficult to solve, in general!

We know how to solve this one, though, and it yields $M(n) = 2^n - 1$. We will leave it to you to verify this. You can do so by checking a few values in the equation above, but we all know that isn't a *proof.* Try working through the inductive steps to actually prove it! We have already done most of the work, but it will be up to you to arrange everything carefully and clearly. Remember that you should identify what the "fact" on each domino is, ensure that Domino 1 falls, and then make a general argument about Domino n toppling into Domino $(n+1)$. Try to write that proof. Do the details make sense to you? Try showing your proof to a friend and see if they understand it. Did you need to tell them anything else or guide them through it? Think about the best way to *explain* your method and steps so that the written version suffices and you don't have to add any verbal explanations.

2.5.3 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) How is a recursive program inductive?

(2) What is the inductive structure of the Tower of Hanoi? Where did we solve the 2-disk puzzle while solving the 3-disk puzzle?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Follow the steps of the psuedocode `factorial` to compute 5!.

(2) Follow the steps of the psuedocode `Fibonacci` to compute $F(5)$.

(3) Solve the Tower of Hanoi puzzle with 4 disks. Make sure that you can do it in the *optimal* number of moves, $2^4 - 1 = 15$.

2.6 Summary

We have now seen some examples of **inductive arguments**. We realized that some of the puzzles we were solving used similar argument styles, and explored several examples to get a flavor for the different issues that might come up in such arguments. Specfically, we saw how inductive arguments are *not* always about proving a summation formula or an equation: inductive arguments can apply to *any* situation where a fact depends on a "previous instance" of that fact. This led us into developing an analogy for how induction works, mathematically speaking. We are comfortbal with thinking of induction in terms of the "Domino Analogy" for now, but one of our main goals in moving forwards is rigorously *stating* and *proving* a principle of induction. For now, let's get lots of practice working with these kinds of arguments. This is what this chapter's exercises are meant to achieve. Later on, once we've formalized induction, we'll be better off for it, and we'll have a thorough understanding of the concept!

2.7 Chapter Exercises

Here are some problems to get you comfortable working with inductive-style arguments. We aren't looking for fully rigorous proofs here, just a good description of what is going on and a write-up of your steps. We'll come back to some of these later and rigorously prove them, once we've established the Principle of Mathematical Induction (PMI) and a corresponding proof strategy.

Problem 2.7.1. Prove the following summation formula holds for every natural number, and for $n = 0$, as well:

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Follow-up question: use this result to state how many games are required to determine a winner in a single-elimination bracket tournament with 2^n teams. (For example, the NCAA March Madness Tournament uses this format, with $n = 6$.)

Problem 2.7.2. Prove that $3^n \geq 2^{n+1}$ for every natural number n that is greater than or equal to 2.

Problem 2.7.3. For which natural numbers n do the following inequalities hold true? State a claim and then prove it.

1. $2^n \geq (n+1)^2$
2. $2^n \geq n!$
3. $3^{n+1} > n^4$
4. $n^3 + (n+1)^3 > (n+2)^3$

Problem 2.7.4. **The December 31 Game:** Two players take turns naming dates from a calendar. On each turn, a player can increase the month or date but not both. The starting position is January 1, and the winner is the person who says December 31. Determine a winning strategy for the first player.

For example, a sequence of moves that yields Player 1 winning is as follows:

> (1) January 10, (2) March 10, (1) August 10, (2) August 25, (1) August 28, (2) November 28, (1) November 30, (2) December 30, (1) December 31

By *winning strategy* we mean a method of play that Player 1 follows that *guarantees* a win, no matter what Player 2 does.

Problem 2.7.5. Find and prove a formula for the sum of a *geometric series*, which is a series of the form

$$\sum_{i=0}^{n-1} q^i$$

for some real number q and some natural number n. (Hint: be careful when $q = 1$.)

Problem 2.7.6. Write a sentence that depends on n such that the sentence is true for all values of n from 1 to 99 (inclusive), but such that the sentence is false when $n = 100$.

Problem 2.7.7. What is wrong with the following "spoof" of the claim that $a^n = 1$ for every n?

"Spoof": Let a be a nonzero real number. Notice that $a^0 = 1$. Also, notice that we can inductively write

$$a^{n+1} = a^n \cdot a = a^n \cdot \frac{a^n}{a^{n-1}} = 1 \cdot \frac{1}{1} = 1$$

"$\square$"

Problem 2.7.8. In a futuristic society, there are only two different denominations of currency: a coin worth 3 Brendans, and a coin worth 8 Brendans. There is also a nation-wide law that says shopkeepers can only charge prices that can be paid in **exact change** using these two coins.

What are the legal costs that a shopkeeper could charge you for a cup of coffee?

Hint: Try a bunch of small values and see what happens.

Problem 2.7.9. Consider a chessboard of size $2^n \times 2^n$, for some arbitrary natural number n. Remove **any** square from the board. Is it possible to tile the remaining squares with L-shaped triominoes?

If your answer is Yes, prove it.

If your answer is No, provide a counterexample argument. (That is, find an n such that no *possible* way of tiling the board will work, and show why this is the case.)

Problem 2.7.10. Consider an $n \times n$ grid of squares. How many sub-squares, of any size, exist within this grid? For example, when $n = 2$, the answer is 5: there are 4 1×1 squares and 1 2×2 square. Find a formula for your answer and try to prove it is correct.

Problem 2.7.11. Prove that, in a line of at least 2 people, if the 1st person is a woman and the last person is a man, then somewhere in the line there is a man standing immediately behind a woman.

Problem 2.7.12. Prove that $n^3 - n$ is a multiple of 3, for every natural number n.

Problem 2.7.13. A **binary n-tuple** is an ordered string of 0s and 1s, with n total numbers in the string. Provide an *inductive argument* to explain why there are 2^n possible binary n-tuples.

Problem 2.7.14. Recall that the **Fibonacci Numbers** are defined by setting $f_0 = 0$ and $f_1 = 1$ and then, for every $n \geq 2$, setting $f_n = f_{n-1} + f_{n-2}$. This produces the sequence $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \dots$

You might not know that the Fibonacci Numbers also have a *closed form*; that is, there is a specific *formula* that defines them, in addition to the usual recursive definition given above. Here it is:

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

Prove that this formula is correct for all values of $n \geq 0$.

Problem 2.7.15. Again, considering the Fibonacci Numbers, f_n, prove the following:

1. $\displaystyle\sum_{i=0}^{n} f_i = f_{n+2} - 1$
2. $\displaystyle\sum_{i=0}^{n} f_i^2 = f_n \cdot f_{n+1}$
3. $f_{n-1} \cdot f_{n+1} - f_n^2 = (-1)^n$
4. $f_{m+n} = f_n \cdot f_{n+1} + f_{m-1} \cdot f_n$
5. $f_n^2 + f_{n+1}^2 = f_{2n+1}$

Problem 2.7.16. Try to provide an inductive argument that explains why every natural number $n \geq 2$ can be written as a product of prime numbers. Can you also show that this product is *unique*? That is, can you also explain why there is *exactly one way* to factor a natural number into primes?

Problem 2.7.17. Prove that

$$\sum_{k=1}^{n} k \cdot k! = 1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1$$

Problem 2.7.18. What is wrong with the following "spoof" that all pens have the same color.

"Spoof": Consider a group of pens with size 1. Since there is only 1 pen, it certainly has the same color as itself.

Assume that any group of n pens has only one color represented inside the group. (Note: we explained why this assumption is valid for $n = 1$ already, so we can make this assumption.) Take any group of $n + 1$ pens. Line them up on a table and number them from 1 to $n + 1$, left to right. Look at the first n of them, i.e. look at pens $1, 2, 3, \ldots, n$. This is a group of n pens so, by assumption, there is only one color represented in the group. (We don't know what color that is yet.) Then, look at the last n of the pens; i.e. look at pens $2, 3, \ldots, n + 1$. This is also a group of n pens so, by assumption, there is only one color represented in this group, too. Now, pen #2 happens to belong to both of these groups. Thus, whatever color pen #2 is, that is also the color of every pen in *both* groups. Thus, all $n + 1$ pens have the same color.

By induction, this shows that any group of pens, of any size, has only one color represented. Looking at the finite collection of pens in the world, then, we should only find one color. "□"

Problem 2.7.19. ⋆ This problem is *extremely difficult* to analyze, and is taken from the blog of the famous mathematician Terence Tao (link here).

There is an island upon which a tribe resides. The tribe consists of 1000 people, with various eye colours. Yet, their religion forbids them to know their own eye color, or even to discuss the topic; thus, each resident can (and does) see the eye colors of all other residents, but has no way of discovering his or her own (there are no reflective surfaces). If a tribesperson does discover his or her own eye color, then their religion compels them to commit ritual suicide at noon the following day in the village square for all to witness. All the tribespeople are highly logical and devout, and they all know that each other is also highly logical and devout (and they all know that they all know that each other is highly logical and devout, and so forth).

(For the purposes of this logic puzzle, "highly logical" means that any conclusion that can logically deduced from the information and observations available to an islander, will automatically be known to that islander.)

Of the 1000 islanders, it turns out that 100 of them have blue eyes and 900 of them have brown eyes, although the islanders are not initially aware of these statistics (each of them can of course only see 999 of the 1000 tribespeople).

One day, a blue-eyed foreigner visits to the island and wins the complete trust of the tribe.

One evening, he addresses the entire tribe to thank them for their hospitality.

However, not knowing the customs, the foreigner makes the mistake of mentioning eye color in his address, remarking *how unusual it is to see another blue-eyed person like myself in this region of the world.*

What effect, if anything, does this faux pas have on the tribe?

2.8 Lookahead

In this chapter, we have introduced you to the concept of **mathematical induction**. We looked at a few examples of puzzles where an inductive process guided our solution, and then we described how a *proof by induction* would follow to *rigorously verify* that solution. With the mathematical techniques and concepts we have at hand thus far, we had to rely on a non-technical analogy to describe this process to you. Thinking of an infinite line of dominos with "facts" written on them knocking into each other is a perfectly reasonable interpretation of this process, but it fails to represent the full mathematical extent of induction. In a way, it's like having a friend describe to you how to swing a golf club, even though you've never played golf before. Sure, they can provide you with some mental imagery of what a swing "feels like", but without getting out there and practicing yourself, how will you truly understand the mechanics of the golf swing? How will you learn how to adapt your swing, or tell the differences between using a driver and a five iron and a sand wedge? By investigating the underlying mechanics and practicing with those concepts, we hope to gain a better understanding of mathematical induction so that, in the future, we can use it appropriately, identify situations where it would be useful, and, eventually, learn how to *adapt* it to other situations. Of course, it will help to have that domino analogy in mind to guide our intuition, but we should also remember that it is not rigorous mathematics. It also doesn't perfectly describe the other examples we discussed, where a falling domino depended on not only the one immediately behind it, but several others before it.

In the next chapter, we will explore some relevant concepts needed to rigorously state and prove mathematical induction as a proof technique. Specifically, we will study some ideas of *mathematical logic* and investigate how to break down complicated mathematical statements and theorems into their constituent parts, and also how to build interesting and complex statements out of basic building blocks. Along the way, we will introduce some new notation and shorthand that will let us condense some of the wordy statements we make into concise (and precise) mathematical language. With that in hand, we will explore some more fundamental proof strategies, that we will then apply to *everything else we do* in this course, including the induction technique, itself! We will also study some of the ideas of *set theory*, a branch of mathematics that forms the foundation for all other branches. This will be extremely useful for organizing our ideas in the future, but it will also help us define the *natural numbers* in a rigorous manner. With some concepts and knowledge from these two branches of mathematics under our collective belts, we will be able to build mathematical induction on a solid foundation and continue to use it properly.

Chapter 3

Sets: Mathematical Foundations

3.1 Introduction

It's now time for sets education! This might seem like a weird jump to make, after the last chapter. You'll have to trust us when we say that this is actually quite natural and, ultimately, essential. Everything we do in mathematics is built upon the foundation of **sets**, so we better get started talking about them and getting used to them.

3.1.1 Objectives

The following short sections in this introduction will show you how this chapter fits into the scheme of the book. They will describe how our previous work will be helpful, they will motivate why we would care to investigate the topics that appear in this chapter, and they will tell you our goals and what you should keep in mind while reading along to achieve those goals. Right now, we will summarize the main objectives of this chapter for you via a series of statements. These describe the skills and knowledge you should have gained by the conclusion of this chapter. The following sections will reiterate these ideas in more detail, but this will provide you with a brief list for future reference. When you finish working through this chapter, return to this list and see if you understand all of these objectives. Do you see why we outlined them here as being important? Can you define all the terminology we use? Can you apply the techniques we describe?

By the end of this chapter, you should be able to ...

- Define what a set is, and identify several common examples.
- Use proper notation to define a set and refer to its elements.

- Define and describe several ways to operate on sets; i.e. identify the ways to take two or more sets and create new sets from them.

- Describe how two sets might be compared, as well as apply a proper technique to prove such claims.

- Explain how the natural numbers are related to sets, and relate this to mathematical induction.

3.1.2 Segue from previous chapter

We are building towards a formal statement of mathematical induction as a *theorem*, which we will then prove. To get there, we need to have some fundamental objects to work with and talk about, logically. Sets are those objects! Historically speaking, mathematics was placed on the *set theory* foundation relatively recently, around the turn of the 20th century. Until then, mathematicians tended to "wave their hands" a bit about what was really going on underneath their work; they made a lot of "intuitive" assumptions and hadn't yet tried to rigorously and *axiomatically* describe everything they did. After the work of the mathematician **Georg Cantor** showed everyone some surprising and counter-intuitive results that were perfectly correct and consistent with our assumptions ... well, we realized that we better decide what we've been talking about all along. This is not meant to discredit the work of mathematicians before 1900, of course! We just mean that they were playing a game all along where they hadn't really agreed on a set of rules yet. That's what the **axioms** of set theory are.

3.1.3 Motivation

We are, of course, motivated by our ongoing desire to learn about **proofs**, discover what they are and how they work, and, in particular, rigorize mathematical induction. More generally, though, we are interested in learning about what mathematicians really do, and we are sure that any mathematician in the world can tell you how important **sets** are in their work. They might do so begrudgingly, and say that they themselves could never work in pure *set theory*, but we doubt you'll find anyone who will deny the importance of sets.

Everything we do later on will involve making some claim about a set of objects; that is, we will attempt to say (and subsequently prove) that some fact is True about some particular objects. The way we specify those objects involves **sets**. The way in which we express such facts will involve mathematical logic, and we will get to that soon enough. For now, we need to learn how to express many types of mathematical objects in the first place, before we can even make claims about them.

3.1.4 Goals and Warnings for the Reader

This chapter will likely involve handling some mathematical ideas that are new to you, as opposed to the previous chapters where we focused on puzzles that only relied on some knowledge of numbers and algebra and arithmetic and critical thinking. These new ideas will require careful reading and thinking. As we introduce these concepts and results, we expect you to read through them carefully and do some thinking on the side. Mathematical exposition requires more of the reader than, say, a newspaper article; it expects an *engaged* reader, one who will think carefully about every sentence and sometimes have to pause for a few minutes to ensure full understanding of what has been said so far. Keep this in mind as you read on: reading mathematics can be difficult, but this is to be expected! Don't let it be discouraging; just think of every sentence as a single jigsaw piece in a larger puzzle to be solved.

In particular, don't be surprised if this chapter takes as long (if not longer) to read through (and work through in class) as the previous two chapters combined! The most baffling part of this, as we have observed over the years, is in the **notation** of sets. This is likely the first time in your mathematical careers where you are expected to be as **precise** and **rigorous** as possible with your writing. It is no longer okay to just "have the right idea" in your written work; we really care that you say exactly what you meant to say, and nothing else. As you read what we have written, ask yourself, "Why does that make sense, as opposed to . . . something else?" After you have written down an answer to a question or homework problem, read it again and ask yourself, "Does this actually make sense? Does it say what I meant to say, what was in my head? Is someone else guaranteed to read it in the same way I wrote it?"

Also, this chapter will involve some more **abstract** thinking than your typical mathematics course. This might be a shock for you, or maybe not. Either way, this is certainly not material that you can just skim through and expect to pick up on first glance. Now, more than ever, you should take the time and effort to internalize this material. Read some pages and then go think about the material while you eat dinner or shower or play basketball. Try to find examples in real life. Talk with your friends about sets. This may sound silly now but, ultimately, it will help you. Trust us.

3.2 The Idea of a "Set"

A "Collection of Objects" with a Common Property

The intuitive notion of a set is probably not entirely new to you. If you're a baseball card collector, having a "complete set" means owning every single card from a particular printing run by a card manufacturer. If you play board games with friends, you agree on a "set of rules" before playing so there are no unresolved disputes later on. If you performed a laboratory experiment in biology or chemistry or physics class, you collect information into a "data set" and analyze those results to test a hypothesis.

Those are three different situations that each refer to the word **set**, so what is it about that word that relates those contexts and gives it a proper meaning? Essentially, a set refers to a collection of objects of some kind that are grouped together on the basis of having some common property. In the first example, a copy of every baseball card produced by Topps in 1995 would belong to that particular set. In the second example, any agreed-upon convention would belong to your set of rules. In the third example, any data point gathered in your experiment would belong to your data set. In each case, there is a common property that lets us associate particular objects with each other and refer to them as one set.

Sets in Mathematics

Sets are very common, popular, useful and fundamental in mathematics. Because mathematicians work with abstract objects and relationships between those objects, it can be quite difficult to describe exactly what one is thinking about without being able to refer to sets of mathematical objects. We have, in fact, already done so!

For instance, when investigating polynomials and the quadratic formula, we mentioned that a quadratic polynomial $p(x) = ax^2 + bx + c$ with a negative discriminant (when $\frac{b^2}{4a} - c < 0$) will have no roots *in the set of real numbers.* What did we mean? Did you understand that sentence? We were trying to convey the idea that no matter what real number x we choose from among the collection of all real numbers, it would be guaranteed that $p(x) \neq 0$. But what exactly is the set of real numbers? How is it defined? How can we be so sure it even exists? These are actually rather difficult questions to answer, and attempting to do so would take us far off course into the world of set theory.

In the language of mathematics, we aim to be *precise* and *unambiguous* with our sentences and statements, and we seek to establish truths based on certain fundamental assumptions. We need to make those assumptions as a starting point, or else we would have nothing to base our truths upon. These assumptions, that everyone agrees to be part of the "set of rules" before "playing the game" of mathematics, are known as **axioms**.

Perhaps, if you have studied some geometry or read about the Greek mathematician Euclid and his treatise, the *Elements*, then you have heard the word "axiom" before. All of the results of basic geometry that Euclid *proved* were founded upon some basic assumptions: that any two points can be joined by a line segment, that a circle with a given center point and radius must exist, that non-parallel lines intersect, and so on. These statements are simply *agreed upon* to be True at the outset.

Another place we find axioms is in the branch of mathematics known as **set theory**. The axioms of this branch place all of the results involving sets on firm foundations, and using those axioms and results derived from them, we can continue to discover new truths in the mathematical universe. Investigating these axioms and their consequences is better suited for a course devoted to set theory, though, and we will take many of the consequences of the set theoretic axioms for granted without rigorously proving them. This is not because such proofs are impossible, but merely because they would take too much time and space in this book to accomplish.

What we *will* do is provide a definition of "set" that is satisfactory for the contexts in which we will be using sets in this book. We will also define some basic properties of sets, share some illustrative examples, and dicuss different operations we can perform on sets to create new ones.

3.3 Definition and Examples

3.3.1 Definition of "Set"

Let's start with a definition. As we started to explain above, we often think of sets as being characterized by the objects that are grouped together into that set and the property that makes that grouping make sense. The following definition attempts to make that notion as precise as we possibly can, while also introducing some relevant notation and terminology.

Definition 3.3.1. *A* **set** *is a collection of all objects that have a common, well-defined property. The objects contained in a set are called* **elements** *of the set. The mathematical symbol "$\in$" represents the phrase "is an element of" (and "$\notin$" represents "is not an element of").*

3.3.2 Examples

Let's dive right in with some specific examples of sets (and non-sets, even) to illustrate this definition. It is common in mathematics to use capital letters to refer to *sets* and lowercase letters to refer to *elements* of sets, and we will frequently follow this convention (but not always). To define or describe a set, we need to identify that common, well-defined property that associates the elements of the set with each other. For instance, we could define B to be the set of all teams in Major League Baseball. Is this a well-defined property? If we present you with an object, is ther a definite Yes/No answer to the question of "Does this object have this defining property?" Yes, this is the case here, so this is a property that characterizes a set. (To avoid confusion for readers in the future, let us be more specific and say B refers to MLB teams from the 2012 season.) In the language of mathematics, we would write

$$B = \{\text{Major League Baseball teams from the 2012 season}\}$$

The "curly braces"—{ and }—indicate that the description between them will identify a set, and the text inside is a description of the objects and their common, well-defined property. It now makes sense to say Pittsburgh Pirates $\in B$ and Pittsburgh Penguins $\notin B$.

Common ways to read the mathematical symbol $\in$ in English are **"is an element of"** or "is a member of" or "belongs to" or "is in". We will mostly use "is an element of" because it is the least ambiguous of them, and uses the mathematical term **element** appropriately. Any of these other, equivalent, phrases may be used, depending on the context, but are less preferable. (In particular, "is in" can be confused with other set relationships, so we will avoid it entirely, and encourage you to do the same.)

We've also already seen some commonly-used sets of numbers. You know what they are from previous work with these numbers, but you might not usually think of them as sets, which is what they are!

$$\begin{aligned}
\mathbb{N} &= \{\,\text{natural numbers}\,\} = \{1, 2, 3, \ldots\} \\
\mathbb{Z} &= \{\,\text{integers}\,\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \\
\mathbb{Q} &= \{\,\text{rational numbers}\,\} \\
&= \{\text{numbers of the form } \frac{a}{b}\ , \text{ where } a, b \in \mathbb{Z} \text{ and } b \neq 0\,\} \\
\mathbb{R} &= \{\text{real numbers}\}
\end{aligned}$$

Think about how the second definition of $\mathbb{Q}$ above makes sense. We will see, quite soon, a more condensed way to write out a phrase like "numbers of the form ... blah blah ... with the additional information that ... blah blah". Also, notice that we can't really define $\mathbb{R}$ except to just say they're the real numbers. How do you even define what a real number is? Have you ever tried?

3.3.3 How To Define a Set

Another way of defining or describing a set is simply listing all of its elements. This is convenient when the number of elements in the set is small. For instance, the following definitions of the set V are all *equivalent*:

$$\begin{aligned}
V &= \{\text{A,E,I,O,U}\} \\
V &= \{\text{vowels in the English language}\} \\
V &= \{\text{U,E,I,A,O}\}
\end{aligned}$$

By "equivalent", we mean that each line above defines the *same* set V, using different terms. (Note: we have adopted the convention that y is a consonant, so $y \notin V$.) The common, well-defined property that associated the objects A, E, I, O, and U is the fact that they are all vowels (exhibited in the second definition) and since there are only five such objects, it is simple and convenient to list them all (as in the first definition).

Order and Repetition Don't Matter

Why do you think the third definition is the same as the others? It refers to the same collection of objects, and any set is completely characterized by its elements, so the *order* in which we write the elements *does not matter*. Is U$\in V$? The answer to this question is "Yes", regardless of whether U is written first or last in the list of elements.

Not only does the order of elements not matter within a set, the *repetition* of elements does not matter! That is, the set $A = \{a, a, a\}$ and the set $A = \{a\}$ are exactly the same. Again, remember that a set is completely characterized by its elements; we only care about what is "in" a set. (We will mention this again in Section 3.4.4, when we talk about the "bag analogy" for sets.) Writing $A = \{a, a, a\}$ is just a triply-redundant way of saying $a \in A$ and that *only* a is an element of A. Thus, $A = \{a\}$ is the most concise way of stating the same information.

The Common Property Might Be Being an Element of That Set

Now, still following the idea that we can define a set by writing all of the elements, consider the following definition of a set A:

$$A = \{2, 7, 12, 888\}$$

Surely, this is a set because we just defined it by listing its elements. What is the common, well-defined property that associates its elements, though? With the set V of vowels, we could list the elements *and* provide a linguistic definition, but for this set A, it seems as though we are relegated to listing the elements without knowing a way of *describing* their common property. Mathematically speaking, though, a common property uniting $2, 7, 12, 888$ is that they are all elements of this set A! In the mathematical universe, we have a license for freedom of abstract thought, and merely by discussing this set A and its elements, we have given them that common property. Does this seem satisfactory to you? Can you come up with *another* common, well-defined property that would yield exactly the elements of A? (Hint: identify a polynomial $p(x)$ whose *roots* are exactly $2, 7, 12$, and 888.) If the elements of a set have more than one property that associates them together, do you think it matters which property we have in mind when referring to the set? And what do you think about the set $S := \{2, 7,$ M, Boston Red Sox$\}$? Could there possibly be a common property other than the fact that we have listed them here?

Ellipses Are Sometimes Okay, But Informal

Sometimes, when there is no confusion about the set in question, or it has been defined in another way and we wish to list a few elements as illustrative examples, then it is convenient to use ellipses to condense the listing of elements of a set. For instance, we might write

$$E = \{\text{even natural numbers}\} = \{2, 4, 6, 8, 10, \dots\}$$

This set is *infinitely large*, in fact, so we could not even list all of its elements if we tried, but it is clear enough from the first few elements listed that we are referring to even numbers, especially because we have already referred to E as "the set of even natural numbers". However, we cannot stress enough that this is *not* a precise definition of the set in question. It suffices in an informal context, but it is not mathematically rigorous, and this will become clear as we discuss the following proper way of defining sets.

Set-Builder Notation

The best way to define or describing a set is to identify its elements as particular objects of another set that have a specific property. For instance, if we wished to refer to the set S of all natural numbers between 1 and 100 (inclusive), we could list all of those elements, but this requires a lot of unnecessary writing. We could also use the ellipsis notation $S = \{1, 2, 3, \ldots, 100\}$ but, again, this is not precise without already having a formal definition of S. (Someone might misinterpret the ellipses in a different way.) It is much more precise *and* concise to write

$$S = \{x \in \mathbb{N} \mid 1 \leq x \leq 100\}$$

We read this as "S is the set of all objects x in the set $\mathbb{N}$ of natural numbers *such that* $1 \leq x \leq 100$".

The bar symbol $|$ is read as **"such that"** and indicates that the information to the left tells us what "larger set" the objects come from, while the information to the right tells us the specific property that those objects should have.

(Caution: do *not* use $|$ in other contexts to mean "such that". This is only acceptable in the context of defining sets. It is just used as a place-holder to separate the left side—the set we use to draw elements—from the right side—a description of the property those elements should have.)

This is an example of the very popular and useful **set-builder notation**. We call it this because we are *building* a set by drawing elements from a "larger" set of possibilities, and only including those that have a particular property. To do this, we need to tell the reader (1) what the larger set is, and (2) what the common property is. Let's illustrate this idea with a few examples:

$$\begin{aligned}
S &= \{x \in \mathbb{N} \mid 1 \leq x \leq 100\} = \{1, 2, 3, \ldots, 100\} \\
T &= \{z \in \mathbb{Z} \mid \text{we can find some } k \in \mathbb{Z} \text{ such that } z = 2k\} \\
&= \{\ldots, -4, -2, 0, 2, 4, \ldots\} \\
U &= \left\{x \in \mathbb{R} \mid x^2 - 2 = 0\right\} = \left\{-\sqrt{2}, \sqrt{2}\right\} \\
V &= \left\{x \in \mathbb{N} \mid x^2 - 2 = 0\right\} = \{\ \}
\end{aligned}$$

The last two examples show how the **context** is extremely important. The same common property (satisfying $x^2 - 2 = 0$) can be satisfied by a different set of elements when we change the *larger set* from which we draw elements. Two real numbers satisfy that property, but no natural numbers satisfy it! Do any rational numbers satisfy that property? What do you think?

This is why it is absolutely essential to specify the larger set. A definition like "$U = \left\{x \mid x^2 - 2 = 0\right\}$ is *meaningless* because it is ambiguous and could yield completely different interpretations.

Reading Notation Aloud

We are really learning a new **language** here, and these are some of the basic words and rules of grammar. We'll need some practice translating these sentences into English (in our heads and out loud) and vice-versa. For example, we can say the definition for S above as any of the following, reasonably:

> S is the set of all natural numbers x such that x is between 1 and 100, inclusive.
>
> S is the set of all natural numbers between 1 and 100, inclusive.
>
> S is the set of all natural numbers x that satisfy the inequality $1 \leq x \leq 100$.
>
> S is the set of natural numbers x with the property that $1 \leq x \leq 100$.

Notice that all of them identified the larger set and the common property; the only differences between them are linguistic/grammatical, and they do not alter the mathematical meanings.

Try to write similar sentences for the other definitions. Try getting a verbal definition of a set from a friend and writing down what they said in mathematical symbols.

Consider a definition of the rational numbers $\mathbb{Q}$ that we saw before, and notice that we can rewrite it as:

$$\begin{aligned}\mathbb{Q} &= \left\{\frac{a}{b}\ , \text{ where } a, b \in \mathbb{Z} \text{ and } b \neq 0\right\} \\ &= \left\{x \in \mathbb{R} \mid \text{we can find } a, b \in \mathbb{Z} \text{ such that } \frac{a}{b} = x \text{ and } b \neq 0\right\}\end{aligned}$$

Notice the subtle difference between the two definitions. The upper one tells us that all rational numbers are **of the form** $\frac{a}{b}$, and then tells us the particular assumptions of a and b that must be satisfied. The lower one tells us that all rational numbers are *real* numbers with a particular property, namely that we can express that real number as a ratio of integers. We strongly prefer the lower definition, because it tells us more information.

In general, if $P(x)$ represents a sentence (involving English and/or mathematical language) that describes a specific, well-defined *property*, and X is a given set, then the notation

$$S = \{x \in X \mid P(x)\}$$

is read as

> "S is the set of all elements x of the set X such that the property $P(x)$ is true".

In the notation $P(x)$, the letter x represents a variable object, and depending on the particular object we use as x, the property $P(x)$ may hold (i.e. $P(x)$ is true) or may fail (i.e. $P(x)$ is false). If the property holds, then we include x in S (so $x \in S$), and if it fails, we do not include x in S (so $x \notin S$).

Returning to our example of the set E of even natural numbers, it is more precise to write

$$\begin{aligned}E &= \{\text{even natural numbers}\} \\ &= \{x \in \mathbb{N} \mid \text{there is a natural number } n \text{ such that } x = 2n\}\end{aligned}$$

Notice that there are two "layers" of properties here. A natural number is included in our set E if we can find *another* natural number n with the additional property that $x = 2n$. Try to write down a similar definition for the set of odd numbers, or the set of perfect squares. What about the set of primes? The set of palindromic numbers? The set of perfect numbers? Can you write definitions for these sets using set-builder notation?

3.3.4 The Empty Set

What if no elements satisfy a property $P(x)$? What happens then? For instance, consider the definition

$$S = \left\{ x \in \mathbb{N} \mid x^2 - 2 = 0 \right\}$$

We know that the number x we are "looking for" with that property is $\sqrt{2}$ (and $-\sqrt{2}$, too) but $\sqrt{2} \notin \mathbb{N}$. Thus, no matter what element of $\mathbb{N}$ we let x represent, the property $P(x)$—given by "$x^2 - 2 = 0$"—actually *fails*. Thus, there are no elements of this set. Is this really a set?

Remember, a set is completely characterized by its elements, and a set having *no elements*, such as this one, is characterized by that fact. If we attempted to list its elements, we would end up writing $\{\}$. This set is so special, in fact, that we give it a name and symbol:

Definition 3.3.2. *The* **empty set** *is the set which has no elements. It is denoted by the symbol $\varnothing$.*

There are many ways to define the empty set using set-builder notation. (And yes, we do mean *the* empty set; there is only one set with no elements!) We saw one example above, and we're sure you can come up with many others. Consider for example, the following sets:

$$\{a \in \mathbb{N} \mid a < 0\}$$
$$\{r \in \mathbb{R} \mid r^2 < 0\}$$
$$\{q \in \mathbb{Q} \mid q^2 \notin \mathbb{Q}\}$$

Do you see why these all define the same set, the one with no elements?

Context Matters

We should also note again the significance of specifying the larger set X from which we draw our variable element x in a set-builder definition like the one above. For instance, consider the following two sets:

$$S_1 = \{x \in \mathbb{N} \mid |x| = 5\} = \{5\}$$
$$S_2 = \{x \in \mathbb{R} \mid |x| = 5\} = \{-5, 5\}$$

(Note: It is also quite common to **index** sets with the subscript notation you see above, allowing us to use the same letter many times.)

This specification is clearly important, in this case, because it yields two entirely different sets! For this reason, we must be precise and clear when defining a set in this way. A definition like $S = \{x \mid |x| = 5\}$ should be regarded as ambiguous and undesirable, since it leads to issues like the one above.

3.3.5 Russell's Paradox

Perhaps it seems like we are picking nits here, but the reasoning behind our vehemence is rooted in some fundamental ideas of set theory. We wish to avoid some complex issues and paradoxes that might arise without this policy in place. There is a particularly famous example of a paradox involving sets that illustraes why we have the requirement described in the above paragraph, namely that we must specify a larger set when we use set-builder notation. This example is known as *Russell's Paradox* (after the British mathematician Bertrand Russell), and we we will present and discuss it in this section.

Sets Whose Elements Are Sets

First, we should point out that this discussion will introduce the notion that sets can also be *elements* of other sets. This may seem like a strange and far-fetchedly abstract idea right now, but it is a fundamental concept in mathematics.

For a concrete example, think back to our set B of all Major League Baseball Teams. We could also regard each team as a set, where its elements are the players on the team. Thus, it would make sense to say

$$\text{Derek Jeter} \in \text{New York Yankees} \in B$$

since Derek Jeter is an element of the set *New York Yankees*, which is itself an element of the set B. (Notice, however, that Derek Jeter $\notin B$. The relationship signified by "$\in$" is not **transitive**. We will hold off on defining this term until much later. For now, we will point out that the relationship signified by "$\leq$" on the set of real numbers *is* transitive. If we know $x \leq y \leq z$, then we can deduce $x \leq z$. This is *not* the case with the "$\in$" relationship, though.)

Another example is $S = \{1, 2, 3, \{10\}, \varnothing\}$. Yes, the empty set itself can be an element of another set, as can the set $\{10\}$. Why couldn't they? As a thought exercise, we suggest thinking about the difference between $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, and so on. Why are they different sets?

One final example involves the natural numbers $\mathbb{N}$. Let's use $\mathbb{O}$ and $\mathbb{E}$ to represent the *odd* and *even* natural numbers, respectively. What, then, is the set $S = \{\mathbb{O}, \mathbb{E}\}$, and how does it differ, if at all, from $\mathbb{N}$? This is a subtle question, so think about it carefully.

The Paradoxical "Set"

Spend some time on the side thinking about this notion of sets whose elements are sets. For now, though, let us forge ahead with our explanation of Russell's Paradox. Consider the following definition of a "set". We say "set" because it is actually *not* a properly-defined set, but it remains to be seen exactly why this is the case. When it becomes clear this is not a set, this will be an argument for *requiring* the specification of a larger set to draw from when we use set-builder notation; this is because the definition below does not specify a larger set. Here is that definition:

$$\mathcal{R} = \{x \mid x \notin x\}$$

That's it! Is this a set? What are the elements of $\mathcal{R}$? Think about what the definition above says: the elements of $\mathcal{R}$ are sets that also happen to *not* have themselves as elements. Can you identify any elements of $\mathcal{R}$? Can you identify any objects that are not elements of $\mathcal{R}$?

The first question is far easier to answer: any of the sets we have discussed so far would be elements of $\mathcal{R}$. For instance, the empty set $\varnothing$ contains *no* elements, so it certainly doesn't have *itself* as an element. Thus, $\varnothing \in \mathcal{R}$. Also, notice that$\mathbb{N} \notin \mathbb{N}$ (because the set of natural numbers is not a natural number, itself) and thus $\mathbb{N} \in \mathcal{R}$.

Identifying objects that are *not* elements of $\mathcal{R}$ is a very tricky matter, and we will help you by asking the following question: Is $\mathcal{R}$ an element of itself? Is it true or false that $\mathcal{R} \in \mathcal{R}$? Think about this carefully before reading on. We will walk you through the appropriate considerations.

- Suppose $\mathcal{R} \in \mathcal{R}$ is True.

  The defining property of $\mathcal{R}$ tells us that any of its elements is a set that does *not* have itself as an element. Thus, we can deduce that $\mathcal{R} \notin \mathcal{R}$.

  Wait a minute! Knowing that $\mathcal{R} \in \mathcal{R}$ led us to deduce that, in fact, $\mathcal{R} \notin \mathcal{R}$. Surely, these contradictory facts cannot both hold simultaneously. Accordingly, it must be that our original assumption was bad, so it must be the case that $\mathcal{R} \notin \mathcal{R}$, instead.

- Now, suppose $\mathcal{R} \notin \mathcal{R}$ is True.

  The defining property of $\mathcal{R}$ tells us that any object that is *not* an element of $\mathcal{R}$ must be an element of itself. (Otherwise, it would have been included as an element of $\mathcal{R}$.) Thus, we can deduce that $\mathcal{R} \in \mathcal{R}$.

  Wait a minute! Knowing that $\mathcal{R} \in \mathcal{R}$ led us to deduce that, in fact, $\mathcal{R} \notin \mathcal{R}$. This is also contradictory.

No matter which option we choose—$\mathcal{R} \in \mathcal{R}$ or $\mathcal{R} \notin \mathcal{R}$—we find that the other must also be true, but certainly these contradictory options cannot both be true.

Therein lies the **paradox**. This is not a properly-defined set. If it were, we would find ourselves stuck in the two cases we just saw, and neither of them can be true. It is also not the case that $\mathcal{R}$ is simply $\varnothing$; no, it must be that $\mathcal{R}$ *does not exist* as a set.

The "Set of all Sets" is *Not* a Set

Could we amend the definition of $\mathcal{R}$ somehow to produce the "set" that the definition is trying to convey? What "larger set" should we draw our objects x from so that the definition makes sense and properly identifies a set?

Look back at the English-language interpretation we wrote after the definition: "the elements of $\mathcal{R}$ are sets that also happen to *not* have themselves as elements." The objects x that we wish to test for the desired property ($x \notin x$) are really *all* sets. Perhaps, then, we should just define X to be the set of all sets, and use the phrase "$x \in X$" as part of our definition of $\mathcal{R}$. That would fix it, right?

$$\mathcal{R} = \{x \in X \mid x \notin x\}$$

Well, no, not at all! **The "set of all sets" is, itself, *not* a set**. If it were, this would lead us to exactly the same paradox as before! Nothing would be different, except we would have explicitly stated the "larger set" from which we draw objects x that was previously left *implicitly*-specified.

The main issue is that not specifying a "larger set" from which to draw objects, or implicitly referring to the "set of all sets", results in this type of undesirable paradox. Accordigly, we must not allow such definitions. Any attempt to define a set that draws objects x from the "set of all sets", whether implicitly or explicitly, is not a *proper definition* of a set.

Further Discussion

There is nothing inherently wrong with the property $P(x)$ given by "$x \notin x$", though. The issue is with that "larger set" we use. For instance, take the set

$$\mathcal{S} = \left\{ x \in \left\{ \frac{1}{2}, \frac{3}{4}, \frac{5}{2} \right\} \,\middle|\, x \notin x \right\}$$

What are its elements? The only possibilities are those elements drawn from the larger set $\left\{\frac{1}{2}, \frac{3}{4}, \frac{5}{2}\right\}$. Notice that none of those numbers are sets that contain themselves as elements. Thus, this is a proper definition of the set $\left\{\frac{1}{2}, \frac{3}{4}, \frac{5}{2}\right\}$, itself! With the previous definition for $\mathcal{R}$, the object we were attempting to define was allowed as one of the variable objects x in its own definition, and that is where the issue arose.

We hope that we haven't led your thoughts too far astray from the original discussion of examples of sets, but we felt it was important to point out that it is possible to construct ill-defined "collections" that are not sets in the mathematical sense of the word. For the most part, we will not face any such issues with the sets we work with in this book, but to gloss over these issues or simply not mention them at all would be unfair to you, as a student. If you find yourself interested in these issues, seek out an introductory book on set theory.

There are other ways that definitions of "sets" can be ill-formed, as well, but the ensuing examples are based on (English) linguistic issues and not any mathematical underpinnings, as in Russell's Paradox. For instance, we could say "Let N be the set of all classic novels from the 20th century." Being a "classic novel" is *not* a well-defined property, and cannot be used to identify elements of such a set. The notion of a "classic" is subjective and not rigorously precise. Also, we could say "Let B be the set of people who will be born tomorrow" but this temporal dependence in the definition ensures that we will never actually know what the elements of B are. When tomorrow arrives, the definition will then refer to the next day, and so on. Can you come up with some other examples of ill-formed "collections" of elements? Can you come up with any paradoxes like the one above?

In general, the following statement is the most important idea to take away from this discussion of Russel's Paradox:

> Under the agreed-upon rules of sets (the axioms of set theory), there is **no** set of all sets.

3.3.6 Standard Sets and Their Notation

We have referred to and used some common sets of numbers already, so we will list now some sets and their standard symbols:

- The *natural numbers*: $\mathbb{N} = \{1, 2, 3, 4, \dots\}$
- The first n natural numbers: $[n] := \{1, 2, 3, \dots, n-1, n\}$
- The *integers*: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- The *rational numbers*: $\mathbb{Q} = \left\{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ and } n \neq 0\right\}$
- The *real numbers*: $\mathbb{R}$
- The *complex numbers*: $\mathbb{C}$

We have used $\mathbb{N}$ and $\mathbb{Z}$ a few times already. The rational numbers $\mathbb{Q}$ (we use $\mathbb{Q}$ since $\mathbb{R}$ was already taken, and rational numbers are *quotients*) are all of the *fractions*, or ratios of integers, both positive and negative. The real numbers are harder to describe. Why could we not list a few elements, like we did with $\mathbb{N}$ and $\mathbb{Z}$? Why is it that $\mathbb{R} \neq \mathbb{Q}$? For now, we essentially take for granted our collective knowledge of these sets of numbers, but think for a minute about that. (We mention the complex numbers $\mathbb{C}$ because you might be familiar with them, but we will not have occasion to use them in this book.)

How do we *know* that a set like $\mathbb{N}$ exists? Why is it that we think of $\mathbb{R}$ as a number line? How many "more" elements are there in $\mathbb{Z}$, as compared to $\mathbb{N}$? How many "more" elements are there in $\mathbb{R}$, as compared to $\mathbb{Q}$? Can we even answer these questions? In the very near future, we will rigorously derive the set $\mathbb{N}$ and prove that it exists as the only set with a particular property. This will be essential when we return to our investigation of mathematical induction. (Remember our goals from that chapter?)

3.3.7 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What does the symbol "$\in$" mean?

(2) How would you read the statement "$x \in S$" out loud?

(3) Is it possible for a set to be an element of another set? If so, give an example. Is it possible for a set to be an element of itself?

(4) How would read the statement "$\{x \in \mathbb{N} \mid x \leq 5\}$" out loud? Can you list the elements of this set?

(5) What is this set: $\{z \in \mathbb{Z} \mid z \in \mathbb{N}\}$?

(6) What is this set: $\{x \in [10] \mid x \geq 7\}$?

(7) For each of the following sets, state *how many* elements they have:

(a) $\varnothing$
(b) $\{1, 2, 10\}$
(c) $\{1, \varnothing\}$
(d) $\{\,\varnothing\,\}$

(8) Is $x \in \{\,1, 2, \{x\}\,\}$? Is $\{x\} \in \{\,1, 2, \{x\}\,\}$?

(9) Let $A = \{a, b, c\}$ and $B = \{b, c, a\}$ and $C = \{a, a, b, c, a, b\}$. Are these sets equal or not?

(10) Is $\mathbb{Z} = \mathbb{Q}$? Why or why not?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Write a definition of the set of natural numbers that are multiples of 4 using set-builder notation.

(2) Consider the set $S = \{3, 4, 5, 6\}$. Define S in two different ways using set-builder notation.

(3) Give an example of a set X that satisfies $\mathbb{N} \in X$ but $\mathbb{Z} \notin X$.

(4) Give an example of a set with 100 elements.

(5) Give an example of a sets A, B, C such that $A \in B$ and $B \in C$ but $A \notin C$.

(6) Write a definition of the set of *odd integers* using set-builder notation.

(7) Write a definition of the set of integers that are not natural numbers using set-builder notation.

(8) Consider the following sets:

$$A = \left\{x \in \mathbb{R} \mid x^2 - 3x + 2 \geq 0\right\}$$
$$B = \{y \in \mathbb{R} \mid y \leq 1 \text{ or } y \geq 2\}$$

Explain why $A = B$.

(9) Consider the following sets:

$$C = \left\{x \in \mathbb{R} \mid x^2 - 4 \geq 0\right\}$$
$$D = \{y \in \mathbb{R} \mid y \geq 2\}$$

Is $C = D$? Why or why not? Write your explanation with good mathematical notation, using $\in$ and $\notin$.

(10) Try explaining Russell's Paradox to a friend, even one who does not study mathematics. What do they understand about it? Do they object? Do their ideas make sense? Have a discussion!

3.4 Subsets

3.4.1 Definition and Examples

Let's discuss a topic whose basic idea we have already been using. Specifically, let's investigate the notion of **subsets**.

Definition 3.4.1. *Given two sets A and B, if every element of A is also an element of B, then we say A is a* **subset** *of B.*

The mathematical symbol for subset is $\subseteq$, so we would write $A \subseteq B$.

If we want to indicate that A is a subset of B but is also not equal *to B, we would write $A \subset B$ and say that A is a* **proper subset** *of B.*

We can also write these relationships as $B \supseteq A$, or $B \supset A$, respectively. In these cases, we would say B is a **superset** *of A or B is a* **proper superset** *of A, respectively.*

Notice the similarities between these symbols and the *inequality* symbols we use to compare real numbers. We write inequalities like $x \leq 2$ or $5 > z > 0$ and understand what those mean based on the "direction" of the symbol and whether we put a bar underneath it. The symbols $\subseteq, \subset, \supseteq, \supset$ work exactly the same way, except they refer to "containment of elements" as opposed to "magnitude of a number".

Standard Sets of Numbers

The standard sets of numbers we mentioned in the last section are related via the subset relation quite nicely. Specifically, we can say

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Again, we take for granted our collective knowledge of these sets of numbers to allow us to make these claims. However, there are some profound and intricate mathematical concepts involved in describing exactly why, say, the set $\mathbb{R}$ exists and is a proper superset of $\mathbb{Q}$. For now, though, we use these sets to illustrate the **subset** relationship.

Since we know the subset relationships above are **proper**, we used that corresponding symbol, "$\subset$". In general, it is common in mathematical writing to simply use the "$\subseteq$" symbol, even if it is known that "$\subset$" would apply. We might only resort to using the "$\subset$" symbol when it is important, in context, to indicate that the two sets are *not equal*. If that information is not essential to the context at hand, then we might just use the "$\subseteq$" symbol.

Set-Builder Notation Creates Subsets

One way that we have already "used" the idea of a subset was in our use of set-builder notation. This is used to define a set to be all of the elements of a "larger" set that satisfy a certain property. We define a property $P(x)$, draw a variable object x from a larger set X, and include any elements x that satisfy the property $P(x)$. Notice that any element of this new set must be an element of X, simply based on the way we defined it. Thus, the following relationship holds

$$\{x \in X \mid P(x)\} \subseteq X$$

regardless of the set X and the property $P(x)$. Depending on the set X and the property $P(x)$, it may be that the proper subset symbol $\subset$ applies but, in general, we can say for sure that $\subseteq$ applies.

Try to come up with some examples of sets X and properties $P(x)$ so that $\subseteq$ applies, then try to come up with some examples where $\subset$ applies. Try to come up with one set X and two different properties $P_1(x)$ and $P_2(x)$ so that $\subset$ applies for $P_1(x)$ and $\subseteq$ applies for $P_2(x)$. Try to identify two *different* sets X_1 and X_2 and two *different* properties $P_1(x)$ and $P_2(x)$ so that

$$\{x \in X_1 \mid P_1(x)\} = \{x \in X_2 \mid P_2(x)\}$$

Can you do it?

Examples

A set is a subset of another set if and only if every element of the first one is an element of the second one. For instance, this means that the following claims all hold:

$$\begin{aligned} \{142, 857\} &\subseteq \mathbb{N} \\ \left\{\sqrt{3}, -\pi, 8.2\right\} &\subseteq \mathbb{R} \\ \left\{x \in \mathbb{R} \mid x^2 = 1\right\} &\subseteq \mathbb{Z} \end{aligned}$$

Do you see why these are True?

For a subset relationship to fail, then, we must be able to find an element of the first set that is *not* an element of the second set. For instance, this means that the following claims all hold:

$$\begin{aligned} \{142, -857\} &\not\subseteq \mathbb{N} \\ \left\{\sqrt{3}, -\pi, 8.2\right\} &\not\subseteq \mathbb{Q} \\ \left\{x \in \mathbb{R} \mid x^2 = 5\right\} &\not\subseteq \mathbb{Z} \end{aligned}$$

Finding All Subsets of a Set

Let's work with a specific set for a little while. Define $A = \{1, 2, 3\}$. Can we identify *all* of the subsets of A? Sure, why not?

$$\begin{aligned} \{1\} &\subseteq A \\ \{2\} &\subseteq A \\ \{3\} &\subseteq A \\ \{1, 2\} &\subseteq A \\ \{1, 3\} &\subseteq A \\ \{2, 3\} &\subseteq A \\ A = \{1, 2, 3\} &\subseteq A \\ \varnothing &\subseteq A \end{aligned}$$

Identifying the first six subsets was fairly straightforward, but it's important to remember that A and $\varnothing$ are subsets, as well. (Notice: it is true, in general, that for any set S, $S \subseteq S$ and $\varnothing \subseteq S$. Think about this!)

Consider the set B whose elements are all of the sets we listed above:

$$B = \left\{ \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A, \varnothing \right\}$$

It is true that any element $X \in B$ satisfies $X \subseteq A$. Do you see why?

3.4.2 The Power Set

This process of identifying all subsets of a given set is common and useful, so we identify the resulting set with a special name.

Definition 3.4.2. *Given a set A, the* **power set** *of A is defined to be the set whose elements are all of the subsets of A. It is denoted by $\mathcal{P}(A)$.*

Our parenthetical observation from the above paragraph tells us that $S \in \mathcal{P}(S)$ and $\varnothing \in \mathcal{P}(S)$, for any set S.

Look back at our example set $A = \{1, 2, 3\}$ above. What do you notice about the number of elements in $\mathcal{P}(A)$? How does it relate to the number of elements in A? Do you think there is a general relationship between the number of elements in S and $\mathcal{P}(S)$, for an arbitrary set S?

Example 3.4.3. Let's find $\mathcal{P}(\varnothing)$. What are the subsets of the empty set? There is only one, the empty set itself! (That is, $\varnothing \subseteq \varnothing$, but no other set satisfies this.) Accordingly, the power set $\mathcal{P}(\varnothing)$ has one element, the empty set:

$$\mathcal{P}(\varnothing) = \{\, \varnothing \,\}$$

Notice that this is *different* from the empty set itself:

$$\varnothing \neq \{\, \varnothing \,\}$$

Why is this true? Compare the elements! The empty set has *no* elements, but the set on the right has exactly *one* element. (In general, this can be a helpful way to compare two sets.) To give you some practice, we'll point out that would read the above line aloud as:

> "The empty set and the set containing the empty set are two different sets."

Example 3.4.4. Let's try this process with another set, say $A = \{\, \varnothing, \{1, \varnothing\} \,\}$. We can list the elements of $\mathcal{P}(A)$ as

$$\mathcal{P}(A) = \{\, \{\varnothing\} \,, \{\{1, \varnothing\}\} \,, \{\varnothing, \{1, \varnothing\}\} \,, \varnothing \,, \}$$

This may look strange, with all of the empty sets and curly braces, but it is important to keep the subset relationships straight. It is true, in this example, that

$$\varnothing \in A, \quad \{\varnothing\} \subseteq A, \quad \{\varnothing\} \in \mathcal{P}(A), \quad \{\varnothing\} \subseteq \mathcal{P}(A)$$

Why are these relationships true? Think carefully about them, and try to write a few more on your own. The distinction between "$\in$" and "$\subseteq$" is very important!

3.4.3 Set Equality

When are two sets equal? The main idea is that two sets are equal if they contain "the same elements", but this is not a precise definition of equality. How can we describe that property more explicitly and rigorously? To say that two sets, A and B, have "the same elements" means that any element of A is also an element of B, and every element of B is also an element of A. If both of these properties hold, then we can be guaranteed that the two sets contain precisely the same elements and are, thus, equal. If you think about it, you'll notice that we can phrase this in terms of **subsets**. How convenient!

Definition 3.4.5. *We say two sets, A and B, are* **equal***, and write $A = B$, if and only if $A \subseteq B$ and $B \subseteq A$.*

(What happens if we use the $\subset$ symbol in the definition, instead of $\subseteq$? Is this the same notion of set equality? Why or why not?)

This definition will be very useful in the future when we learn how to *prove* two sets are equal and we can't simply list the elements of each and compare them. By constructing two arguments and proving the subset relationship in "both directions", we can show that two sets are equal. For now, let's see this definition applied to a straightforward example.

Example 3.4.6. How can we use this to definition to observe that the following equality holds?

$$\{x \in \mathbb{Z} \mid x \geq 1\} = \mathbb{N}$$

We just need to see that the $\subseteq$ and $\supseteq$ relationship applies between the two sides. First, is it true that every integer that is at least 1 is a natural number? Yes! This explains why

$$\{x \in \mathbb{Z} \mid x \geq 1\} \subseteq \mathbb{N}$$

Second, is it true that every natural number is a positive integer that is at least 1? Yes! This explains why

$$\{x \in \mathbb{Z} \mid x \geq 1\} \supseteq \mathbb{N}$$

Together, this shows that the equality stated above is correct.

3.4.4 The "Bag" Analogy

It has been our experience that **sets** are a rather difficult notion to grasp when they are introduced. Specifically, the **notation** associated with sets throws students for a loop, and they end up writing down things that make no sense! It is essential to keep straight the differences between the symbols $\in$ and $\subseteq$.

Here is a helpful analogy to keep in mind: a set is like a **bag** with some stuff in it. The bag itself is irrelevant; we just care about what *kind* of stuff inside (i.e. what the elements are). Think of the bag as a non-descript plastic bag you'd get at the grocery store, even. All those bags are identical; to distinguish between any two bags, we need to know what kind of things are *inside* them.

If I put an apple and an orange in a grocery bag, surely it doesn't matter in what *order* I put them in. All you would need to know is that I have some apples and oranges. It also doesn't matter how *many* apples or oranges I have in the bag, because we only care about what *kind* of stuff is in there. Think of it as answering questions of the form "Are there any ______s in the bag? Yes or no?" It doesn't matter if I have two identical apples or seven or just one in my bag; if you ask me whether I have *any* apples, I'll just say "Yes". This is related to the notion that the order and repetition of elements in a set don't matter. A set is completely characterized by what its elements are.

This also helps when we think about sets as elements of other sets, themselves. Who's to stop me from just putting a whole bag inside another bag¿ Look at the set A we defined in the example above:

$$A = \{\ \varnothing\ ,\ \{1, \varnothing\}\ \}$$

This set A is a bag. What's inside the bag? There are two objects inside the bag (i.e. there are two elements of A). They both happen to be bags, themselves! One of them is a plain-old empty bag, with nothing inside it. (That's the empty set.) Okay, that's cool. The other one has two objects inside it. One of those objects is the number 1. Cool. The other such object is another empty bag.

Distinguishing "$\in$" and "$\subseteq$"

This analogy also helps with understanding the differences between "$\in$" and "$\subseteq$". Keep the example A in mind again. When we write $x \in A$, we mean x is an object inside the bag A. If we peeked into A, we would see an x sitting there at the bottom amongst the stuff. Let's use this idea to compare two examples.

- We see that $\varnothing \in A$ is true here. If we look inside the bag A, we see an empty bag amongst the stuff (the elements).

- We also see that $\{\varnothing\} \notin A$ is true here. If we look inside the bag A, we don't see a bag containing *only* an empty bag. (This is what $\{\varnothing\}$ is, mind you: an empty bag inside another bag.)

  Do you see such an object? Where? I defy you to show me, amongst the stuff inside the bag A, a bag containing *only* an empty bag.

  What do I see inside the bag A? Well, I see two things: an empty bag, and a bag that has *two* objects inside it (an empty bag, and the number 1). Neither of those objects is what we were looking for!

When we write $X \subseteq A$, we mean that the two bags, X and A, are somehow comparable. Specifically, we are saying that all of the stuff inside X is also stuff inside A. We are really rooting through all of the objects inside X, taking them out one by one, and making sure we also see that object inside A. Let's use this idea to compare two examples.

- We see that $\{\varnothing\} \subseteq A$ is true here. We are *comparing* the bag on the left with the bag on the right. What stuff is inside the bag on the left?

There's just one object in there, and it is an empty bag, itself. Now, we peek inside A. Do we also see an empty bag in there? Yes we do! Thus, the "$\subseteq$" symbol applies here.

- We also see that $\{1\} \not\subseteq A$ is true here. To compare these two bags, we'll pull out an object from the bag on the left and see if it is also in the bag A. Here, we only have one object to pull out: the number 1. Now, let's peek inside the bag A. Do we see a 1 sitting in there amongst the stuff? No, we don't!

  We would have to peek *inside* something at the bottom of the bag A to find the number 1; that number isn't just sitting out in plain sight. Thus, $\{1\} \not\subseteq A$.

Look back over some examples we have discussed already with this new analogy in mind. Does it help you understand the definitions and examples? Does it help you understand the difference between "$\in$" and "$\subseteq$" and "$\supseteq$"? If not, can you think of another analogy that would help you?

3.4.5 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) Is $\mathbb{N} \subseteq \mathbb{R}$? Is $\mathbb{R} \subseteq \mathbb{N}$? Is $\mathbb{Q} \subseteq \mathbb{Z}$? Why or why not?

(2) What is the difference between $\subset$ and $\subseteq$? Give an example of sets A, B such that $A \subseteq B$ is True but $A \subset B$ is False.

(3) What is the difference between $\in$ and $\subseteq$? Give an example of sets C, D such that $C \subseteq D$ but $C \notin D$.

(4) Let S be any set. What is the **power set** of S? What type of mathematical object is it? How is it defined?

(5) Suppose $S \subseteq T$. Does this mean $S = T$? Why or why not?

(6) Explain why $\varnothing \subseteq S$ and $\varnothing \in \mathcal{P}(S)$ for any set S.

(7) Suppose $X \in \mathcal{P}(A)$. How are X and A related, then?

(8) Is it possible for $A = \mathcal{P}(A)$ to be true? (This one is rather tricky, but think about it!)

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Write out the elements of the set $\mathcal{P}(\mathcal{P}(\varnothing))$.

(2) Write out the elements of the sets $\mathcal{P}([1])$ and $\mathcal{P}([2])$ and $\mathcal{P}([3])$. Can you make a conjecture about how many elements $\mathcal{P}([n])$ has? (Can you prove it? We don't expect you to *now*, but soon enough; think about it!)

(3) Let $A = \{x, \heartsuit, \{4\}, \varnothing\}$. For each of the following statements, decide whether it is True or False and briefly explain why.

(a) $x \in A$
(b) $x \subseteq A$
(c) $\{x, \heartsuit\} \subseteq A$
(d) $\{x, \varnothing\} \subset A$
(e) $\{x, \heartsuit, z, 7\} \supseteq A$
(f) $\{x\} \in \mathcal{P}(A)$
(g) $\{x\} \subseteq \mathcal{P}(A)$
(h) $\{\heartsuit, x\} \in \mathcal{P}(A)$
(i) $\{4\} \in \mathcal{P}(A)$
(j) $\{\varnothing\} \in \mathcal{P}(A)$
(k) $\{\varnothing\} \subseteq \mathcal{P}(A)$

Hint: 7 of these are True, and 4 are False.

(4) Give an example of sets A, B such that $A \in B$ and $A \subseteq B$ are both true.

(5) Is $\{1, 2, 12\} \subseteq \mathbb{R}$?

(6) Is $\{-5, 8, 12\} \subseteq \mathbb{N}$?

(7) Is $\{1, 3, 7\} \in \mathcal{P}(\mathbb{N})$?

(8) Is $\mathbb{N} \in \mathcal{P}(\mathbb{Z})$?

(9) Is $\mathcal{P}(\mathbb{N}) \subseteq \mathcal{P}(\mathbb{Z})$? Are they equal sets? Why or why not?

(10) Give an example of an infinite set T such that $T \in \mathcal{P}(\mathbb{Z})$ but $T \notin \mathcal{P}(\mathbb{N})$.

(11) Suppose G, H are sets and they satisfy $\mathcal{P}(G) = \mathcal{P}(H)$. Can we conclude that $G = H$? Why or why not? (Don't try to formally prove this; just think about it and try to talk it out.)

(12) Give an example of a set W such that $W \subseteq \mathcal{P}(\mathbb{N})$ but $W \notin \mathcal{P}(\mathbb{N})$.

3.5 Set Operations

When you first learned about numbers, a natural next step was to learn about how to *combine* them: multiplication, addition, and so on. Thus, a natural next step for us now is to investigate how we can take two sets and *operate* on them to produce other sets. How can we *combine* sets in interesting ways? There are several such operations that have standard, notational symbols and we will introduce you to those operations now.

Throughout this section, we assume that we are given two sets A and B that are each subsets of a larger **universal set** U. That is, we assume $A \subseteq U$ and $B \subseteq U$. The reason we make this assumption is that each operation involves defining another set by identifying elements of a larger set with a specific property, so we must have some set U that is guaranteed to contain all of the elements of A and B so we can even work with those elements. (Again, ensuring this may seem nit-picky, but it is meant to avoid nasty paradoxes like the one we investigated before.) Assuming those sets A, B, U exist, though, we can forge ahead with our definitions.

3.5.1 Intersection

This operation collects the elements common to two sets and includes them in a new set, called the **intersection**.

Definition 3.5.1. *Let A and B be any sets. The* **intersection** *of A and B is the set of elements that belong to both A* and *B, and is denoted by $A \cap B$. Symbolically, we define*

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$

Example 3.5.2. Define the following sets:

$$\begin{aligned} S_1 &= \{1, 2, 3, 4, 5\} \\ S_2 &= \{1, 3, 7\} \\ S_3 &= \{2, 4, 7\} \\ U &= \mathbb{N} \end{aligned}$$

Then, we see that, for example,

$$\begin{aligned} S_1 \cap S_2 &= \{1, 3\} \\ S_1 \cap S_3 &= \{2, 4\} \\ S_2 \cap S_3 &= \{7\} \end{aligned}$$

Also, since $S_1 \cap S_2$ is, itself, a set, it makes sense to consider $(S_1 \cap S_2) \cap S_3$. However, those two sets share no elements, so we write

$$(S_1 \cap S_2) \cap S_3 = \varnothing$$

The situation where two sets have no common elements, as seen in the above example, is common enough that we have a specific term to describe such sets:

Definition 3.5.3. *If $A \cap B = \varnothing$, then we say A and B are* **disjoint**.

Intersections and Subsets

You might have observed already that we can say $A \cap B \subseteq A$ and $A \cap B \subseteq B$, no matter what A and B are. Let's prove this fact!

Proposition 3.5.4. *Let A and B be any sets. Then,*

$$A \cap B \subseteq A$$

and

$$A \cap B \subseteq B$$

By the way, a **proposition** like this is just a "mini result". It's not difficult or important enough to be called a theorem, but it does require a little proof.

Proof. Let's say we have two sets, A and B. To prove a subset relationship, like $A \cap B \subseteq A$, we need to show that every **element** of the set on the left ($A \cap B$) is also an element of the set on the right (A).

Let's consider an arbitrary element $x \in A \cap B$. By the definition of $A \cap B$, we know that $x \in A$ and $x \in B$. Thus, we know that $x \in A$. This was our goal, so we have shown that $A \cap B \subseteq A$.

Also, we know that $x \in B$, so we have also shown that $A \cap B \subseteq B$. □

This might seem like a simple observation and an easy proof, but we still need to go through these logical steps to rigorously explain why those subset relationships hold true. Also, notice the type of **proof structure** we used here. To prove a subset relationship holds true, we need to consider an **arbitrary element** of one set and deduce that it is also an element of the other set. This will be our method for proving any claim about subsets.

What if $A \subseteq B$? What can we say about $A \cap B$, in relation to A and B? Try to prove a statement about this!

3.5.2 Union

This operation collects the elements of either of two sets and includes them in a new set, called the **union**.

Definition 3.5.5. *Let A and B be any sets. The* **union** *of A and B is the set of elements that belong to either A* or *B, and is denoted by $A \cup B$. Symbolically, we define*

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$

Notice that the "or" in the definition is an *inclusive* "or", meaning that $A \cup B$ includes any element that belongs to A or B or possibly both sets.

Example 3.5.6. Returning to the sets S_1, S_2, S_3 we defined above in Example 3.5.2, we can say

$$S_1 \cup S_2 = \{1, 2, 3, 4, 5, 7\}$$
$$S_1 \cup S_3 = \{1, 2, 3, 4, 5, 7\}$$
$$S_2 \cup S_3 = \{1, 2, 3, 4, 7\}$$

Also, since each of these unions are sets themselves, we could find their union with another set. For example,

$$(S_1 \cup S_2) \cup S_3 = \{1, 2, 3, 4, 5, 7\} \cup \{2, 4, 7\} = \{1, 2, 3, 4, 5, 7\}$$

Unions and Subsets

Notice that $A \subseteq (A \cup B)$ and $B \subseteq (A \cup B)$, no matter what A and B are. Let's prove that!

Proposition 3.5.7. *Let A and B be any sets. Then,*

$$A \subseteq (A \cup B)$$

and

$$B \subseteq (A \cup B)$$

Proof. Let's say we have two sets, A and B. To prove $A \subseteq (A \cup B)$, we need to show that every element of A is also an element of $A \cup B$.

Let $x \in A$ be arbitrary and fixed. Then it is certainly that $x \in A$ or $x \in B$ (since $x \in A$). This shows $x \in A \cup B$. Since x was arbitrary, we have shown $A \subseteq A \cup B$.

Let $y \in B$ be arbitrary and fixed. Then it is certainly true that $y \in A$ or $y \in B$ (since we already know $y \in B$). This shows $y \in A \cup B$. Since y was arbitrary, we have shown $B \subseteq A \cup B$. $\square$

What can you say about the relationship between $A \cap B$ and $A \cup B$? If $A \subseteq B$, can we say anything about the relationship between B and $A \cup B$? Try to prove your observations!

We should emphasize that claims like this—that $A \subseteq A \cup B$ for any sets A and B—need to be proven; they do not hold **by definition**. The definition of the union of two sets is given above. Notice it says nothing about how A and $A \cup B$ are related; it just tells us what the object $A \cup B$ actually is. When you invoke or cite a definition and use it, be sure to do so; but also, be sure to explain any claim that isn't exactly a definition. Since we have proven these two little lemmas, we get to use them in the future by referencing them; had we not done so, we would have to re-explain these little facts every time we try to invoke them!

3.5.3 Difference

This operation takes the elements of one set and removes the elements that also belong to another set.

Definition 3.5.8. *The* **difference** *between A and B, denoted by $A - B$, is the set of all elements of A that are* not *elements of B. Symbolically, we define*

$$A - B := \{x \in U \mid x \in A \text{ and } x \notin B\}$$

Example 3.5.9. Returning to the sets S_1, S_2, S_3 we defined above in Example 3.5.2, we can say, for example, that

$$\begin{aligned} S_1 - S_2 &= \{2, 4, 5\} \\ S_2 - S_1 &= \{7\} \\ S_2 - S_3 &= \{1, 3\} \end{aligned}$$

Set Difference Is *Not* Symmetric

Notice that $S_1 - S_2 \neq S_2 - S_1$ in the example above. In general, the operation "$-$", in the context of sets, is not **symmetric**, and this example here shows that. Can you find two sets A, B so that $A - B = B - A$? Can you find two sets A, B so that $A - B = B - A \neq \varnothing$?

Each of the other operations we have defined thus far is, in fact, symmetric. That is, $A \cap B = B \cap A$ and $A \cup B = B \cup A$. Look back at the definitions for these operations and see why this makes sense. What is it about the *language* used in the property definition of the operation that makes this true?

Notation Notes

One more comment on this set difference notation. Notice that we use the standard subtraction symbol, "$-$", but this has nothing to do with "subtraction" in the way we usually think of it, like with numbers. This might be the first time you've encountered this ambiguity, or perhaps not, but there is a larger point that is relevant to mathematical notation and terminology: many symbols have different meanings depending on the *context*.

When we write $7 - 5$, we clearly mean subtraction, i.e. $7 - 5 = 2$. However, when we write $A - A$ where A has been identified as a *set*, we mean the set difference operation, i.e. $A - A = \varnothing$. Be sure to check the context of any statement to ensure that the symbols therein do mean what you think they mean!

3.5.4 Complement

This operation identifies all of the elements that lie "outside" a set. This operation depends on the context of the universal set U. You'll notice that this is evident in the deifnition, and we will illustrate this through examples, as well.

Definition 3.5.10. *The* **complement** *of A is the set of all elements that are* not *elements of A, and is denoted by $\bar{A}$. Symbolically, we define*

$$\bar{A} = \{x \in U \mid x \notin A\}$$

Remember that we assumed A, B, U are given sets that satisfy $A \subseteq U$ and $B \subseteq U$. Within this context, the set $\bar{A}$ is well-defined, but this set certainly depends on A and U!

Example 3.5.11. For instance, let's return to the sets S_1, S_2, S_3 we defined above in Example 3.5.2. There, we used the context $U = \mathbb{Z}$. In that case,

$$\bar{S}_1 = \{6, 7, 8, 9, \dots\}$$

However, what if we had used $U = \{1, 2, 3, 4, 5, 6, 7\}$? In that case,

$$\bar{S}_1 = \{6, 7\}$$

Since the symbolic notation $\bar{A}$ makes no indication of the set U that it depends on, it is important to make this set clear in whatever context we are working. Try identifying some sets A, U_1, U_2 so that $\bar{A}$ in U_1 is different from $\bar{A}$ in U_2, and try identifying some sets so that $\bar{A}$ is the same in both cases.

3.5.5 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What is the difference between a union and intersection of two sets?

(2) What does it mean for two sets to be disjoint?

(3) What is $\mathbb{Z} \cap \mathbb{N}$? What is $\mathbb{Z} \cup \mathbb{N}$? What is $\mathbb{Z} - \mathbb{N}$?

(4) Is it possible for $A - B = B - A$ to be true? How?

(5) What is $\overline{[3]}$ in the context of $\mathbb{N}$? What about in the context of $\mathbb{Z}$? Of $\mathbb{R}$? Try writing your answers using good mathematical notation, and set-buidler notation, perhaps.

(6) Is $(A \cap B) \cap C = (A \cap B) \cap C$ always true? Why or why not? What about with $\cup$ instead of $\cap$?

(7) What is the difference between the statements "$7 - 5$" and "$[7] - [5]$"?

(8) Suppose $x \in A$. Does $A - x$ make sense, notationally? How can you change it to make sense?

(9) What is $(\mathbb{Z} - \mathbb{N}) \cup \mathbb{R}$?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) List the elements of the following sets:

  (a) $[7] \cup [10]$
  (b) $[10] \cap [7]$
  (c) $[10] - [7]$
  (d) $([12] - [3]) \cap [8]$
  (e) $(\mathbb{N} - [3]) \cap [7]$
  (f) $(\mathbb{Z} - \mathbb{N}) \cap \mathbb{N}$
  (g) $\overline{\mathbb{N}} \cap \{0\}$, in the context of $\mathbb{Z}$

(2) Find an example of sets A, B, C such that $(A - B) - C = A - (B - C)$. Then, find an example where they are **not** equal.

(3) State and prove a relationship between $\overline{A}$ and $U - A$.

(4) Let $A = [12]$, let E be the set of even integers, and let P be the set of prime natural numbers. What is $A \cap E$? What is $A \cap P$? What is $(A \cap E) \cap P$? Is it the same as $A \cap (E \cap P)$?

  Suppose the context is $U = \mathbb{N}$. What are $\overline{A \cap E}$ and $\overline{A} \cap \overline{E}$?

(5) What is $\{1\} \cap \mathcal{P}(\{1\})$?

(6) Consider the sets $\{1\}$ and $\{2, 3\}$. Compare the sets $\mathcal{P}(\{1\} \cup \{2, 3\})$ and $\mathcal{P}(\{1\}) \cup \mathcal{P}(\{2, 3\})$. What do you notice?

  Repeat this exercise with "$\cap$" instead of "$\cup$". What do you notice?

(7) Let A, U be sets, and suppose $A \subseteq U$. Let $B = \overline{A}$, in the context of U. What do you think $\overline{B}$ is? Why?

3.6 Indexed Sets

3.6.1 Motivation

Let's discuss a notion that we referenced briefly before and have been using already: the concept of **indexing** a collection of sets. This type of notation is convenient when we wish to define or refer to a large number of sets without writing out all of them explicitly. Using similar notation with the set operations we have defined already, we will be able to "combine" and "operate on" a large number of sets "all at once". There is really no new mathematical content in this section, but the notation involved in these ideas can be confusing and difficult to work with, at first, so we want to guide you through these ideas carefully.

Relation to Summation Notation

We'll start with a related concept that we have seen before. Remember when we investigated sums of natural numbers in Chapter 1? We mentioned some special notation that allowed us to condense a long string of terms in a sum into one concise form, using the $\sum$ symbol. For instance, we could write an informal sum ("informal" meaning "not rigorous" because of the use of ellipses) in the $\sum$ notation as follows:

$$1 + 2 + 3 + 4 + \cdots + (n-1) + n = \sum_{i=1}^{n} i$$

Why does this notation work and make sense? The **index variable** i is the key component of condensing the sum into this form. Writing "$i = 1$" underneath the $\sum$ symbol means that the value of the variable i should start at 1 and increase by 1 until it reaches the terminal value, n, written above the $\sum$ symbol. For each allowable value of i in that range (from 1 to n), we include a term in the sum of the form written to the right of the $\sum$ symbol; in this case, that term is i. Thus, we should have the terms $1, 2, 3, \dots, n$ with a $+$ sign between each.

We should point out that it is implicitly understood that writing $i = 1$ and n as the **limits** on the index variable i means i assumes all values that are natural numbers between 1 and n.

Example

Let's see the process of defining indexed sets via an example first. We will also see how to apply set operations to several sets by using an index variable.

Example 3.6.1. We can similarly condense some set operation notation. For instance, let's define the sets $A_1, A_2, A_3, \dots, A_{10}$ by

$$\begin{aligned} A_1 &= \{1, 2\} \\ A_2 &= \{2, 4\} \\ A_3 &= \{3, 6\} \\ &\vdots \\ A_i &= \{i, 2i\} \\ &\vdots \\ A_{10} &= \{10, 20\} \end{aligned}$$

We included the definition of A_i for an *arbitrary* value i to give these sets a rigorous definition. Without defininining that set—which defines A_i for any relevant value of i—we would be leaving it up to the reader to interpret the pattern among the sets A_1, A_2, A_3, A_{10}, and there could be multiple ways of interpreting that. By defining the term A_i explicitly like this, there is no confusion as to what we want these ten sets to be.

Furthermore, we can more easily express the union of all of these sets, for instance. Remember that the union of two sets is the set containing all elements of both sets (i.e. an element is included in the union if it is in the first set *or* the second set, or possibly both). What is the union of more than two sets? It follows the same idea as the definition for just two sets; we want to include an element in the union if it is in *any* of the constituent sets we are combining via the union operation.

How can we write this union concisely and precisely? Let's follow the same motivation of the $\sum$ notation. The index of these sets runs from 1 to 10, so we should write $i = 1$ below a "$\cup$" symbol and 10 above it. Each term in the union is of the form $\{i, 2i\}$, so we should write that to the right of the "$\cup$" symbol. For *indexed* unions like this one, though, we use a slightly larger "$\bigcup$" symbol, like so:

$$A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_{10} = \bigcup_{i=1}^{10} A_i = \bigcup_{i=1}^{10} \{i, 2i\}$$

This is far more concise than writing the elements of all 10 sets, so you can see how *useful* this notation is. We will keep reminding you of the imprecision of the ellipses in the union on the left and tell you that, in fact, an expression like the one on the right is a truly rigorous mathematical statement about this union. The expression on the left is more of an intuitive, heuristic way of describing the union operation applied to these ten sets.

When The Index Set Is Not a Range of Numbers

Let's examine a more difficult example to motivate the next development in this notation technique. What if we asked you to write the following sum in summation notation: the sum of the squared reciprocals of all prime numbers. How can we accomplish this? (Note: We just want to express all the terms of the sum without *evaluating* the sum. That's a difficult endeavor left for another time!)

Unfortunately, we cannot use the exact same notation as above, because we don't want to sum over a range of index values between two natural numbers; rather, we want to only include terms in the sum corresponding to prime numbers. The solution to this is to define an **index set** I that will describe the allowable values of the index that we will then "plug into" the arbitrary term written to the right of the sum.

In this case, if we have a prime number i, we would like to include the term $\frac{1}{i^2}$ in our sum, so this expression will be written to the right of the $\sum$ symbol. We would like to express in our notation that the value i should be a prime number and that all possible prime numbers should be included. The index set I of allowable values should, therefore, be the set of all prime numbers. That is, we can write this sum as

$$\sum_{i \in I} \frac{1}{i^2} \quad \text{, where } I = \{i \in \mathbb{N} \mid i \text{ is prime}\}$$

Look at what this notation accomplishes! Not only have we condensed an infinite number of terms into one expression, we have indicated that the values of the arbitrary index i should be restricted to prime numbers, which do not behave in the "usual" and convenient way as with a sum like $\sum_{i=1}^{n} i$.

Example 3.6.2. This concept of an *index set* is extremely useful and extends to arbitrary sets and even non-mathematical objects. For instance, in our discussion of sets above we used the set B of all Major League Baseball *teams*. How can we use this set to express the set P of all Major League Baseball *players*? Each team is, itself, a set whose elements are the players on that team, so a union of all of the teams (i.e. a union of all sets in B) should produce exactly this set of all players! In this case, our index set is B, and for each element $b \in B$, we want to include b as a *set* in our union. Thus, we would write

$$P = \bigcup_{b \in B} b$$

The individual terms in this union are not even dependent on natural numbers, so there would have been no way to express this union without the use of an index set, like this. Also, this union is dependent on the fact that the terms of the union are elements of the index set B, but they are also sets themselves; thus, applying the union operation to them makes mathematical sense. This might still seem like an odd idea, so be sure to think carefully about this idea of sets having elements that are sets, themselves.

Reading Indexed Expressions Aloud

To verbalize these types of expressions, and to help you think of them in your head, let's give you an example. We might read the expression up above as

> "The sum, over all i that are prime, of $\frac{1}{i^2}$."
> or
> "The sum of $\frac{1}{i^2}$, where i ranges over all prime numbers."

Likewise, we might read the other expression above as

> "The union, over all b that are MLB teams in the 2012 season, of those b."
> or
> "The union of all sets b, where b ranges over all MLB teams from the 2012 season."

3.6.2 Indexed Unions and Intersections

Let's give a precise definition of this union operation for more than one set, since we have only rigorously defined the union of two sets.

Definition 3.6.3. *The union of a collection of sets A_i indexed by the set I is*

$$\bigcup_{i \in I} A_i = \{x \in U \mid x \in A_i \textit{ for some (i.e. at least one) } i \in I\}$$

where we assume there is a set U such that $A_i \subseteq U$ for every $i \in I$.

In mathematical language, the phrase "for some $i \in I$" means that we want there to be *at least one* $i \in I$ with the specified property. If an element x satisfies $x \notin A_i$ for *every* $i \in I$, then this says x is not in any of the sets in our collection, so it should not be included in the union.

Following this idea, we can make a similar definition for set intersections.

Definition 3.6.4. *The intersection of a collection of sets A_i indexed by the set I is*

$$\bigcap_{i \in I} A_i = \{x \in U \mid x \in A_i \textit{ for every } i \in I\}$$

where we assume there is a set U such that $A_i \subseteq U$ for every $i \in I$.

3.6.3 Examples

Let's return to a previous example and make these ideas clearer.

Example 3.6.5. Previously, in Example 3.6.1, we defined

$$A_i = \{i, 2i\}$$

for every natural number i between 1 and 10. Another way of defining this collection is to consider the index set $I = [10]$ (recall the notation $[n] = \{i \in \mathbb{N} \mid 1 \leq i \leq n\}$) and define A to be the set

$$A = \{A_i \mid i \in I\} \text{ , where } A_i = \{i, 2i\} \text{ for every } i \in I$$

This defines every set A_i, dependent on the index value i chosen from the index set I, and it "collects" all of these sets into one set A. Then, another way of writing that union we wrote before would be

$$\bigcup_{i \in I} A_i$$

with the given definitions of I and A_i.

(Think carefully about how this union differs from the set A. Also, what exactly is this union? How can we express its elements conveniently? Do we need to list every element? What if we change the index set I to be $\mathbb{N}$? What is the union in that case?)

Example 3.6.6. Let $I = \{1, 2, 3\}$ and, for every $i \in I$, define

$$A_i = \{i-2, i-1, i, i+1, i+2\}$$

Let's identify and write out the elements of the following sets:

$$\bigcup_{i \in I} A_i \qquad \text{and} \qquad \bigcap_{i \in I} A_i$$

Notice that we can write out the elements of each A_i set, as follows:

$$A_1 = \{-1, 0, 1, 2, 3\}$$
$$A_2 = \{0, 1, 2, 3, 4\}$$
$$A_3 = \{1, 2, 3, 4, 5\}$$

Thus,

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup A_3 = \{-1, 0, 1, 2, 3, 4, 5\}$$

and

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap A_3 = \{1, 2, 3\}$$

Now, consider $J = \{-1, 0, 1\}$, with A_j defined in the same way as before. Let's identify the elements of the sets

$$\bigcup_{j \in J} A_j \qquad \text{and} \qquad \bigcap_{j \in J} A_j$$

Writing out the elements of each set, we can determine that

$$\bigcup_{j \in J} A_j = A_{-1} \cup A_0 \cup A_1 = \{-3, -2, -1, 0, 1, 2, 3\}$$

and

$$\bigcap_{j \in J} A_j = A_{-1} \cap A_0 \cap A_1 = \{-1, 0, 1\}$$

Try answering the same questions with different index sets.

For instance, consider $K = \{1, 2, 3, 4, 5\}$ or $L = \{-3, -2, -1, 0, 1, 2, 3\}$.

Example 3.6.7. Define the index set $I = \mathbb{N}$. For every $i \in I$, define the set

$$C_i = \left\{ x \in \mathbb{R} \mid 1 \leq x \leq \frac{i+1}{i} \right\}$$

Then we claim that

$$\bigcup_{i \in I} C_i = \{y \in \mathbb{R} \mid 1 \leq y \leq 2\} \qquad \text{and} \qquad \bigcap_{i \in I} C_i = \{1\}$$

Can you see why these are true? We will discuss the techniques required to prove such equalities later on. For now, we ask you to just think about why these are true. Can you explain them to a classmate or a friend? What sort of techniques might you use to prove these claims?

Example 3.6.8. Let S be the set of students taking this course. For every $s \in S$, let C_s be the set of courses that student s is taking this semester. What do the following expressions represent?

$$\bigcup_{s \in S} C_s \qquad \text{and} \qquad \bigcap_{s \in S} C_s$$

We bet you can identify at least one element of the set on the right!

3.6.4 Partitions

Now that we have a way of writing down a union of many sets, we can define a helpful notion: that of a **partition**. Linguistically speaking, a partition is a way of "breaking something apart into pieces", and that's pretty much what this word means, mathematically speaking.

To wit, a partition is just a collection of subsets of a set that do not overlap and whose union is the entire set. Let's write down that definition here and then see some examples and non-examples. We will have occasion to use this definition many times in the future, so let's get a handle on it now while we're talking about sets and indexed unions.

Definition 3.6.9. *Let A be a set. A* **partition** *of A is a collection of sets that are pairwise disjoint and whose union is A.*

That is, a partition is formed by an index set I and non-empty sets S_i (defined for every $i \in I$) that satisfy the following conditions:

(1) For every $i \in I$, $S_i \subseteq A$.

(2) For every $i, j \in I$ with $i \neq j$, we have $S_i \cap S_j = \varnothing$.

(3) $\displaystyle\bigcup_{i \in I} S_i = A$

The sets S_i are called **parts** *of the partition.*

The idea here is that the sets S_i "carve up" the set A into non-overlapping, nonempty pieces.

Example 3.6.10. Let's see a couple of examples.

(1) Consider the set $\mathbb{N}$. Let O be the set of odd natural numbers, and let E be the set of even natural numbers. Then $\{O, E\}$ is a partition of $\mathbb{N}$. This is because

- $E, O \neq \varnothing$, and
- $E, O \subseteq \mathbb{N}$, and
- $E \cap O = \varnothing$, and
- $E \cup O = \mathbb{N}$

(2) Consider the set $\mathbb{R}$. For every $z \in \mathbb{Z}$, define the set S_z by

$$S_z = \{r \in \mathbb{R} \mid z \leq r < z + 1\}$$

We claim $\{\ldots, S_{-2}, S_{-1}, S_0, S_1, S_2, \ldots\}$ is a partition of $\mathbb{R}$. Can you see why? Try to write out the conditions required for this collection of sets to be a partition, and see if you can understand why they hold.

Specifically, remember that we need these sets to be *pairwise* disjoint. This means that *any* two sets must be disjoint. Notice that this is quite different from requiring the the intersection of *all* the sets together to be empty.

For instance, consider the collection of sets

$$\big\{ \{1,2\}, \{2,3\}, \{3,4\} \big\}$$

This collection is *not* pairwise disjoint because, for example,

$$\{1,2\} \cap \{2,3\} = \{2\} \neq \varnothing$$

However, the intersection of all three sets is empty, because no element is common to all three of them together.

Example 3.6.11. Now, let's see a couple of non-examples.

(1) Consider the set $\mathbb{R}$. Let P be the set of positive real numbers and let N be the set of negative real numbers. Then $\{N, P\}$ is not a partition because $0 \notin N \cup P$.

Can you modify the choices we made here to identify a partition of $\mathbb{R}$ into two parts?

(2) Consider the set $\mathbb{Z}$. Let A_2 be the set of integers that are multiples of 2, let A_3 be the set of integers that are multiples of 3, and let A_5 be the set of integers that are multiples of 5. The collection $\{A_2, A_3, A_5\}$ is not a partition for two reasons.

First, these sets are not pairwise disjoint. Notice that $6 \in A_2$ and $6 \in A_3$, since $6 = 2 \cdot 3$. Second, these sets do not "cover" all of $\mathbb{Z}$. Notice that $7 \in \mathbb{Z}$ but $7 \notin A_2 \cup A_3 \cup A_5$.

As we mentioned, we will have occasion to use this definition frequently in the future, so keep it in mind.

3.6.5 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What is an index set?

(2) Let $I = \mathbb{N}$, and for every $i \in I$, let $A_i = \{i, -i\}$. Why are the following sets all the *same* set?

$$\bigcup_{i \in I} A_i \qquad \bigcup_{x \in \mathbb{N}} A_x \qquad \bigcup_{j \in I} A_j$$

By the way, what are the elements of this set?

(3) List the elements of the following sets:

(a) $\displaystyle\bigcup_{x \in \mathbb{N}} \{x\}$

(b) $\displaystyle\bigcap_{x \in \mathbb{N}} \{x\}$

(c) $\displaystyle\bigcup_{x \in \mathbb{N}} \{x, 0, -x\}$

(4) Why do you think we didn't talk about an "indexed difference" or an "indexed complementation", and only talked about unions and intersections?

(5) What is a partition? What conditions does a collection of sets have to satisfy to be a partition of a set?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Let $A = \{-2, -1, 0, 1, 2\}$. Let $B = \{1, 3, 5\}$.

For every $i \in \mathbb{Z}$, let $S_i = \{i - 2, i, i + 2, i + 4\}$.

What is $\displaystyle\bigcup_{i \in A} S_i$? What is $\displaystyle\bigcap_{x \in B} S_x$?

(2) For every $n \in \mathbb{N}$, let $A_n = [n]$. What is $\displaystyle\bigcap_{n \in \mathbb{N}} A_n$? What about $\displaystyle\bigcup_{n \in \mathbb{N}} A_n$?

(3) Find a way to write the set of all integers between -10 and 10 (inclusive) using set-builder notation. Then, define the same set using an indexed union. Can you do this in a way so that the sets in your union are pairwise-disjoint (meaning that no two of them have any elements in common)? (Hint: Yes, you can.)

(4) For every $n \in \mathbb{N}$, let M_n be the set of all *multiples* of n. (For example, $M_3 = \{3, 6, 9, \dots\}$.) Write a definition for M_n using set-builder notation. Then, express $\mathbb{N}$ as a union, using these sets.

(**Challenge:** Can you use these sets to define a *partition* of $\mathbb{N}$?)

(5) Let X be any set. What is $\displaystyle\bigcup_{S \in \mathcal{P}(X)} S$? What about $\displaystyle\bigcap_{S \in \mathcal{P}(X)} S$?

(It might help to try this with a specific set, like $X = \{1, 2\}$, to see what happens, first.)

(6) Identify an index set and define some sets that allow you to express $\mathbb{Q}$ as an indexed union.

Can you do this so that there are infinitely many elements in the index set?

(**Challenge:** Can you make this collection a *partition* of $\mathbb{Q}$?)

3.7 Cartesian Products

There is one more way of "combining" sets to produce other sets that we want to investigate. This method is based on the idea of **order**. When we define sets by listing the elements, the order is irrelevant; that is, the sets $\{1, 2, 3\}$ and $\{3, 1, 2\}$ and $\{2, 1, 3\}$ are all equal because they contain the same elements. (More specifically, they are all subsets of each other in both directions). Looking at mathematical objects where order *is* relevant, though, allows us to combine sets in new ways and produce new sets.

You are likely already familiar with the idea of the real plane, $\mathbb{R}^2$ (also known as the **Cartesian plane** after the French matheamtician René Descartes). Each "point" on the plane is described by two values, an x-coordinate and a y-coordinate, and the order in which we write those coordinates is important. We usually think of the x-coordinate as first and the y-coordinate as second, and this helps to distinguish two points based on this order. For instance, the point $(1, 0)$ lies on the x-axis but the point $(0, 1)$ lies on the y-axis. They are not the same point.

There is a deeper, mathematical idea underlying the Cartesian plane. Given any two sets, A and B, we can look at the set of all **ordered pairs** of elements from A and B. By **pair** we mean an expression (a, b) where a and b are elements of A and B, respectively. By **ordered** we mean that writing a first and b second is important. In the case of the real plane, it is especially important because any real number could appear as the x-coordinate *or* the y-coordinate of a point, but the point (x, y) is generally different from the point (y, x). (When are they equal? Think carefully about this.)

3.7.1 Definition

Let's give an explicit definition of this new set before examining some examples.

Definition 3.7.1. *Given two sets, A and B, the* **Cartesian product** *of A and B is written as $A \times B$ and defined to be*

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

This definition tells us that the Cartesian product $A \times B$ collects into a new set all of the ordered pairs (a, b), where a is allowed to be any element of A and b is allowed to be any element of B.

Some Technicalities

Notice that we have dropped the assumption of a universal set U. We have discussed some of the issues that arise when we do *not* specify a universal set, but from now on the sets we work with will not address any of these issues. Accordingly, we will only specify a universal set when not doing so would lead to ambiguity.

In the case of this definition, we could specify a universal set by defining the ordered pair (a, b) as a *set*.Specifically, we could define

$$(a, b) = \{\,\{a\}, \{a, b\}\,\}$$

This definition incorporates the *order* of the pair, as well, in the sense that

$$(a, b) = (c, d) \text{ if and only if } a = c \text{ and } b = d$$

Checking the singleton element in the set tells us the first coordinate, and checking the other element in the set with two elements tells us the second coordinate. If we have the ordered pair (a, a), then the set reduces to $\{\{a\}\}$, which tells us a appears in both coordinates.

Using this definition, we could use the universal set $U = \mathcal{P}(\mathcal{P}(A \cup B))$. We won't delve into the technical details of these sets and definitions, but we thought it prudent to point out that such definitions exist. The important point to remember from this section is given above:

> Two ordered pairs are equal if and only if *both* of their coordinates are equal.

This is why we call them **ordered pairs**.

3.7.2 Examples

The Cartesian plane is $\mathbb{R} \times \mathbb{R}$, which is why we sometimes see this written as $\mathbb{R}^2$. Indeed, if $A = B$, then we sometimes write the Cartesian product as $A \times A = A^2$, if there is no confusion about the fact that A is a set (and not a number). Let's see some more examples where the two sets in the Cartesian product are not the same.

Example 3.7.2. Define the sets $A = \{a, b, c\}$ and $B = \{6, 7\}$ and $C = \{b, c, d\}$. Then we can list the elements of the following Cartesian products:

$$\begin{aligned}
A \times B &= \{(a,6),(a,7),(b,6),(b,7),(c,6),(c,7)\} \\
B \times C &= \{(6,b),(6,c),(6,d),(7,b),(7,c),(7,d)\} \\
A \times C &= \{(a,b),(a,c),(a,d),(b,b),(b,c),(b,d),(c,b),(c,c),(c,d)\} \\
C \times B &= \{(b,6),(b,7),(c,6),(c,7),(d,6),(d,7)\}
\end{aligned}$$

Notice that, in general, $B \times C \neq C \times B$, as this example shows.

(Can you identify the situations where $A \times B = B \times A$? What conditions must we impose on the sets A and B to make this equality true?)

Ordered Triples and Beyond

This idea also extends to Cartesian products of three or more sets. We simply write ordered *triples* for a Cartesian product of three sets and, in general, for the Cartesian product of n sets, we write ordered n-tuples. (Again, we point out that there are set-theoretic ways of defining these ordered n-tuples, but we will not investigate those details.)

Example 3.7.3. The Cartesian product $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ (sometimes written as $\mathbb{N}^3$) is the set of all ordered triples of natural numbers. For instance, $(1, 2, 3) \in \mathbb{N}^3$ and $(7, 7, 100) \in \mathbb{N}^3$, but $(0, 1, 2) \notin \mathbb{N}^3$ and $(1, 2, 3, 4) \notin \mathbb{N}^3$.

Notice the subtle distinction between $\mathbb{N}^3$ and $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$. A typical element of $\mathbb{N}^3$ is an ordered *triple* whose coordinates are each a natural number. A typical element of $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ is an ordered *pair*, the first coordinate of which is also an ordered pair (of natural numbers) and the second coordinate of which is a natural number. That is, $((1, 2), 3) \in (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ but $((1, 2), 3) \notin \mathbb{N}^3$. This shows the two are *different sets*.

There is, however, a *natural* way of relating the two sets which essentially "drops the parentheses" around the first coordinate (the ordered pair). We will discuss this later on when we examine functions and *bijections*. For now, though, we just want you to notice the subtle differences between the two sets and remember that a Cartesian product of two sets is a *set* of *ordered pairs*, where each coordinate is drawn from the corresponding constituent set.

Example 3.7.4. What happens if $B = \varnothing$, say? Look back at the definition of $A \times B$. There are actually *no* elements of B to write as the second "coordinate" of the ordered pair, so we actually have no elements of $A \times B$ to include! Thus,

$$A \times \varnothing = \varnothing$$

for any set A. Similarly, $\varnothing \times B = \varnothing$, for any set B.

3.7.3 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What is the difference between $\mathbb{R} \times \mathbb{N}$ and $\mathbb{N} \times \mathbb{R}$? Give an example of an ordered pair that is an element of one set, but not the other. Then, give an example of an ordered pair that is actually an element of *both* sets.

(2) What is $\varnothing \times \mathbb{Z}$?

(3) Write out all the elements of the set $\{\heartsuit, \diamondsuit\} \times \{\smiley, \square, \heartsuit\}$.

(4) What is the difference between $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ and $\mathbb{N} \times (\mathbb{N} \times \mathbb{N})$? Why aren't they technically the same set? Can you explain why they are "essentially" the same set?

(5) Let A, B, C be sets. Suppose $A \subseteq B$. Do you think $A \times C \subseteq B \times C$ is true? Why or why not?

(6) Give an example of a set S such that $\left(\frac{1}{2}, -1\right) \in S$.

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Write out the elements of $[3] \times [2]$.

Can you make a conjecture about how many elements $[m] \times [n]$ has, for any $m, n \in \mathbb{N}$? (How might you try to prove your conjecture?)

(2) Give an example of an element of the set $\mathbb{N} \times \mathcal{P}(\mathbb{Z})$.

(3) Give an example of an element of the set $\big((\mathbb{R} \times \mathbb{N}) \times \mathbb{Q}\big) \cap \big((\mathbb{Q} \times \mathbb{Z}) \times \mathbb{N}\big)$.

(4) Give an example of sets C, D such that $C \times D = D \times C$.

Follow-up challenge: Can you characterize *all possible situations* like this one. What must be true about C and D? Can you prove it?

(5) Write out the elements of $\mathcal{P}\big([1] \times [2]\big)$.

(6) For every $n \in \mathbb{N}$, let $A_n = [n] \times [n]$. Consider the set

$$B = \bigcup_{n \in \mathbb{N}} A_n$$

Is $B = \mathbb{N} \times \mathbb{N}$ or not? Explain, with examples.

(7) If you know some simple computer programming, try writing code (in your favorite language) that will input $m, n \in \mathbb{N}$ and print out all the elements of $[m] \times [n]$. (Use some pseudocode if you're not totally comfortable with programming.) How long do you think this takes to run, depending on m and n?

3.8 [Optional Reading] Defining the Set of Natural Numbers

Our goal in this section is to put the natural numbers $\mathbb{N}$ on a rigorous, mathematical foundation. Specifically, we will prove that the natural numbers exist, by defining and deriving them from the axioms and principles of set theory. We will then discuss a few of their properties. We will use some of those properties to define and prove the Principle of Mathematical Induction in Chapter 5, after discussing some basic principles and results of mathematical logic.

3.8.1 Definition

How do we *define* the natural numbers in terms of sets? We intuitively know what they are. We start with 1 and repeatedly add 1, obtaining all of the other natural numbers. Thus, we have to identify what we mean by "1" and what we mean by "add 1", in terms of sets. To do this, let's start by thinking about 0. We stated before that we will not include 0 in the set $\mathbb{N}$, but some authors do, and it will aid us in deriving $\mathbb{N}$, right now, to consider it. We know of exactly one set that contains no elements, the empty set. Thus, it makes sense to *associate* 0 with the empty set; in fact, we *define* $0 = \varnothing$. Next, we wish to define 1, and following our definition of 0, it makes sense to choose a set that has exactly one element. (A set with one element is also known as a **singleton**.) There are several such sets:

$$\{\varnothing\}, \{\{\varnothing\}\}, \{\{\varnothing, \{\varnothing\}\}\}$$

How do we choose a *representative* singleton to represent 1? Keeping in mind that we want to continue this process and eventually define 2 (and 3, and so on) in terms of previous numbers, it makes sense now to define 1 in terms of the only object we have at our disposal: 0. Thus, let us *choose* to define

$$1 = \{0\} = \{\varnothing\}$$

This guarantees $0 \neq 1$.

Next to define 2, we consider sets containing two elements, like

$$\{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\{\varnothing\}\}\}, \{\{\varnothing\}, \{\{\varnothing\}\}\}$$

and so on. We seek a natural representative, and we notice that the first set listed above contains the two objects, 0 and 1, that we have already defined! Thus, defining $2 = \{0, 1\}$ is a natural choice and, again, we know $2 \neq 0$ and $2 \neq 1$.

Successors

This gives us an intuitive idea of how to continue this process and define any natural number: for any $n \in \mathbb{N}$, we define

$$n = \{0, 1, 2, \ldots, n-2, n-1\}$$

However, given a set, it would be quite difficult to verify, using this definition, whether or not that set represents a natural number. We would like a *better* definition of the elements of $\mathbb{N}$; we want to know, given any set, whether it belongs in $\mathbb{N}$. Look back at the element n above; we could also write

$$n = \{0, 1, 2, \ldots, n-2, n-1\} = \{0, 1, 2, \ldots, n-2\} \cup \{n-1\} = (n-1) \cup \{n-1\}$$

Look at that! We have a natural way of defining an element of $\mathbb{N}$ in terms of the previous element and in terms of set operations. This motivates the following definition.

Definition 3.8.1. *Given any set X, the* **successor** *of X, denoted by $S(X)$, is defined to be $S(X) = X \cup \{X\}$.*

This definition applies to all sets, but in the context of natural numbers, it means that the successor of n is precisely that natural number we "know" intuitively to be one larger, namely $n + 1$.

Inductive Sets

This brings us closer to our definition of $\mathbb{N}$. We certainly want $1 \in \mathbb{N}$ and we also want $S(n) \in \mathbb{N}$ for any element $n \in \mathbb{N}$. To codify this symbolically, we make the following definitions:

Definition 3.8.2. *A set I is called* **inductive** *provided*

1. $1 \in I$
2. *If $n \in I$, then $S(n) \in I$, as well.*

Certainly, $\mathbb{N}$ itself (as we hope to define it) should be an inductive set. Are there *other* inductive sets? Think about this. What properties would they have? Would they contain elements that are *not* natural numbers? We don't want to address these questions in depth, but for the sake of our discussion here, we will point out that there are, indeed, other inductive sets. We don't want any of those sets to be $\mathbb{N}$, so we make this definition:

Definition 3.8.3. *The set of all **natural numbers** is the set*

$$\mathbb{N} := \{x \mid \text{ for every inductive set } I,\ x \in I\}$$

Put another way, $\mathbb{N}$ *is the* smallest *inductive set, in the sense of set inclusion:*

$$\mathbb{N} = \bigcap_{I \in \{S \mid S \text{ is inductive}\}} I$$

This dictates that $\mathbb{N}$ *is a subset of every inductive set.*

This gives us the "checking property" we desired. Any set x is a natural number (i.e. $x \in \mathbb{N}$) if and only if it is an element of *every* inductive set (i.e. $x \in I$ for every inductive set I). This also tells us that $\mathbb{N} \subseteq I$ for every inductive set I.

There are some other set theoretic discussions that could be made here: How do we know that such an infinite set exists? (In actuality, we need to make this an *axiom* of set theory! Assuming these types of sets exist, how do we characterize those other inductive sets that are not $\mathbb{N}$? Addressing these questions lies outside the scope and goals of this course, so we will not address them. We will, however, mention a few properties of $\mathbb{N}$ now, specifically ones that will be useful in setting mathematical induction on a rigorous foundation. (In case you're wondering, think about the set of integers, $\mathbb{Z}$. Try to explain why this set is, indeed, inductive. What about $\mathbb{R}$? What about $\mathbb{Z} - \mathbb{N}$?)

Properties of $\mathbb{N}$

Before we define the principle of induction, let's think about some of the common properties and uses of natural numbers: orderings and arithmetic. Given any two natural numbers, we can *compare* them and decide which one is larger and which one is smaller (or if they are equal). We usually write this with symbols like $1 < 3$, $1 \leq 5$, $4 \not< 2$, $3 = 3$, etc.

Can we phrase these comparisons in terms of *sets*, knowing that we have now defined the elements of $\mathbb{N}$ as sets, themselves? Yes, we can! Look back at the definition of *successor*. Built into that definition is the fact that $X \in S(X)$! This observation gives us the following definition:

Definition 3.8.4. *Given two natural numbers $m, n \in \mathbb{N}$, we write $m < n$ if and only if $m \in n$.*

This defines an *order relation* on the set $\mathbb{N}$. We will discuss the concepts of relations and orders later on in the book (in Section 6.3).

What about arithmetic? What is $m + n$ in terms of the sets m and n? How do we define this operation and its output? How do we know $m + n$ is another natural number? Can we be sure that $m + n = n + m$? These are questions we can address later on after discussing functions and relations.

3.8.2 Principle of Mathematical Induction

For now, let us present a more rigorous version of induction:

Theorem 3.8.5 (Principle of Mathematical Induction)**.** *Let $P(n)$ be some "fact" or "observation" that depends on the natural number n. Assume that*

1. *$P(1)$ is a true statement.*
2. *Given any $k \in \mathbb{N}$, if $P(k)$ is true, then we can conclude* necessarily *that $P(k+1)$ is true.*

Then the statement $P(n)$ must be true for every *natural number $n \in \mathbb{N}$.*

Let us first prove this theorem before discussing its assumptions and consequences in detail.

Proof. Define the set S to be the natural numbers for which the statement P is true. That is, define $S = \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$. By definition, $S \subseteq \mathbb{N}$.

Furthermore, the assumptions of the theorem guarantee that $1 \in S$ and that whenever $k \in S$, we know $k+1 \in S$, as well. This means S is an *inductive* set. By the observation we made after defining $\mathbb{N}$, we know that $\mathbb{N} \subseteq S$.

Therefore $S = \mathbb{N}$, so the statement $P(n)$ is true for every natural number n. □

This is pretty *slick*, right? It seems that all of the desired conclusions "fell out of" our definitions! In this sense, the definitions and axioms are *natural* choices, because they accomplish what our *intuition* already "knew" about the set $\mathbb{N}$ and its properties.

There are a few minor issues that we have left undiscussed. Specifically, what do we mean by a "fact" or "observation" that *depends* on a natural number n? What does it mean to *necessarily conclude* that $P(k+1)$ is true when $P(k)$ is true? What do we even mean by *true*? These are all deep mathematical questions and involve a thorough study of logic, and we will discuss these issues in the next chapter! Onward! Huzzah!

3.8.3 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What is an inductive set? Give an example of one that is not $\mathbb{N}$ or $\mathbb{Z}$.

(2) We defined $S = \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$ in the proof of the Principle of Mathematical Induction. What does this mean? Describe this set in words.

(3) Come up with your own analogy for how Induction works.

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) What if we changed the definition of **successor** to be $S(X) = \{X\}$. Using $0 = \varnothing$, what are 1, 2, 3, and 4 in terms of sets? Do they still satisfy the equality $n = \{0, 1, \dots, n-1\}$? If not, do they satisfy some other relationship? Explore!

(2) Have a debate with a friend about whether or not infinite sets exist. Why do we need to *assume* the existence of an inductive set to define $\mathbb{N}$? Does this seem valid to you? Does it make sense, physically? Mathematically?

(3) Consider a simple arithmetic statement, like $1 + 2 = 3$. Write out the numbers 1, 2, and 3 in terms of sets, and see how this equation might make sense. What does "+" mean, in this context?

(4) Investigate how one might define $\mathbb{Z}$, using $\mathbb{N}$. Do some exploring online or in books, or make up an idea on your own.

3.9 Proofs Involving Sets

Now that we've gone through many definitions and examples, to introduce what sets are and how to manipulate them, let's actually write up some rigorous, mathematically correct, and well-written **proofs** about sets. All of the propositions/lemmas contained here are useful facts that we can cite later on, and we would expect you to be able to prove claims like these. (Note: A lemma is just a small result that requires some proof, and can be cited later to prove more significant theorems.) Furthermore, all of these proofs are of the type of quality and rigor that we will expect from you in the future, the very near future . . . Use these as guidelines, if you'd like!

3.9.1 Logic and Rigor: Using Definitions

The main point we'd like to emphasize here—as we transition from descriptive, "wordy", and intuitive proofs into more rigorous, mathematically correct, and formally-written ones—is that **formal definitions are very important**. Fundamentally, they're essential because when we say, for example, "$A \cup B$", we need to know that you know exactly what that symbol means and how it operates on the sets A and B.

As another example, when we say "Prove $A = B$", we have a very specific goal in mind, and you need to be on the same page. It always helps to have an intuitive understanding of the main concepts—"Oh, the statement $A = B$ just means that A and B have the same elements in them"—but this is *not* the type of language/ideas we want to use in a rigorous proof. To prove a statement like $A = B$, we need you to **appeal to the definition** of "=" in the context of sets: $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

This is what we mean when we say "satisfy a definition" or "appeal to a definition": to prove that some mathematical object has a certain property, you must demonstrate that the object satisfies the formal definition of that property. If you aren't familiar with that definition, or have forgotten how to state it precisely ... by all means, go look it up! We realize this is a lot of new information to ingest, and there's nothing wrong with forgetting something when it's still new to you. By doing this, you'll start to internalize these ideas more quickly and more solidly.

You'll see how we use the definitions of, for instance, "$\subseteq$" and "=" and "$\cap$" and so on in the examples below. For each proposition/lemma, we will end up writing a formal proof, but we will also write a little bit about how we would approach *coming up with* such a proof. Oftentimes this is the difficult part! We think you'll notice that many of those explanations will amount to just recalling a relevant definition and thinking about what it means and how it applies in the given situation. In a way, that's what a lot of mathematics is. We just allow our definitions we use to get more and more complicated.

3.9.2 Proving "$\subseteq$"

Recall the definition of **subset**, because we will use it frequently here:

Definition 3.9.1. *Given two sets A and B, if every element of A is* also *an element of B, then we say A is a* **subset** *of B.*

Say we are presented with the following problem:

> Let A be the set ... and let B be the set ... Prove that $A \subseteq B$.

How can we satisfy the definition of $A \subseteq B$ to prove this claim? Yes, the intuitive idea is that "every element of A is also an element of B", but we shouldn't just try to dance around the issue and try to make that sentence our conclusion. Rather, we need to verify that *every* element of A is also *necesarily* an element of B. This is where the wonderful phrase **"arbitrary and fixed"** will come in handy!

The Phrase "Arbitrary and Fixed"

How can we talk about *all possible elements* of A all at once? Of course, we might not need to do this if A has only, say, 3 elements; then, we can just work with them one by one. But what if A has 100 elements? Or 1 million? Or *infinitely* many? How can we prove something about all of them at once in a reasonable way?

What we will do is introduce an **arbitrary and fixed** element of A so we have something to work with. This element will be **arbitrary** in the sense that we make no extra assumptions about what it is or what properties it has, only that it is an element of A. This element will be **fixed** in the sense that we will assign it some variable name (usually a letter, like a or x or t or something) and this letter will represent the *same* object throughout the remainder of our proof. As long as we can prove our goal for this element, then we will have simultaneously proven something about *all* elements of A. Voilà!

Examples

Let's see this process in action to really get the point across. We'll begin with the statement to be proven, then describe our thought processes in coming up with a proof, and then present our formal, written proof.

Lemma 3.9.2. *Let A, B, X be any sets.*

If $X \subseteq A$ and $X \subseteq B$, then $X \subseteq A \cap B$.

Intuition: Consider drawing a Venn diagram to represent this situation. To make sure the assumptions $X \subseteq A$ and $X \subseteq B$ both hold true, we need to make the set X "lie inside" both A and B. Accordingly, this means X must lie entirely "inside" where A and B overlap, which is what $A \cap B$ represents. This helps us realize that this statement is, indeed, True. But it doesn't prove anything!

To *prove* the statement, we will introduce an arbitrary and fixed element $x \in X$. What do we know about it? Well, we assumed that $X \subseteq A$. The definition of "$\subseteq$" means that any element of X is *also* an element of A. But we know x is an element of X; this means it is also an element of A. How convenient! We can make some similar statements about x and X and B that will tell us $x \in B$. What does this mean, overall? Oh hey, the definition of "$\cap$" applies, and tells us $x \in A \cap B$. Brilliant! Now, let's write it up.

Proof. Let $x \in X$ be arbitrary and fixed.

By assumption $X \subseteq A$, so $x \in A$, as well, by the definition of $\subseteq$.

Similarly, by assumption $X \subseteq B$, so $x \in B$, as well.

Since $x \in A$ *and* $x \in B$, this means that $x \in A \cap B$, by the definition of $\cap$.

Overall, we have shown that whenever $x \in X$, it is also true that $x \in A \cap B$. Since $x \in X$ was arbitrary, we conclude that $X \subseteq A \cap B$. $\square$

Not so bad, right? Let's try another one, a slightly harder one, even.

Proposition 3.9.3. *Let A and B be any sets. Then, $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.*

Whoa, is this really true? Look back at Problem 6 in Section 3.5, and you'll see an example. This claim states that it is true, *in general*, and not just for that example. Let's figure out why, and then prove it.

Intuition: There are several layers of definitions at work here. In particular, the *power set* operation might be confusing to you. The key is to just remember that definition: $\mathcal{P}(A)$ is the set of all *subsets of* A. Now, the main claim here is one of a *subset* relationship: whatever the set $\mathcal{P}(A) \cap \mathcal{P}(B)$ is (we'll analyze it later, but it's important that you recognize immediately what *type* of object it is: a *set*), it is supposed to be a subset of whatever the set $\mathcal{P}(A \cap B)$ is. That's it, and it's important to notice that this is really motivates the overarching form of the forthcoming proof.

Without even having to think about what $\mathcal{P}(A) \cap \mathcal{P}(B)$ means, we can be sure that our proof will start with "Let $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ be arbitrary and fixed". This is because we need to satisfy the definition of "$\subseteq$" by taking any old element of the set on the left and deducing that it is also an element of the set on the right. This is what we mean by the **structure** of the proof.

What does an element $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ "look like"? It's a set, and it's an element of both $\mathcal{P}(A)$ and $\mathcal{P}(B)$. This means ... well, we're actually going to skip ahead and jump right into the formal proof now, because we'll just find ourselves repeating the same words down below anyway. But before going ahead to read *ours*, we think you should go off and try to write your *own* proof. Then, when you're done, you can compare and see whether you are correct, whether it has the same steps as ours, whether it's written clearly, and so on. See what you can do!

Proof. Let $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ be arbitrary and fixed.

By the definition of $\cap$, this means $X \in \mathcal{P}(A)$ *and* $X \in \mathcal{P}(B)$.

Since $X \in \mathcal{P}(A)$, we know $X \subseteq A$, by the definition of power set.

Similarly, since $X \in \mathcal{P}(B)$, we know $X \subseteq B$.

Since $X \subseteq A$ and $X \subseteq B$, we know that $X \subseteq A \cap B$ by Lemma 3.9.2 that we just proved.

Now, since $X \subseteq A \cap B$, we know $X \in \mathcal{P}(A \cap B)$, by the definition of power set.

Since X was arbitrary, we conclude that $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$. $\square$

Did you do what we did? Did you also cite the previous lemma? Did you instead prove that result all over again without realizing it? Consider that a lesson learned! One of the major benefits of proving results is that we get to use them in later proofs! There's nothing technically wrong with proving the previous result again in the middle of this proof; it just might save a little bit of time and writing to not do so. If you find yourself working on a problem and thinking, "Hey, this feels familiar ...", go back and look for related theorems or lemmas or examples. Maybe you can use some already-acquired knowledge to your advantage.

3.9.3 Proving "="

Double-Containment Proofs

Again, we will need to recall the definition of "=" (in the context of sets), since we will be using it frequently here.

Definition 3.9.4. *We say two sets, A and B, are* **equal**, *and write $A = B$, if and only if $A \subseteq B$ and $B \subseteq A$.*

That's it! It's completely built up from a previous definition, that of "$\subseteq$" (since that of "$\supseteq$" is completely equivalent). Thus, this isn't really a new technique, per se, because it's really a repeated application of a previous technique. That is to say, to prove $A = B$, we just need to use the technique used in the last subsection and prove $A \subseteq B$ and then prove $B \subseteq A$.

This technique is so common, in fact, that it is given a name: **double-containment**. When we prove two sets are subsets of each other, both ways, and conclude that they are equal, we call this a **double-containment proof**.

Examples

Let's see an example of this double-containment technique in action.

Lemma 3.9.5. *Let A and B be any sets. Then, $A - (A \cap B) = A - B$.*

Intuition: As usual, we could draw a Venn diagram to convince ourselves of this truth, but that doesn't prove anything. Instead, we will follow a double-containment proof. If we take an element $x \in A - (A \cap B)$, we can apply the definition of "$-$" first, and then "$\cap$", to deduce something about x. Hopefully, it will tell us that $x \in A - B$. Then, if we take an element $y \in A - B$, we can apply some definitions to hopefully deduce that $x \in A - (A \cap B)$. Maybe we aren't sure yet exactly how to do so, but by looking at that Venn diagram and using the definitions, we can surely figure it out. Why don't you try to do it first, then read our proof!

Proof. We will show $A - (A \cap B) = A - B$ by a double-containment proof.

("$\subseteq$") First, let $x \in A - (A \cap B)$ be arbitrary and fixed. By the definition of "$-$", we know that $x \in A$ and $x \notin A \cap B$. This means it is *not* true that x is an element of *both* A and B. We already know $x \in A$, so we deduce that $x \notin B$.

Thus, $x \in A$ and $x \notin B$, so by the definition of "$-$", we deduce that $x \in A - B$. This shows $A - (A \cap B) \subseteq A - B$.

("$\supseteq$") Second, let $y \in A - B$ be arbitrary and fixed. By the definition of "$-$", this means $y \in A$ and $y \notin B$. Now, since y is not an element of B, this means that certainly y is not an element of *both* A and B. That is, $y \notin A \cap B$, by the definition of "$\cap$".

Since we know $y \in A$ and $y \notin A \cap B$, we deduce that $y \in A - (A \cap B)$. This shows $A - B \subseteq A - (A \cap B)$.

Overall, a double-containment proof has shown that $A - (A \cap B) = A - B$. $\square$

Look at the overall structure of this proof. We knew there would be two parts to it, since it is a double-containment proof, but we were also kind enough to *point this out ahead of time* for our intrepid reader, and separate those two sections appropriately. It would be technically correct to ignore this and just dive right in to the proof, but this might leave a reader confused. The whole point of a proof is to *convince someone else* of a truth that you have already figured out, so you might as well make it as easy as possible for them to follow what you're doing.

Let's see another example of proving two sets are equal. This one will be a little different, because one of the parts of the double-containment will make use of the complement operation. As a preview, spend a minute now thinking about why the statements $A \subseteq B$ and $\overline{B} \subseteq \overline{A}$ are *equivalent* (supposing there is some universal set $A, B \subseteq U$). Draw a Venn diagram and try some examples. Try to prove it, even!

Proposition 3.9.6.

$$\left\{ x \in \mathbb{N} \mid x + \frac{8}{x} \leq 6 \right\} = \{2, 3, 4\}$$

Proof. Let's define $A = \left\{ x \in \mathbb{N} \mid x + \frac{8}{x} \leq 6 \right\}$, and $B = \{2, 3, 4\}$.

To show $A = B$, we will show $A \subseteq B$ and $B \subseteq A$.

First, we will show $B \subseteq A$. We can consider each of the three elements separately, and verify that they satisfy the defining inequality of B:

$$\begin{aligned} 2 + \frac{8}{2} &= 6 \leq 6 \\ 3 + \frac{8}{3} &= \frac{17}{3} \leq 6 \\ 4 + \frac{8}{4} &= 6 \leq 6 \end{aligned}$$

Since $2, 3, 4 \in \mathbb{N}$, we deduce that $2 \in A$ and $3 \in A$ and $4 \in A$, so $B \subseteq A$.

Next, to show $A \subseteq B$, we will show that $\overline{B} \subseteq \overline{A}$, where the complement is taken in the context of $\mathbb{N}$. That is, we will show that all of the natural numbers $1, 5, 6, 7, \dots$ are *not* elements of A.

To show this, we will verify that the defining inequality of A is *not* satisfied by any of those elements.

The first two cases can be considered easily: $1 + \frac{8}{1} = 9 \not\leq 6$ and $5 + \frac{8}{5} = \frac{33}{5} \not\leq 6$.

To consider the other cases, we can take an arbitrary and fixed $x \in \mathbb{N}$ with $x \geq 6$. Notice, then, that $x + \frac{8}{x} \geq 6 + \frac{8}{x} > 6$, since $\frac{8}{x} > 0$.

This shows that *only* 2,3,4 satisfy the defining inequality of A.

Overall, by a double-containment argument, we have proven that $A = B$. $\square$

Think carefully, again, about why the method employed in the second half of the proof is valid. (It is actually an instance of using the **contrapositive** of a conditional statement, but we haven't yet defined any of those terms; we will do so in the next chapter on logic.)

Let's see another example of proving set equality. This one is only slightly different in that we are proving some set is actually the *empty set* and, to do so, we will prove that it has *no elements*.

Proposition 3.9.7. *For every $n \in \mathbb{N}$, define $S_n = \mathbb{N} - [n]$. Then*

$$\bigcap_{n\in\mathbb{N}} S_n = \varnothing$$

We suggest you play around with this statement first, if it doesn't make sense. For instance, try identifying the element of the sets S_1, and $S_1 \cap S_2$, and $S_1 \cap S_2 \cap S_3$, and so on. Try to come up with a candidate element of the big intersection on the left, and then figure out why it actually is *not* an element of that set. After that, try to figure out a formal proof and write it out; then, look at ours below!

Proof. Let's define $T = \bigcap_{n\in\mathbb{N}} S_n$, so we can refer to it later.

To prove $T = \varnothing$, we will show that T does not contain any elements. Notice that T is formed by an intersection of many sets of natural numbers, so it's clear that the only *possibilities* for elements of T are natural numbers.

Consider an arbitrary and fixed $x \in \mathbb{N}$. We want to show that $x \notin T$.

Observe that $x \in [x] = \{1, 2, \dots, x\}$. Thus, $x \notin \mathbb{N} - [x]$, by the definition of "$-$".

By definition, T contains the elements that belong to all of the sets of the form $\mathbb{N} - [n]$. We have identified (at least) one set, $\mathbb{N} - [x]$, of the intersection such that x does *not* belong to that set. Accordingly, x cannot be an element of T, since it does not belong to *all* such sets. Therefore, $x \notin T$.

Since $x \in \mathbb{N}$ was arbitrary, we have proven that T contains no natural numbers as elements, and therefore it has *no* elements at all. $\square$

Summary: Let's make one more statement about why this technique works. We showed that there are no elements of T, i.e. that $T \subseteq \varnothing$. This completes the entire process, because it is trivially true, as well, that $\varnothing \subseteq T$. (This claim holds for any set.) Thus, one of the parts of the double-containment argument is already achieved, and we can conclude $T = \varnothing$.

Alright, one more example. We want to include this one because it gives us further practice in working with indexed set operations. You will find many similar problems in the exercises for this section. We encourage you to work on as many of them as you can!

Proposition 3.9.8. *For every* $n \in \mathbb{N}$*, define* $A_n = \left\{ x \in \mathbb{R} \mid 0 \leq x < \frac{1}{n} \right\}$*. Then,*

$$\bigcap_{n \in \mathbb{N}} A_n = \{0\}$$

Think about what this claim means. Draw a picture of the A_n sets on a number line. What does the "$\bigcap$" intersection accomplish? Why does it work out that 0 is an element of that intersection? Why is it the *only* element?

The definition of $\bigcap$ will be crucial in this proof, so let's recall the definition here. The key phrase is *for every*:

Definition 3.9.9. *The intersection of a collection of sets* A_i *indexed by the set* I *is*

$$\bigcap_{i \in I} A_i = \{x \in U \mid x \in A_i \text{ for every } i \in I\}$$

where we assume there is a set U *such that* $A_i \subseteq U$ *for every* $i \in I$*.*

That is, remember that the indexed intersection of several sets collects together the elements that belong to *all* of the constituent sets. Thus, in our proof below, you will see that we need to prove that (1) 0 is, indeed, an element of *all* of the A_n sets, and (2) *no other* number is an element of all of them, i.e. for every nonzero real number, we can identify at least one of the A_n sets such that the number is not an element of that set.

Proof. First, we will prove that

$$\{0\} \subseteq \bigcap_{n \in \mathbb{N}} A_n$$

This requires us to show that $0 \in A_n$ for *every* $n \in \mathbb{N}$.

Let $n \in \mathbb{N}$ be arbitrary and fixed. Notice that the inequality $0 \leq 0 < \frac{1}{n}$ does, indeed hold.

(Note: You might be worried because "in the limit" 0 is not less than every fraction $\frac{1}{n}$ "all at once", but that is not the point! Think of it this way: Is $0 \in A_1$? Yes, $0 \leq 0 < 1$. Is $0 \in A_2$? Yes, $0 \leq 0 < \frac{1}{2}$. Is $0 \in A_3$? Yes, $0 \leq 0 < \frac{1}{3}$. And so on. The inequality holds for every $n \in \mathbb{N}$ *individually*, so 0 is an element of *every* such set. If you weren't worried about this, never mind! Move right along!)

Thus, $0 \in A_n$ for every $n \in \mathbb{N}$, and so $0 \in \bigcap_{n \in \mathbb{N}} A_n$, by the definition of "$\bigcap$".

This shows that $\{0\} \subseteq \bigcap_{n \in \mathbb{N}} A_n$.

Second, we will prove that

$$\bigcap_{n\in\mathbb{N}} A_n \subseteq \{0\}$$

We will do this by considering the *complements* of these sets, in the context of $\mathbb{R}$. Specifically, we will show that

$$\overline{\{0\}} \subseteq \overline{\bigcap_{n\in\mathbb{N}} A_n}$$

which means we will show that every nonzero real number is *not* an element of *every* A_n.

Let $x \in \mathbb{R}$ be arbitrary and fixed, with the property that $x \neq 0$. Either $x > 0$ or $x < 0$, then, so let's consider each case separately.

Case 1: Suppose $x > 0$. Consider the number $\frac{1}{x} \in \mathbb{R}$. Since the natural numbers are infinite and unbounded in $\mathbb{R}$, we can choose a natural number M that is *bigger* than that real number. That is, we can choose $M \in \mathbb{N}$ such that $M > \frac{1}{x}$.

(Note: Think about why this works. We haven't *proven* that $\mathbb{N}$ is infinite, or that the numbers "go on forever" along the number line of $\mathbb{R}$, but we hope these ideas make sense to you, intuitively.)

Take such an $M \in \mathbb{N}$ with $M > \frac{1}{x}$. Since $x > 0$, we can multiply the inequality on both sides by x; since $M > 0$ (so $\frac{1}{M} > 0$) we can then multiply again by $\frac{1}{M}$. This yields $x > \frac{1}{M}$. Accordingly $x \notin A_M$, because $-\frac{1}{M} < x < \frac{1}{M}$ is False.

Since $x \notin A_M$, then surely x is not an element of *all* such sets. Therefore, $x \notin \bigcap_{n\in\mathbb{N}} A_n$.

Case 2: Next, suppose that $x < 0$. We will make a similar argument as the previous case; this time, we will just consider $-x$, since $-x > 0$. Using the same logic as above, we can surely identify a natural number $M \in \mathbb{N}$ that satisfies $M > \frac{1}{-x} = -\frac{1}{x}$. Manipulating the inequality tells us that $x < -\frac{1}{M}$. Thus, $x \notin A_M$, and so $x \notin \bigcap_{n\in\mathbb{N}} A_n$.

Therefore, we have shown that any $x \in \mathbb{R}$ with $x \neq 0$ is not an element of at least one of the A_n sets, so any such x is not an element of their intersection. Thus, $\overline{\{0\}} \subseteq \overline{\bigcap_{n\in\mathbb{N}} A_n}$, and we have proven the claim by a double-containment argument. □

This proof is harder than the other ones, we think, so make sure to read it a couple times to make sure you see what happens in every step. In particular, think about how we came up with the step where we chose $M \in \mathbb{N}$ that satisfies $M > \frac{1}{x}$. Do you think we magically intuited that choice? Or do we think we recognized that we wanted $x < \frac{1}{M}$ to be true for some M, and manipulated the inequality backwards to figure out how to make that happen?

3.9.4 Disproving Claims

Motivating Example

Consider the following proposed claim:

For any sets F, G, H, if $F \subseteq G \cup H$, then either $F \subseteq G$ or $F \subseteq H$.

Is this claim True? If so, how would we prove it? Well, we'd take an arbitrary and fixed element $x \in F$. Since $F \subseteq G \cup H$, this would tell us $x \in G \cup H$, as well. Accordingly, either $x \in G$ or $x \in H$. Is that it? Are we done with the proof?

We hope you recognize that this does *not* work! In particular, we have not satisfied the definition of "$\subseteq$" at the end. If our goal is to prove "either $F \subseteq G$ or $F \subseteq H$", then we should conclude that one or the other of those claims holds: that *every* element of F is also an element of G, or else *every* element of F is also an element of H.

What we found was that every element of F is itself either an element of G or H, but we cannot decide collectively that *all* elements of F are elements of one or the other, G or H. Read through these last two paragraphs again to make sure you follow that logical observation. It might be easy to actually write up a "proof" for this claim and not realize that you've made a false step!

Identifying Errors

This recognition of an error is one of the skills we are developing, and it will be helpful in several ways. You'll notice that many exercises (some thus far, but many more as we move onwards) ask you to **find the flaw** in a proposed "proof" of some claim. By pointing out that there exists a flaw, we are perhaps helping you to find it (or them, as the case may be). Reading a proposed proof for logical, factual, and clarity errors is an essential skill. What's more, this careful reading of others' writing will necessarily make you a more critical reader of *your own* writing, and it will help you to catch potential errors like the one in the preceding paragraphs. Do not worry if you didn't catch it; now that you've seen it, you'll be on the lookout for similar mistakes in the future! Like we said, as well, this skill is ongoing development, and by the end of this book, you will be a great *reader* of mathematical proofs, as well as a great *writer*.

Counterexamples

So, now what do we do? We just recognized that our "proof" above did not work. Does this mean the claim is actually False? Actually, all this means (so far) is that our attempt at a proof failed. Maybe some other logical route will magically take us to the elusive conclusion.

Or, maybe the claim really is False. How could we show that? Think about the logical form of the claim: it says some statement holds true for *any* sets F, G, H. It says that the assumption $F \subset G \cup H$ will always imply, necessarily, that $F \subseteq G$ or $F \subseteq H$. To show that this does *not* always happen, we need to find what's called a **counterexample**.

We will discuss all of these ideas again in the next chapter, when we formalize **logic**, but what you need to know for now is this: a **counterexample** is a specific, detailed, and described example that illustrates how a statement about "every ..." or "any ..." or "all possible ..." does *not* actually hold for every case. A counterexample amounts to **disproving** a statement that a whole class of objects has a certain property, by exhibiting one object in that class *without* that property.

Example

Let's see how the process of finding and stating a counterexample would work for our example above.

Example 3.9.10. Recall the claim:

For any sets F, G, H, if $F \subseteq G \cup H$, then either $F \subseteq G$ or $F \subseteq H$.

This claim is supposed to work for any sets F, G, H, so when we describe our counterexample, we better describe *exactly* what those three sets are going to be. We can't just explain our way around the issue and argue about how there might exist three sets out there with a certain property. Nope, we have to tell a reader exactly what they are by explicitly defining them. This is what the first line of our disproof of the claim will be, but we can't just jump right into that, because we don't know how to define them yet!

This is where the fun/work is: we need to play around with the desired properties of these sets to help us come up with an example. Recall that we want these sets to satisfy some properties: we should make sure the assumption $F \subseteq G \cup H$ holds True, but we want the conclusion—that either $F \subseteq G$ or $F \subseteq H$—to be False.

What does this mean? Well, we think you'll agree that, logically speaking, the "opposite" or "negation" of a statement like that would be "both $F \not\subseteq G$ and $F \not\subseteq H$". (This concept of **logical negation** will return in the next chapter; for now, we think you can understand it by applying the logical principles that guide your daily life. Soon, we will formalize this idea.)

We now have a specific goal: to find three sets F, G, H that satisfy all three of the following:

$$F \subseteq G \cup H$$
$$F \not\subseteq G$$
$$F \not\subseteq H$$

One thing left to consider is what "$\not\subseteq''$ means. We have a definition of "$\subseteq$", so what is the "opposite" or "negation" of that? For $F \subseteq G$ to be true, we require that every element of F is also an element of G; so, if this *fails*, then we must have at least one element of F that is *not* an element of G. The same observation applies to $F \nsubseteq H$. Now, we can restate our goals in a helpful way, by applying definitions:

Every element of F is an element of either G or H

There is at least one element of F that is not an element of G

There is at least one element of F that is not an element of H

This will be incredibly helpful in finally finding our counterexample! We've boiled down all the essential parts of the claim and have restated the properties in a more intuitive way. The rest of the work is to just play around on some scratch paper and see what we can come up with. One approach is to draw a sort of "empty" Venn diagram, for F and G and H and their potential "overlaps", and then fill in enough elements so that the three above properties are satisfied.

The first condition requires the set F to "lie inside" both G and H, entirely; but, the second and third conditions require the existence of two elements of F, one of whom is not an element of G and the other of whom is not an element of H. That's all we need! A simple example, you might say, but an *effective* one, we say. Let's jump in and write up our disproof now:

Proof. The following claim is False:

For any sets F, G, H, if $F \subseteq G \cup H$, then either $F \subseteq G$ or $F \subseteq H$.

We will disprove it with a counterexample.

Define $F = \{1, 2\}$ and $G = \{1\}$ and $H = \{2\}$.

Notice that $G \cup H = \{1, 2\}$. Since $F = G \cup H$, then certainly $F \subseteq G \cup H$. Thus, the hypothesis of the claim holds true.

However, notice that $2 \in F$ but $2 \notin G$. Thus, $F \nsubseteq G$.

Likewise, notice that $1 \in F$ but $1 \notin H$. Thus, $F \nsubseteq H$.

Therefore, the claim is False. $\square$

One important lesson from this example is the following:

Tour counterexample does not have to be the most interesting or complicated one, nor do you somehow need to characterize all possible counterexamples. We just need to see one counterexample, and we need to see how it works.

That's it! This is exactly what we did in the above proof: we defined all of the important objects (the three sets F, G, H), and then we pointed out and described all the relevant properties they had. We did not leave it to the reader to check that the counterexample works; we showed them the details. We did not argue that some such sets exist somewhere out there in the universe; we defined them explicitly.

This is important, and we expect your counterexamples to have similar proof structure to ours above. Most of the work will go on "behind the scenes", before the proof starts, when you try to come up with your examples. Once you have it, though, just write it up much like we did.

3.9.5 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What is the definition of $\subseteq$? How do we use it to prove $A \subseteq B$?

(2) What does it mean for two sets to be equal?

(3) What is a *double-containment* proof?

(4) What is a *counterexample*?

(5) Suppose A, B, U are sets and $A, B \subseteq U$. Why can we prove $\overline{B} \subseteq \overline{A}$ to prove that $A \subseteq B$? Try to convince a friend that this is a valid technique.

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) First, **prove** the following claim:

> For any sets A, B, C, the subset relationship $A - (B - C) \subseteq (A - B) \cup C$ holds.

Second, find a *counterexample* to the claim that those sets are actually always *equal*.

(2) Suppose A, B, C are sets and $A \subseteq B$. Prove that $A \times C \subseteq B \times C$.

(3) Suppose $A \subseteq C$ and $B \subseteq D$. Prove that $A \times B \subseteq C \times D$.

(4) Let $A = \{x \in \mathbb{R} \mid x^2 > 2x + 8\}$ and $B = \{x \in \mathbb{R} \mid x > 4\}$. For each of the following claims, either *prove* it is correct or provide a *counterexample* to show it is False.

(a) $A \subseteq B$
(b) $B \subseteq A$

(5) Let A, B, U be sets with $A, B \subseteq U$. Prove that $A - B = A \cap \overline{B}$ by a *double-containment argument.*

(6) Let $S = \{x \in \mathbb{R} \mid -2 < x < 5\}$ and $T = \{x \in \mathbb{R} \mid -4 \leq x \leq 3\}$. What is $S \cap \overline{T}$, in the context of $\mathbb{R}$? Identify a set and then *prove* it is correct, using a double-containment argument.

(7) **Prove** the following claim: If $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

(8) For every $n \in \mathbb{N}$ let $S_n = \left\{x \in \mathbb{R} \mid -\frac{1}{n} < x < \frac{1}{n}\right\}$. Prove that

$$\bigcap_{n \in \mathbb{N}} S_n = \{0\}$$

(9) Let $I = \{x \in \mathbb{R} \mid 0 < x < 1\}$. For every $x \in I$, define $S_x = \{y \in \mathbb{R} \mid x < y < x + 1\}$. Prove that

$$\bigcup_{x \in I} S_x = \{z \in \mathbb{R} \mid 0 < z < 2\}$$

(10) For every $n \in \mathbb{N}$, define the sets A_n and B_n by

$$A_n = \left\{x \in \mathbb{R} \mid 0 \leq x < \frac{n-1}{n}\right\}$$
$$B_n = \left\{y \in \mathbb{R} \mid -\frac{1}{n} < y < 1\right\}$$

Prove the following set equality by a double-containment argument:

$$\bigcup_{n \in \mathbb{N}} A_n = \bigcap_{n \in \mathbb{N}} B_n$$

3.10 Summary

This was our first foray into some abstract conepts and results. We introduced the notion of a **set**, motivating it via several examples. We discussed the key relationships of being an **element** and being a **subset**, and pointed out how important is to distinguish the two! (Keeping the "Bag Analogy" in mind might help you in this regard.) We also discussed some notation, included *set-builder* notation. As we continue to move into more abstract mathematics, using correct, formal notation will be more important than ever to ensure that we are properly expressing our ideas. One key idea that came up is the notion of the *power set*, which represents a place where the *element* and *subset* relationships are both at work.

A discussion of set *operations* showed us how to combine sets and create new ones. All of these operations will be used throughout the remainder of our work in this book. We also showed how these operations can be *indexed*. This allows us to use shorthand to write a union of several sets using just a few definitions and symbols. Again, these ideas will re-appear quite often throughout our work, so we will present many exercises relating to these ideas; we encourage you to attempt and work through as many as you can!

We saw a proof technique relating to sets: namely, **double-containment arguments**. This is a fundamental proof technique in mathematics. You will see us use it often, and you will find it appearing in other courses and studies, as well.

A couple of discussions came up that allowed us to touch upon some profound ideas in abstract set theory, although we couldn't completely dive into them. For one, *Russell's Paradox* showed us that there is no "set of all sets". For another, we talked about how the natural numbers can be formally defined in terms of *sets*. In practice, we won't use this definition, and will continue to rely on our intuitions about $\mathbb{N}$. However, we hope it was interesting and somehow informative to read such a discussion.

3.11 Chapter Exercises

These problems incorporate all of the material covered in this chapter, as well as any previous material we've seen, and possibly some assumed mathematical knowledge. We don't expect you to work through **all** of these, of course, but the more you work on, the more you will learn! Remember that you can't truly *learn* mathematics without *doing* mathematics. Get your hands dirty working on a problem. Read a few statements and walk around thinking about them. Try to write a proof and show it to a friend, and see if they're convinced. Keep practicing your ability to take your thoughts and *write* them out in a clear, precise, and logical way. Write a proof and then edit it, to make it better. Most of all, just keep *doing* mathematics!

Short-answer problems, that only require an explanation or stated answer without a rigorous *proof*, have been marked with a ►.

Particularly challenging problems have been marked with a ★.

Problem 3.11.1. ► For each of the following statements about elements and subsets, state whether it is True or False. Be prepared to defend your choice to a skeptical friend!

Throughout this problem, we will use the following definitions:

$$\begin{aligned} A &= \{x \in \mathbb{Z} \mid -3 \le x \le 3\} \\ B &= \{y \in \mathbb{Z} \mid -5 < y < 6\} \\ C &= \left\{x \in \mathbb{R} \mid x^2 \ge 9\right\} \\ D &= \{x \in \mathbb{R} \mid x < -3\} \\ E &= \{n \in \mathbb{N} \mid n \text{ is even }\} \end{aligned}$$

(a) $A \subseteq B$

(b) $C \cap D = \varnothing$

(c) $4 \in E \cap B$

(d) $\{4\} \subseteq A \cap E$

(e) $10 \in C - D$

(f) $A \cup B \supseteq C$

(g) $3 \in A \cap C$

(h) $0 \in (A - B) \cup D$

(i) $E \cap C \subseteq \mathbb{Z}$

(j) $0 \notin B - C$

Problem 3.11.2. ► Let $m, n \in \mathbb{N}$. Suppose $m \leq n$. Explain why $\mathcal{P}([m]) \subseteq \mathcal{P}([n])$.

Problem 3.11.3. Look back at Problem 7 in Section 3.9. We proved that whenever two sets satisfy $A \subseteq B$, then they must also satisfy $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Read through that proof, too, to remind yourself of the details.

Now, does this claim "work the other way"? That is, suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Can you prove that $A \subseteq B$ is also true? Or can you find an example where this is not true?

Problem 3.11.4. Rewrite the following sentences using the "set-builder notation" to define a set. Then, if possible, **write out** all the elements of the set, using set braces; if not possible, explain why not and write out **three** example elements of the set.

(a) Let A be the set of all natural numbers whose squares are less than 39.

(b) Let B be the set of all real numbers that are roots of the equation $x^2 - 3x - 10 = 0$.

(c) Let C be the set of pairs of integers whose sum is non-negative.

(d) Let D be the set of pairs of real numbers whose first coordinate is positive and whose second coordinate is negative and whose sum is positive.

Problem 3.11.5. Define the following sets:

$$A = \left\{x \in \mathbb{R} \mid x^2 - x - 12 > 0\right\}$$
$$B = \{y \in \mathbb{R} \mid -3 < y < 4\}$$

Prove that $A = B$.

Problem 3.11.6. Let X be the set of students at your school.

Identify a property $P(x)$ such that $A := \{x \in X \mid P(x)\}$ is a proper subset of X and $A \neq \varnothing$.

Then, identify a property $Q(x)$ such that $B := \{x \in X \mid Q(x)\}$ is a proper subset of A (i.e. $B \subset A$) and $B \neq \varnothing$.

Problem 3.11.7. Let A, B, and C be sets with $A \subseteq C$ and $B \subseteq C$.

(a) Draw a Venn diagram for the sets $\overline{A} \cap \overline{B}$ and $\overline{(A \cap B)}$.

(b) Prove that $\overline{A} \cap \overline{B} \subseteq \overline{(A \cap B)}$.

(c) Define specific sets A, B, C such that the containment is *strict*, i.e. $\overline{A} \cap \overline{B} \subset \overline{(A \cap B)}$

(d) Define specific sets A, B, C such that $\overline{A} \cap \overline{B} = \overline{(A \cap B)}$.

Problem 3.11.8. Let $S = \left\{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid m = n^2\right\}$. How does S compare to the set $T = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid n = m^2\}$? If one is a subset of the other, prove it. If not, provide examples to show this.

Problem 3.11.9. Let (a,b) be a point on the Cartesian plane, i.e. $(a,b) \in \mathbb{R} \times \mathbb{R}$. Let ε (the Greek letter *epsilon*) be a nonnegative real number, i.e. $\varepsilon \in \mathbb{R}$ and $\varepsilon \geq 0$.

Let $C_{(a,b),\varepsilon}$ be the set of real numbers that are "close" to (a,b), defined as follows:

$$C_{(a,b),\varepsilon} = \left\{(x,y) \in \mathbb{R} \times \mathbb{R} \mid \sqrt{(x-a)^2 + (y-b)^2} < \varepsilon\right\}$$

1. Come up with a geometric description of the set $C_{(a,b),\varepsilon}$.

   What happens to the set as we change a and b?

   What happens as we change ε?

2. What is $C_{(0,0),1} \cap C_{(0,0),2}$?

3. What is $C_{(0,0),1} \cup C_{(0,0),2}$?

4. What is $C_{(0,0),1} \cap C_{(2,2),1}$?

Problem 3.11.10. Consider the (false!) claim that

$$\bigcup_{n \in \mathbb{N}} \mathcal{P}([n]) = \mathcal{P}(\mathbb{N})$$

(a) What is wrong with the following "proof" of the claim? Point out any error(s) and explain why it/they ruin the "proof".

> First, we will show that
>
> $$\bigcup_{n \in \mathbb{N}} \mathcal{P}([n]) \subseteq \mathcal{P}(\mathbb{N})$$

Consider an arbitrary element X of the union on the left.

By the definition of an indexed union, we know there exists some $k \in \mathbb{N}$ such that $X \subseteq [k]$.

Since $[k] \subseteq \mathbb{N}$, and $X \subseteq [k]$, we deduce that $X \subseteq \mathbb{N}$.

Thus, $X \in \mathcal{P}(\mathbb{N})$.

Second, we will prove the "$\subseteq$" relationship holds in the other direction, as well.

Consider an arbitrary $Y \subseteq \mathbb{N}$.

By the definition of subset, and the fact that Y is a set of natural numbers, we know there exists some $\ell \in \mathbb{N}$ such that $Y \subseteq [\ell]$.

By the definition of indexed union, we know $Y \in \bigcup_{n \in \mathbb{N}} \mathcal{P}([n])$.

Since we have shown $\subseteq$ and $\supseteq$, we know the two sets are equal.

(b) Disprove the claim by defining an **explicit** example of a set S such that

$$S \in \mathcal{P}(\mathbb{N}) \qquad \text{and} \qquad S \notin \bigcup_{n \in \mathbb{N}} \mathcal{P}([n])$$

Problem 3.11.11. Let $A = [3] \times [4]$. (Remember that $[n] = \{1, 2, 3, \ldots, n\}$.)

Let $B = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq 3x - y + 1 \leq 9\}$.

(a) **Prove** that $A \subseteq B$.

(b) Is it true that $A = B$? Why or why not? **Prove** your claim.

Problem 3.11.12. Let $n \in \mathbb{N}$ be a fixed natural number. Let $S = [n] \times [n]$. Let T be the set

$$T = \big\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq nx + y - (n + 1) \leq n^2 - 1\big\}$$

Prove that $S \subseteq T$ but $S \neq T$.

Problem 3.11.13. Suppose A and B are sets.

(a) **Prove** that

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$$

(b) Provide an **explicit** example of A and B where the containment in (a) is **strict**.

Problem 3.11.14. Let S and T be sets whose elements are sets, themselves. Suppose that $S \subseteq T$.

Prove that

$$\bigcup_{X \in S} X \subseteq \bigcup_{Y \in T} Y$$

Problem 3.11.15. Let A, B, C, D be sets.

(a) **Prove** that
$$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$$

(b) Provide an **explicit** example of A, B, C, D where the containment in (a) is **strict**.

Problem 3.11.16. Let A, B, C be sets. Prove that
$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$
and
$$A \times (B - C) = (A \times B) - (A \times C)$$

Problem 3.11.17. Let X, Y, Z be sets. Prove that $(X \cup Y) - Z \subseteq X \cup (Y - Z)$ but equality *need not* hold.

Problem 3.11.18. Find an example of a set S such that $S \in \mathcal{P}(\mathbb{N})$ and S contains exactly 4 elements.

Then, find an example of a set T such that $T \subseteq \mathcal{P}(\mathbb{N})$ and T contains exactly 4 elements.

Problem 3.11.19. Find examples of sets R, S, T such that $R \in S$ and $S \in T$ and $R \subseteq T$ but $R \notin T$.

Problem 3.11.20. Identify what each of the following sets are, and **prove** your claims.
$$\bigcap_{n \in \mathbb{N}} [n] \qquad \text{and} \qquad \bigcup_{n \in \mathbb{N}} [n]$$

Problem 3.11.21. Let $I = \{-1, 0, 1\}$. For each $i \in I$, define $A_i = \{i-2, i-1, i, i+1, i+2\}$ and $B_i = \{-2i, -i, i, 2i\}$.

(a) Write out the elements of $\bigcup_{i \in I} A_i$.

(b) Write out the elements of $\bigcap_{i \in I} A_i$.

(c) Write out the elements of $\bigcup_{i \in I} B_i$.

(d) Write out the elements of $\bigcap_{i \in I} B_i$.

(e) Use your answers above to write out the elements of $\left(\bigcup_{i \in I} A_i\right) - \left(\bigcup_{i \in I} B_i\right)$.

(f) Use your answers above to write out the elements of $\left(\bigcap_{i \in I} A_i\right) - \left(\bigcap_{i \in I} B_i\right)$.

(g) Write out the elements of $\bigcup_{i \in I}(A_i - B_i)$. How does this compare to your answer in (e)?

(h) Write out the elements of $\bigcap_{i \in I}(A_i - B_i)$. How does this compare to your answer in (f)?

Problem 3.11.22. In this problem, we are going to "prove" the existence of the negative integers! We say "prove" because we won't really understand what we've done until later but, trust us, it's what we're doing.

Because of this goal, you cannot **assume** any integers strictly less than 0 exist, so your algebraic steps, especially in part (d), should not involve any terms that might be negative.

That is, if you consider an equation like

$$x + y = x + z$$

we **can** deduce that $y = z$, by subtracting x from both sides, since $x - x = 0$.

However, if we consider an equation like

$$x + y = z + w$$

we **cannot** deduce that $x - z = w - y$. Perhaps $y > w$, so $w - y$ does not exist in our context ...

Let $P = \mathbb{N} \times \mathbb{N}$. Define the set R by

$$R = \{((a, b), (c, d)) \in P \times P \mid a + d = b + c\}$$

(a) Find three different pairs (c, d) such that $((1, 4), (c, d)) \in R$.

(b) Let $(a, b) \in P$. Prove that $((a, b), (a, b)) \in R$.

(c) Let $((a, b), (c, d)) \in R$. Prove that $((c, d), (a, b)) \in R$, as well.

(d) Assume $((a, b), (c, d)) \in R$ and $((c, d), (e, f)) \in R$.

Prove that $((a, b), (e, f)) \in R$, as well.

3.12 Lookahead

Now that we've introduced sets, defined them, seen many examples, and talked about operations and how to manipulate sets, it's time to move on to logic. We've already previewed some important logical ideas, specifically in Section 3.9 on how to write **proofs** about sets. In the next Chapter, we will make all of these logical ideas more formal, explicit and rigorous. We will develop some notation and grammar that will help us express logical ideas more precisely and concisely. We will use these to express our mathematical thoughts in a common language and communicate our ideas with others. In short, we will be able to confidently talk and write about mathematics!

Chapter 4

Logic: The Mathematical Language

4.1 Introduction

We are moving on to learn about the language of mathematics! We will learn how to express our ideas formally and precisely and concisely. This will require learning some new terminology and notation, all the while thinking and writing in a more formal way. Ultimately, this will allow us to solve problems and write good, clear, and correct mathematical **proofs**.

4.1.1 Objectives

The following short sections in this introduction will show you how this chapter fits into the scheme of the book. They will describe how our previous work will be helpful, they will motivate why we would care to investigate the topics that appear in this chapter, and they will tell you our goals and what you should keep in mind while reading along to achieve those goals. Right now, we will summarize the main objectives of this chapter for you via a series of statements. These describe the skills and knowledge you should have gained by the conclusion of this chapter. The following sections will reiterate these ideas in more detail, but this will provide you with a brief list for future reference. When you finish working through this chapter, return to this list and see if you understand all of these objectives. Do you see why we outlined them here as being important? Can you define all the terminology we use? Can you apply the techniques we describe?

By the end of this chapter, you should be able to . . .

- Define variable propositions using proper notation.

- Define mathematical statements using quantifiers and other proper notation, and characterize sentences that are not proper mathematical statements.
- Understand and explain the difference between two types of quantifiers, as well as how they are used.
- Define and understand the meanings of several logical connectives, as well as use them to define more complicated mathematical statements.
- Apply proof techniques to create formal arguments that demonstrate the truth of a mathematical statement.
- Compare and contrast different types of proof techniques, as well as understand when and how to use them, depending on the situation.

4.1.2 Segue from previous chapter

We introduced sets to have some standard, fundamental mathematical objects to work with. You probably noticed, though, that we used a lot of phrases like "If ..., then ..." and "for *every*" and "there *exists*" and "for *at least one*" and "and" and "or" and True and False and so on and so forth ... We relied on your intuitive understanding, and previous knowledge, of these concepts. As a living, breathing human being who converses with others, you have some kind of understanding of what **logic** is. Our goal now is to build upon those intuitions, and help you learn to read and write and speak mathematics.

4.1.3 Motivation

In mathematics, we are interested in identifying True claims and subsequently explaining to others *how* and *why* we know those claims are True. Thus far, we have already presumed some familiarity with logical terminology and truth. For instance, look back at the assumptions of the PMI (Principle of Mathematical Induction, Theorem 3.8.5). We needed to know that *if* $P(k)$ is true *then* $P(k+1)$ is true. What does this mean? What does this say about how the statements $P(k)$ and $P(k+1)$ are connected? What does it even mean for something to be True?!?!

Our goals for this section are many, but the major emphasis is on defining and identifying what types of statements in mathematics are meaningful and interesting. Once we do that, we can figure out how to express those statements in concise and precise terms. Ultimately, we will learn how to apply general techniques to **prove** that those statements are True (or False, as the case may be).

4.1.4 Goals and Warnings for the Reader

Keep this in mind throughout this chapter:

You are learning a **language**.

Some of this material will seem difficult, some will seem boring, and some might seem both! But this is all essential.

Have you ever learned another language? Think back to a foreign language class you took in school, perhaps. How did you start? We bet that you didn't jump right in and try to write beautiful poetry. You learned the basic grammar and syntax and vocabulary. You learned important articles, like "the" and "an". You learned basic verbs like "to be" and "to have" and how to conjugate them. You learned some common nouns, like "apple" and "dog" and "friend". From there, you started to piece phrases together and, over time, you learned to create more complex sentences from all of the tools you developed. All along, you probably had some great ideas for wonderful sentences in mind, but you just didn't know how to express them in your new language until you learned the necessary words and grammar.

We will be doing exactly this in the current chapter, but here our language is **mathematics**. You might have some great ideas for wonderful mathematical sentences in mind, but you just aren't sure how to express them. Interestingly enough, as well, we've already been "speaking" a lot of mathematics with each other! We've solved some puzzles, we introduced a proof technique (induction), and we worked with some building blocks of mathematical objects (sets); all along, we've made sure that we've understood each other, being verbose with our writing and explaining lots of details. In a way, we've been communicating without setting down a common language. This is a lot like how you'd survive in a foreign country without knowing the language: you'd use a lot of hand gestures and charades, you'd try to listen to others speak and pick up some key words, you'd draw pictures and make noises, and so on. This is all well and good if you're just on a week-long vacation, say, but if you're going to *live* there, you'll have a lot more work ahead of you.

This is precisely the situation we face now. We'd like to inhabit this world of mathematics, so we need to settle down and really learn the language of its people. Once we get through that, we'll feel more at home, like native speakers. Then, we can maybe be a little less careful with our words and grammar, use some slang or abbreviations or common idioms. (Think of some English examples of phrases and sentences that technically make no sense, grammatically or in terms of vocabulary, but are still understood by your fellow speakers.) But only then can we do so.

In the meantime, we will be much more formal and pedantic with our language. *If we don't force ourselves to do this now, we won't truly all speak the same mathematical language.*

4.2 Mathematical Statements

Our first step is to discuss what types of sentences are even reasonable to consider as mathematical truths that need to be proven or disproven. Completing this step is actually quite difficult! Many authors tend to gloss over this subject or offer a simple definition that ignores the many subtleties of mathematical language and logic. We feel tied, as well, because the time and space provided in this book/course are not sufficient to properly study the field of abstract logical theory. We encourage you to investigate some books or websites that contain relevant information. For the current context, we will have to sweep many details under the rug, so to speak. Suffice it to say, though, there is a very deep, rich, and fruitful field of mathematical research concerning exactly what we will be discussing here in a more heuristic way.

Remember that we mentioned we will have to assume the existence of the real numbers $\mathbb{R}$ and their usual arithmetic properties. Likewise, we will assume many of the results and concepts of mathematical logic, often without even realizing it (until we point it out for you). These details can be studied more in-depth later on in your mathematical careers.

4.2.1 Definition

For now, let us discuss what we mean by a **mathematical statement**. We want this term to encapsulate the kinds of "things" that we can prove or disprove.

Mathematics is unique among the sciences in that the results of this field are **proven** rigorously, and not hypothesized and then "confirmed" via laboratory experiments or real-world observations. In mathematics, we assume a set of common **axioms** and then follow rigorous logical inferences to deduce truths from these axioms (and from other truths we have proven thus far). If we encounter a falsity, we would have to show or demonstrate that it is, indeed, False.

With these ideas in mind, we can now consider and agree on several examples of what such a **mathematical statement** or **proposition** could be. (We have even proven a few already!) For instance, the sentence

> For any real numbers $x, y \in \mathbb{R}$, the inequality $2xy \leq x^2 + y^2$ holds.

is a valid mathematical statement. In fact, it is True, and we will prove it later on in Section 4.9.2. (It is sometimes referred to as the *AGM Inequality*, short for the *Arithmetic-Geometric Mean Inequality*.) We should point out that the word "holds" is often used in mathematics to mean "holds true" or "is a true statement".

Here's another example of a mathematical statement:

> For any sets S, T, U, if $S \cap T \subseteq U$ then $S \subseteq U$ or $T \subseteq U$.

This statement, however, is False, as the following **counterexample** demonstrates:

> Let $S = \{1, 2, 3\}$ and $T = \{2, 3, 4\}$ and $U = \{2, 3, 5\}$.
>
> Observe that $S \cap T = \{2, 3\} \subseteq U$ but $S \nsubseteq U$ and $T \nsubseteq U$.

Why does this example *disprove* the statement? Do you understand? Can you explain it? We will discuss that in more detail later on in this chapter, but we hope that, for now, we all somehow recognize that this example accomplishes exactly that.

We can also agree that a sentence like

Why do we have class at 9:00 am?!

is definitely *not* a mathematical statement. It's a perfectly valid English sentence, but it is not meaningful, mathematically speaking: we can't *prove* or *disprove* it.

Likewise, the sentence

$x^2 - 1 = 0$

is *not* a mathematical statement, despite being composed entirely of mathematical symbols. The problem is that we cannot verify whether it is True or False purely from axioms and logical inferences. This statement *depends* on x, whatever that value is (i.e. x is a **variable**) and without imposing extra assumptions about it, we cannot declare whether this sentence is True or False. This type of sentence will be referred to later as a **variable proposition**: its truth depends on a variable inside the sentence.

All of these observations and examples/non-examples motivate the following definition:

Definition 4.2.1. *A* **mathematical statement** *(or* **proposition** *or* **logical statement***) is a grammatically correct sentence (or string of sentences), composed of English words/symbols and mathematical symbols that has* exactly *one truth value, either* True *or* False*.*

4.2.2 Examples and Non-examples

By "grammatically-correct" we mean that the words and symbols contained in the sentence are used and combined correctly and make sense. This eliminates strings of symbols/words that are nonsensical when placed together, like

$1+ = 2$, $\text{Brendan}^2 = 1$, $\{\{\varnothing\}\} - 7 > 5\pi$, You am smart

For instance, the third one above is not a mathematical statement because $\{\{\varnothing\}\}$ is not a number, so we don't know how to interpret "subtracting 7" from that set.

By "has *exactly* one truth value", we mean that the statement should be either True or False, but certainly cannot be both or neither or something else in between. This eliminates the "$x^2 - 1 = 0$" example above, because it has no truth value. (Without a declaration of what x is, we cannot decide, either way.)

Not Knowing the Truth Value

One strange/interesting/complicated aspect of our definition is that we might not know the truth value for a given statement, even though we can be sure that there is *only* one such value. By way of illustration, consider the following statement:

> Any even natural number greater than or equal to 4 can be written as the sum of two prime numbers.

Is this statement True or False? If you have a proof or disproof, then the world of mathematics would love to see it! The statement above is known as the **Goldbach Conjecture** and it is a very famous unsolved (for now, we hope!) problem in mathematics. Nobody knows yet whether the claim is True or False, but it is certainly the case that *only one* of those truth values applies. That is, this statement cannot be both True and False, nor can it somehow be somewhere in between. Either all even natural numbers greater than or equal to 4 *do* have the stated property, or there is at least one that does *not* have the property. We can state this "either/or" property even without yet knowing which of the two possibilities is the correct one. As such, this sentence *does* actually satisfy our definition of *mathematical statement*.

(Terminology note: In general, a **conjecture** is a claim that someone believes to be true but has not yet been proven/disproven.)

Paradoxical Sentences

One way to have a sentence that does *not* have a truth value is to create a **paradox**. Consider this sentence:

> This sentence is False.

Pretty weird, right? The sentence itself is asserting something about its own truth value. Let's try to analyze what truth value it has:

- Let's say the sentence is True. Then, the sentence itself tells us that it is, in fact, False.
- Let's say the sentence is False. Similarly, then, the sentence tells us that it is, in fact, True.

This cannot work! This sentence is somehow both True and False at the same time, or somehow neither, or ... Whatever it is, it's a bad idea. We do *not* want to deal with strangeness like this in mathematics, so our definition disallows this sentence as a mathematical statement.

(*Question:* What happens if you *do* allow sentences like this to be proper mathematical statements? What if you don't adhere to the principle that every sentence we care about must be either True or False? Think about it! Is this somehow *wrong*, or is it just a different mathematical universe? ...)

In general, **self-referential** sentences like the one above (that is, sentences that make reference to themselves) are quite bizarre and can produce some paradoxes that we want to disallow.

A variant of the above paradoxical claim is given in a cartoon drawing, wherein Pinocchio says, "My nose will grow now!" Does it then grow? If he's telling the truth, then it will grow, but that only happens when he's lying! If he's lying, then his nose will grow (by definition), but then his statement is actually true! Yikes!

Source: http://www.the-drone.com/magazine/wp-content/uploads/2010/04/BLA6.jpg

An even stranger example of this phenomenon is *Quine's Paradox*:

> "Yields falsehood when preceded by its quotation" yields falsehood when preceded by its quotation.

We'll let you think about that one on your own. Suffice it to say that paradoxical claims like this are too ill-behaved for us to worry about. This is why our definition outlaws them.

4.2.3 Variable Propositions

Other examples of sentences that are not mathematical statements are sentences that involve **unquantified variables**. For instance, take the sentence

> " $x^2 - 1 = 0$ "

This is certainly grammatically correct and we can make sense of it, but what is its truth value? We don't know! If $x = 1$, then the sentence is True, but if $x = 8$, it is False, and if $x = \mathbb{N}$ or $x =$ Brendan, then the sentence doesn't even make sense! As such, we want to disallow sentences like this, as well. These types of sentences are useful and common, though; we will call them **variable propositions** because they make a claim that *depends* on some variable.

In the case of the above sentence, we might define $P(x)$ to be the variable proposition "$x^2 - 1 = 0$". We would usually write this declaration as

> Let $P(x)$ be the statement "$x^2 - 1 = 0$".

It is common to use capital letters to denote variable propositions and mathematical statements, and lowercase letters to denote the variables contained therein. (This is not a *requirement*, though, merely a common convention.)

With this variable proposition now defined, we can create proper mathematical statements by *assigning* particular values to the variable x in the expression. We can say that $P(1)$ is True and $P(0)$ is False. We can also make **quantified** claims about $P(x)$. For instance, we claim that the following sentence is a True mathematical statement:

> There exists an $x \in \mathbb{R}$ such that the proposition $P(x)$ is True.

whereas the following sentence is a False mathematical statement:

> For every $x \in \mathbb{R}$, the proposition $P(x)$ is True.

Think about why these statements have the truth values we have claimed. Can you see why they are mathematical statements to begin with? How would you *prove* these claims?

Defining Variable Propositions

Notice the format we used to define variable propositions, like the one above: (1) We give the proposition a letter name (like P); (2) we indicate its dependence on some number of variables, each of which has a letter (like x and y); (3) we put quotes around the actual proposition itself; and (4) we don't include any new letters that have no meaning within the context of the proposition.

This format has been chosen carefully because it is precise and unambiguous. It assigns a meaning to every letter in the proposition and clearly distinguishes what is and isn't part of the proposition.

For example, the following are **BAD** "definitions" of variable propositions. We will give you some reasons as to why they are bad and provide some proper amendments of the propositions.

- Let $Q(y)$ be the proposition "$x < 0$".

  Reason: What is x? Where is y? We have *no idea* what x is, inside the context of the proposition, so this is a poor definition.

  If we had said

  > Let $Q(x)$ be the statement "$x < 0$".

  that would have been perfect. The variable inside the parentheses is the one that appears in the statement in quotes later. Great.

- Let $P(x)$ be the proposition $x^2 \geq 0$, for every $x \in \mathbb{R}$.

  Reason: Does the writer of this sentence want to assert that $x^2 \geq 0$, no matter what $x \in \mathbb{R}$ is? Is that phrase "for every $x \in \mathbb{R}$" meant to be *part* of the proposition, or not?

  If we interpret this to mean that $P(x)$ is defined as "$x^2 \geq 0$", and this definition is made for every $x \in \mathbb{R}$, then ... okay, that might be reasonable.

  However, if we interpret this to mean that $P(x)$ is defined as "$x^2 \geq 0$ for every $x \in \mathbb{R}$" then ... well, this is certainly *different*. In fact, it's not even a properly-defined proposition! The proposition $P(x)$ should *depend* on the input value x, but it shouldn't be allowed to *change* or further *quantify* that variable *inside* the proposition!

The way this proposition was originally written, there are two possible interpretations and they are very different. Accordingly, this is a poor definition.

If we had said,

> Let $P(x)$ be the statement "$x^2 \geq 0$", defined for every $x \in \mathbb{R}$.

that would have been fine. As we mention below, as well, we don't technically have to tell the reader which values of x we want the proposition defined for. Perhaps this is just some helpful information to include, though, so it doesn't hurt.

- Let $T(x, y) =$ "$x^2 - 7 = y$".

  Reason: Ugh! What does "=" mean in this context? That symbol applies when we wish to compare two *numbers* and say they are *equal* in value (or two *sets* and say they are equal in terms of their elements). The object $T(x, y)$ is meant to be a *mathematical statement*, something that is either True or False. Thus, it does not have a numerical value to compare with anything else.

  Likewise, given a value for x and y, the statement "$x^2 - 7 = y$" is either True or False, so it makes no sense to say that equation "equals" something else. It has a truth value, not a numerical value.

  If we had said,

  > Let $T(x, y)$ be "$x^2 - 7 = y$".

  that would have been perfect.

Okay, that's enough *non*-examples for now. We don't want to put any bad ideas in your head, really! However, from past experience, we know that these are common ways for students to write propositions (either accidentally, or without realizing *why* they're wrong), so we felt compelled to share.

One final note on variable propositions. It is not essential to say where the variables come from when defining a proposition. That can be filled in later when the proposition is invoked, or when a specific value of a variable is used or quantified. That is, we can make the definition

> Let $T(x, y)$ be "$x^2 - 7 = y$".

without needing to specify whether x and y are natural numbers, or integers, or complex numbers, or anything like that. Later on, we can say that $T(3, 2)$ is True and $T(\pi, -1)$ is False, and that $T(\varnothing, \mathbb{N})$ has *no meaning*, but we wouldn't need to somehow anticipate any of those interpretations when defining $T(x, y)$.

4.2.4 Word Order Matters!

The notion of **quantifying variables** is something we will discuss in detail in the very next section. For now, we want to consider one more striking example of a mathematical statement that illustrates the importance of **word order** in sentences. Analyzing the structure of sentences like the following will be a major goal of the following section, as well.

There is a real number y such that $y = x^3$ for every real number x.

What does this claim say? It says we can find a number $y \in \mathbb{R}$ such that $y = x^3$ is True, *no matter what* $x \in \mathbb{R}$ is. This is ridiculous! How can there be a single number that is the cube of *all* numbers? This sentence is, indeed, a mathematical statement, but it is decidedly False. But what about the following claim?

For every real number x there is a real number y such that $y = x^3$.

This one is True! Do you see the difference between the two sentences? They contain exactly the same words and symbols, but in a different order. Whereas the former sentence asserts that there is some number that is the cube of every real number (which is False), the latter asserts that every real number has a cube root, which is True. This example emphasizes the importance of word order.

4.2.5 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What are the important, defining properties of a mathematical statement?

(2) What is the difference between a mathematical statement and a variable proposition?

(3) Why is the Goldbach Conjecture a mathematical statement?

(4) What is wrong with the following attempt at defining a variable proposition?

Let $Q(x, y, z)$ be $7x - 5y + z$

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) For each of the following sentences, decide whether it is a **mathematical statement** or not. If it is, decide whether it is True or False. If it is not, explain why.

(a) $142857 \cdot 5 = 714285$

(b) For every $n \in \mathbb{N}$, $\sum_{k \in [n]} k = \frac{n(n+1)}{2}$.

(c) For any sets A and B, if $A \subseteq B$, then $B \subseteq A$.

(d) For any sets A and B, if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

(e) Math is cool.

(f) $1 + 2 = 0$

(g) For any $x, y \in \mathbb{Z}$, if $x \cdot y$ is even, then x and y are both even.

(h) For any $x, y \in \mathbb{Z}$, if x and y are both even, then $x \cdot y$ is even.

(i) $1 + = 2$

(j) $-5 + \mathbb{Z} \geq \pi$

(k) $x = 7$

(l) This sentence is not True.

(2) Look back through the first three chapters and identify some examples and non-examples of mathematical statements.

Can you also find any variable propositions? Are they written in the way we specified in this section? Can you amend them so that they are written properly?

(3) Write a proper definition of a variable proposition that is true when two inputted values have a non-negative sum.

Then, find two instances each of when the proposition is True and when it is False.

(4) Let S be the set $\{1, 2, 3, 6, 8, 10\}$.

(a) Write a proper definition of a variable proposition that inputs two variables and decides whether the absolute value of their difference is an element of S. Then, find two instances each of when the proposition is True and when it is False.

(b) Write a proper definition of a variable proposition that inputs two sets and determines whether their intersection is a subet of S. Then, find two instances each of when the proposition is True and when it is False.

(Note: Given any set X and any object x, it must be that either $x \in X$ or $x \notin X$.)

(5) Come up with another mathematical statement that is True but becomes False when we switch the order of some words. (See the example in the last subsection for some inspiration.)

(6) For each of the following attempts at defining a variable proposition, determine if it is correct or not. Note: This does not mean determine if it is True or False; rather, we want to know whether the statement is well-written and sensible.

If an attempt is incorrect for some reason, explain that reason and write a new statement that fixes that error.

(a) Let $P(x)$ be "$x > 1$".
(b) Let $Q(x)$ be the proposition "$x^2 - 1 > 0$".
(c) Let $R(a, b)$ be "$a^3 = b$", for every $a, b \in \mathbb{R}$.
(d) Let $P(x)$ be $x > 1$.
(e) Let $T(z) =$ "z is prime".
(f) Let $Q(x)$ be the proposition "$x^2 - 1 > 0$", for every $x \in \mathbb{R}$.
(g) For every $x \in \mathbb{R}$, let $Q(x)$ be "$x^2 - 1 > 0$".
(h) Let $S(a)$ be "$b^2 > 4$".
(i) Let $Q(x)$ be $x^2 - 1 > 0$ for every $x \in \mathbb{R}$.

4.3 Quantifiers: Existential and Universal

We will now introduce some convenient notation that allows us to shorten some statements we have seen so far and express wordy, language-based phrases with mathematical symbols. Another benefit of the forthcoming notation is that we will be able to more easily express and analyze mathematical statements. Specifically, we will now introduce the symbols "$\forall$" and "$\exists$".

Definition 4.3.1. *The symbol "$\forall$" stands for the phrase "**for all**".*

*The symbol "$\exists$" stands for the phrase "**there exists**".*

We call "$\forall$" the universal quantifier *and "$\exists$" the* existential quantifier*.*

A mathematical statement beginning with "$\forall$" is said to be "universally quantified", and one beginning with "$\exists$" is said to be "existentially quantified".

4.3.1 Usage and notation

Other common phrases that "$\forall$" replaces are "for every" and "for arbitrary" or "whenever" and "given any" and even "if".

Other common phrases that "$\exists$" replaces are "for some" and "there is at least one" and "there is" and even "some".

Example 4.3.2. Let's consider some simple examples first, to get our feet wet. In each case, we are looking to express a mathematical thought using these symbols, or trying to interpret a quantified statement in a more "wordy" way.

- "Every real number squared is non-negative."

  This is a straightforward statement that is, in fact, True. We would write it as:

  $$\forall x \in \mathbb{R} \,\bullet\, x^2 \geq 0$$

  The "big dot" separates the quantified part of the statement from the claim made about the variable x (which was introduced in the quantification).

  Another way to write this would be:

  > Define $S(x)$ to be "$x^2 \geq 0$". Then the claim is: $\forall x \in \mathbb{R} \,\bullet\, S(x)$.

- "There is a subset of $\mathbb{N}$ that has 7 as an element."

  This is an *existence* claim. It asserts that we can find an object with a particular property. We would write it as:

  $$\exists S \in \mathcal{P}(\mathbb{N}) \,\bullet\, 7 \in S$$

  Remember that $\mathcal{P}(\mathbb{N})$ is the *power set* of $\mathbb{N}$, the set of all subsets of $\mathbb{N}$; thus, saying $S \in \mathcal{P}(\mathbb{N})$ means $S \subseteq \mathbb{N}$, as desired.

- "Every integer has an *additive inverse* (i.e. a number that, when added to the original number, yields 0)."

  This idea of an "additive inverse" is a general concept that applies to some mathematical objects known as *rings* and *fields*. We won't discuss those objects in this book, but you will touch on them in any course on abstract algebra.

  We would write this claim as

  $$\forall a \in \mathbb{Z} \,\bullet\, \exists b \in \mathbb{Z} \,\bullet\, a + b = 0$$

  and we would read this aloud as

  > For any integer a, there exists an integer b such that $a + b = 0$.

  or perhaps

  > No matter what integer a we are given, we can find an integer b with the property that $a + b = 0$.

  Again, we could shorten the notation slightly by defining $I(a, b)$ to be "$a + b = 0$", and then writing the claim as

  $$\forall a \in \mathbb{Z} \,\bullet\, \exists b \in \mathbb{Z} \,\bullet\, I(a, b)$$

Example 4.3.3. Here are some examples of proper usage of "$\forall$", and some equivalent formulations of how to use this symbol.

- $\forall x \in \mathbb{R}.\ x^2 \geq 0$
- For all real numbers x, we have $x^2 \geq 0$.
- Every real number x satisfies $x^2 \geq 0$.
- Whenever x is a real number, we know $x^2 \geq 0$.

Likewise, here are some examples of proper usage, and equivalent formulations, of the symbol "$\exists$".

- $\exists x \in \mathbb{R}.\ x^2 - 4x + 4 = 0$
- There exists a real number x such that $x^2 - 4x + 4 = 0$.
- There is a real number x that satisfies $x^2 - 4x + 4 = 0$.
- Some real number x has the property taht $x^2 - 4x + 4 = 0$.

Reading Quantified Statements Aloud

Example 4.3.4. Now for some harder examples. Let's look back at the phrases we wrote at the end of the last section and express them using this new notation. Consider this statement:

> There is a real number y such that $y = x^3$ for every real number x.

To express thi in symbolic form, we will define $P(x, y)$ to be the proposition "$y = x^3$" and then write the statement as

$$\exists y \in \mathbb{R}.\ \forall x \in \mathbb{R}.\ P(x, y)$$

This is correct, logically-speaking, but it is rather terse. For now, we will sometimes rewrite the statement using some "helping words" to aid our reading of the statement. In particular, we would say such words when reading the sentence aloud, so by occasionally writing them here, we provide you with some extra practice in interpreting logical notation verbally. We would read the above statement aloud as

> There exists a real number y such that, for every real number x, the statement $P(x, y)$ holds.

The phrase "*such that*" is a "helper phrase" that links an existential quantification to the rest of the phrase. The next subsection contains some important information about when and how to use this helper phrase!

The "big dot" between the quantified parts of the statement above just serves to separate the pieces of the statement and make it easier to read. It corresponds to a pause or rest in speaking, like a comma, but sometimes it has a vocalized meaning (like the "such that" after the "$\exists y \in \mathbb{R}$" part).

We don't want to use commas, though, because we already use them for other meanings. For example, we write

$$x, y \in S$$

to mean "both x and y are elements of the set S". The "big dot" is just a different symbol to use.

Since our mathematical careers are still young, relatively speaking, we encourage you to sometimes write the helping phrases like "such that" and "holds True" to guide your understanding, whenever possible. This reminds you what the sentences mean and helps you practice reading and writing statements like this in such a condensed form. Remember that you are learning a *language* here and you need to practice *translating* sentences from one language you know (English) to another (mathematics). For instance, you might want to write out the line above as

$$\exists y \in \mathbb{R} \text{ such that } \forall x \in \mathbb{R} \centerdot\ P(x, y) \text{ is True.}$$

or, at least, say it this way in your head.

(By the way, when writing on a white/chalkboard or on paper, it's common to write "s.t." in place of "such that", to save a few moments of writing. That just goes to show how ubiquitous the phrase "such that" is in mathematical writing; we already have an agreed-upon abbreviation for it!)

4.3.2 The phrase "such that", and the order of quantifiers

Notice that the helping phrase "such that" always follows an *existential* quantification, and *only* such a quantification. This is because a claim with "$\exists$" asserts something about the existence of an object with a certain property, and the rest of the sentence is the description of that special property. Thus, "such that" makes sense and helps us read the sentence properly. Consider this mathematical statement:

$$\exists y \in \mathbb{R} \centerdot\ \forall x \in \mathbb{R} \centerdot\ P(x, y)$$

What would happen if we read it out loud but misplaced the phrase "such that" and used it after the "$\forall$" instead of the "$\exists$"? That would yield this sentence:

$$\exists y \in \mathbb{R} \quad \forall x \in \mathbb{R} \text{ such that } P(x, y) \text{ is True.}$$

We claim that this can be interpreted in two ways, *neither* of which is really the correct intended meaning, which is why we've written in red!

On the one hand, one might argue that such a sentence is *not* grammatical at all and has no meaning, because "such that" does not belong after a *universal* quantification. This amounts to just throwing up one's hands and saying, "I have no idea what you meant there!"

On the other hand, one might read into the sentence a little bit and argue that what the writer really meant was

$$\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, \text{ such that } P(x, y) \text{ is True.}$$

or, writing out the words,

There exists an $x \in \mathbb{R}$, for each $y \in \mathbb{R}$, such that $P(x, y)$ is True.

Here, the commas indicate an *inversion* of phrase order, as is common in English language. (For instance, consider the following sentence: "I laugh, at every episode of *30 Rock*, wholeheartedly." This is the same as saying "I laugh wholeheartedly at every episode of *30 Rock*.") This sentence would be equivalent, then, to writing

$$\forall x \in \mathbb{R}\,.\ \exists y \in \mathbb{R} \text{ such that } P(x, y) \text{ is True.}$$

This is *not* the same as the original mathematical statement we considered and, in fact, it is actually the *other* statement we saw in the previous section (see Section 4.2.4), which was False! Recall that the other statement was similar but the phrases were reversed:

> There is a real number x such that, for every real number y, we have $y = x^3$.

which we can symbolize as

$$\exists x \in \mathbb{R}\,.\ \forall y \in \mathbb{R} \text{ such that } P(x, y) \text{ is true}$$

Look at that! The misplacement of the phrase "such that" led to a reasonable linguistic interpretation of the sentence that has the exact opposite meaning as what was originally intended. Yikes! This is why we must be careful to use "such that" *always and only* after an **existential quantification**. Remember that we will not always write that helper phrase, so you must remember to use it properly when reading a sentence to yourself in your head, or out loud to others, to make sure you have the correct, intended interpretation.

The point of this example in the previous section was to point out how important *word order* is. Now that we have symbols to replace some words and phrases, we want to emphasize how important the order of those symbols is, as well. The two mathematical statements we see above contain the exact same words and symbols, but in a different order, and one is False whereas the other is True. Clearly, order is extremely important!

4.3.3 "Fixed" Variables and Dependence

While we are on the topic of order of quantifiers, we will also mention the following example to emphasize that the order of quantifiers dictates when to consider variables as **fixed** in an expression.

Consider the statement "Any even natural number greater than or equal to 4 can be written as the sum of two primes." (Recall that this is the famous **Goldbach Conjecture** we discussed in the previous section.) To express this statement logically and symbolically, we would write

Let X be the set of even natural numbers, except 2.

Let P be the set of prime numbers.

Define $Q(n, a, b)$ to be "$n = a + b$".

Then the claim is:

$\forall n \in X \centerdot \exists a, b \in P \centerdot Q(n, a, b)$

Notice that we used some shorthand here. A phrase like "$\exists a, b \in P$" really means "there exists some $a \in P$ and there exists some $b \in P$", and it would be perfectly acceptable to express the above statement instead as

$$\forall n \in X \centerdot \exists a \in P \centerdot \exists b \in P \centerdot Q(n, a, b)$$

When two variables are quantified as elements from the same set, though, and the quantifications follow one another immediately in a sentence, it is very common to combine them into one quantification. We might even see mathematical statements like,

$$\forall x, y \in \mathbb{Z} \centerdot \exists a, b, c, d \in \mathbb{Z} \centerdot a + b + c + d = x + y \text{ and } a + b \neq x \text{ and } c + d \neq y$$

(What is this statement asserting, by the way? Is it True or False? Does it depend on the context of $\mathbb{Z}$? What if we used $\mathbb{N}$ or $\mathbb{R}$ instead in both places?)

Quantification "Fixes" a Variable

Look back at the example above, where we defined $Q(n, a, b)$. The reason we brough up that example was to mention that the initial quantification "$\forall n \in X$" serves to *fix* a particular value of n that will be used for the rest of the statement. After that, the assertion that "$\exists a, b \in P$" with the subsequent property $Q(n, a, b)$ depends on that *fixed, but arbitrary,* value of n.

The statement, as a whole, is saying that no matter what n is chosen, we can find values a, b that satisfy the property Q. (Notice that those values of a, b might *depend* on n, of course.) However, the *order* of quantification is telling us that those values a, b might *depend* on the chosen n. This is what we want to emphasize.

As an example, consider a particular value of the variable n in the statement. We know $8 \in X$ because 8 is even and $8 \geq 4$. What happens when $n = 8$? Can you find $a, b \in P$ such that $a + b = 8$? Sure, we can use $a = 3$ and $b = 5$. Okay, what about when $n = 14$? Can you find $a, b \in P$ that satisfy $a + b = 14$? Surely, your choices now have to be *different* than before. This is what we mean when we say a and b *depend* on n. (By the way, *can* you find a and b in this case, with $n = 14$? We can think of a couple of choices that would work!)

To make sure you're understanding this discussion, think about the following question and answer it: What is the difference between the statement above and the following one?

$$\exists n \in X \centerdot \exists a, b \in P \centerdot Q(n, a, b)$$

Is this statement True or False? Why?

4.3.4 Specifying a quantification set

Another aspect of quantifiers we want to emphasize is that we must specify a *set* whenever we use quantifiers. The sentence

$$\forall x \centerdot\ x^2 \geq 0$$

may "look true" but it is, in fact, **meaningless**. What is x? Where does it come from? "For every x ..." from where? What if x is not a number?

We *need* to specify where the object x "comes from" so that we know whether $x^2 \geq 0$ is even a well-defined, grammatical phrase, let alone whether it is True. If we amend the sentence to say

$$\forall x \in \mathbb{R} \centerdot\ x^2 \geq 0$$

then this is a well-defined, grammatical (and True!) mathematical statement. However, if we amend the sentence to say

$$\forall x \in \mathbb{C} \centerdot\ x^2 \geq 0$$

then this is a well-defined yet False mathematical statement! This is because $i \in \mathbb{C}$ but $i^2 = -1 < 0$. (Remember, we will not make significant use of the set of complex numbers $\mathbb{C}$ in this book, but it makes for interesting and enlightening examples, like this.)

The main lesson here is that **context** really matters. It can change the meaning of a statement, as well as its truth value. For this reason, we must always be sure to specify a set from which we draw variable values.

One Exception

We sheepishly admit that there is one exception to this "always specify a quantification set" rule, but there's a good reason for the exception. Consider the following claim:

> For any sets A, B, C, the equality $(A \cup B) \cap C = (A \cap C) \cup (A \cap B)$ holds true.

This is a True mathematical statement. (Can you prove it? Try using a double-containment argument!)

How might we try to write this statement in symbolic form? This is a *universal* quantification ("for any ...") so we need to use a "$\forall$" symbol. The variables here (denoted by A and B and C) are *sets*. Where do they come from? What is the set of objects we would draw them from?

We're pretty sure you're tempted to say "the set of all sets". Right? That's a big problem, though! Remember our discussion in the previous chapter about Russell's Paradox? (See Section 3.3.5 to remind yourself.) That object—the collection of all possible sets—is *not*, itself, a set! Thus, we cannot write this statement symbolically as

$$\forall A, B, C \in \underline{\quad\quad} \centerdot\ (A \cup B) \cap C = (A \cap C) \cup (A \cap B)$$

because we don't know how to fill in the blank with a *set*.

Because of this issue, we will continue to use phrases like "For any sets $A, B, C\ \ldots$", instead of a symbolic form. When taking notes on your own, or working out a problem on scratch paper, feel free to write "$\forall A, B, C$" and know that it really represents a quantification of sets. However, when writing more formally (say, on written homework), you should stick to the phrasing used above.

4.3.5 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What is the difference between $\forall$ and $\exists$?

(2) How would you read the following statement out loud?

$$\forall x \in \mathbb{R}.\ \exists y \in \mathbb{R}.\ x = y^3$$

(3) Why is the following sentence **not** a proper mathematical statement?

$$\exists y.\ y + 3 > 10$$

What is the difference, if anything, between the following two statements?

$$\exists x \in \mathbb{N}.\ \exists y \in \mathbb{N}.\ x + y = 5$$

$$\exists x, y \in \mathbb{N}.\ x + y = 5$$

Are they True or False?

(4) What is the difference, if anything, between the following two statements?

$$\exists a, b \in \mathbb{Z}.\ a \cdot b = -3$$

$$\exists \heartsuit, \diamondsuit \in \mathbb{Z}.\ \heartsuit \cdot \diamondsuit = -3$$

Are they True or False?

(5) Why are the following sentences *not* properly quantified statements?

- $\exists x.\ x > 7$
- $\forall y \in \mathbb{Z}$
- $\forall z > 2.\ z^2 > 4$
- $\forall w \in \mathbb{Z}.\ w^2 = t.\ \exists t \in \mathbb{N}$

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Look back at Section 4.3.3 where we expressed the Goldbach Conjecture in symbolic notation. We defined X to be the set of all even natural numbers except 2.

Write a definition of X using symbols, with quantifiers and set builder notation (and perhaps set operations, depending on how you do it).

(2) Write an example of a mathematical statement that starts with a quantifier, and such that the statement is True if that quantifier is "$\exists$" but the statement is False if that quantifier is "$\forall$".

(3) Write an example of a variable proposition $P(x)$ such that

$$\forall x \in \mathbb{Z}.\ P(x)$$

is True but

$$\forall x \in \mathbb{N}.\ P(x)$$

is False.

(4) For each of the following mathematical statements, write it in symbolic form using quantifiers. (Be sure to properly define any variable propositions you might need, first!) Then, determine whether the statement is True or False.

(a) There is a real number that is strictly bigger than every integer.
(b) Each integer has the property that its square is less than or equal to its cube.
(c) Every natural number's square root is a real number.
(d) Every subset of $\mathbb{N}$ has the number 3 as an element.

(5) For each of the following quantified statements, say it out loud by reading the symbolic notation. Then, determine wheter the statement is True or False.

(a) $\forall x \in \mathbb{N}.\ \exists y \in \mathbb{Z}.\ x + y < 0$
(b) $\exists x \in \mathbb{N}.\ \forall y \in \mathbb{Z}.\ x + y < 0$
(c) $\exists A \in \mathcal{P}(\mathbb{Z}).\ \mathbb{N} \subset A \subset \mathbb{Z}$

(Recall that $\subset$ means "is a *proper* subset of".)

(d) Let P be the set of prime numbers.

$\forall x \in P.\ \exists t \in \mathbb{Z}.\ x = 2t + 1$

(e) $\forall a \in \mathbb{N}.\ \exists b \in \mathbb{Z}.\ \forall c \in \mathbb{N}.\ a + b < c$
(f) $\exists b \in \mathbb{Z}.\ \forall a, c \in \mathbb{N}.\ a + b < c$

4.4 Logical Negation of Quantified Statements

Let's return to those example statements we have used before. Define $P(x, y)$ to be "$y = x^3$" and then define Q_1 to be the statement

$$\text{“}\exists y \in \mathbb{R} \,.\, \forall x \in \mathbb{R} \,.\, P(x, y)\text{”}$$

and Q_2 to be

$$\text{“}\forall x \in \mathbb{R} \,.\, \exists y \in \mathbb{R} \,.\, P(x, y)\text{”}$$

Remember that Q_1 is False and Q_2 is True.

How is it that we *know* Q_1 is False? It says that there is some real number with a certain property. To declare the entire statement to be False, we might have to verify that the property does *not* hold for *every* real number y, but that would take a long time! The set $\mathbb{R}$ is infinitely large! A far more efficient approach is to show that the **negation** of this statement is True.

By "negation", we mean the **logical negation**, the statement that is the "opposite" of the original statement, in the logical sense. The logical negation of a mathematical statement has the exact opposite truth value as the original, so if we examine Q_1's negation and show it is True, then we have proven that Q_1 itself is False.

How do we negate this statement, though? We already had the right idea in mind when we noticed that we would somehow have to prove something about *every* real number y, since the original statement makes a claim of *existence*. In this section, we will explore how to properly negate statements like these.

We should note that there are some subtle, yet deep, mathematical concepts underlying what we have discussed thus far. Why is it that a mathematical statement is either True or False? Well, a cheeky (and completely correct, mind you) response would be, "Because you defined '**mathematical statement**' to be that way, silly!" Yes, indeed, we did, but *why* did we do so? What is it about the duality of True/False that is somehow *helpful* to mathematics, or *essential*? These are meaningful and difficult questions, and are definitely worth thinking about. Discussions of these topics will necessarily delve into the philoshophy of mathematics and human thought which are interesting and worthwhile pursuits, certainly, but beyond the scope and goals of this book/course. We will rely on our common, intuitive understandings of truth.

4.4.1 Negation of a universal quantification

In general, the negation of a universal (i.e. "$\forall$") claim is one of existence (i.e. "$\exists$"), and vice versa. Before we tackle the larger problem of negating any quantified statement, let's look at a simple case.

Assume S is a set and $R(x)$ is a mathematical statement, defined for every $x \in S$. The statement

$$\forall x \in S \,.\, R(x)$$

asserts the truth value of a variable proposition for *every* possible value of the variable x from the set S. It says that *no matter what* element x of the set S we are referring to, we can *necessarily* conclude that the proposition $R(x)$ is true. Now, how could this statement be False, and how could we *prove* that?

If it's False that every element $x \in S$ satisfies a certain property, it must be that *at least one* element does *not* satisfy that property. To prove this, we would be expected to produce such a value; we would have to define (i.e. identify) an element x and explain why $R(x)$ does not hold for that particular element. (Think about how we understand this negation linguistically. We do this all the time in everyday language without even thinking about it.) The conclusion, then, is that the negation of the original statement is

$$\exists x \in S \text{ such that } R(x) \text{ is } \mathsf{False}$$

We now introduce the notational symbol $\neg$ to mean **"logical negation"** or **"not"**. With this in hand we can rewrite the negated statement

$$\neg\big(\forall x \in S \,\centerdot\, R(x)\,\big)$$

as

$$\exists x \in S \,\centerdot\, \neg R(x)$$

The concluding phrase of that statement, $\neg R(x)$, could be simplified, depending on what $R(x)$ is.

For instance, if $S = \mathbb{R}$ and $R(x)$ is "$x^2 \geq 0$", then the negated statement would read

"$\exists x \in \mathbb{R}$ such that $x^2 < 0$"

since "$x^2 < 0$" is logically equivalent to "$\neg(x^2 \geq 0)$".

In general, though, we must leave it as "$\neg R(x)$" without knowing anything further about the proposition R. We will also point out that, in general, the phrases "$R(x)$ is False" and "$\neg R(x)$ is True" are logically equivalent; they both assert that the proposition $R(x)$ is not true.

This notion we are developing right now is what is meant by a *counterexample*, a term you have likely heard before. To *disprove* a universally quantified statement, we must prove an existentially quantified statement; that proof involves explicitly defining an element of a set that does *not* satisfy the specified property, whence the word **counterexample**.

4.4.2 Negation of an existential quantification

A statement like

$$\exists x \in S \,\centerdot\, R(x)$$

makes an existence claim. It says that there must be some element x that satisfies the property $R(x)$. To disprove a claim like this, we would seek to show that *any* value of x actually *fails* to satisfy the property R. Accordingly, we can say that the statement

$$\neg\big(\,\exists x \in S \,\centerdot\, R(x)\,\big)$$

is logically equivalent to the statement

$$\forall x \in S \,.\, \neg R(x)$$

This makes sense if we think about how to disprove such an existential claim. Pretend you are having a debate with a friend who told you that some kwyjibo has the property that it is a zooqa. How would you disprove him/her? You might say something like, "Nuh uh! Show me any kwyjibo you want to. I know it can't possibly be a zooqa because of the following reasons ..." and then you would explain why the property fails, no matter what.

Now, when you say "show me any" you are really performing a universal quantification! You are saying that *no matter* which kwyjibo you consider, something is true; that is, *for every* kwyjibo, or $\forall x \in K$ (where K is the set of all kwyjibos), something is True.

Think about this and consider why the logical negations we have discovered/defined make sense to you. Later on in the chapter, when we consider proof techniques, we will explain the strategy of considering an *arbitrary* kwyjibo and why this actually proves the logical negation we just wrote above. For now, we hope it is clear that

$$\forall x \in S \,.\, \neg R(x)$$

and

$$\exists x \in S \,.\, R(x)$$

have opposite truth values.

4.4.3 Negation of general quantified statements

The observations we have made so far motivate a general procedure for negating quantified statements. The statement A we defined above is of the form

$$\exists y \in \mathbb{R} \,.\, C(y)$$

where $C(y)$ is the rest of the statement (which *depends* on the value of y, of course). We think of $C(y)$ as some *property* of the quantified variable y; that property might have other quantifiers and variables inside it, but at a fundamental level, it is merely asserting some truth about y.

To negate this statement, we follow the method discussed above and write

$$\forall y \in \mathbb{R} \,.\, \neg C(y)$$

Now, we know that $C(y)$ is a universally quantified statement itself:

$$\forall x \in \mathbb{R} \,.\, y = x^3$$

We know how to negate that type of statement, too! That negation, $\neg C(y)$, is

$$\exists x \in \mathbb{R} \,.\, y \neq x^3$$

This step just uses the other negation procedure that we saw above. Then, putting it all together, we can say that $\neg A$ is the statement

$$\forall y \in \mathbb{R} \,.\, \exists x \in \mathbb{R} \,.\, y \neq x^3$$

This claim we can *prove* to be true, thus showing that the original statement must be False.

(We leave this proof as an exercise. *Hint:* Given any $y \in \mathbb{R}$, define a value of x that will force $y \neq x^3$ to be true. Notice that your choice of x will depend the value of y; how does it?)

Look at how this negation came about: we recognized that the original statement was a sequence of **nested quantifiers** (i.e. a sequence of several quantified variables in a row) with a variable proposition at the end, and we saw that we could treat part of the sequence of quantifiers as its own statement. We then "passed the negation" from the outside quantifier to the inside one, and pieced those negations together.

Following this same idea, we can figure out how to identify a statement with a longer sequence of quantifiers. For instance, look at a statement like

$$\forall a \in A \,.\, \exists b \in B \,.\, \exists c \in C \,.\, \forall d, e \in D \,.\, Q(a, b, c, d, e)$$

To start negating it, we would break off the first quantification, and treat the rest as its own proposition, $R(a)$, that depends only on a:

$$\forall a \in A \,.\, \big(\underbrace{\exists b \in B \,.\, \exists c \in C \,.\, \forall d, e \in D \,.\, Q(a, b, c, d, e)}_{R(a)}\big)$$

The negation can therefore be written as

$$\exists a \in A \,.\, \neg R(a)$$

but we would then have to figure out another way to write $\neg R(a)$. But hey, we would just do the same thing! We would just separate "$\exists b \in B$" from the rest and . . . you see where this is going. Try working out the steps on your own, and make sure that you end up with the following as the logical negation of the original statement:

$$\exists a \in A \,.\, \forall b \in B \,.\, \forall c \in C \,.\, \exists d, e \in D \,.\, \neg Q(a, b, c, d, e)$$

In general, we can say this: To negate a statement composed *only* of quantifiers and variable propositions, just switch every "$\forall$" to "$\exists$", and vice-versa, and negate the propositions. Don't alter any of the sets over which we quantify, merely the quantifiers themselves and the ensuing propositions; it wouldn't make sense to change the universe of discourse. Later on, we will look at how to negate other types of statements, more complicated ones built from other connectives. Before we do that, we need to move on and define and discuss those other connectives.

4.4.4 Method Summary

Let's summarize what we have discovered in this section.

- **Negating a universal quantification:**
  Let X be a set and let $P(x)$ be a proposition. Then the negation of a universal quantification, like this,

  $$\neg\big(\forall x \in X \centerdot P(x)\big)$$

  is written as

  $$\exists x \in X \centerdot \neg P(x)$$

  In words, we have shown that saying

  It is *not* the case that, for every $x \in X$, $P(x)$ holds.

  is equivalent to saying

  There exists an element $x \in X$ such that $P(x)$ fails.

- **Negating an existential quantification:**
  Let X be a set and let $Q(x)$ be a proposition. Then the negation of an existential quantification, like this,

  $$\neg\big(\exists x \in X \centerdot Q(x)\big)$$

  is written as

  $$\forall x \in X \centerdot \neg Q(x)$$

  In words, we have shown that saying

  It is *not* the case that there exists an $x \in X$ such that $Q(x)$ holds.

  is equivalent to saying

  For every element $x \in X$, $Q(x)$ fails.

Don't Change the Quantification Set!

We mentioned above that it wouldn't make sense to change the universe of discourse when negating a statement. To think about why this makes sense, take a real-life example.

Suppose we said "Every book on this bookshelf is written in English." How would you prove to us that we are lying, that our statement is actually False? You would have to produce a book *on this shelf* that is written in a different language. You couldn't bring in a French novel from the room down the hall and say, "See, you were wrong!" That wouldn't prove anything about the claim we made; the realms of discourse are different, and we didn't make any claim about what's going on in any bookshelves in other rooms. We only asserted something about this *particular* shelf.

For the same reason, when negate a statement like

$$\forall b \in T \,.\, P(b)$$

we obtain

$$\exists b \in T \,.\, \neg P(b)$$

without changing that realm of discourse, the set T. The original claim only asserts something about elements of T, so its negation does only that, as well.

4.4.5 The Law of the Excluded Middle

You know what? Let's actually discuss *why* we can talk about a statement and its **logical negation**. Built into our definition of **mathematical/logical statement** is the idea that such a sentence must have exactly one truth value, either True or False. Why can we do this? Well, we're in charge of the definitions here! Mathematicians have to set the ground rules—the **axioms**—of their systems and we want our logical system to ensure that every claim we make is decidedly True or False, and not both, and not neither.

This dichotomy is truly an **axiom** of our system. It is widely adopted in most of mathematics, and is famously known as **The Law of the Excluded Middle**. The name comes from this very idea, that every claim is True or False, so there is no *middle ground* between those two sides; that middle is excluded.

In essence, this makes what we do in mathematics fruitful: every claim has a truth value, and our goal is to find that truth value. Sometimes, though, we have to fall back on this axiom, this law we agreed upon, and just *guarantee* that some claim is either True or False, without knowing *which* truth value actually applies. We present an interesting and striking example of this idea here.

Proposition 4.4.1. *There exist real numbers a and b that are both irrational such that a^b is rational.*

(Remember that a **rational number** is one that can be expressed as a fraction of integers, and an **irrational number** is a real number that is *not* rational. Can you think of some examples of both rational and irrational numbers?)

Proof. We know $\sqrt{2}$ is irrational. (Question: Why? Can you prove that? Try it now. We will prove this very soon, as well!)

The number $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational. (This is where the Excluded Middle is used.) Let's consider these two cases separately.

- Suppose that the number $\sqrt{2}^{\sqrt{2}}$ is, indeed, rational. Then $a = \sqrt{2}$ and $b = \sqrt{2}$ is the example we seek, because a and b are both irrational and a^b is rational.

- Now, suppose that the number $\sqrt{2}^{\sqrt{2}}$ is irrational. In this case, we can use $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ as the example we seek, because a and b are both irrational and

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$$

which is rational.

In either case, we have found an example of real numbers $a, b \in \mathbb{R}$ such that both a and b are irrational and yet a^b is rational. This proves the claim. $\square$

This is an example of a **non-constructive** proof. It tells us something exists (and narrows it down to two possibilities, even) without actually telling us *exactly* which possibility is the one we sought all long. It is a direct use of the Law of the Excluded Middle that causes this.

(Question: Can you prove somehow that $\sqrt{2}^{\sqrt{2}}$ is irrational? It is True, but there is no known "simple" proof of this fact. Maybe you can find one!)

Most of the proofs we do here will be of the **constructive** variety (but not all). These might be more satisfying to you, and we're inclined to agree. If we claim something exists, we should be able to *show* it to you, right? If we just talked for a while about *why* some such object exists somewhere else, without being able to point to it, you would have to believe us, but you might not feel great about it. Constructive proofs are *subjectively better* because of this, and we will always strive for one when we can. Sometimes, though, a constructive proof is not immediately clear, and we have to make a non-constructive one, like we did here.

4.4.6 Looking Back: Indexed Set Operations and Quantifiers

Look back at Section 3.6.2, where we defined set operations—union and intersection, in Definitions 3.6.3 and 3.6.4, respectively—performed over index sets. The main idea was that we could express the union/intersection of an entire class of sets all at once using a shorthand notation.

Look carefully at those definitions. What characterized whether an object actually *is* an element of an indexed union, for example? That object needed to be an element of *at least one* of the constituent sets of the union. That is, there needed to *exist* some set of which that obejct is an element. This sounds like an *existential quantification*, doesn't it?

Likewise, what characterized whether an object is an element of an indexed intersection? That object needed to be an element of *all* the constituent sets. That is, *for all* of those sets, that object must be an element thereof. This is a *universal quantification*.

With those observations now made, we can rewrite those definitions of indexed set operations using our new quantifier notation:

Definition 4.4.2. *Suppose I is an index set and $\forall i \in I \bullet A_i \subseteq U$, for some universal set U. Then*

$$\bigcup_{i \in I} A_i = \{x \in U \mid \exists k \in I \bullet x \in A_k\}$$

$$\bigcap_{i \in I} A_i = \{x \in U \mid \forall i \in I \bullet x \in A_i\}$$

Try working with some of the examples and exercises in that Section 3.6.2 again. Do the definitions make more sense now?

4.4.7 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What is the **negation** of a mathematical statement? How are a statement and its negation related?

(2) Why is the negation of a $\forall$ claim an $\exists$ one?

Why is the negation of an $\exists$ claim a $\forall$ one?

(3) What is a non-constructive proof? To what type of claim—$\exists$ or $\forall$—does this term apply?

(4) Consider the claim

$$\forall x \in S \bullet P(x)$$

Why is its negation *neither* of the following?

$$\forall x \notin S \bullet P(x)$$

$$\exists x \notin S \bullet \neg P(x)$$

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) For each of the following statements, write its negation. Which one—the original or the negation—is True?

(a) $\forall x \in \mathbb{R} \text{.}\ \exists n \in \mathbb{N} \text{.}\ n > x$
(b) $\exists n \in \mathbb{N} \text{.}\ \forall x \in \mathbb{R} \text{.}\ n > x$
(c) $\forall x \in \mathbb{R} \text{.}\ \exists y \in \mathbb{R} \text{.}\ y = x^3$
(d) $\exists y \in \mathbb{R} \text{.}\ \forall x \in \mathbb{R} \text{.}\ y = x^3$

(2) For each of the following statements, write its negation. Which one—the original or the negation—is True?

(a) $\exists S \in \mathcal{P}(\mathbb{N}) \text{.}\ \forall x \in \mathbb{N} \text{.}\ x \in S$
(b) $\forall S \in \mathcal{P}(\mathbb{N}) \text{.}\ \exists x \in \mathbb{N} \text{.}\ x \in S$
(c) $\forall x \in \mathbb{N} \text{.}\ \exists S \in \mathcal{P}(\mathbb{N}) \text{.}\ x \in S$
(d) $\exists x \in \mathbb{N} \text{.}\ \forall S \in \mathcal{P}(\mathbb{N}) \text{.}\ x \in S$

(3) Let $I = \{x \in \mathbb{R} \mid 0 < x < 1\}$.

For each of the following defined sets, write out the defining condition that determines whether a number $y \in \mathbb{R}$ is an element of the set, using quantifiers.

Then, determine what the set is, and write your answer using set-builder notation.

(Try to *prove* your claim, as well, using a double-containment argument!)

(a)
$$S = \bigcup_{x \in I} \{y \in \mathbb{R} \mid x < y < 2\}$$

(b)
$$T = \bigcap_{x \in I} \{y \in \mathbb{R} \mid -x < y < x\}$$

(c)
$$V = \bigcup_{x \in I} \{y \in \mathbb{R} \mid -3x < y < 4x\}$$

(4) Let $P = \{y \in \mathbb{R} \mid y > 0\}$. Consider this statement:

$$\forall \varepsilon \in P \text{.}\ \exists \delta \in P \text{.}\ \forall x \in \{y \in \mathbb{R} \mid -\delta < y < \delta\} \text{.}\ |x^3| < \varepsilon$$

Write out the logical negation of this statement.

What does this statement say? What does its negation say?

Which one is True? Can you prove it?

(5) Let A, B, C, D be arbitrary sets.

Let $P(x), Q(x, y), R(x, y, z)$ be arbitrary variable propositions.

Write the negation of each of the following statements.

(a) $\forall a \in A \,.\, \exists b \in B \,.\, Q(a,b)$
(b) $\forall a \in A \,.\, \neg P(a)$
(c) $\forall c \in C \,.\, \forall d \in D \,.\, \neg Q(c,d)$
(d) $\exists a_1, a_2 \in A \,.\, \forall d \in D \,.\, R(a_1, a_2, d)$
(e) $\forall b_1, b_2, b_3 \in B \,.\, \neg R(b_1, b_2, b_3)$
(f) $\exists b \in B \,.\, \forall c \in C \,.\, \forall d \in D \,.\, R(d, b, c)$

4.5 Logical Connectives

To build mathematical statements from simpler ones (meaning ones composed of just quantifiers and propositions) we can connect several statements with certain words and phrases—such as "and", "or", and "implies"—to create more complicated statements and assert further claims and truths. We call these words and phrases **logical connectives**, and each of them has their own corresponding mathematical symbol and meaning. These meanings will make sense to you, based on our intuitive grasp of the English language and rational thought, but we emphasize that one of the major goals of introducing mathematical logic and its corresponding notation is to build these intuitions into rigorous and unambiguous concepts.

Throughout this section, let us assume that P and Q are arbitrary mathematical statements. These statements themselves can be composed of complicated combinations of quantifiers and other connectives and all sorts of mathematical notions. The point is that the way we combine P and Q into a larger statement is independent of their individual compositions. Before, we saw that "$\neg(\forall x \in X \,.\, R(x))$" is equivalent to "$\exists x \in X \,.\, \neg R(x)$", regardless of what the statement $R(x)$ was and how complicated it might have been. This idea continues here. We can talk about how to combine two statements without knowing what they are, individually.

We should also point out that these constituent statements, P and Q, may actually be variable propositions. For instance, we will consider how to connect two variable propositions, $P(x)$ and $Q(x)$, that each depend on some variable x. The definitions and methods we develop in this section apply to these variable propositions even though these propositions, themselves, do not have truth values without being told what the value of the variable x is.

When we want to talk about those propositions meaningfully and mathematically, we will have to **quantify** the variable x. Thus, if we have variable propositions $P(x)$ and $Q(x)$, we can still meaningfully define $P(x) \wedge Q(x)$ (where $\wedge$ means "and" as you'll see in the next section). We could then, in an example or a problem, talk about a claim of the form

$$\exists x \in X \,.\, P(x) \wedge Q(x)$$

This is a mathematical **statement**.

Essentially, the point we want to make is that these connectives still apply to variable propositions, but the relevant variables will have to be quantified *somewhere* in an overall statement to make the variable proposition into a proper **mathematical statement**.

4.5.1 And

To say

$$\text{“}P \text{ and } Q\text{” is } \mathsf{True}$$

means that *both* statements have the truth value: True. If either one of the statements P or Q were False, then the statement "P and Q" would be False, as well. This definition encapsulates this idea:

Definition 4.5.1. *We use the symbol "$\wedge$" between two mathematical statements to mean "and". For instance, we read "$P \wedge Q$" as "P and Q".*

*This is referred to as the **conjunction** of P and Q.*

The truth value of "$P \wedge Q$" is True *when both P and Q are true, and the truth value is* False *otherwise.*

Here are some examples to demonstrate this definition:

Example 4.5.2.

$$
\begin{array}{ll}
(1+3=4) \wedge (\forall x \in \mathbb{R}.\ x^2 \geq 0) & \quad \mathsf{True} \\
(1+3=5) \wedge (\forall x \in \mathbb{R}.\ x^2 \geq 0) & \quad \mathsf{False} \\
(1+3=5) \wedge (\exists x \in \mathbb{Q}.\ x^2 = 2) & \quad \mathsf{False}
\end{array}
$$

Notation: Parentheses

It's sometimes common to drop the parentheses that we used in the examples above. For example, the first line in the above example can be written equivalently as

$$1+3=4 \ \wedge \ \forall x \in \mathbb{R}.\ x^2 \geq 0$$

Using the parentheses tends to make the statement more readable. Without them, we have to think for a few extra moments about where one part of the statement ends and the next one begins, but we can still eventually make sense of it. We will try to use parentheses whenever they make a statement more easily understandable.

Notation: Sets and Logic

You might notice the similarity between the logical connective "$\wedge$" and the set operator "$\cap$". This is not a coincidence!

As we will discuss below in Section 4.5.4, we can write the definition of "$\cap$" using the connective "$\wedge$" because of the underlying logic of that set operator. Try it now, and then glance ahead to that section briefly, if you'd like. In general, though, be careful to keep these two notations separate! If A and B are sets, the phrase "$A \wedge B$" is not well-defined; what was meant is "$A \cap B$".

4.5.2 Or

To say

$$\text{“}P \text{ or } Q\text{” is } \mathsf{True}$$

means that “P is True, or Q is True”. We need to know that *one* of the statements is True to declare that the entire statement has the truth value True. We don't care whether *both* P and Q are true or not, merely that *at least one* of them is true.

This is in contrast with the so-called “exclusive OR” of computer science, also known as `XOR`, which declares “P `XOR` Q” to be False when both P and Q are True. In mathematics, we use the **inclusive “or”**. We only care whether at least one of the statements holds.

Definition 4.5.3. *We use the symbol $\vee$ between two mathematical statements to mean “or”. For instance, we read “$P \vee Q$” as “P or Q”.*

This is referred to as the **disjunction** *of P and Q.*

The truth value of “$P \vee Q$” is True *when* **at least one** *of P and Q is* True *(even when both are* True*), and the truth value is* False *otherwise.*

Example 4.5.4.

$$\begin{array}{ll} (1+3=4) \vee (\forall x \in \mathbb{R}.\ x^2 \geq 0) & \mathsf{True} \\ (1+3=5) \vee (\forall x \in \mathbb{R}.\ x^2 \geq 0) & \mathsf{True} \\ (1+3=5) \vee (\exists x \in \mathbb{R}.\ x^2 < 0) & \mathsf{False} \end{array}$$

Notation

The same notes about notation that we mentioned in the previous subsection apply here, as well. First, the use of parentheses—like in the above examples—is helpful but not technically required. We will try to use them whenever it helps, though.

Second, you might notice the similarity between the logical connective “$\vee$” and the set operator “$\cup$”. Again, this is not a coincidence! Try rewriting the definition of “$\cup$” using “$\vee$”, and glance ahead briefly at Section 4.5.4. In general, though, be careful to keep these two notations separate! If A and B are sets, the phrase “$A \vee B$” is not well-defined; what was meant is “$A \cup B$”.

4.5.3 Conditional Statements

This is the hardest logical connective to work with and continually gives students some problems, so we want to be extra careful and clear about this one. We want the statement **“If P, then Q”** (sometimes written as “P implies Q”) to have the truth value True when the truth of Q *necessarily* follows from the truth of P. That is, we want this statement to be True if the following holds:

> Whenever P is True, Q is *also* True.

Truth Table and Definition

Since this is the hardest connective to suss out, semantically, let's introduce the idea of a **truth table** to make the notation easier:

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

You may have seen a truth table before, in other mathematics courses, but even if you haven't, don't worry! Here's the main idea: Each column corresponds to a particular mathematical statement and its corresponding truth values. Each row corresponds to a particular *assigment* of truth values to the constituent statements, P and Q.

Notice that there are 4 rows because P and Q can each have one of two different truth values, so there are 4 possible combinations of those choices. Reading across a particular row, we find the corresponding truth values for other statements, based on what the T and F assignments for P and Q are in the first two columns.

Notice that the columns for $P \wedge Q$ and $P \vee Q$ follow the definitions given above. The column for $P \wedge Q$ has only one T, and it corresponds to the case where *both* P and Q are True. All other cases make $P \wedge Q$ a False statement. Likewise, the column for $P \vee Q$ has only one F, and it corresponds to the case where *both* P and Q are False. All other cases make $P \vee Q$ a True statement.

Now, why are the last two columns the way they are? Let's say that I make the claim "If you work hard, then you will get an A in this course". Here, P is "You work hard" and Q is "You will get an A". When can you call me a *liar*? When can you declare I told the truth? Certainly, if you work hard and get an A, I told the truth. Also, if you work hard and don't get an A, then I lied to you. However, if you don't work hard, then no matter what happens, *you don't get to call me a liar!* My claim didn't cover your situation; I was assuming all along you would just work hard! Thus, I didn't speak an untruth and so, by the Law of the Excluded Middle, I *did* speak the truth. The negation of a lie is a truth.

This situation—where the third and fourth rows of the $P \implies Q$ column are True—is known as a **false hypothesis**. When the statement on the left of the " $\implies$ " does not hold, then we are not in a situation that is meant to be addressed by the claim, so we cannot assert that the claim is False. Therefore, the claim must be True (again, by the Law of the Excluded Middle).

Let's make the proper definition of this symbol and then consider more examples to illustrate the definition.

Definition 4.5.5. *We use the symbol " $\implies$ " between to mathematical statements to mean "If ... then" or "implies". For instance, we read "$P \implies Q$" as "If P, then Q" or "P implies Q".*

This is referred to as a **conditional statement**.

The truth value of "$P \implies Q$" is True *assuming that Q holds whenver P holds.*

The truth value is False only *in the case where P is* True *and yet Q is* False.

We refer to P as the **hypothesis** *of the conditional statement and Q as the* **conclusion**.

That key word "whenever" in the definition should indicate to you why the *false hypothesis* cases make sense. When we know P is true and can deduce that Q is also true, then we get to declare $P \implies Q$ as True. If P wasn't true to begin with, we cannot declare $P \implies Q$ to be False. We only get to say $P \implies Q$ is false when Q did not necessarily follow from P, i.e. when there is an instance where the hypothesis P is True but the conclusion Q is False.

Examples

Here are several examples to help you get the idea:

$$\begin{array}{rl}
(1+3=4) \implies (\forall x \in \mathbb{R} \,.\, x^2 \geq 0) & \mathsf{True} \\
(1+3=5) \implies (\forall x \in \mathbb{R} \,.\, x^2 \geq 0) & \mathsf{True} \\
(1+3=5) \implies (\text{Abraham Lincoln is alive}) & \mathsf{True} \\
(1+1=2) \implies (0=1) & \mathsf{False} \\
(0=0) \implies (\exists x \in \mathbb{R} \,.\, x^2 < 0) & \mathsf{False} \\
(\text{Pythagorean Theorem}) \implies (1=1) & \mathsf{True} \\
(0=1) \implies (1=1) & \mathsf{True}
\end{array}$$

Notice that the second and third examples are True because they have the false hypothesis "$1+3=5$". Regardless of the conclusion, the entire conditional statement must be True because of this. It doesn't matter that "$\forall x \in \mathbb{R} \,.\, x^2 \geq 0$" happens to be True or that "Abraham Lincoln is alive" happens to be False; that false hypothesis determines the statement's truth value.

Also, notice that the second-to-last example is True, but it doesn't help us determine whether or not the Pythagorean Theorem itself is True! This is what we did in the False "spoof" of the theorem back in Chapter 1. Look back to Section 1.1.1, specficially "Proof 2". We assumed the Pythagorean Theorem was True and then logically derived a True statement from that assumption. That does not make the hypothesis valid, just because we derived a valid conclusion!

This idea is so important, that we will even show you again this striking example. Notice that it's logical form is exactly the same as that other spoof:

"Proof". Assume $1=0$. Then, by the symmetric property of $=$, it is also true that $0=1$. Adding these two equations tells us $1=1$, which is True. Therefore, $0=1$. $\square$

This is the main point here:

> Knowing a conditional statement, overall, is True, doesn't tell us *anything* about the truth values of the constituent propositions.

This is also strikingly illustrated in the third and seventh statements above; both conditional claims are True, but we certainly don't get to conclude that Abraham Lincoln is alive, or that $0 = 1$.

"Implies" is not the same as "Can be deduced from"

There is often some confusion with using the word "implies" to mean an "If ... then ..." statement, a conditional statement. We belive this arises because of some connotations surrounding the word "implies"; specifically, it seems to convey some sort of *causality*. For instance, consider this statement:

$$1 + 3 = 4 \implies 2 + 3 = 5$$

This is a True conditional statement, and our minds probably recognize this because we can just take the hypothesis, namely $1 + 3 = 4$, and add 1 to both sides, yielding the equation in the conclusion. In this sense, it seems that the truth of the hypothesis has some influence on the truth of the conclusion: we can deduce one *directly* from the other. This does not have to be the case, in general!

Look back at the first example given above:

$$(1 + 3 = 4) \implies (\forall x \in \mathbb{R}.\ x^2 \geq 0)$$

What does the fact that $1+3 = 4$ have to do with the fact that any real number squared is non-negative? Does it even have any connection? We don't actually care! We can still identify this conditional statement as True, whether or not we can find a way to deduce the conclusion directly *from* the hypothesis (and whether or not such a deduction even exists). Only the truth values of the constituent statements matter.

Granted, when we work on proving conditional statements, we will likely try to deduce one statement directly from another. It's important to keep in mind, though, that this is a consequence of our proof strategy, and not an underlying part of how conditional statements are defined. For these reasons, we tend to write conditional statements using the "If ... then ..." form, instead of using "implies". We might sometimes use it, and we're sure you'll see it in other mathematical writings. For now, though, we'll try to avoid it as much as possible, while we're still learning about these logical statements and connectives.

Quantifying Variables: Still Important!

In mathematics, we often want to prove conditional statements that involve variables. For instance, we might want to show that, in the context of the real numbers $\mathbb{R}$, the following conditional claim holds:

$$x > 1 \implies x^2 - 1 > 0$$

That sentence, written in the line above, is itself a **variable proposition**, and the definition of the symbol "$\implies$" applies to it.

If we knew that $x > 1$ and also $x^2 - 1 > 0$, then we could declare the conditional to be True. If we knew that $x \leq 1$, then we wouldn't even care whether $x^2 - 1 > 0$ or not; we could declare the conditional to be True. This is how the definition of "$\implies$" applies here.

Remember, though, that the conditional claim, as written above, is not technically a mathematical statement. We were making that claim in the context of the real numbers, so it would really make sense to write

$$\forall x \in \mathbb{R}. \left(x > 1 \implies x^2 - 1 > 0\right)$$

This is, ultimately, what the writer was trying to claim, so they should just say so! We make the same recommendation to you. These logical connectives—$\wedge$ and $\vee$ and $\implies$—make sense and can be applied to variable propositions. Outside of that scope, somewhere else in the statement you're putting together, there must be some kind of quantification on those variables. Only then can we be assured that the sentence is a mathematical statement with one truth value.

Writing "$\implies$" using "$\vee$"

There is a useful and important idea worth mentioning. This is partly because we will use it later, but also partly because it might help you understand conditional statements and learn how to use them.

This idea hinges on the notion of a *false hypothesis*. Consider a conditional statement, $P \implies Q$. If P fails, then the entire statement is True, regardless of Q's truth value. However, if P holds, then we definitely need Q to hold, as well, to declare the entire statement to be True.

These observations allow us to identify two ways in which a conditional statement can hold, and write these two ways in an "or" statement. Either $\neg P$ holds (i.e. a false hypothesis), or else Q holds. In either of these situations, the conditional statement $P \implies Q$ must hold! Let's state this claim outright for you to consider:

> The conditional statement "$P \implies Q$" and the statement "$\neg P \vee Q$" have the same truth value.

This is a good example of a **logical equivalence**, which is a topic we will discuss in the next section. For now, we will present the truth table for the two statements mentioned above. Notice that they have the same truth value, regardless of the truth values of the constituent statements, P and Q. This serves as further verification that the statements are equivalent, in addition to the description we provided above.

P	Q	$\neg P$	$\neg P \vee Q$	$P \implies Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Investigating More Examples

Let's consider some more examples of conditional claims and decide whether they are True or False. In so doing, we are helping you to better understand how $\implies$ works.

Then, we'll move on to proof *strategies* and discuss how to formally and rigorously prove claims like these, with logical connectives and quantifiers.

Example 4.5.6. We will start here with a "real world" example, to get used to the logic involved. Throughout this example, pretend we are in a class that only has lectures officially scheduled on Mondays, Wednesdays, and Fridays.

You'll notice that we will take two statements, P and Q, and consider all four possible combinations of these statements and their negations to make conditional statements.

- "If we have lecture today, then it is a weekday."

  (Note: There is some *implicit quantification* in this sentence. We are really saying that "For all days d in the weekly calendar, if we have lecture on day d, then d is a weekday." We think that the main idea is conveyed more succinctly by the sentence above, so we will use that version. Keep in mind that this is the meaning of the sentence and, in our discussion below, we will have to consider the different cases of that quantification.)

  This can be written logically by defining P to be "We have lecture today" and Q to be "Today is a weekday"; then the claim is $P \implies Q$.

  Is this True? Notice that the statements P and Q don't specify *what day it is*, so if we were to assert this claim to be True, that truth should be *independent* of the current day. That is, *whatever* day it is, we would have to show that $P \implies Q$ holds. Let's do that by considering a few cases:

  – Pretend today is Saturday or Sunday. Since we never have lecture on these days, the conditional claim is not a lie, so it is True.
  – Pretend today is Monday or Wednesday or Friday. If we do, indeed, have lecture today, then it is definitely a weekday, so the claim is True.
  – Pretend today is Tuesday or Thursday. We don't typically have lecture today, but even in the special case that we did (for some rescheduling reason), it would still be a weekday, so the claim is True.

  In any of the possible cases, the claim holds. Thus, $P \implies Q$ is True.

  You might interject to say, "Why bother with the cases at all? Couldn't we just say that no matter what day it is, supposing we have lecture, then we conclude it is definitely a weekday?" Well, yes, we could! That's actually a better strategy, a more *direct* route, you might say.

  This hints at how we will prove conditional claims in the future. Since we don't, in fact, care about the situations where we don't have lecture (the *false hypothesis*) we only need to *suppose* we have lecture on day X and *deduce* that X is a weekday. This is the method we will use to **directly prove** a conditional claim.

- "If it is a weekday, then we have lecture today."

  This is logically written as $Q \implies P$, using the same definitions of P and Q as the previous example.

  Is this claim True? Definitely not! We didn't have lecture on the first Tuesday of the semester, yet that day was a weekday. Thus, the claimer lied in that instance! On that Tuesday, Q was True but P was False. Thus, $Q \implies P$ is False.

- "If it is not a weekday, then we don't have lecture today."

  This is logically written as $\neg Q \implies \neg P$, using the same definitions of P and Q as the example above.

  Is this claim True? Yes, and we can prove it directly. Suppose that it is not a weekday; that is, pretend today is Saturday or Sunday. Obviously, the university would not be so sadistic as to schedule a lecture on a weekend, so we can necessarily declare that we don't have lecture, i.e. $\neg P$ holds. This shows that $\neg Q \implies \neg P$ is a True statement.

  (Question: Why did we not need to consider the case where today is a weekday?)

- "If we don't have lecture today, it is not a weekday."

  This is logically written as $\neg P \implies \neg Q$, using the same definitions of P and Q as the example above.

  Is this claim True? Well, let's think about it. What if we pretend we don't have lecture today. What can we necessarily say? Is it definitely not a weekday? I don't think so! Maybe it's a Tuesday, and we just don't have a scheduled lecture. This shows that the claim is False; we have an instance where the hypothesis ($\neg P$) holds, and yet the conclusion ($\neg Q$) does not hold.

  Notice that there *are* situations where $\neg P$ holds *and* $\neg Q$ does, as well. For instance, if today were Saturday, then certainly we don't have lecture *and* it is not a weekday. This *specific instance* does not meant that the claim is True, though! We need to verify its truth for *all instances*.

Example 4.5.7. Let's do the same kind of analysis with a more "mathy" example. Throughout this example, let A and B be arbitrary sets. Also, let P be "$A \subseteq B$", and let Q be "$A - B = \varnothing$".

We will do what we did in the previous example and consider all four possible ways of combining P and Q and their negations to make conditional statements.

- Is $P \implies Q$ True?

Yes! Let's pretend A and B satisfy the relationship $A \subseteq B$. This means *every* element of A is also an element of B. Therefore, we cannot possibly have an element of A that does *not* belong to B, Since $A - B$ is the set of elements that belong to A and not B, we conclude that there are no such elements, so $A - B = \varnothing$.

- Is $Q \implies P$ True?

  Yes! Let's pretend $A - B = \varnothing$. This means there are *no* elements of A that are also not elements of B. (Think about this.) Put another way, any element $x \in A$ *cannot* have the property that $x \notin B$ (or else $x \in A - B$ and so $A - B \neq \varnothing$); thus, $x \in B$, necessarily. Hey, this is exactly what $A \subseteq B$ means! Whenever $x \in A$, we conclude $x \in B$, too. This shows $Q \implies P$ is true.

- Is $\neg Q \implies \neg P$ True?

  Hmm, this is harder to figure out. Let's pretend $\neg Q$ holds; this means $A - B \neq \varnothing$. That is, there exists some element x that satisfies $x \in A$ and $x \notin B$. Certainly, then $A \not\subseteq B$, because we have identified an element of A that is not an element of B (whereas the $\subseteq$ relationship would dictate that every element of A is also an element of B). Thus, $\neg Q \implies \neg P$ is True.

- Is $\neg P \implies \neg Q$ True?

  Again, we need to think about this. Let's just write down what $\neg P$ means. To say $A \not\subseteq B$ means there exists some element $x \in A$ that also satisfies $x \notin B$. (This is what we used in the previous case, too.) Okay, what does that tell us? Consider the set $A - B$. Does it have any elements? Yes, it has at least x as an element! Since $x \in A \wedge x \notin B$, we can say $x \in A - B$. Thus, $A - B \neq \varnothing$, so we conclude that $\neg P \implies \neg Q$ is True.

Observations and Facts About "$\implies$"

Okay, now we have some practice working with conditional statements and determining their truth values. What you should notice from the examples we discussed is that knowing $P \implies Q$ holds does **not** tell us anything about $Q \implies P$. In both of these examples above, $P \implies Q$ was True; however, $Q \implies P$ was True in one example and False in the other. There is nothing we can necessarily say, with certainty, about $Q \implies P$, even if we know the truth value of $P \implies Q$. This idea is so important, that we will touch on it in the next subsection.

For now, let's make a few more remarks about the "$\implies$" connective.

- Remember that, given mathematical statements P and Q, the sentence "$P \implies Q$" is, itself, another mathematical statement. It has a truth value. That truth value *depends* on P and Q (in the way we defined it above), but it does not tell us *anything* about the truth values of P and Q. So, if you just write down the claim

$$\text{Blah blah} \implies \text{Yada yada}$$

on your paper, we have no idea if you're trying to assert whether "Blah blah" or "Yada yada" are True or False! To a mathematician, this just says:

> The conditional statement " 'Blah blah' implies 'Yada yada' " is True.

If you wish to make some kind of inference or deduction, then use some helping words and sentences to indicate that. Write something like this:

> $P \implies Q$ because ...
>
> Also, P holds because ...
>
> Therefore, Q holds.

If you have studied formal logic before, or have seen this type of argument in a philosophy course, then you might recognize this as **Modus Ponens**.

- The idea of a **false hypothesis** yielding a True conditional is kind of weird; we realize this. It's a direct consequence of the Law of the Excluded Middle. Under a false hypothesis, we don't get to say the overall statement is False, so it must be True, since it must be one or the other.
- Remember that we can always write a conditional statement without the " $\implies$ " symbol by converting it to an "or" statement.

  > The statements "$P \implies Q$" and "$\neg P \vee Q$" always have they always have the same truth value.

Converse and Contrapositive

Let's give some names to the different types of conditional statements related to a given conditional statement. We will refer to these frequently later on.

Definition 4.5.8. *Let P and Q be mathematical statements. Consider the "original" claim, $P \implies Q$.*

We refer to $Q \implies P$ as the **converse** *of the original claim.*

We refer to $\neg Q \implies \neg P$ as the **contrapositive** *of the original claim.*

By our observations in the previous subsection, we know that the **converse** does not *necessarily* have the same truth value as the original. What we will see (and prove) in the next section is that the **contrapositive** always has the *same* truth value as the original claim. (This is the notion of **logical equivalence**, which we will discuss in full detail in the next section.)

You might wonder why we need this terminology at all. Well, since the contrapositive can be shown to be *logically equivalent* to the original claim, it gives rise to a valid proof method when we try to prove conditional statements. We will develop that very soon. That's why we use the contrapositive.

The converse is interesting because its truth value is not necessarily tied to that of the original statement: even knowing the original is True, the converse might be True and it might be False. Thus, whenever we prove a claim $P \implies Q$ to be true, a mathematician (probably) immediately wonders, "Hmm, does the converse also hold?" It's a natural question to ask, and worth thinking about whenever you face a conditional statement. (In fact, if you ever find yourself at a party with mathematicians, and you hear someone talking about an "If ... then ..." statement, you should ask, "Does the converse hold, as well?" You might impress your fellow guests.)

The converse is also the subject of a common logical fallacy you might encounter in everyday life. Perhaps you are trying to argue that $A \implies B$ in a debate with a friend. What if they retort, "Well, B doesn't necessarily imply A! Your argument is wrong!" Have you ever been frustrated by that situation? You might have been tempted to shout, "So what? I wasn't trying to say anything about whether $B \implies A$. I was talking about $A \implies B$, you ..." (We'll cut ourselves off before we get mean.) Whether or not your friend is right, knowing the truth value of the converse doesn't tell you anything about the truth value of your original claim. You should tell them that! Next time, just say, "You're talking about the converse, which is not necessarily logically connected to my claim."

Okay, now that we have defined all of the requisite logical symbols and seen some examples, it's time to move on and start proving things about them! But first, a short aside about set operations, and then a few practice problems.

4.5.4 Looking Back: Set Operations and Logical Connectives

Look back at Sections 3.4 and 3.5, where we defined subsets and set operations. All of those definitions made use of some logical ideas, but we wrote them in English back then, relying on our collective intuition and working knowledge of logic. We can rewrite them now using quantifiers and connectives!

First, recall the definition of **subset**. We write $A \subseteq B$ if the following holds: whenever $x \in A$, we can also say $x \in B$. Notice that key word, "whenever", which signals both a *universal quantification* and a *conditional statement*. Think about how you would rewrite the definition of $A \subseteq B$, using this notion, then read on to see our version ...

Definition 4.5.9. *Let A, B, U be sets, where $A, B \subseteq U$ (i.e. U is a universal set). We say A is a* **subset** *of B, and write $A \subseteq B$, if and only if*

$$\forall x \in U \,.\, x \in A \implies x \in B$$

This makes sense because it asserts that "whenever" statement we wrote in the above paragraph: whenever $x \in A$, we must also be able to conclude $x \in B$; "if $x \in A$, then $x \in B$" must hold.

Look back again at the definitions of the set operations we gave. Try to write your own versions of those definitions using logical symbols and then read ours here. Think about how they make sense, how they express the same underlying ideas.

Definition 4.5.10. *Let A, B, U be sets, where $A, B \subseteq U$ (i.e. U is a universal set). Then,*

$$\begin{aligned} A \cap B &= \{x \in U \mid x \in A \ \wedge \ x \in B\} \\ A \cup B &= \{x \in U \mid x \in A \ \vee \ x \in B\} \\ A - B &= \{x \in U \mid x \in A \ \wedge \ \neg(x \in B)\} = \{x \in U \mid x \in A \ \wedge \ x \notin B\} \\ \overline{A} &= \{x \in U \mid \neg(x \in A)\} = \{x \in U \mid x \notin A\} \end{aligned}$$

While we're here, we can also redefine a **partition** of a set. This will make use of logical connectives, but this also hearkens back to indexed sets and how they are defined in terms of quantifiers. Everything we've learned is coming together here!

Definition 4.5.11. *Let A be a set. A* **partition** *of A is a collection of sets that are pairwise disjoint and whose union is A.*

That is, a partition is formed by an index set I and non-empty sets S_i (defined for every $i \in I$) that satisfy the following conditions:

(1) $\forall i \in I \bullet S_i \subseteq A.$

(2) $\forall i, j \in I \bullet i \neq j \implies S_i \cap S_j = \varnothing.$

(3) $\displaystyle\bigcup_{i \in I} S_i = A$

Look back to Definition 3.6.9 to see how we originally defined a partition. Do you see how we are saying the same thing here, just using logical symbols?

4.5.5 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What is the difference between $\wedge$ and $\vee$?

(2) What is the difference between $\wedge$ and $\cap$?

What is the difference between $\vee$ and $\cup$?

(3) Write out a truth table for the statement $P \implies Q$.

(4) Why are $P \implies Q$ and $\neg P \vee Q$ logically equivalent statements?

(5) What is the converse of a conditional statement?

What is the contrapositive of a conditional statement?

(6) Are the truth values of a conditional statement and its converse related?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) For each of the following sentences, rewrite it using logical notation and determine whether it is True or False.

(a) Every integer is either strictly positive or strictly negative.

(b) For any given real number, there exists a natural number that is strictly bigger.

(c) For every real number, if it is negative, then its cube is also negative.

(d) There is a subset of $\mathbb{Z}$ that has the property that whenever a number is an element of that set, so is its square.

(e) There is a natural number that is both even and odd.

(2) Rewrite each of the following $\forall$ claims as a conditional statement, and determine whether it is True or False.

(a) $\forall x \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z} .\ y = 2k\} .\ x^2 \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z} .\ y = 2k\}$

(b) $\forall x \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z} .\ y = 2k+1\} .\ x^2 \in \{y \in \mathbb{N} \mid \exists k \in \mathbb{Z} .\ y = 2k+1\}$

(c) $\forall t \in \{z \in \mathbb{R} \mid z^2 > 4\} .\ t > 2$

(3) Rewrite each of the following conditional statements as a $\forall$ claim, using set-builder notation, and determine whether it is True or False.

(a) $\forall x \in \mathbb{R} .\ x > 3 \implies x^2 < 9$

(b) $\forall x \in \mathbb{R} .\ x < 3 \implies x^2 < 9$

(c) $\forall t \in \mathbb{R} .\ t^2 - 6t + 9 \geq 0 \implies t \geq 3$

(4) Let's define the following variable propositions:

$$P(x) \text{ is “ } \frac{1}{2} < x \text{ ”}$$
$$Q(x) \text{ is “ } x < \frac{3}{2} \text{ ”}$$
$$R(x) \text{ is “ } x^2 = 4 \text{ ”}$$
$$S(x) \text{ is “ } x + 1 \in \mathbb{N} \text{ ”}$$

For each of the following statements, determine whether it is True or False.

(a) $\forall x \in \mathbb{N} .\ P(x)$

(b) $\forall x \in \mathbb{N} .\ Q(x) \implies P(x)$

(c) $\forall x \in \mathbb{Z} .\ Q(x) \implies P(x)$

(d) $\exists x \in \mathbb{N} .\ \neg S(x) \vee R(x)$

(e) $\exists x \in \mathbb{Z} .\ R(x) \wedge \neg S(x)$

(f) $\forall x \in \mathbb{R} .\ R(x) \implies S(x)$

(g) $\exists x \in \mathbb{R} .\ P(x) \wedge S(x)$

(h) $\forall x \in \mathbb{Z} .\ R(x) \implies \big(P(x) \vee Q(x)\big)$

(5) For each of the following conditional statements, write it in logical notation, and use this write its converse and its contrapositive; then, determine the truth values of all three: the original statement, the converse, and the contrapositive.

(a) If a real number is strictly between 0 and 1, then so is its square.

(b) If a natural number is even, then so is its cube.

(c) Whenever an integer is a multiple of 10, it is a multiple of 5.

4.6 Logical Equivalence

In this section, the major goal is to introduce the idea of **logical equivalence** and prove a few fundamental claims. Essentially, we want to decide when some complicated logical statements are actually “the same”, in the sense of truth values. Since mathematical statements may depend on some propositional variables, we might not be able to conclude anything specific about their truth values. However, we can sometimes prove that two mathematical statements will have *the same truth value*, for all possible values of the variables they contain. That's a really nice conclusion to make! We get to say that they have the same truth value, regardless of what it is. In that sense, we are proving the two statements to be **equivalent**, in a logical sense.

4.6.1 Definition and Uses

The following definition introduces a convenient symbol for the notion of logical equivalence described in the above paragraph:

Definition 4.6.1. *Let P and Q be mathematical statements. We use the symbol "$\Longleftrightarrow$" to mean "is* **logically equivalent** *to", or "has the same truth value as".*

That is, we write "$P \Longleftrightarrow Q$" when P and Q always have the same truth value, regardless of whether it is T *or* F*.*

We read "$P \Longleftrightarrow Q$" aloud as "P is logically equivalent to Q" or "P **if and only if** *Q".*

This type of statement is known as a **biconditional** *(or a* **bi-implication***).*

Let's take the truth tables we saw in the last section and add a new column for this symbol:

P	Q	$\neg P$	$\neg P \vee Q$	$P \implies Q$	$Q \implies P$	$P \Longleftrightarrow Q$
T	T	F	T	T	T	T
T	F	F	F	F	T	F
F	T	T	T	T	F	F
F	F	T	T	T	T	T

In the column for $P \Longleftrightarrow Q$, an entry has the truth value T when (and only when) P and Q have the same truth value. This happens in Row 1, where both are T, and in Row 4, where both are F. Notice, then, that $P \Longleftrightarrow Q$ has the truth value T if and only if

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

is a True statement. This is the notion of **logical equivalence**: $P \Longleftrightarrow Q$ means that both $P \implies Q$ and $Q \implies P$ hold. Whatever truth value P has, Q is guaranteed to have the same truth value, and vice-versa:

- Supposing that P is True, then $P \implies Q$ tells us that Q must also be True.
- Supposing that P is False, then $Q \implies P$ tells us that Q *cannot* be True (since $Q \implies P$ would be False, in that case), so Q must also be False.

Either way, P and Q have the same truth value.

Examples

Example 4.6.2. Look again at the third and fourth columns in the truth table above. They prove the following logical equivalence:

$$(P \implies Q) \Longleftrightarrow (\neg P \vee Q)$$

Whatever the truth value of $P \implies Q$ (which, of course, depends on P and Q), it must be the same as the truth value of $\neg P \vee Q$. We've mentioned this equivalence before, and we will make use of it fairly often in the future.

Example 4.6.3. Look at this truth table:

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

Regardless of the truth values of P and Q, we find that $P \implies Q$ and $\neg Q \implies \neg P$ have the *same* truth values. Thus, they are *logically equivalent*, and we can write:

$$(P \implies Q) \iff (\neg Q \implies \neg P)$$

This is the fact that we stated (without proof) in the previous section:

> The contrapositive of a conditional statement is logically equivalent to the original statement.

A different proof of this fact makes use of the way to express a conditional statement as a disjunction. Recall the logical equivalence

$$\big(P \implies Q\big) \iff \big(\neg P \vee Q\big)$$

that we mentioned in the previous example. Now, think about the contrapositive of that original conditional statement:

$$\neg Q \implies \neg P$$

Applying the same disjunctive form to that statement yields the following equivalence:

$$\big(\neg Q \implies \neg P\big) \iff \big(\neg(\neg Q) \vee \neg P\big)$$

Now, noticing that $\neg(\neg Q)$ is equivalent to just Q, and remembering that the order of a disjunction is irrelevant (i.e. $P \vee Q$ and $Q \vee P$ have the same truth value) we find that

$$\big(\neg Q \implies \neg P\big) \iff \big(\neg P \vee Q\big) \iff \big(P \implies Q\big)$$

This shows, in another way, that a conditional statement and its contrapositive have the same truth value!

Example 4.6.4. Later in this section, we will prove the following logical equivalences, which hold no matter what the propositions P and Q and R are:

$$\begin{aligned}
\neg(P \wedge Q) &\iff \neg P \vee \neg Q \\
(P \wedge Q) \wedge R &\iff P \wedge (Q \wedge R) \\
P \vee (Q \wedge R) &\iff (P \vee Q) \wedge (P \vee R) \\
\neg(P \implies Q) &\iff P \wedge \neg Q
\end{aligned}$$

Each of these is an assertion that the expressions on both sides of the $\iff$ symbol have the same truth value. Can you see why these claims are True? Can you think of how to prove them?

If and Only If

Logical equivalence has a nice relationship with the phrase "if and only if". To say "P if and only if Q" means we are asserting that both "P if Q" and "P only if Q" hold. One of these corresponds to $P \implies Q$ and the other corresponds to $Q \implies P$, so asserting both are true means exactly what we have described:

$$P \iff Q \quad \text{is the same as saying} \quad (P \implies Q) \wedge (Q \implies P)$$

Now, which one is which, though? When we say "P if Q", this means "If Q, then P." That is,

$$\text{“}P \text{ if } Q\text{”} \quad \text{is the same as saying} \quad Q \implies P$$

Sussing out the other direction is a little harder! What does "P *only if* Q" really mean? This sentence is asserting that, in a situation where P holds, it must also be the case that Q holds. That is, knowing P holds means we also immediately know Q holds. Put even another way, whenever P is true, we necessarily know that Q is true. This is the same as saying $P \implies Q$ holds!

Another way of thinking about it is as follows. Saying "P only if Q" is the same as saying it cannot be the case that P holds and Q does not. Written logically, we have

$$\neg\big(P \wedge \neg Q\big)$$

Later on in this section, we will state and prove **DeMorgan's Laws for Logic**. One of those laws tells us how to negate that statement inside the parentheses. (You might already know these logical laws, in fact. If not, you can glance ahead at Sections 4.6.5 and 4.6.6 for a preview.) The conclusion is:

$$\neg P \vee Q$$

Hey look, that's logically equivalent to $P \implies Q$, as we observed already! Cool. Just further confirmation that "P only if Q" means $P \implies Q$.

Using "$\iff$" in Definitions

We will also often use the "$\iff$" symbol in a **definition** to indicate that the term defined is an equivalent term for the property that is used in the definition. For example:

$$\text{We say } x \in \mathbb{Z} \text{ is } \textbf{even} \iff \exists k \in \mathbb{Z}\,.\; x = 2k$$

That is, the notion of an integer being even is equivalent to knowing that the number is twice an integer. Similarly, we can define **odd**:

$$\text{We say } x \in \mathbb{Z} \text{ is } \textbf{odd} \iff \exists k \in \mathbb{Z}\,.\; x = 2k + 1$$

These are formal definitions, mind you, and are the only way of guaranteeing an integer is even (or odd). We will use these definitions soon to rigorously prove some facts about integers and arithmetic. Every time we want to assert a particular integer (call it x) is even, we need to show there exists an integer k that satisfies $x = 2k$. That is, we have to *satisfy the definition* by appealing to the logical equivalence given in the definition.

Biconditional Statements: A Technical Distinction

We can also use the symbol "$\iff$" to express two conditional statements at once. Technically speaking, this is not *exactly* the same as asserting a logical equivalence, but it conveys a similar idea, so we allow the symbol to be used in both ways.

A logical equivalence involves some undefined propositions, and it asserts that the two statements will have the same truth value, regardless of the truth values of those propositions. For instance,

$$(P \implies Q) \iff (\neg P \vee Q)$$

is a perfect example of a logical equivalence. Without telling you what P and Q are, we can't be sure exactly what $P \implies Q$ and $\neg P \vee Q$ mean. However, we don't need to know what P and Q are to know that those two statements definitely have the same truth value.

The situation is slightly different when the two statements on either side of the "$\iff$" are actually proper mathematical statements, with no undefined propositions. For instance, consider this statement:

$$\forall x \in \mathbb{R}.\ (x > 0) \iff \left(\frac{1}{x} > 0\right)$$

This is a logical claim, and it asserts that, whenever x is a real number, knowing one of those two facts—$x > 0$ or $\frac{1}{x} > 0$—necessarily guarantees the other. That is, if I told you I have a real number in mind and it is positive, you get to conclude that its reciprocal is positive, too. Also, if I told you I have a real number in mind whose reciprocal is positive, you would get to conclude that the number itself is positive, too. It goes *both ways*. (Question: What if I told you I had a *negative* real number in mind? Could you conclude anything about its reciprocal? Why or why not?)

Do you see how this is different? Given an arbitrary $x \in \mathbb{R}$, the statement "$x > 0$" is decidedly either True or False. Its truth value isn't left undetermined. This distinguishes it from the example given above, where the truth value of the individual statements is unknown, yet we can still declare those truth values must be identical.

For lack of a better, widespread term for these kinds of statements, we will refer to them as **biconditionals**. This is because they are really meant to represent two conditional statements that go "in opposite directions":

$$\forall x \in \mathbb{R}.\ \left[\left((x > 0) \implies \left(\frac{1}{x} > 0\right) \right) \wedge \left(\left(\frac{1}{x} > 0\right) \implies (x > 0) \right) \right]$$

This is what the statement above says: each part of the statement implies the other one.

This term is not necessarily standard in other mathematical writing, but we wanted to point out this technical distinction so you are aware of it. You might approach a mathematicial logician or set theorist and use the phrase "logical equivalence", and they might be confused or take offense to the way in which you use it. This is not a big worry, mind you! Since we are learning about these fundamental ideas now for the first time, we don't necessarily have to keep in mind all of the technical details that lie underneath these concepts. Also, in the remainder of this book, we might use "logical equivalence" and "biconditional" interchangeably. This is fine and acceptable for now.

The main point behind using the "$\iff$" symbol is to assert that two statements *have the same truth value*. The only difference between a "logical equivalence" and a "biconditional" is whether or not those statements contained therein have any arbitrary, undefined propositions. This is a minor distinction to be made, in the grand scheme of things, so we will consider it only briefly here.

4.6.2 Necessary and Sufficient Conditions

There are two terms occasionally used in mathematics that convey the two directions of a biconditional statement: **necessary** and **sufficient**. They correspond exactly to the "only if" and "if" parts of the biconditional. These terms are motivated by the natural types of questions mathematicians ask.

Sufficient: P, if Q

If we identify some interesting fact or property—call it P—of a mathematical object, we might wonder, "When can we *guarantee* such a property holds? Is there some condition we can check that will give us a 'Yes' answer right away?" This is what a **sufficient** condition is, a property that guarantees P will also hold. It is "sufficient" in the sense that it is "enough" to conclude P; we don't need any other outside information.

Let's say we have identified a proposition Q as a sufficent condition for P. How can we express this logically? Well, knowing Q is sufficient to conclude P, so we can easily write this as a conditional statement:

$$Q \implies P \qquad \text{means } Q \text{ is a } \textbf{sufficient} \text{ condition for } P$$

Said another way, this conditional statement expresses: "P, if Q".

Necessary: P only if Q

We also might wonder, "How can we guarantee that P fails? Is there some condition we can check that will tell us this right away?" This is what a **necessary** condition is, a property that is necessary or *essential* for the property P to hold. This condition is not necessarily enough to conclude that P holds, but for P to even have a chance of holding, this condition better hold, too.

Think about the logical connections here. Say we have established a property Q that is a **necessary** condition for P. How can we express the relationship between P and Q, symbolically? That's right, we can use a conditional statement. Knowing P holds tells us that Q definitely holds; it was necessary for P

to be true. This is expressed as

$$P \implies Q \qquad \text{means } Q \text{ is a } \textbf{necessary} \text{ condition for } P$$

Said another way, this conditional statement expresses: "P only if Q".

We could also think of this in terms of the contrapositive. If Q does not hold, then P cannot hold, either. That is,

$$\neg Q \implies \neg P$$

which is the contrapositive of the conditional statement above, $P \implies Q$. We know these are logically equivalent forms of the same statement.

Examples

Example 4.6.5. Let $P(x)$ the proposition "x is an integer that is divisible by 6". For each of the following conditions, let's identify whether it is a **necessary** or **sufficient** condition (or possibly both!) for $P(x)$ to hold.

(1) Let $Q(x)$ be "x is an integer that is divisible by 3".

To determine whether $Q(x)$ is a necessary condition, let's assume $P(x)$ holds. Can we deduce $Q(x)$ holds, too? Well, yes! To say an integer x is divisible by 6 means that it is divisible by both 2 and 3. Thus, it is certainly divisible by 3, so $Q(x)$ holds.

To determine whether $Q(x)$ is a sufficient condition, let's assume $Q(x)$ holds. Can we deduce $P(x)$ holds, too? Hmm ... knowing that x is an integer divisible by 3, is it also *definitely* divisible by 2, allowing us to conclude it is divisible by 6? We think not! Consider $x = 3$; notice $Q(3)$ holds but $P(3)$ does not.

This shows $Q(x)$ is only a necessary condition, and not a sufficient one.

(2) Let $R(x)$ be "x is an integer that is divisible by 12."

Following similar reasoning to the above example, we can conclude that $R(x)$ is a sufficient condition for $P(x)$, but not a necessary one (because we can have $x = 6$, where $P(6)$ holds but $R(6)$ does not hold).

(3) Let $S(x)$ be "x is an integer such that x^2 is divisible by 6".

We'll let you work with this one on your own ... Is $S(x)$ a necessary condition for $P(x)$? Is it a sufficient one?

Be careful, and notice that we specified x, itself, is an integer ...

4.6.3 Proving Logical Equivalences: Associative Laws

Now, let's actually **prove** some logical equivalences! In doing so, we will be working on our ability to read and understand and write logical statements using quantifiers and connectives. We will also be developing some fundamental logical results that we can apply in the near future to develop proof techniques. These techniques will be the foundation of the rest of our work, and everything else we do will involve implementing some combination of these proof strategies and logical concepts.

Let's start with some of the simpler symbolic logical laws. Showing something is *associative* essentially means we can "move around the parentheses" willy-nilly and end up with the same thing. You probably use the fact that addition is associative all the time! To add x to $y+z$, we can just add z to $x+y$ instead and know we get the same answer. That is, we can rest assured that

$$x + (y + z) = (x + y) + z$$

We can *move* the parentheses around wherever we want to and so, ultimately, we can just pretend as if they aren't even there and just write

$$x + y + z$$

because the order in which we interpret the two additions is irrelevant. The same kind of result applies to conjuctions and disjunctions of logical statements, and that's what we will prove now.

Theorem 4.6.6. *Let P, Q, R be logical statements. Then*

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

and

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

We will actually prove these claims in two separate ways: (1) via truth tables, and (2) via semantics (i.e. words). They are both perfectly valid, but we want to show you both of them to let you decide which style you like better.

Proof 1. First, we will prove these claims via truth tables. Observe the table for conjunctions:

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

Thus, $P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R$ because their corresponding columns are identical, in every case.

Next, observe the table for disjunctions:

P	Q	R	$P \vee Q$	$Q \vee R$	$P \vee (Q \vee R)$	$(P \vee Q) \vee R$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
T	F	F	T	F	T	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

Thus, $P \vee (Q \vee R) \Longleftrightarrow (P \vee Q) \vee R$ because their corresponding columns are identical, in every case. □

Proof 2. Second, let's prove these claims by analyzing them, semantically. Consider the first claim,

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

To show that the two sides are *logically equivalent*, we need to show both of the following conditional statements are True:

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

and

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

($\implies$) Let's prove the first conditional statement. Suppose $P \wedge (Q \wedge R)$ is True. This means P is True and $Q \wedge R$ is True. By definition, this means P is True and Q is True and R is True. Certainly, then $P \wedge Q$ is True and R is True, by definition. Thus, $(P \wedge Q) \wedge R$ is True, as well.

($\Longleftarrow$) Now, let's prove the second conditional statement. Suppose $(P \wedge Q) \wedge R$ is True. This means $P \wedge Q$ is True and R is True. By definition, this means P is True and Q is True and R is True. Certainly, then P is True and $Q \wedge R$ is True, by definition. Thus, $P \wedge (Q \wedge R)$ is True, as well.

Since we have shown both conditional statements, we conclude the two sides are, indeed, logically equivalent.

Next, consider the second claim of the theorem,

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

To show that the two sides are *logically equivalent*, we need to show both of the following conditional statements are True:

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

and

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

($\implies$) Let's prove the first conditional statement. Suppose $P \vee (Q \vee R)$ is True. This means either P is True or $Q \vee R$ is True. This gives us two cases.

1. Suppose P is True. This means $P \vee Q$ is True, by definition. Thus, $(P \vee Q) \vee R$ is True, also by definition.
2. Suppose $Q \vee R$ is True. This means either Q is True or R is True. Again, this gives us two cases.
   (a) Suppose Q is True. This means $P \vee Q$ is True, by definition. Thus, $(P \vee Q) \vee R$ is True, also by definition.
   (b) Suppose R is True. This means $(P \vee Q) \vee R$ is True, by definition.

In any case, we find that $(P \vee Q) \vee R$ is True. Thus, this conditional statement is True.

($\Longleftarrow$) Let's prove the second conditional statement. Suppose $(P \vee Q) \vee R$ is True. This means either $P \vee Q$ is True or R is True. This gives us two cases.

1. Suppose $P \vee Q$ is True. This means either P is True or Q is True. This gives us two cases.
   (a) Suppose P is True. This means $P \vee (Q \vee R)$ is true, by definition.
   (b) Suppose Q is True. This means $Q \vee R$ is True, by definition. Thus, $P \vee (Q \vee R)$ is true, also by definition.
2. Suppose R is True. This means $Q \vee R$ is True, by definition. Thus, $P \vee (Q \vee R)$ is True, also by definition.

In any case, we conclude that $P \vee (Q \vee R)$ is True. Thus, this conditional statement is True.

Since we have shown both conditional statements hold, we conclude the two sides are, indeed, logically equivalent. $\square$

Okay, what have we accomplished with these proofs? What have we proven, and how? Why did it work?

Let's mention a consequence of these proofs, before going on to discuss and compare the proffs, themselves. We proved that the "$\wedge$" and "$\vee$" connectives are associative, so the order in which we evaluate parenthetical statements involving only one such connective does not matter. For example, we now know that "$P \wedge (Q \wedge R)$" has the same meaning as "$(P \wedge Q) \wedge R$". Accordingly, in the future, we will just write these statements without the parentheses: "$P \wedge Q \wedge R$".

Reflecting: Truth Tables vs. Semantics

Let's talk about the truth tables first. Since P, Q, and R are logical statements, they are each, individually, True or False. The eight rows of the truth tables consider all possible assignments of truth values to those three constituent statements. The first three columns tell us whether P, Q, R are True or False. The next two columns correspond to the more complicated constituent parts of the logical statements in the claim, and the last two columns correspond to the two parts of the actual claim in the theorem. By comparing those last two columns, we can decide whether or not those two statements are logically equivalent. (Remember that "logically equivalent" means "has the same truth value as, no matter the assignment of truth values to P and Q and R". Thus, observing that the two columns have identicals entries, row by row, is sufficient to show that the two statements are logically equivalent.)

Next, let's talk about the semantic proofs. How do you feel about them? They were certainly longer, right? Disregarding that, though, did they feel like good proofs? Were they clear? Correct, even? Reread the proofs above and think about these questions. We will emphasize that they are fully correct proofs. The use of cases is essential when trying to prove a disjunction (an "*or*" statement) holds. When we suppose something is True and deduce that something else is True, that's how we prove a conditional statement is True. We will further analyze these techniques very soon, but we hope that giving you a first example like this will help you later on.

For the remainder of this section, we will use a truth table to verify simple claims like these. The proofs are much shorter that way! We are sure that you can go through the details of a semantic proof, like the ones we gave above, if you need further convincing or extra practice with interpreting symbolic logical claims as English sentences.

4.6.4 Proving Logical Equivalences: Distributive Laws

In arithmetic, you've used the fact that multiplication **distributes** across addition. That is, we know that

$$\forall x, y, z \in \mathbb{R}.\ x \cdot (y + z) = x \cdot y + x \cdot z$$

Hey, look, we wrote this in symbolic notation! Do you see why it says what you already know about the distributive property?

Here we will state and prove two similar laws. They will tell us that the logical connectives "$\wedge$" and "$\vee$" also distribute across each other.

Theorem 4.6.7. *Let P, Q, and R be logical statements. Then*

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$$

and

$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$$

Proof. We will use truth tables to verify these two claims. Observe, for the first claim, that

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

Notice that the last two columns are identical, thus proving the desired logical equivalence.

Observe, for the second claim, that

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

Again, notice that the last two columns are identical, thus proving the desired logical equivalence. $\square$

4.6.5 Proving Logical Equivalences: De Morgan's Laws (Logic)

Let's prove some logical equivalences involving **negations**. The following two laws are named for the British mathematician **Augustus De Morgan**. He is credited with establishing these logical laws, as well as introducing the term **mathematical induction**! We are grateful and indebted to his work in mathematics.

De Morgan's Laws for Logic state some logical equivalences about negating conjunctions and disjunctions.

Theorem 4.6.8. *Let P and Q be logical statements. Then*

$$\neg\big(P \wedge Q\big) \iff \neg P \vee \neg Q$$

and

$$\neg\big(P \vee Q\big) \iff \neg P \wedge \neg Q$$

Proof. We prove the first claim by a truth table:

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

And then we prove the second claim by a truth table:

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

□

These two laws are extremely useful! In fact, we can use them to prove similar statements about sets.

4.6.6 Using Logical Equivalences: DeMorgan's Laws (Sets)

The following statements "look a lot like" the statements in DeMorgan's Laws for Logic we saw above. We will see exactly why they look so similar when we see the proof!

Theorem 4.6.9. *Let A and B be any sets, and suppose that $A, B \subseteq U$, so the complement operation is defined in the context of U. Then,*

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

and

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

We will prove these claims using logical equivalences and DeMorgan's Laws for Logic. Our method will be to show that, in either case, the property of being an element of the set on the left-hand side of the equation is logically equivalent to being an element of the set on the right-hand side. This proves both parts of a double-containment argument in one fell swoop.

Proof. Let's prove the first set equality. Let $x \in U$ be arbitrary and fixed. Then,

$$\begin{aligned}
x \in \overline{A \cup B} &\iff x \notin A \cup B && \text{Definition of complement} \\
&\iff \neg\,(x \in A \cup B) && \text{Definition of } \notin \\
&\iff \neg\,[(x \in A) \vee (x \in B)] && \text{Definition of } \cup \text{ and } \vee \\
&\iff \neg(x \in A) \wedge \neg(x \in B) && \text{DeMorgan's Law for Logic} \\
&\iff (x \notin A) \wedge (x \notin B) && \text{Definition of } \notin \\
&\iff (x \in \overline{A}) \wedge (x \in \overline{B}) && \text{Definition of complement} \\
&\iff x \in \overline{A} \cap \overline{B} && \text{Definition of } \wedge \text{ and } \cap
\end{aligned}$$

Remember that" $\wedge$" is a *logical* operation, while "$\cap$" is a *set* operation. We had to be careful about which one made sense in every sentence we wrote. Also, notice that we used DeMorgan's Law for Logic in the middle of the proof, to convert a negation of a disjunction into the conjunction of two negations.

This chain of logical equivalences shows that

$$x \in \overline{A \cup B} \iff x \in \overline{A} \cap \overline{B}$$

so, in the context of U, the property of being an element of $\overline{A \cup B}$ is logically equivalent to the property of being an element of $\overline{A} \cap \overline{B}$. Therefore,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Let's prove the second equality now, with a similar method. Let $x \in U$ be arbitrary and fixed. Then,

$$\begin{aligned}
x \in \overline{A \cap B} &\iff x \notin A \cap B && \text{Definition of complement} \\
&\iff \neg\,(x \in A \cap B) && \text{Definition of } \notin \\
&\iff \neg\,[(x \in A) \wedge (x \in B)] && \text{Definition of } \cap \text{ and } \wedge \\
&\iff \neg(x \in A) \vee \neg(x \in B) && \text{DeMorgan's Law for Logic} \\
&\iff (x \notin A) \vee (x \notin B) && \text{Definition of } \notin \\
&\iff (x \in \overline{A}) \vee (x \in \overline{B}) && \text{Definition of complement} \\
&\iff x \in \overline{A} \cup \overline{B} && \text{Definition of } \vee \text{ and } \cup
\end{aligned}$$

This chain of logical equivalences shows that

$$x \in \overline{A \cap B} \iff x \in \overline{A} \cup \overline{B}$$

so, in the context of U, the property of being an element of $\overline{A \cap B}$ is logically equivalent to the property of being an element of $\overline{A} \cup \overline{B}$. Therefore,

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Voilà! We have proven both equalities stated in the theorem. $\square$

Notice the striking similarities between the two proofs. They used exactly the same method, and the only real difference is flipping a "$\cap$" to a "$\cup$", and vice-versa. Because we proved something about how to do this already (DeMorgan's Laws for Logic), we can cite that result and make this proof short and sweet. Wouldn't you agree this is far easier and more concise than writing out a full double-containment proof for these two claims? (Try it!)

4.6.7 Proving Set Containments via Conditional Statements

Whenever you can, go ahead and use the method we used in the previous section, with DeMorgan's Laws for Logic and Sets; that is, feel free to prove set relationships via conditional statements and logical equivalences. In general, when you're proving an equality, you need to be sure that all of your claims really are "$\Longleftrightarrow$" claims. In the previous section, we only applied definitions and a theorem about logical equivalences, so we were positive about all of the directions of the "$\Longleftrightarrow$" arrows in the proof. Whenever you write a proof like this, read over it again once you're done and ask yourself at every line, "Does this actually work? Does the implication work both ways here?"

Let's see another example of this technique in action. It will be slightly more complicated, in that we have to define some variable propositions because the claim given is not fundamentally identical to DeMorgan's Laws for Logic. We will, though, invoke a *logical* law that we just proved, and use it to establish a *sets* law.

Proposition 4.6.10. *Let A, B, C be any sets, with $A, B, C \subseteq U$, where U is a universal set. Then,*

$$A \cap (B - C) = (A \cap B) - C$$

Much like the previous example, DeMorgan's Laws for Sets, we will establish a logical equivalence between being an element of the left-hand side and being an element of the right-hand side. (Again, this is like proving both sides of a double-containment proof all at once.) To do this, we will just establish some variable propositions that refer to the properties of being an element of A, B, and C, respectively. From there, the result will follow from a logical law.

Proof. Let A, B, C be any sets, with $A, B, C \subseteq U$, where U is a universal set. We define the following variable propositions:

$$\begin{aligned} &\text{Let } P(x) \text{ be } \text{"}x \in A\text{"} \\ &\text{Let } Q(x) \text{ be } \text{"}x \in B\text{"} \\ &\text{Let } R(x) \text{ be } \text{"}x \in C\text{"} \end{aligned}$$

Let $x \in U$ be arbitrary and fixed. With these definitions, we can write the following chain of logical equivalences (where "Defn" is just space-saving shorthand for "Definition"):

$$\begin{aligned} x \in A \cap (B - C) &\iff x \in A \wedge (x \in B - C) && \text{Defn of } \cap \\ &\iff x \in A \wedge (x \in B \wedge x \notin C) && \text{Defn of } - \\ &\iff P(x) \wedge (Q(x) \wedge \neg R(x)) && \text{Defn of } P(x), Q(x), R(x), \notin \\ &\iff (P(x) \wedge Q(x)) \wedge \neg R(x) && \text{Associative Law for } \wedge \\ &\iff (x \in A \wedge x \in B) \wedge x \notin C && \text{Defn of } P(x), Q(x), R(x) \\ &\iff x \in A \cap B \ \wedge \ x \notin C && \text{Defn of } \cap \\ &\iff x \in (A \cap B) - C && \text{Defn of } - \end{aligned}$$

This shows that

$$x \in A \cap (B - C) \iff x \in (A \cap B) - C$$

holds True for any element x in the universe U. Therefore,

$$A \cap (B - C) = (A \cap B) - C$$

$\square$

Think about why we needed to make sure all of these claims are truly *if and only if* statements. We are ensuring that any element x that is an element of a set on one side of the equality is also necessarily an element of the set on the other side; but, furthermore, we are ensuring that any element x that is *not* an element of one set is *also* not an element of the other set. The biconditional statements "go both ways", so we prove both the "is an element of" and "is *not* an element of" parts of the claim all at once.

To illustrate our previous warnings, consider the following claim as an example of a proof where one "direction" of a $\iff$ claim *fails*.

Proposition 4.6.11. *Let X, Y, Z be any sets, with $X, Y, Z \subseteq U$, for some universal set U. Then, the following containment holds:*

$$(X \cup Y) - Z \subseteq X \cup (Y - Z)$$

You might recognize this claim as Problem 3.11.17! In that problem, we asked you to prove this claim using a containment argument, taking an arbitrary $x \in U$ and supposing it is an element of the left-hand side set, then deducing it must also be an element of the right-hand side set. We will do (essentially) the same thing here, but the argument will be recast in logical terms and symbols. We will do this to (1) give us more practice with making these types of arguments, but also (2) to recognize precisely *where* in the argument the "reverse" direction *fails*. Remember that, in Problem 3.11.17, we also asked you to find an example that shows that the $\supseteq$ direction is not *necessarily* True. This means that the logical argument working in that direction would break down somewhere. We will see precisely where that is, and we can use it to help us come up with that required counterexample.

Proof. Let X, Y, Z be any sets, with $X, Y, Z \subseteq U$, for some universal set U. Let $x \in U$ be arbitrary and fixed. We can write the following chain of logical equivalences:

$$\begin{aligned} x \in (X \cup Y) - Z &\iff x \in X \cup Y \ \wedge \ x \notin Z && \text{Defn of } - \\ &\iff (x \in X \ \vee \ x \in Y) \wedge x \notin Z && \text{Defn of } \cup \\ &\iff (x \in X \ \wedge \ x \notin Z) \vee (x \in Y \ \wedge \ x \notin Z) && \text{Distr. Law} \end{aligned}$$

Scratch work:

From here, what further logical equivalences could we assert? We could simplify the right-hand side and express it as

$$x \in X - Z \lor x \in X - Z$$

and, therefore,

$$x \in (X - Z) \cup (Y - Z)$$

This is not what the claim was, but this procedure so far would be a valid proof of a *different* claim, namely that

$$(X \cup Y) - Z = (X - Z) \cup (Y - Z)$$

However, our right-hand side is

$$X \cup (Y - Z)$$

but we are not trying to prove an equality, merely a *containment*. Thus, the goal of the rest of our proof is to prove this conditional claim:

$$\Big((x \in X \land x \notin Z) \lor (x \in Y \land x \notin Z) \Big) \implies x \in X \cup (Y - Z)$$

To help us figure out how to get there, let's do some scratch work here to rewrite the statement on the right-hand side; then, we can see how to get there from where we are already:

$$\begin{aligned} x \in X \cup (Y - Z) &\iff x \in X \lor x \in Y - Z && \text{Defn of } \cup \\ &\iff x \in X \lor (x \in Y \land x \notin Z) && \text{Defn of } - \end{aligned}$$

This is similar to the last logical equivalence we derived up above, but this one differs in the term on the left. Can you see how the one up above *implies* this one? Think about it, and then read on for the rest of our proof, resumed.

Now, we want to show that

$$\Big((x \in X \land x \notin Z) \lor (x \in Y \land x \notin Z) \Big) \implies x \in X \cup (Y - Z)$$

To do this, let's suppose the expression on the left-hand side is True. This means either

$$x \in X \land x \notin Z$$

or

$$x \in Y \land x \notin Z$$

(or possibly both). Thus, we have two cases:

1. Suppose the first expression is True, so that $x \in X \wedge x \notin Z$. This certainly means that $x \in X$, and thus $x \in X \vee x \in Y - Z$ holds.
2. Suppose the second expression is True, so that $x \in Y \wedge x \notin Z$. This means that $x \in Y - Z$, and thus $x \in X \vee x \in Y - Z$ holds.

In either case, we find that $x \in X \vee x \in Y - Z$ holds, and therefore,

$$x \in X \cup (Y - Z)$$

holds, in either case, by the definition of $\cup$.

Overall, this shows that

$$x \in (X \cup Y) - Z \implies x \in X \cup (Y - Z)$$

holds for every element $x \in U$. Therefore, by the definition of $\subseteq$, we have

$$(X \cup Y) - Z \subseteq X \cup (Y - Z)$$

$\square$

Recognizing where we are, and where we wanted to go, helped us finish this proof. We had no hope of completing it using logical equivalences alone because, in fact, the sets given in the claim are not always equal! Looking back at the proof, can we identify the step whose logical equivalence was *invalid*, and can we use it to help construct a counterexample to the (False) claim that those sets are always equal?

We had reached as far as this valid statement

$$(x \in X \wedge x \notin Z) \vee (x \in Y \wedge x \notin Z)$$

and we used it to deduce this statement

$$x \in X \vee (x \in Y \wedge x \notin Z)$$

It seems clear, from our argument in the proof, that the first statement does *imply* the second one; that is, if we *suppose* the first statement holds, we can figure out that the second statement one holds, as well. The only difference between them is in the first term, and knowing *two* parts of an "$\wedge$" statement hold certainly lets us conclude a particular *one* of them holds.

This deduction does *not* work in the other direction. Suppose that second statement holds. If it's the right term that is valid—that $x \in Y \wedge x \notin Z$— then this also makes the first statement hold. However, since we have an "$\vee$" statement, we have to consider the case where the left term is the one that holds. In that case, knowing only $x \in X$ does not let us deduce that $x \in X \wedge x \notin Z$ holds. *Supposing* an "$\wedge$" holds lets us deduce either one of its parts holds, but just *knowing* only one part cannot tell us that both hold!

We can use this to construct a counterexample. We see that we just need to ensure that there is some particular element $x \in U$ that satisfies the left term in the second statement, namely $x \in X$, but does *not* satisfy the left term in the first statement, namely $x \in X \wedge x \notin Z$. Said another way, we just need to ensure that there *is* an element $x \in X \cap Z$. The following example accomplishes exactly that.

Example 4.6.12. We claim that

$$(X \cup Y) - Z \subseteq X \cup (Y - Z)$$

holds for *any* sets X, Y, Z, but equaltiy *need not* hold. See the proof of Proposition 4.6.11 to see why the containment claimed above does hold.

Now, consider the following example. Let's define

$$\begin{aligned} X &= \{1\} \\ Y &= \{2\} \\ Z &= \{1, 2\} \end{aligned}$$

Notice that

$$(X \cup Y) - Z = (\{1\} \cup \{2\}) - \{1, 2\} = \{1, 2\} - \{1, 2\} = \varnothing$$

and

$$X \cup (Y - Z) = \{1\} \cup (\{2\} - \{1, 2\}) = \{1\} \cup \{\varnothing\} = \{1\}$$

Since $\varnothing \subset \{1\}$ (a *proper*) subset, we conclude that

$$(X \cup Y) - Z \neq X \cup (Y - Z)$$

in this case. This shows that equality need not hold in the claim above.

This strategy now lets us go back and complete many proofs involving sets in a more efficient and rigorous manner! Rather than fumbling through the linguistics of "ands" and "ors", we can use our logical notation and laws that we have *proven*. Many of the exercises in this section deal with sets, specifically because of this. If you need to flip back to Chapter 3 and remind yourself of any relevant definitions, go right ahead!

4.6.8 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) What are the Associative Laws for Logic?

(2) What are the Distributive Laws for Logic?

(3) What are DeMorgan's Laws for Logic? What are DeMorgan's Laws for Sets? How are they related?

(4) What is the difference between a necessary and a sufficient condition?

(5) What happens when a condition is both necessary and sufficient?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) We used Truth Tables to prove DeMorgan's Laws for Logic. Can you come up with a semantic proof? Can you explain DeMorgan's Laws to a non-mathematician friend and convince them they are valid?

(2) Let $P(x)$ be the variable proposition "x is an integer that is divisible by 10". Come up with two necessary conditions and two sufficient conditions for this statement.

(3) Let A, B, C be any sets, where $A, B, C \subseteq U$, for some universal set U.

Use logical equivalences and logical laws to prove the following claims.

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(b) $(A \cup B) \cap \overline{A} = B - A$
(c) $\overline{\overline{A} \cup B} = A \cap \overline{B}$
(d) $(A - B) \cap \overline{C} = A - (B \cup C)$

(4) Use conditional statements and logical equivalences to prove that the containment

$$A - (B \cup C) \subseteq A \cap \left(\overline{B \cap C}\right)$$

holds for any sets A, B, C.

Then, find an example that shows that equality *need not* hold.

(**Hint:** In general, a helpful idea in constructing a *strict* set containment is to see if you can make one side the *empty set*.)

(5) Let D, E, F be any sets. Consider the sets

$$D - (E - F)$$

and

$$(D - E) - F$$

How do they compare? Are they always equal? Is one always a subset of the other, or vice-versa?

Clearly state your claims, then either prove them or provide relevant counterexamples.

4.7 Negation of Any Mathematical Statement

We saw already how to negate quantified statements. With DeMorgan's Laws in hand, we now know how to negate $\wedge$ and $\vee$ statements. What's left? Aha, conditional statements!

4.7.1 Negating Conditional Statements

Consider a claim of the form $P \implies Q$. It says that *whenever* P is true, Q is also true. How do we negate such a statement? What would the logical negation even mean? Think back to how we defined " $\implies$ " as a logical connective. In which cases did we get to call the speaker of the conditional statement a *liar*. Those are precisely the cases where we would say the logical negation is True. The *only* such case was when the hypothesis P was True but the conclusion Q was False.

To prove this equivalence, we need to remember the way to write $P \implies Q$ as an "$\vee$" statement:

$$(P \implies Q) \iff (\neg P \vee Q)$$

This will help us in the proof of the following claim.

Lemma 4.7.1. *The logical negation of a conditional statement is given by*

$$\neg(P \implies Q) \iff P \wedge \neg Q$$

Proof. Observe that

$$\begin{aligned} \neg(P \implies Q) &\iff \neg(\neg P \vee Q) && \text{Logical equivalence proven already} \\ &\iff \neg(\neg P) \wedge \neg Q && \text{DeMorgan's Law for Logic} \\ &\iff P \wedge \neg Q && \text{since } \neg(\neg P) \iff P \end{aligned}$$

□

This makes intuitive sense: to show that a conditional claim is False, we need to find a case where the hypothesis holds but the conclusion fails.

Despite the risk of putting bad ideas into your head that weren't already there, we are going to point out some statements that are **NOT** logically equivalent to $\neg(P \implies Q)$. These are common mistakes that we see students use fairly often. Let's check them out and see why they don't actually work. For each of them, keep in mind that we want the logical negation $\neg(P \implies Q)$ to be *guaranteed to have the exact opposite truth value* of the original statement $P \implies Q$. In each of these cases, we can see that this relationship would not hold.

- $\neg P \implies Q$

  This conditional statement has no logical connection to the original claim, $P \implies Q$. Remember that the statement $P \implies Q$ makes *no claim* about whether Q is true or not in the cases where P is False. (Think about the "If it is raining, then I carry my umbrella" example. If it's not raining, who knows what I'm carrying!) Thus, why would we expect Q to be *necessarily true* in those cases, like this statement says?

- $P \implies \neg Q$

  Again, this conditional statement has no logical connection to the original claim. Think about the umbrella example again. This statement would say "If it is raining, then I will **not** be carrying an umbrella." Is that what it means for the original claim to be False? Definitely not!

- $P \not\Longrightarrow Q$

  This one is more subtle. A mathematician would read "$P \not\Longrightarrow Q$" as "P does *not necessarily* imply Q". That is, it would say that there are assignments of truth values where $P \implies Q$ is valid and there are assignments where $P \implies Q$ is invalid; those cases would depend on what the individual statements P and Q are. This is a somewhat meaningful claim to make, depending on the situation, but it is not, strictly speaking, the **logical negation** of the original claim.

  In particular, we run into an issue when we try to take the logical negation of *this* statement. What does it mean to say that "It is not the case that P does not necessarily imply Q"? Does that mean there exists cases where P does not imply Q but there are also cases where P does imply Q? That sounds an awful lot like the actual claim $P \not\Longrightarrow Q$, itself ...

  For these reasons, we want to avoid using this notation: $\not\Longrightarrow$. It does have some kind of meaning in mathematics, but it is not really well-defined in a symbolic logical sense. And in any event, it is definitely *not* the logical negation of $\implies$.

Now that we have these common *errors* out of the way, let's stress the *correct* negation of $P \implies Q$. We find that it's quite helpful to remember the "$\vee$" version of a conditional statement; from there, it's easy to apply DeMorgan's Law and negate the statement:

$$\boxed{\neg(P \implies Q) \iff \neg(\neg P \vee Q) \iff P \wedge \neg Q}$$

Negating "$\iff$"

To negate a biconditional statement, we just write it as a conjuction of two conditional statements:

$$\neg(P \iff Q) \iff [\neg(P \implies Q) \vee \neg(Q \implies P)] \iff (P \wedge \neg Q) \vee (Q \wedge \neg P)$$

If you do any kind of comptuer programming, you might recognize the statement on the right as the `XOR` operator! It says that *exactly one* statement is True, either P or Q, but *not both*.

4.7.2 Negating Any Statement

That's it, right? We have now discussed how to negate any fundamental mathematical claim: $\exists$, $\forall$, $\wedge$, $\vee$, and $\implies$. Everything else we write will be a combination of these basic claims, so we should be able to just apply these techniques over and over and negate any statement we come across. Essentially, we just read the statement left to right and negate every piece in turn. Come across a "$\exists$"? Just switch it to a "$\forall$" and negate the property that comes after! Come across an "$\vee$"? Negate both sides and switch it to and "$\wedge$"! Come across a conditional? Apply the technique we just showed above!

Let's see several examples to get the idea.

Example 4.7.2. Find the logical negation of

$$\forall x \in \mathbb{R}.\ x < 0 \vee x > 0$$

This statement says "Every real number x satisfies either $x < 0$ or $x > 0$."

The logical negation is

$$\neg\left(\forall x \in \mathbb{R}.\ x < 0 \vee x > 0\right) \iff \exists x \in \mathbb{R}.\ x \geq 0 \wedge x \leq 0$$

Notice that we applied DeMorgan's Law for Logic to negate the $\vee$ claim on the right-hand side, and we used the fact that $x \not> 0$ is logically equivalent to $x \leq 0$.

We see that this negation is True because $0 \in \mathbb{R}$ and $0 \leq 0$ and $0 \geq 0$. Thus, the original statement was False.

Example 4.7.3. Find the logical negation of

$$\exists n \in \mathbb{N}.\ n \geq 10 \wedge \sqrt{n} \leq 3$$

This statement says "There exists a natural number n that satisfies both $n \geq 10$ and $\sqrt{n} \leq 3$.

The logical negation is

$$\forall n \in \mathbb{N}.\ n < 10 \vee \sqrt{n} > 3$$

That is, the logical negation says "Every natural number n satisfies either $n > 10$ or $\sqrt{n} < 3$.

Example 4.7.4. Find the logical negation of

$$\exists x \in \mathbb{R} \centerdot \forall y \in \mathbb{R} \centerdot x \geq y \implies x^2 \geq y^2$$

This statement says "There exists a real number x such that whenever we have a real number y that satisfies $x \geq y$, we may conclude that $x^2 \geq y^2$".

The logical negation is

$$\forall x \in \mathbb{R} \centerdot \exists y \in \mathbb{R} \centerdot x \geq y \wedge x^2 < y^2$$

Can you prove that this logical negation is, in fact, the True statement? Try it!

Example 4.7.5. Find the logical negation of

$$\forall X \in \mathcal{P}(\mathbb{Z}) \centerdot (\forall x \in X \centerdot x \geq 1) \implies X \subseteq \mathbb{N}$$

This statement says that "For every subset X of the integers $\mathbb{Z}$, if every element x of the set X satisfies $x \geq 1$, then X is a subset of the natural numbers $\mathbb{N}$."

The logical negation is

$$\exists X \in \mathcal{P}(\mathbb{Z}) \centerdot (\forall x \in X \centerdot x \geq 1) \wedge X \not\subseteq \mathbb{N}$$

This statement says that "There is a subset $X \subseteq \mathbb{Z}$ such that every element $x \in X$ satisfies $x \geq 1$ and yet $X \not\subseteq \mathbb{N}$." We could even rewrite the last part further by noting that

$$X \not\subseteq \mathbb{N} \iff \exists y \in X \centerdot y \notin \mathbb{N}$$

although this wouldn't be totally essential.

Which statement (the original or the negation) is True? Can you prove it?

Compare the statement used in the example above with the following one:

$$\forall X \in \mathcal{P}(\mathbb{Z}) \centerdot \forall x \in X \centerdot \big(x \geq 1 \implies X \subseteq \mathbb{N}\big)$$

The only difference between them is the location of the parentheses, but this completely changes the statement's meaning!

The statement used in the example asserts something about *every* subset of the integers. That is, no matter what subset $X \subseteq \mathbb{Z}$ is introduced, the statement says that *if* that set has the property that all of its elements are at least 1, *then* that set X is actually a subset of $\mathbb{N}$, as well.

The new statement written in this box says something else: no matter what subset $X \subseteq \mathbb{Z}$ is introduced and, furthermore, no matter what element

x of *that* set X is introduced, the statement says that *if* that element x is at least 1, *then* that set X is a subset of $\mathbb{N}$, as well.

Do you see why this is different? The issue is where the "if" happens: where does the quantification end and the conditional statement begin? The first statement, from the above example, puts the quantification over elements of X inside the "if" part of the conditional statement. The second statement, in this box, puts that quantification before the conditional statement entirely.

We claim that this second version, in this box, is False, and we encourage you to figure out why (if you haven't already).

Example 4.7.6. Let $O(x)$ be the proposition "x is odd", and let $E(x)$ be the proposition "x is even". Find the logical negation of the statement

$$\forall x, y \in \mathbb{Z}.\ O(x \cdot y) \iff (O(x) \wedge O(y))$$

This statement says that "For every two integers x and y, their product is odd if and only if they are both odd, themselves".

Before we find the logical negation, remember the $\iff$ means "$\implies$ and $\impliedby$". Let's rewrite the claim that way first, so that we can negate it properly:

$$\forall x, y \in \mathbb{Z}.\ [O(x \cdot y) \implies (O(x) \wedge O(y))] \wedge [(O(x) \wedge O(y)) \implies O(x \cdot y)]$$

The logical negation is

$$\begin{aligned}
&\neg\Big(\forall x, y \in \mathbb{Z}.\ [O(x \cdot y) \implies (O(x) \wedge O(y))] \wedge [(O(x) \wedge O(y)) \implies O(x \cdot y)]\Big) \\
&\iff \exists x, y \in \mathbb{Z}.\ \neg\,[O(x \cdot y) \implies (O(x) \wedge O(y))] \\
&\qquad\qquad\qquad \vee \neg\,[(O(x) \wedge O(y)) \implies O(x \cdot y)] \\
&\iff \exists x, y \in \mathbb{Z}.\ [O(x \cdot y) \wedge \neg(O(x) \wedge O(y))] \vee [(O(x) \wedge O(y)) \wedge \neg O(x \cdot y)] \\
&\iff \exists x, y \in \mathbb{Z}.\ [O(x \cdot y) \wedge (E(x) \vee E(y))] \vee [(O(x) \wedge O(y)) \wedge E(x \cdot y)]
\end{aligned}$$

That is, the logical negation says "There exist integers x and y such that either their product is odd and yet (at least) one of them is even, or they are both odd and yet their product is even.

Can you prove which one of these claims is True?

4.7.3 Questions & Exercises

Remind Yourself

Answering the following questions briefly, either out loud or in writing. These are all based on the section you just read, so if you can't recall a specific definition or concept or example, go back and reread that part. Making sure you can confidently answer these before moving on will help your understanding and memory!

(1) How is a mathematical statement related to its logical negation?

(2) What is the logical negation of a conditional statement?

(3) Consider the statement $P \implies Q$. What is its contrapositive? What is the logical negation of that contrapositive? Can you see that it must have the *same* truth value as the logical negation of the original statement?

(4) What is the logical negation of an *if and only if* statement, $P \iff Q$? Why does this make sense, considering what such a statement says about the *truth values* of P and Q?

Try It

Try answering the following short-answer questions. They require you to actually write something down, or describe something out loud (to a friend/classmate, perhaps). The goal is to get you to practice working with new concepts, definitions, and notation. They are meant to be easy, though; making sure you can work through them will help you!

(1) Write out the logical negation of each of the following mathematical statements.

Then, determine the *truth value* of each statement.

(If you're feeling ambitious, formally prove/disprove each statement!)

(a) $\exists x \in \mathbb{N} \,.\, \forall y \in \mathbb{N} \,.\, y - x^2 \geq 0$

(b) $\exists x \in \mathbb{Z} \,.\, \forall y \in \mathbb{R} \,.\, xy = 0$

(c) $\exists x \in \mathbb{Z} \,.\, \forall y \in \mathbb{Z} \,.\, (y \neq 0 \implies xy > 0)$

(d) $\forall a, b \in \mathbb{Q} \,.\, ab \in \mathbb{Z} \implies (a \in \mathbb{Z} \vee b \in \mathbb{Z})$

(e) $\forall x \in \mathbb{R} \,.\, x > 0 \implies \big(\exists y \in \mathbb{R} \,.\, y < 0 \wedge xy > 0 \big)$

(f) $\forall x \in \mathbb{R} \,.\, \left| x + \frac{1}{x} \right| = 2 \iff x = 1$

(2) Let $A = \{1, 2, 3, 4\}$ and $B = \{2, 3\}$.

What is the difference between the following two statements? Determine the truth value of each one.

Then, negate each one, and explain how those negations also differ. What are their truth values?

(a) $\forall x \in A \,.\, \forall y \in B \,.\, (x \geq y \implies x^2 \geq 4)$

(b) $\forall x \in A \,.\, (\forall y \in B \,.\, x \geq y) \implies x^2 \geq 4$

(3) Let $P = \{x \in \mathbb{R} \mid x > 0\}$. Write the logical negation of each of the following statements, and determine their truth values.

(a) $\forall \varepsilon \in P \,.\, \forall x \in P \,.\, \exists \delta \in P \,.\, \forall y \in \mathbb{R} \,.\, \left(|x - y| < \delta \implies \left| \frac{1}{x} - \frac{1}{y} \right| < \varepsilon \right)$

(b) $\forall \varepsilon \in P \,.\, \exists \delta \in P \,.\, \forall x \in P \,.\, \forall y \in \mathbb{R} \,.\, \left(|x-y| < \delta \implies \left| \frac{1}{x} - \frac{1}{y} \right| < \varepsilon \right)$

Hint/suggestion: A statement like $|a| < b$ can be written as $-b < a < b$. Also, a statement like $a < b < c$ can be written as $a < b \wedge b < c$. This might help you rewrite the statements when determining their truth values.

(4) Let $P(n)$ be the proposition "n is odd" and let $Q(n)$ be the proposition "$n^2 - 1$ is divisible by 8".

Write the logical negation of the statement

$$\forall n \in \mathbb{N} \,.\, P(n) \iff Q(n)$$

and determine its truth value.

(5) Let $P = \{x \in \mathbb{R} \mid x > 0\}$. Write the logical negation of each of the following statements, and determine their truth values.

(a) $\forall \varepsilon \in P \,.\, \exists \delta \in P \,.\, \forall x \in \mathbb{R} \,.\, 0 < x < \delta \implies \frac{1}{x} > \frac{10}{\varepsilon}$

(b) $\forall \varepsilon \in P \,.\, \exists x \in \mathbb{R} \,.\, \forall n \in \mathbb{N} \,.\, \left(n > x \implies \frac{(-1)^n}{n} < \varepsilon \right)$

(c) $\forall \varepsilon \in P \,.\, \exists x \in \mathbb{R} \,.\, \forall n \in \mathbb{N} \,.\, \left(n > x \iff \frac{(-1)^n}{n} < \varepsilon \right)$

4.8 [Optional Reading] Truth Values and Sets

There is a convenient and interesting relationship between sets (and their corresponding relationships and operations) and logical truth values (and their corresponding relationships and connectives). We will mention it here and demonstrate some examples, and leave it to you to investigate it further, if you'd like. We won't need these kinds of ideas in the rest of our work, but we believe that thinking about these ideas and sorting them out in your head will really help your understanding of the fundamentals of logic, as well as sets.

Suppose we have two variable propositions, $P(x)$ and $Q(x)$. Further, suppose these propositions make sense for any input x that comes from some universal set U. (This set U depends on the specific statements inside $P(x)$ and $Q(x)$, of course, but we don't really care what they are for this general discussion.) For each of these propositions, we can define a **truth set**; that is, we can consider the set of all instances x from the universe U that make those propositions evaluate as True. We define

$$T_P = \{x \in U \mid P(x) \text{ is True}\}$$
$$T_Q = \{x \in U \mid Q(x) \text{ is True}\}$$

Perhaps the propositions $P(x)$ and $Q(x)$ are related somehow. Let's suppose that, in fact,

$$\forall x \in U \,.\, P(x) \implies Q(x)$$

holds. What does this say about those **truth sets**? This conditional statement says that any x that satisfies $P(x)$ (i.e. makes $P(x)$ True) must *also* satisfy $Q(x)$. Written another way, using those truth sets, we have

$$\forall x \in U \,.\, x \in T_P \implies x \in T_Q$$

This is precisely the definition of "subset"! What we have just discovered is that

$$T_P \subseteq T_Q$$

when that conditional statement above holds.

Let's suppose even further, now, that

$$\forall x \in U \,.\, P(x) \iff Q(x)$$

holds. We just discovered that $T_P \subseteq T_Q$, and applying the exact same reasoning to the "other direction" of that $\iff$ statement (that is, the $Q(x) \implies P(x)$ part of it) will show us that $T_Q \subseteq T_P$, as well. By the definition of set equality, this means that

$$T_P = T_Q$$

when that biconditional statement above holds.

How else might we combine the propositions $P(x)$ and $Q(x)$? Let's consider the proposition $P(x) \wedge Q(x)$. What are the instances x that make this conjunction True? How can we characterize those instances in terms of the truth sets we defined? Think about it for a minute, and you'll see that all of those instances are characterized by the intersection of those sets; we need *both* $P(x)$ and $Q(x)$ to hold, so we need an instance that comes from both of the truth sets.

Similarly, we can consider the conjunction $P(x) \vee Q(x)$. An instance x makes this statement True when that x makes *at least one* of the propositions True. Thus, that x must come from at least one of the sets, so it must come from their *union*.

Let's summarize these relationships we have discovered:

$$\begin{aligned}
\forall x \in U \,.\, \big(P(x) \implies Q(x)\big) &\iff \big(T_P \subseteq T_Q\big) \\
\forall x \in U \,.\, \big(P(x) \iff Q(x)\big) &\iff \big(T_P = T_Q\big) \\
\forall x \in U \,.\, \big(P(x) \wedge Q(x)\big) &\iff \big(x \in T_P \cap T_Q\big) \\
\forall x \in U \,.\, \big(P(x) \vee Q(x)\big) &\iff \big(x \in T_P \cup T_Q\big)
\end{aligned}$$

Can you come up with some characterizations, using truth sets, for the following statements? Fill in the blanks!

$$\forall x \in U \,.\, \big(P(x) \wedge \neg Q(x)\big) \iff \underline{\hspace{3cm}}$$

$$\big(\exists x \in U \,.\, P(x)\big) \iff \underline{\hspace{3cm}}$$

$$\forall x \in U \,.\, \big(\neg P(x) \iff \underline{\hspace{3cm}}\big)$$

(Careful: how are the previous statement and the next one different?)

$$\big(\forall x \in U \,.\, \neg P(x)\big) \iff \underline{\hspace{3cm}}$$

4.9 Writing Proofs: Strategies and Examples

We are now prepared to fully tackle the goal we have been building towards all along: writing PROOFS!

In this section, we will apply all of these fundamental logical principles we have developed in this chapter. Specifically, we will learn how to use them to write formal arguments that demonstrate the truth (or falsity) of mathematical statements. In general, it's hard to describe how to figure out which mathematical statements are True and which are False. In a way, though, the strategies we develop here will help us discover truths. More importantly, though, they will provide us with templates and guidelines for how to actually present a truth to someone else and describe *why* it is, indeed, a truth.

As we have discussed, it is not enough to figure out some interesting fact and just hope that others will trust us about it. We need to be able to *explain* that fact; we need to present an argument that will *convince* someone else of its truth. We don't necessarily have to explain where it came from, or why we cared to investigate it in the first place (although sometimes you might want to answer these implicit questions, if you think it would help a potential reader). In general, we just need to make sure that someone else—a peer, a classmate, a fellow mathematician—can pick up our written proof, read it, and afterwards be fully convinced that what we claimed to be True is, indeed, True.

Outline of this section

Mostly, we hope you will see how the ensuing strategies come directly from the underlying logical principles associated with propositions and quantifiers and connectives and negations. We have split the section into several subsections, each one corresponding to a particular quantifier or connective.

When you face a mathematical statement and have to prove it, just start reading the statement left to right. What do you encounter first? If it's a "$\exists$" quantifier, look at Section 4.9.1. If it's a "$\forall$" quantifier, look at Section 4.9.2. After that, what type of claim do you face? What form does the ensuing variable proposition take? Is it an "$\vee$" statement? Look at Section 4.9.3. Is it a conditional statement? Look at section 4.9.5. Is it a conditional statement where the hypothesis is an "$\vee$" statement and the conclusion is an "$\wedge$" statement? Look at all three Sections—4.9.3 and 4.9.4 and 4.9.5—and combine them appropriately! In general, every proof we write from now on (except for induction proofs, which we will return to in the next chapter) will be a combination of these strategies. Which ones you use and how you combine them depends on the statement you're trying to prove and how you've decided to approach it.

Within each subsection, we have provided some templates and some examples. You might find the templates too restrictive, perhaps too formal; we understand, but we think that following our formats as closely as possible for now will help you in the long run. These templates—as well as how we've used them in the examples provided—are meant to emphasize the logical principles behind these proof strategies. Working with them closely will give you extra practice with these logical concepts and, we strongly believe, help you adapt them for your own uses in the future.

For each example provided, we have boxed the proof strategy in blue and the example implementation in green and any necessary scratch work in red. Any other discussion of the strategy or the implementation appears outside of those boxes.

Also, several of the examples we consider in this section (and the next one) are interesting and useful results, in their own right. You'll notice that some of them have a name or a descriptive title, which is meant to indicate this fact. While the main emphasis of this section is on the **proof strategies**—developing them and seeing how to use them—we encourage you to also keep in mind these examples as interesting facts, themselves. We'll bring up this idea again when it's warranted, but we'll keep those discussions brief, so as not to distract from the overall structure of this section.

Direct vs. Indirect methods

You will also notice that each subsection includes strategies for both **direct** and **indirect** methods. These terms might not be familiar to you yet. All they refer to is whether or not we try to prove a statement (1) directly by demonstrating that it is True, or (2) indirectly by invoking the Law of the Excluded Middle, by demonstrating that its logical negation is False.

Both forms of strategy are, in general, equally valid, but **direct** proofs are typically considered subjectively better by many readers. (Sometimes, you might write an indirect proof that is actually hiding a direct proof inside it!) These subjective ideas will be assessed and discussed as we work through examples and ask you to write proofs on your own, in the exercises.

You'll notice that all of our indirect proofs begin with the phrase "Assume for sake of contradiction", usually abbreviated as "AFSOC". This is an important and helpful phrase. It signals to the reader of our proof that we are going to make an assumption but we don't *really* think that the assumption is valid. Rather, we are going to use this assumption to derive something False, a **contradiction**. This will allow us to conclude that our original assumption was invalid, so its logical negation (i.e. our original statement that we hoped to prove) is actually True. You'll see that we use the symbol " ⨳ " to indicate a contradiction, but we also make sure to point out *why* we have found a contradiction. We don't leave it to the reader to figure it out!

Alright, that's enough preamble. Let's dive right in and WRITE SOME PROOFS!

4.9.1 Proving $\exists$ Claims

An "$\exists$" claim is one of *existence*. It asserts that some particular object exists as an element of some set and that it has a certain property. To prove such a claim, we need to exhibit such an object and verify, for our reader, that (1) that object is an element of the correct set and (2) that object has the correct property.

Direct Method

Strategy:

Claim: $\exists x \in S \,.\, P(x)$

Direct proof strategy:

Define a specific example, $y =$ ______.

Prove that $y \in S$.

Prove that $P(y)$ holds true.

Example 4.9.1. *Solving a system of linear equations:*

Statement: Fix $a, b, c, d, e, f \in \mathbb{R}$ with the property that $ad - bc \neq 0$.

We claim that one can simultaneously solve

$$ax + by = e \tag{4.1}$$
$$cx + dy = f \tag{4.2}$$

for some $x, y \in \mathbb{R}$.

Define $S(x, y)$ to be the statement "x and y simultaenously satisfy both equations, (4.1) and (4.2), above". Then we claim

$$\exists x, y \in \mathbb{R} \,.\, S(x, y)$$

First, we must do some scratch work to *construct* the solution. Then, we can write a proof that defines the objects x and y and shows why they work.

Scratch work:

We need $ax + by = e$ and $cx + dy = f$, and we want to know which x and y make this work.

Let's multiply the first and second equations by the right coefficients (namely, d and -b, respectively) so we can cancel the y terms by adding the two lines:

$$\begin{array}{r} adx + bdy = de \\ +\big(-bcx - bdy = -bf\big) \\ \hline (ad-bc)x = de - bf \end{array}$$

Dividing tells us $x = \frac{de-bf}{ad-bc}$, which is okay because $ad - bc \neq 0$.

Doing something similar, canceling the x terms, tells us how to get y:

$$\begin{array}{r} acx + bcy = ce \\ +\big(-acx - ady = -af\big) \\ \hline (bc-ad)y = ce - af \end{array}$$

Dividing tells us $y = \frac{af-ce}{ad-bc}$.

The main lesson here is that we do not need to show this scratch work in our proof below! We don't assume that a reader would care to wade through our messy notes about *how* we came up with the solution to the system of linear equations. Rather, we assume the the reader only cares about *what* the solution is and *why* it's a solution. Also, this makes the proof much more concise, so it can be read more easily and quickly.

Implementation:

Proof. Since $ad - bc \neq 0$ (by assumption), we may define

$$x = \frac{de-bf}{ad-bc} \qquad \text{and} \qquad y = \frac{af-ce}{ad-bc}$$

and know that $x, y \in \mathbb{R}$. Then,

$$ax + by = \frac{(ade - abf) + (abf - bce)}{ad-bc} = \frac{ade-bce}{ad-bc} = \frac{e(ad-bc)}{ad-bc} = e$$
$$cx + dy = \frac{(cde - bcf) + (adf - cde)}{ad-bc} = \frac{adf-bcd}{ad-bc} = \frac{f(ad-bc)}{ad-bc} = f$$

so $S(x, y)$ holds. □

If you've studied some linear algebra before, you'll recognize the term $ad-bc$ as the **determinant** of the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. The stipulation that $ad - bc \neq 0$ means that we require this matrix of coefficients to *have an inverse*, to be "nonsingular". In that situation, we have a solution to the system for any $e, f \in \mathbb{R}$.

Indirect Method (Proof by Contradiction)

This strategy relies on the logical negation of an $\exists$ claim:

$$\neg\big(\exists x \in S \,.\, P(x)\big) \iff \forall x \in S \,.\, \neg P(x)$$

We will assume this negation and deduce something contradictory from it, meaning the negation is False so the original is True.

Claim: $\exists x \in S \,.\, P(x)$

Indirect proof strategy:

AFSOC that for every $y \in S$, $\neg P(y)$ holds.

Find a contradiction.

Example 4.9.2. *A version of the Pigeonhole Principle:*

Statement: Suppose $n \in \mathbb{N}$ and we have n real numbers, $a_1, a_2, \ldots, a_n \in \mathbb{R}$.

We claim that one of the numbers is at least as large as their average. That is,

$$\exists B \in [n] \,.\, a_B \geq \frac{1}{n}\sum_{i=1}^{n} a_i$$

Proof. AFSOC none of the numbers are at least as large as the average, i.e.

$$\forall i \in [n] \,.\, a_i < \frac{1}{n}\sum_{i=1}^{n} a_i$$

Define the constant $S = \sum_{i=1}^{n} a_i$, so that $a_i < \frac{S}{n}$.

Then we can sum all of the a_is and observe that

$$S = \sum_{i=1}^{n} a_i < \sum_{i=1}^{n} \frac{S}{n} = n \cdot \frac{S}{n} = S$$

This shows that the real number S is *strictly* less than itself: $S < S$. This is a contradiction. ※

Therefore, the original assumption was false, and the claim follows. $\square$

As stated, this is a version of the **Pigeonhole Principle**. We will investigate and use this principle again in Section 8.6, when we study **combinatorics**.

4.9.2 Proving ∀ Claims

A "∀" claim is one of *universality*. It asserts that *all* elements of a set have some common property. To prove such a claim, we need to show that *every* element of the set has that property. To accomplish this "all at once", we will consider an **arbitrary and fixed** element of the set, and prove that it has the desired property. Because this object is arbitary, our argument applies to every element of the set. Because this object is fixed, we are allowed to refer to it by name throughout the proof.

Direct Method

Strategy:

Claim: $\forall x \in S \centerdot P(x)$

Direct proof strategy:

Let $y \in S$ be arbitrary and fixed.

Prove that $P(y)$ holds true.

Example 4.9.3. *A version of the AGM Inequality:*

Statement: $\forall x, y \in \mathbb{R} \centerdot xy \leq \left(\frac{x+y}{2}\right)^2$

Implementation:

Proof. Let $x, y \in \mathbb{R}$ be arbitrary and fixed.

We know $0 \leq (x-y)^2$.

Multiplying out and rearranging, we get $2xy \leq x^2 + y^2$.

Adding $2xy$ to both sides, we get $4xy \leq x^2 + 2xy + y^2$.

Factoring, we get $4xy \leq (x+y)^2$.

Dividing by 4 and putting that into the square, we get

$$xy \leq \left(\frac{x+y}{2}\right)^2$$

□

This result is known as the **AGM Inequality** because it deals with the Arithmetic Mean (AM) and the Geometric Mean (GM) of two real numbers.

The Arithmetic Mean of x and y is $\frac{x+y}{2}$.

The Geometric Mean of x and y is $\sqrt{xy}$. (Notice that this only applies when

$xy \geq 0$, i.e. when x and y have the *same sign* be it positive or negative, or zero.)

The AGM Inequality asserts that the AM is always at least as large as the GM. A helpful mnemonic is to read "**AGM**" as "**A**rithmetic Mean **G**reater than **G**eometric **M**ean".

What we proved above is a slightly more general version, because it applies to *all* real numbers x and y, and not just those with the same sign. Supposing that $xy \geq 0$, though, one can simply take the square root of both sides and obtain the "usual" statement of the AGM Inequality: $\sqrt{xy} \leq \frac{x+y}{2}$.

Indirect Method (Proof by Contradiction)

Claim: $\forall x \in S \,.\, P(x)$

Indirect proof strategy:

> AFSOC that $\exists y \in S$ such that $\neg P(y)$ holds.
>
> Find a contradiction.

Example 4.9.4. $\sqrt{2}$ *is irrational:*

Statement: $\forall a, b \in \mathbb{Z} \,.\, \frac{a}{b} \neq \sqrt{2}$

(Note: This claim is appealing directly to the definition of the rational numbers $\mathbb{Q}$. It is saying that $\sqrt{2} \notin \mathbb{Q}$ because that number has *no* representation as a ratio of integers.)

Implementation:

Proof. AFSOC $\exists a, b \in \mathbb{Z} \,.\, \frac{a}{b} = \sqrt{2}$.

We may assume that $\frac{a}{b}$ is given in *reduced form*, so that a and b have no common factors. (If this were not the case, we could just reduce the fraction and obtain such a form.)

Let such $a, b \in \mathbb{Z}$ be given.
(**Note:** We discuss this phrase, "let such ______ be given", below in Section 4.9.8. It is meant to not only assert that such an $a, b \in \mathbb{Z}$ *exist*, but also that we want some *particular* instances of those variables so that we can work with them for the rest of the proof.)

This means $\frac{a}{b} = \sqrt{2}$, so $\frac{a^2}{b^2} = 2$.

Thus, $2b^2 = a^2$, so a^2 is even, by definition.

Since a^2 is even, this tells us a is even.

(**Note:** You should prove this. We will prove it in Section 4.9.6, but you should try to do it on your own now.)

Thus, $\exists k \in \mathbb{Z}.\ a = 2k$. Let such a k be given, so $a^2 = 4k^2$.

Then $2b^2 = 4k^2$, so $b^2 = 2k^2$.

Thus, b^2 is even, by definition. By the same reasoning as above with a^2 and a, we deduce here that b is even.

This shows both a and b are even so, in fact, they have a common factor of 2.

This contradicts our assumption that a and b have no common factors. ※

Therefore, the original assumption must be False, so the claim is True. $\square$

4.9.3 Proving $\vee$ Claims

An "$\vee$" claim asserts that at least one of two statements must be True. If it just so happens that one of the two statements is clearly False, then just try to prove the other one is True. This is what the direct method is here; it is straightforward, so we will not provide an example of implementation.

Direct Method

Strategy:

Claim: $P \vee Q$

Direct proof:

Prove that P is True, or else prove that Q is True.

This relies on you being able to decide ahead of time which one of the statements (P or Q) is True, of course. If you can do so, then this isn't even really a "strategy". Just implement whatever strategy applies to P (or Q, as the case may be).

Indirect Method (Proof by "Otherwise")

This method is far more interesting than the direct one. In general, it is helpful when the statements P and Q are actually variable propositions, and for some instances P is True whereas for other instances Q is the True one. In that case, rather than characterize *exactly* which instances satisfy P and which satisfy Q, we can just say, "Well, if P is True, then our proof is already complete. Thus, all we need to worry about are the cases where P is False; for those cases, we need to show that Q is still True."

Strategy:

Claim: $P \vee Q$

Indirect proof strategy 1:

Suppose that $\neg P$ holds. Prove that Q holds.

To reiterate the strategy: If P holds, then the claim holds, and in fact we don't care whether Q holds or not. *Otherwise*, in the case where P fails, we need to guarantee that Q holds.

Notice that $P \vee Q \iff Q \vee P$ (i.e. the order is irrelevant in a logical disjunction) so we can rewrite our claim as $Q \vee P$ and rewrite the above strategy as:

Suppose $\neg Q$ holds. Prove that P holds.

This is the exact same strategy on the equivalent statement $Q \vee P$, i.e. with the roles of P and Q switched.

Example 4.9.5. *When a real number is less than its square:*

Statement: Suppose that $x \in \mathbb{R}$ and $x^2 \geq x$.

We claim that $x \geq 1$ or $x \leq 0$.

Implementation:

Proof. Let $x \in \mathbb{R}$ be arbitrary and fixed, and suppose that $x^2 \geq x$.

If it were the case that $x \leq 0$, we would be done; so, suppose otherwise.

That is, suppose $x > 0$.

By assumption, $x^2 \geq x$. Since $x > 0$, we can divide both sides by x.

This yields $x \geq 1$. $\square$

This proves a *necessary* condition for a real number to be less than (or equal to) its square. Is this condition—namely, $x \geq 1 \vee x \leq 0$—also a *sufficient* condition? Prove it! It's easy, and once you've done so, we will have together proven this *biconditional* statement:

$$\forall x \in \mathbb{R}.\ x^2 \geq x \iff (x \geq 1 \vee x \leq 0)$$

Indirect Method (Proof by Contradiction)

This method is more like the indirect methods considered above, in that we suppose the logical negation is valid and then deduce something absurd. We will illustrate this strategy by applying it to the same claim in the directly previous example.

Strategy:

Claim: $P \vee Q$

Indirect proof strategy 2:

AFSOC that $\neg P \wedge \neg Q$ holds. Find a contradiction.

Implementation:

Proof. Let $x \in \mathbb{R}$ be arbitrary and fixed, and suppose that $x^2 \geq x$.

AFSOC that $0 < x$ and $x < 1$.

Since $x > 0$, we can multiply both sides of these inequalities by x and preserve the sign.

Multiplying $x < 1$ by x, then, we find that $x^2 < x$.

This contradicts our assumption that $x^2 \geq x$ ※

Thus, our assumption was invalid, so the claim is True. □

How does this compare to the previous implementation? We are proving the exact same claim, but the proofs are slightly different. Which do you think is better, in your opinion? Which do you think was easier to write? Furthermore, could you go back and rewrite the original claim using quantifiers and "$\implies$"? After doing that, do you see what these two proofs accomplish? Try it!

4.9.4 Proving $\wedge$ Claims

An "$\wedge$" claim asserts that both of two statements are True. There's one obvious and direct way to do this: just prove one statement and then prove the other!

We will show you an example implementation of this method because the $\wedge$ statement of our example comes *after* an $\exists$ claim. Thus, there's actually some scratch work to be done to figure out how to define an object that will, indeed, satisfy both of the desired properties. This will be our first illustrative example of how these proof strategies can be **combined** to prove statements that use both quantifiers and connectives.

Direct Method

Strategy:

Claim: $P \wedge Q$

Direct proof strategy:

Prove that P holds. Prove that Q holds.

Example 4.9.6. **A smaller number whose square is bigger:**

Statement: $\forall x \in \mathbb{R}.\ \exists y \in \mathbb{R}.\ \big(x \geq y \wedge x^2 < y^2 \big)$

Scratch work:

How does this work? Let's take a specific x, like $x = 4$. We need to find a smaller real number whose square is bigger than $x^2 = 16$.

The key is that we want $y \in \mathbb{R}$, so we can use *negative* numbers. In this case, picking a negative number with larger *magnitude*, like $y = -5$, will work.

Let's take a different x, like $x = -2$. This number is already negative, so just picking any smaller number, like $y = -3$, will work.

The proof we follow below splits into two cases, based on whether x is positive or non-positive.

Now we are ready to prove our claim.

Implementation:

Proof 1. Let $x \in \mathbb{R}$ be arbitrary and fixed. We consider two cases.

(1) Suppose $x \leq 0$.

Define $y = x - 1$. Notice $y \in \mathbb{R}$.

Notice $y \leq x$. Also, notice that

$$y^2 = (x-1)^2 = x^2 - 2x + 1 = x^2 - (2x - 1)$$

Since $x \leq 0$, we know $2x \leq 0$ and so $2x - 1 \leq -1$. Thus,

$$x^2 - (2x - 1) \geq x^2 - 1 > x^2$$

and therefore, $y^2 > x^2$.

(2) Now, suppose $x > 0$.

Define $y = -x - 1$. Notice $y \in \mathbb{R}$.

Notice $y < 0$ and $x > 0$, so $y \leq x$. (In fact, $y < x$, even.)

Also, notice that

$$y^2 = (-x-1)^2 = x^2 + 2x + 1 = x^2 + (2x + 1)$$

Since $x > 0$, we know $2x + 1 > 0$. Thus,

$$x^2 + (2x + 1) > x^2$$

and therefore, $y^2 > x^2$.

In either case, we found a y with the desired properties, namely $y \in \mathbb{R}$ and $y \leq x$ and $x^2 < y^2$. Therefore, the claim is True. $\square$

Why did we call this "Proof 1"? We split the proof into two cases based on our observations in the scratch work. Specifically, we recognized that we will define y (in terms of x) *differently*, depending on the sign of x. We claim that it is possible to rewrite this proof in a way that *avoids* these cases. This is what "Proof 2" will be, and we want you to write it! To reiterate the goal, we want you to rewrite the above proof so that y is defined in terms of x in one general way that works regardless of the sign of x.

(*Hint:* What is $-x$ when $x < 0$? Is this a function we've seen before?)

Indirect Method (Proof by Contradiction)

This method is just like the other indirect methods. We just take the logical negation of a claim, assume it holds, and deduce something absurd. This means that the assumption was invalid, so the original statement is the True one.

We will leave it to you to try to apply this method to the claim used in the previous example. (Note: You might want to do this *after* finding the "second proof" we hinted at just above this.) Then, you can compare how the two methods played out and decide which one you prefer, in this case.

Strategy:

Claim: $P \wedge Q$

Indirect proof:

AFSOC that $\neg P \vee \neg Q$ holds.

Consider the first case, where $\neg P$ holds. Find a contradiction.

Consider the second case, where $\neg Q$ holds. Find a contradiction.

4.9.5 Proving $\implies$ Claims

It might help you to look back at Section 4.5.3, where we introduced the connective "$\implies$". Specifically, we want you to recall that $P \implies Q$ means that *whenever* P holds, Q also *necessarily* holds. This conditional statement is True in the cases where P itself (the **hypothesis**) is False. Thus, our proof strategy does not need to consider such cases. All we need to do is *suppose* that P holds, and deduce that Q also holds. This takes care of the "whenever P holds, so does Q" consideration.

Direct Method

Strategy:

Claim: $P \implies Q$

Direct proof strategy:

Suppose P holds. Prove that Q holds.

Example 4.9.7. *Monotonicity of squares:*

Statement: $\forall y \in \mathbb{R}.\ y > 1 \implies y^2 - 1 > 0$

Implementation:

Proof. Let $y \in \mathbb{R}$ be arbitrary and fixed.

Suppose $y > 1$.

Multiplying both sides by y (since $y > 0$), we obtain $y^2 > y$.

Since $y > 1$, this tells us $y^2 > y > 1$, and so $y^2 > 1$.

Subtracting yields the desired conclusion: $y^2 - 1 > 0$. $\square$

We called this "monotonicity of squares" because it states a particular property of real numbers that is **monotone**. This is a term that is used to indicate a certain inequality is preserved under an operation. In this case, the fact that some number being greater than 1 is preserved by the "squaring operation". That is, we proved that if $y > 1$, then $y^2 > 1^2$, as well.

Now, this was a pretty easy example to prove, but we wanted to include it to emphase the proof strategy for conditional statements. Let's work with a more difficult example now.

(You'll also notice that Exercise 4.11.22 has a similar-looking problem statement. Perhaps you want to work on that one after following this example.)

Example 4.9.8. *Working with inequalities:*

Statement: We define the following variable propositions:

$$P(x) \text{ is } \text{“}\frac{x-3}{x+2} > 1 - \frac{1}{x}\text{”}$$
$$Q(x) \text{ is } \text{“}\frac{x+3}{x+2} < 1 + \frac{1}{x}\text{”}$$

Define $S = \{x \in \mathbb{R} \mid x > 0\}$.

We claim that

$$\forall x \in S \,.\, P(x) \implies Q(x)$$

Scratch work:

We're guessing that a direct method will work here, so let's try to manipulate the inequality stated inside $P(x)$ and make it "look like" the inequality inside $Q(x)$.

So we start with that inequality

$$\frac{x-3}{x+2} > 1 - \frac{1}{x}$$

and we'll try multiplying both sides by $x+2$. Can we do this? Oh right, $x > 0$ and so $x+2 > 0$, as well. Phew! This gives us

$$x - 3 > (x+2) - \frac{x+2}{x} = x + 2 - 1 - \frac{2}{x} = x + 1 - \frac{2}{x}$$

We want to see an $x+3$ somewhere, so we'll add/subtract on both sides:

$$x - 1 + \frac{2}{x} > x + 3$$

Can we divide by $x+2$ and make the right fraction? Hmm ... Oh wait! We already simplified the fraction $\frac{x+2}{x}$ and moved it to one side. Maybe we shouldn't have simplified it first, so let's try undoing that:

$$x + 3 < x - 1 + \frac{2}{x} = (x+2) + \frac{x+2}{x} - 4 = (x+2)\left(1 + \frac{1}{x}\right) - 4$$

Aha, that looks better! We even have some "wiggle room" in the form of the negative 4 there. We know the right-hand side is less than what we wanted it to be, so the result holds.

Let's take these algebraic steps we worked on here, reorder them a bit and explain them, and wrap it all together in a formal proof.

Implementation:

Proof. Let $x \in S$ be arbitrary and fixed.

Suppose that $P(x)$ holds; that is, suppose

$$\frac{x-3}{x+2} > 1 - \frac{1}{x}$$

We will show that the inequality

$$\frac{x+3}{x+2} < 1 + \frac{1}{x}$$

also holds, necessarily.

Since $x \in S$, we know $x > 0$ and so, certainly, $x + 2 > 0$, as well. Thus, we can multiply both sides of the known inequality by $x + 2$, yielding

$$x - 3 > (x+2)\left(1 - \frac{1}{x}\right) = x + 2 - \frac{x+2}{x}$$

Adding $3 + \frac{x+2}{x}$ to both sides, subtracting 2 from both sides, and rewriting in the reverse direction (for ease of reading), we obtain

$$x + 3 < x - 2 + \frac{x+2}{x}$$

Since $x - 2 < x + 2$, we deduce that

$$x + 3 < x + 2 + \frac{x+2}{x}$$

and factoring tells us

$$x + 3 < (x+2)\left(1 + \frac{1}{x}\right)$$

Again, since $x + 2 > 0$, we can divide both sides by $x + 2$, obtaining

$$\frac{x+3}{x+2} < 1 + \frac{1}{x}$$

which was the desired inequality. This shows $P(x) \implies Q(x)$, and since x was arbitrary, we have proven the claim. □

A key lesson here lies in how we took our scratch work and presented it in a different way in our proof. We cut out the unnecessary simplification and refactoring steps, but we also noted why each step was valid as we performed it. A more seasoned mathematician would likely skip several of these steps and leave it to the reader to verify the algebraic work, but since we are early on in our mathematical careers, we thought it would be prudent to show as many details as possible.