Proofs and Concepts

the fundamentals of abstract mathematics

by

Dave Witte Morris and Joy Morris

University of Lethbridge

incorporating material by

P. D. Magnus

University at Albany, State University of New York

Preliminary Version 0.78 of May 2009

The presentation of logic in this textbook is adapted from

forallχ
An Introduction to Formal Logic

P. D. Magnus
University at Albany, State University of New York

The most recent version of forallχ is available on-line at
http://www.fecundity.com/logic

We thank Professor Magnus for making forallχ *freely available,*
and for authorizing derivative works such as this one.
He was not involved in the preparation of this manuscript,
so he is not responsible for any errors or other shortcomings.

Please send comments and corrections to:
Dave.Morris@uleth.ca or Joy.Morris@uleth.ca

to Harmony

Contents

Part I. Introduction to Logic and Proofs

Part IV. Other Fundamental Concepts

Part V. Topics

Part I

Introduction to Logic and Proofs

Chapter 1

What is Logic?

> *. . . it is undesirable to believe a proposition when there is no ground whatsoever for supposing it is true.*
>
> Bertram Russell (1872–1970), British philosopher
> *On the Value of Scepticism*

For our purposes, logic is the business of deciding whether or not a deduction is valid; that is, deciding whether or not a particular conclusion is a consequence of particular assumptions (or "hypotheses"). Here is one possible deduction:

Hypotheses:

(1) It is raining heavily.

(2) If you do not take an umbrella, you will get soaked.

Conclusion: You should take an umbrella.

(The validity of this particular deduction will be analyzed in section 1B.)

This chapter discusses some basic logical notions that apply to deductions in English (or any other human language, such as French). Later, we will translate deductions from English into mathematical notation.

1A. Assertions and deductions

In logic, we are only interested in sentences that can figure as a hypothesis or conclusion of a deduction. These are called assertions: an **assertion** is a sentence that is either true or false. (If you look at other textbooks, you may find that some authors call these *propositions* or *statements* or *sentences*, instead of assertions.)

You should not confuse the idea of an assertion that can be true or false with the difference between fact and opinion. Often, assertions in logic will express things that would count as facts—such as "Pierre Trudeau was born in Quebec" or "Pierre Trudeau liked almonds." They can also express things that you might think of as matters of opinion—such as, "Almonds are yummy."

EXAMPLE 1.1.

- **Questions** The sentence "Are you sleepy yet?", is *not* an assertion. Although you might be sleepy or you might be alert, the question itself is neither true nor false. For this reason, questions will not count as assertions in logic. Suppose you answer the question: "I am not sleepy." This is either true or false, and so it is an assertion in the logical sense. Generally, *questions* will not count as assertions, but *answers* will. For example, "What is this course about?" is not an assertion, but "No one knows what this course is about" is an assertion.

- **Imperatives** Commands are often phrased as imperatives like "Wake up!," "Sit up straight," and so on. Although it might be good for you to sit up straight or it might not, the command is neither true nor false. Note, however, that commands are not always phrased as imperatives. "If you sit up straight, then you will get a cookie" is either true or false, and so it counts as an assertion in the logical sense.
- **Exclamations** "Ouch!" is sometimes called an exclamatory sentence, but it is neither true nor false. We will treat "Ouch, I hurt my toe!" as meaning the same thing as "I hurt my toe." The "ouch" does not add anything that could be true or false.

Throughout this text, you will find practice problems that review and explore the material that has just been covered. There is no substitute for actually working through some problems, because mathematics is more about a way of thinking than it is about memorizing facts.

EXERCISES 1.2. Which of the following are "assertions" in the logical sense?

1) England is smaller than China.

2) Greenland is south of Jerusalem.

3) Is New Jersey east of Wisconsin?

4) The atomic number of helium is 2.

5) The atomic number of helium is π.

6) I hate overcooked noodles.

7) Overcooked noodles are disgusting.

8) Take your time.

9) This is the last question.

We can define a **deduction** to be a series of hypotheses that is followed by a conclusion. (The conclusion and each of the hypotheses must be an assertion.) If the hypotheses are true and the deduction is a good one, then you have a reason to accept the conclusion. Consider this example:

Hypotheses:

There is coffee in the coffee pot.

There is a dragon playing bassoon on the armoire.

Conclusion: Pablo Picasso was a poker player.

It may seem odd to call this a deduction, but that is because it would be a terrible deduction. The two hypotheses have nothing at all to do with the conclusion. Nevertheless, given our definition, it still counts as a deduction—albeit a bad one.

1B. Two ways that deductions can go wrong

Consider the deduction that you should take an umbrella (on p. 3, above). If hypothesis (1) is false—if it is sunny outside—then the deduction gives you no reason to carry an umbrella. Even if it is raining outside, you might not need an umbrella. You might wear a rain poncho or keep to covered walkways. In these cases, hypothesis (2) would be false, since you could go out without an umbrella and still avoid getting soaked.

Suppose for a moment that both the hypotheses are true. You do not own a rain poncho. You need to go places where there are no covered walkways. Now does the deduction show you that you should take an umbrella? Not necessarily. Perhaps you enjoy walking in the rain, and you would like to get soaked. In that case, even though the hypotheses were true, the conclusion would be false.

For any deduction, there are two ways that it could be weak:

1) One or more of the hypotheses might be false. A deduction gives you a reason to believe its conclusion only if you believe its hypotheses.
2) The hypotheses might fail to entail the conclusion. Even if the hypotheses were true, the form of the deduction might be weak.

The example we just considered is weak in both ways.

When a deduction is weak in the second way, there is something wrong with the *logical form* of the deduction: hypotheses of the kind given do not necessarily lead to a conclusion of the kind given. We will be interested primarily in the logical form of deductions.

Consider another example:

Hypotheses:

You are reading this book.

This is an undergraduate textbook.

Conclusion: You are an undergraduate student.

This is not a terrible deduction. Most people who read this book are undergraduate students. Yet, it is possible for someone besides an undergraduate to read this book. If your mother or father picked up the book and thumbed through it, they would not immediately become an undergraduate. So the hypotheses of this deduction, even though they are true, do not guarantee the truth of the conclusion. Its logical form is less than perfect.

A deduction that had no weakness of the second kind would have perfect logical form. If its hypotheses were true, then its conclusion would *necessarily* be true. We call such a deduction "deductively valid" or just "valid."

Even though we might count the deduction above as a good deduction in some sense, it is not valid; that is, it is "invalid." The task of logic is to sort valid deductions from invalid ones.

1C. Deductive validity

A deduction is **valid** if and only if its conclusion is true whenever all of its hypotheses are true. In other words, it is impossible for the hypotheses to be true *at the same time* that the conclusion is false. Consider this example:

Hypotheses:

Oranges are either fruits or musical instruments.

Oranges are not fruits.

Conclusion: Oranges are musical instruments.

The conclusion of this deduction is ridiculous. Nevertheless, it follows validly from the hypotheses. This is a valid deduction; that is, *if* both hypotheses were true, *then* the conclusion would necessarily be true. For example, you might be able to imagine that, in some remote river valley, there is a variety of orange that is not a fruit, because it is hollow inside, like a gourd. Well, if the other hypothesis is also true in that valley, then the residents must use the oranges to play music.

This shows that a deductively valid deduction does not need to have true hypotheses or a true conclusion. Conversely, having true hypotheses and a true conclusion is not enough to make a deduction valid. Consider this example:

Hypotheses:

London is in England.

Beijing is in China.

Conclusion: Paris is in France.

The hypotheses and conclusion of this deduction are, as a matter of fact, all true. This is a terrible deduction, however, because the hypotheses have nothing to do with the conclusion. Imagine what would happen if Paris declared independence from the rest of France. Then the conclusion would be false, even though the hypotheses would both still be true. Thus, it is *logically possible* for the hypotheses of this deduction to be true and the conclusion false. The deduction is invalid.

The important thing to remember is that validity is not about the actual truth or falsity of the assertions in the deduction. Instead, it is about the form of the deduction: The truth of the hypotheses is incompatible with the falsity of the conclusion.

EXERCISES 1.3. Which of the following is possible? If it is possible, give an example. If it is not possible, explain why.

1) A valid deduction that has one false hypothesis and one true hypothesis.

2) A valid deduction that has a false conclusion.

3) A valid deduction that has at least one false hypothesis, and a true conclusion.

4) A valid deduction that has all true hypotheses, and a false conclusion.

5) An invalid deduction that has at least one false hypothesis, and a true conclusion.

1D. Other logical notions

In addition to deductive validity, we will be interested in some other logical concepts.

1D.1. Truth-values. True or false is said to be the **truth-value** of an assertion. We defined assertions as sentences that are either true or false; we could have said instead that assertions are sentences that have truth-values.

1D.2. Logical truth. In considering deductions formally, we care about what would be true *if* the hypotheses were true. Generally, we are not concerned with the actual truth value of any particular assertions—whether they are *actually* true or false. Yet there are some assertions that must be true, just as a matter of logic.

Consider these assertions:

1. It is raining.
2. Either it is raining, or it is not.
3. It is both raining and not raining.

In order to know if Assertion 1 is true, you would need to look outside or check the weather channel. Logically speaking, it might be either true or false. Assertions like this are called *contingent* assertions.

Assertion 2 is different. You do not need to look outside to know that it is true. Regardless of what the weather is like, it is either raining or not. This assertion is *logically true*; it is true merely as a matter of logic, regardless of what the world is actually like. A logically true assertion is called a **tautology**.

You do not need to check the weather to know about Assertion 3, either. It must be false, simply as a matter of logic. It might be raining here and not raining across town, it might be raining now but stop raining even as you read this, but it is impossible for it to be both raining

and not raining here at this moment. The third assertion is *logically false*; it is false regardless of what the world is like. A logically false assertion is called a **contradiction**.

To be precise, we can define a **contingent assertion** as an assertion that is neither a tautology nor a contradiction.

Remark 1.4. An assertion might *always* be true and still be contingent. For instance, if there never were a time when the universe contained fewer than seven things, then the assertion "At least seven things exist" would always be true. Yet the assertion is contingent; its truth is not a matter of logic. There is no contradiction in considering a possible world in which there are fewer than seven things. The important question is whether the assertion *must* be true, just on account of logic.

EXERCISES 1.5. For each of the following: Is it a tautology, a contradiction, or a contingent assertion?

1) Caesar crossed the Rubicon.

2) Someone once crossed the Rubicon.

3) No one has ever crossed the Rubicon.

4) If Caesar crossed the Rubicon, then someone has.

5) Even though Caesar crossed the Rubicon, no one has ever crossed the Rubicon.

6) If anyone has ever crossed the Rubicon, it was Caesar.

EXERCISES 1.6. Which of the following is possible? If it is possible, give an example. If it is not possible, explain why.

1) A valid deduction, the conclusion of which is a contradiction.

2) A valid deduction, the conclusion of which is a tautology.

3) A valid deduction, the conclusion of which is contingent.

4) An invalid deduction, the conclusion of which is a contradiction.

5) An invalid deduction, the conclusion of which is a tautology.

6) An invalid deduction, the conclusion of which is a contingent.

7) A tautology that is contingent.

1D.3. Logical equivalence. We can also ask about the logical relations *between* two assertions. For example:

John went to the store after he washed the dishes.

John washed the dishes before he went to the store.

These two assertions are both contingent, since John might not have gone to the store or washed dishes at all. Yet they must have the same truth-value. If either of the assertions is true, then they both are; if either of the assertions is false, then they both are. When two assertions necessarily have the same truth value, we say that they are **logically equivalent**.

EXERCISES 1.7. Which of the following is possible? If it is possible, give an example. If it is not possible, explain why.

1) Two logically equivalent assertions, both of which are tautologies.

2) Two logically equivalent assertions, one of which is a tautology and one of which is contingent.

3) Two logically equivalent assertions, neither of which is a tautology.

4) Two tautologies that are *not* logically equivalent.

5) Two contradictions that are *not* logically equivalent.

6) Two contingent sentences that are *not* logically equivalent.

1E. Logic puzzles

Clear thinking (or logic) is important not only in mathematics, but in everyday life, and can also be fun; many logic puzzles (or games), such as Sudoku, can be found on the internet or in bookstores. Here are just a few.

EXERCISE 1.8 (found online at http://philosophy.hku.hk/think/logic/puzzles.php). There was a robbery in which a lot of goods were stolen. The robber(s) left in a truck. It is known that:

1) No one other than A, B and C was involved in the robbery.

2) C never commits a crime without inviting A to be his accomplice.

3) B does not know how to drive.

So, can you tell whether A is innocent?

EXERCISES 1.9. On the island of Knights and Knaves*, every resident is either a Knight or a Knave (and they all know the status of everyone else). It's important to know that:

- Knights *always* tell the truth.
- Knaves *always* lie.

You will meet some residents of the island, and your job is to figure out whether each of them is a Knight or a Knave.

1) You meet Alice and Bob on the island. Alice says "Bob and I are Knights." Bob says, "That's a lie — she's a Knave!" What are they?

2) You meet Charlie, Diane, and Ed on the island. Charlie says, "Be careful, not all three of us are Knights." Diane says, "But not all of us are Knaves, either." Ed says, "Don't listen to them, I'm the only Knight." What are they?

3) You meet Frances and George on the island. Frances mumbles something, but you can't understand it. George says, "She said she's a Knave. And she sure is — don't trust her!" What are they?

Here is a version of a famous difficult problem that is said to have been made up by Albert Einstein when he was a boy, but, according to Wikipedia, there is no evidence for this.

EXERCISE 1.10 ("Zebra Puzzle" or "Einstein's Riddle"). There are 5 houses, all in a row, and each of a different colour. One person lives in each house, and each person has a different nationality, a different type of pet, a different model of car, and a different drink than the others. Also:

- The Englishman lives in the red house.
- The Spaniard owns the dog.
- Coffee is drunk in the green house.
- The Ukrainian drinks tea.
- The green house is immediately to the right of the ivory house.
- The Oldsmobile driver owns snails.
- A Cadillac is driven by the owner of the yellow house.

*http://en.wikipedia.org/wiki/Knights_and_knaves

- Milk is drunk in the middle house.
- The Norwegian lives in the first house.
- The person who drives a Honda lives in a house next to the person with the fox.
- The person who drives a Cadillac lives next-door to the house where the horse is kept.
- The person with a Ford drinks orange juice.
- The Japanese drives a Toyota.
- The Norwegian lives next to the blue house.

Who owns the zebra? (Assume that one of the people *does* have a zebra!)

SUMMARY:

- Important definitions:
  - assertion
  - deduction
  - valid, invalid
  - tautology, contradiction
  - contingent assertion
  - logical equivalence

Chapter 2

Propositional Logic

You can get assent to almost any proposition so long as you are not going to do anything about it.

Nathaniel Hawthorne (1804–1864), American author

This chapter introduces a logical language called Propositional Logic. It provides a convenient way to describe the logical relationship between two (or more) assertions.

2A. Using letters to symbolize assertions

In Propositional Logic, capital letters are used to represent assertions. Considered only as a symbol of Propositional Logic, the letter A could mean any assertion. So, when translating from English into Propositional Logic, it is important to provide a **symbolization key** that specifies what assertion is represented by each letter.

For example, consider this deduction:

Hypotheses:

There is an apple on the desk.

If there is an apple on the desk, then Jenny made it to class.

Conclusion: Jenny made it to class.

This is obviously a valid deduction in English. In symbolizing it, we want to preserve the structure of the deduction that makes it valid. What happens if we replace each assertion with a letter? Our symbolization key would look like this:

A: There is an apple on the desk.

B: If there is an apple on the desk, then Jenny made it to class.

C: Jenny made it to class.

We would then symbolize the deduction in this way:

Hypotheses:

A

B

Conclusion: C

There is no necessary connection between some assertion A, which could be any assertion, and some other assertions B and C, which could be any assertions. The structure of the deduction has been completely lost in this translation.

The important thing about the deduction is that the second hypothesis is not merely *any* assertion, logically divorced from the other assertions in the deduction. The second hypothesis

contains the first hypothesis and the conclusion *as parts*. Our symbolization key for the deduction only needs to include meanings for A and C, and we can build the second hypothesis from those pieces. So we symbolize the deduction this way:

Hypotheses:

A

If A, then C.

Conclusion: C

This preserves the structure of the deduction that makes it valid, but it still makes use of the English expression "If... then..." Although we ultimately want to replace all of the English expressions with mathematical notation, this is a good start.

The assertions that are symbolized with a single letter are called *atomic assertions*, because they are the basic building blocks out of which more complex assertions are built. Whatever logical structure an assertion might have is lost when it is translated as an atomic assertion. From the point of view of Propositional Logic, the assertion is just a letter. It can be used to build more complex assertions, but it cannot be taken apart.

There are only twenty-six letters in the English alphabet, but there is no logical limit to the number of atomic assertions. We can use the same English letter to symbolize different atomic assertions by adding a subscript (that is, a small number written after the letter). For example, we could have a symbolization key that looks like this:

A_1: The apple is under the armoire.

A_2: Deductions always contain atomic assertions.

A_3: Adam Ant is taking an airplane from Anchorage to Albany.

$\vdots$ $\qquad$ $\vdots$

A_{294}: Alliteration angers all astronauts.

Keep in mind that A_1,A_2,A_3,... are all considered to be different letters—when there are subscripts in the symbolization key, it is important to keep track of them.

2B. Connectives

Logical connectives are used to build complex assertions from atomic components. There are five logical connectives in Propositional Logic. This table summarizes them, and they are explained below.

symbol	nickname	what it means
$\neg$	not	"It is not the case that _____"
$\&$	and	"Both _____ and _____"
$\vee$	or	"Either _____ or _____"
$\Rightarrow$	implies	"If _____ then _____"
$\Leftrightarrow$	iff	"_____ if and only if _____"

As we learn to write proofs, it will be important to be able to produce a deduction in Propositional Logic from a sequence of assertions in English. It will also be important to be able to retrieve the English meaning from a sequence of assertions in Propositional Logic, given a symbolization key. The table above should prove useful in both of these tasks.

NOTATION 2.1. The symbol "$\therefore$" means "therefore," and we sometimes use

$$A_1, A_2, \ldots, A_n, \therefore B$$

as an abbreviation for the deduction

Hypotheses:

A_1

A_2

$\vdots$

A_n

Conclusion: C.

2B.1. Not ($\neg$)**.** As an example, consider how we might symbolize these assertions:

1. Mary is in Barcelona.
2. Mary is not in Barcelona.
3. Mary is somewhere other than Barcelona.

In order to symbolize Assertion 1, we will need one letter. We can provide a symbolization key:

B: Mary is in Barcelona.

Note that here we are giving B a different interpretation than we did in the previous section. The symbolization key only specifies what B means *in a specific context*. It is vital that we continue to use this meaning of B so long as we are talking about Mary and Barcelona. Later, when we are symbolizing different assertions, we can write a new symbolization key and use B to mean something else.

Now, Assertion 1 is simply B.

Since Assertion 2 is obviously related to Assertion 1, we do not want to introduce a different letter to represent it. To put it partly in English, the assertion means "It is not true that B." For short, logicians say "Not B." This is called the **logical negation** of B. In order to convert it entirely to symbols, we will use "$\neg$" to denote logical negation. Then we can symbolize "Not B" as $\neg B$.

Assertion 3 is about whether or not Mary is in Barcelona, but it does not contain the word "not." Nevertheless, it is obviously logically equivalent to Assertion 2. They both mean, "It is not the case that Mary is in Barcelona." As such, we can translate both Assertion 2 and Assertion 3 as $\neg B$.

> An assertion can be symbolized as $\neg\mathcal{A}$ if
> it can be paraphrased in English as "It is not the case that $\mathcal{A}$."

Consider these further examples:

4. The widget can be replaced if it breaks.
5. The widget is irreplaceable.
6. The widget is not irreplaceable.

If we let R mean "The widget is replaceable," then Assertion 4 can be translated as R.

What about Assertion 5? Saying the widget is irreplaceable means that it is not the case that the widget is replaceable. So even though Assertion 5 is not negative in English, we symbolize it using negation as $\neg R$.

Assertion 6 can be paraphrased as "It is not the case that the widget is irreplaceable." Now, as we have already discussed, "The widget is irreplaceable" can be symbolized as "$\neg R$." Therefore, Assertion 6 can be formulated as "it is not the case that $\neg R$." Hence, it is the negation of $\neg R$, so it can be symbolized as $\neg\neg R$. This is a *double negation*. If you think about the assertion in English, it is logically equivalent to Assertion 4. In general, we will see that if A is any assertion, then A and $\neg\neg A$ are logically equivalent.

More examples:

7. Elliott is short.

8. Elliott is tall.

If we let S mean "Elliot is short," then we can symbolize Assertion 7 as S.

However, it would be a mistake to symbolize Assertion 8 as $\neg S$. If Elliott is tall, then he is not short—but Assertion 8 does not mean the same thing as "It is not the case that Elliott is short." It could be that he is not tall but that he is not short either: perhaps he is somewhere between the two (average height). In order to symbolize Assertion 8, we would need a new assertion letter.

For any assertion $\mathcal{A}$:

- If $\mathcal{A}$ is true, then $\neg\mathcal{A}$ is false.
- If $\neg\mathcal{A}$ is true, then $\mathcal{A}$ is false.

Using "T" for true and "F" for false, we can summarize this in a *truth table* for negation:

$\mathcal{A}$	$\neg\mathcal{A}$
T	F
F	T

EXERCISES 2.2. Using the given symbolization key, translate each English-language assertion into Propositional Logic.

M: Those creatures are men in suits.

C: Those creatures are chimpanzees.

G: Those creatures are gorillas.

1) Those creatures are not men in suits.

2) It is not the case that those creatures are not gorillas.

3) Of course those creatures are not chimpanzees!

EXERCISES 2.3. Using the same symbolization key, translate each symbolic assertion into English.

1) G

2) $\neg M$

3) $\neg\neg C$

2B.2. And (&). Consider these assertions:

9. Adam is athletic.

10. Barbara is athletic.

11. Adam is athletic, and Barbara is also athletic.

We will need separate assertion letters for Assertions 9 and 10, so we define this symbolization key:

A: Adam is athletic.

B: Barbara is athletic.

Assertion 9 can be symbolized as A.

Assertion 10 can be symbolized as B.

Assertion 11 can be paraphrased as "A and B." In order to fully symbolize this assertion, we need another symbol. We will use "&." We translate "A and B" as $A\&B$. Officially, the logical

connective "&" is called *conjunction*, and A and B are each called *conjuncts*. Unofficially, the name of this connective is "and."

Notice that we make no attempt to symbolize "also" in Assertion 11. Words like "both" and "also" function to draw our attention to the fact that two things are being conjoined. They are not doing any further logical work, so we do not need to represent them in Propositional Logic.

Some more examples:

12. Barbara is athletic and energetic.
13. Barbara and Adam are both athletic.
14. Although Barbara is energetic, she is not athletic.
15. Barbara is athletic, but Adam is more athletic than she is.

Assertion 12 is obviously a conjunction. The assertion says two things about Barbara, so in English it is permissible to refer to Barbara only once. It might be tempting to try this when translating the deduction: Since B means "Barbara is athletic," one might paraphrase the assertions as "B and energetic." This would be a mistake. Once we translate part of an assertion as B, any further structure is lost. B is an atomic assertion; it is nothing more than true or false. Conversely, "energetic" is not an assertion; on its own it is neither true nor false. We should instead paraphrase the assertion as "B and Barbara is energetic." Now we need to add an assertion letter to the symbolization key. Let E mean "Barbara is energetic." Now the assertion can be translated as $B \,\&\, E$.

> An assertion can be symbolized as $\mathcal{A} \,\&\, \mathcal{B}$ if
> it can be paraphrased in English as "Both $\mathcal{A}$, and $\mathcal{B}$."

Assertion 13 says one thing about two different subjects. It says of both Barbara and Adam that they are athletic, and in English we use the word "athletic" only once. In translating to Propositional Logic, it is important to realize that the assertion can be paraphrased as, "Barbara is athletic, and Adam is athletic." Thus, this translates as $B \,\&\, A$.

Assertion 14 is a bit more complicated. The word "although" sets up a contrast between the first part of the assertion and the second part. Nevertheless, the assertion says both that Barbara is energetic and that she is not athletic. In order to make the second part into an atomic assertion, we need to replace "she" with "Barbara."

So we can paraphrase Assertion 14 as, "*Both* Barbara is energetic, *and* Barbara is not athletic." The second part contains a negation, so we paraphrase further: "*Both* Barbara is energetic *and it is not the case that* Barbara is athletic." This translates as $E \,\&\, \neg B$.

Assertion 15 contains a similar contrastive structure. It is irrelevant for the purpose of translating to Propositional Logic, so we can paraphrase the assertion as "*Both* Barbara is athletic, *and* Adam is more athletic than Barbara." (Notice that we once again replace the pronoun "she" with her name.) How should we translate the second part? We already have the assertion letter A which is about Adam's being athletic and B which is about Barbara's being athletic, but neither is about one of them being more athletic than the other. We need a new assertion letter. Let M mean "Adam is more athletic than Barbara." Now the assertion translates as $B \,\&\, M$.

> Assertions that can be paraphrased "$\mathcal{A}$, but $\mathcal{B}$" or "Although $\mathcal{A}$, $\mathcal{B}$"
> are best symbolized using "and": $\mathcal{A} \,\&\, \mathcal{B}$.

It is important to keep in mind that the assertion letters A, B, and M are atomic assertions. Considered as symbols of Propositional Logic, they have no meaning beyond being true or false. We have used them to symbolize different English language assertions that are all about people

being athletic, but this similarity is completely lost when we translate to Propositional Logic. No formal language can capture all the structure of the English language, but as long as this structure is not important to the deduction there is nothing lost by leaving it out.

For any assertions $\mathcal{A}$ and $\mathcal{B}$,

$\mathcal{A}\&\mathcal{B}$ is true if and only if both $\mathcal{A}$ and $\mathcal{B}$ are true.

We can summarize this in the truth table for "and":

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A}\&\mathcal{B}$
T	T	T
T	F	F
F	T	F
F	F	F

The connective "and" is *commutative* because we can swap the two terms without changing the truth-value of the assertion: regardless of what $\mathcal{A}$ and $\mathcal{B}$ are, $\mathcal{A}\&\mathcal{B}$ is logically equivalent to $\mathcal{B}\&\mathcal{A}$.

EXERCISES 2.4. Using the given symbolization key, translate each English-language assertion into Propositional Logic.

E_1: Ava is an electrician.

E_2: Harrison is an electrician.

F_1: Ava is a firefighter.

F_2: Harrison is a firefighter.

S_1: Ava is satisfied with her career.

S_2: Harrison is satisfied with his career.

1) Ava and Harrison are both electricians.

2) Harrison is an unsatisfied electrician.

3) Neither Ava nor Harrison is an electrician.

4) Both Ava and Harrison are electricians, but neither of them find it satisfying.

5) It cannot be that Harrison is both an electrician and a firefighter.

6) Ava is neither an electrician, nor a firefighter.

EXERCISES 2.5. Using the given symbolization key, translate each symbolic assertion into English.

J: Romeo likes Juliet.

M: Mercutio likes Juliet.

T: Romeo likes Tybalt.

1) $M \,\&\, J$

2) $J \,\&\, \neg T$

3) $\neg M \,\&\, J$

2B.3. Or ($\vee$). Consider these assertions:

16. Either Denison will play golf with me, or he will watch movies.

17. Either Denison or Ellery will play golf with me.

For these assertions we can use this symbolization key:

D: Denison will play golf with me.

E: Ellery will play golf with me.

M: Denison will watch movies.

Assertion 16 is "Either D or M." To fully symbolize this, we introduce a new symbol. The assertion becomes $D \vee M$. Officially, the "$\vee$" connective is called **disjunction**, and D and M are called **disjuncts**. Unofficially, the name of this connective is "or."

Assertion 17 is only slightly more complicated. There are two subjects, but the English assertion only gives the verb once. In translating, we can paraphrase it as. "Either Denison will play golf with me, or Ellery will play golf with me." Now it obviously translates as $D \vee E$.

An assertion can be symbolized as $\mathcal{A} \vee \mathcal{B}$ if
it can be paraphrased in English as "Either $\mathcal{A}$, or $\mathcal{B}$."

Sometimes in English, the word "or" excludes the possibility that both disjuncts are true. This is called an **exclusive or**. An *exclusive or* is clearly intended when it says, on a restaurant menu, "Entrees come with either soup or salad." You may have soup; you may have salad; but, if you want *both* soup *and* salad, then you have to pay extra.

At other times, the word "or" allows for the possibility that both disjuncts might be true. This is probably the case with Assertion 17, above. I might play with Denison, with Ellery, or with both Denison and Ellery. Assertion 17 merely says that I will play with *at least* one of them. This is called an **inclusive or**.

The symbol "$\vee$" represents an *inclusive or*. So $D \vee E$ is true if D is true, if D is true, or if both D and E are true. It is false only if both D and E are false. We can summarize this with the truth table for "or":

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$
T	T	T
T	F	T
F	T	T
F	F	F

Like "and," the connective "or" is commutative: $\mathcal{A} \vee \mathcal{B}$ is logically equivalent to $\mathcal{B} \vee \mathcal{A}$.

In mathematical writing, "or" *always* means **inclusive** or.

These assertions are somewhat more complicated:

18. Either you will not have soup, or you will not have salad.
19. You will have neither soup nor salad.
20. You get either soup or salad, but not both.

We let S_1 mean that you get soup and S_2 mean that you get salad.

Assertion 18 can be paraphrased in this way: "Either *it is not the case that* you get soup, or *it is not the case that* you get salad." Translating this requires both "or" and "not." It becomes $\neg S_1 \vee \neg S_2$.

Assertion 19 also requires negation. It can be paraphrased as, "*It is not the case that* either you get soup or you get salad." We use parentheses to indicate that "not" negates the entire assertion $S_1 \vee S_2$, not just S_1 or S_2: "It is not the case that $(S_1 \vee S_2)$." This becomes simply $\neg(S_1 \vee S_2)$.

Notice that the parentheses are doing important work here. The assertion $\neg S_1 \vee S_2$ would mean "Either you will not have soup, or you will have salad."

Assertion 20 is an *exclusive or*. We can break the assertion into two parts. The first part says that you get one or the other. We translate this as $(S_1 \vee S_2)$. The second part says that you do not get both. We can paraphrase this as, "It is not the case that both you get soup and you get salad." Using both "not" and "and," we translate this as $\neg(S_1 \,\&\, S_2)$. Now we just need to put the two parts together. As we saw above, "but" can usually be translated as "and." Assertion 20 can thus be translated as $(S_1 \vee S_2) \,\&\, \neg(S_1 \,\&\, S_2)$.

Although "$\vee$" is an *inclusive or*, the preceding paragraph illustrates that we can symbolize an *exclusive or* in Propositional Logic. We just need more than one connective to do it.

EXERCISES 2.6. Using the given symbolization key, translate each English-language assertion into Propositional Logic.

M: Those creatures are men in suits.

C: Those creatures are chimpanzees.

G: Those creatures are gorillas.

1) Those creatures are men in suits, or they are not.

2) Those creatures are either gorillas or chimpanzees.

3) Those creatures are either chimpanzees, or they are not gorillas.

EXERCISES 2.7. Give a symbolization key and symbolize the following assertions in Propositional Logic.

1) Either Alice or Bob is a spy, but not both.

2) Either Bob is a spy, or it is the case both that the code has been broken and the German embassy is in an uproar.

3) Either the code has been broken or it has not, but the German embassy is in an uproar regardless.

4) Alice may or may not be a spy, but the code has been broken in any case.

EXERCISES 2.8. Using the given symbolization key, translate each assertion into English.

J: Romeo likes Juliet.

M: Mercutio likes Juliet.

T: Romeo likes Tybalt.

1) $M \vee T$

2) $T \vee (\neg J \,\&\, M)$

3) $\neg(M \vee J) \,\&\, \neg T$

2B.4. Implies ($\Rightarrow$). For the following assertions, let R mean "You will cut the red wire" and B mean "The bomb will explode."

21. If you cut the red wire, then the bomb will explode.

22. The bomb will explode if you cut the red wire.

23. The bomb will explode only if you cut the red wire.

Assertion 21 can be translated partially as "If R, then B." We can rephrase this as "R implies B." We will use the symbol "$\Rightarrow$" to represent "implies": the assertion becomes $R \Rightarrow B$. Officially, the connective is called a **conditional**. The assertion on the left-hand side of the conditional (R in this example) is called the **antecedent**. The assertion on the right-hand side (B) is called the **consequent**. Unofficially, the name of the connective is "implies." We call R the **hypothesis** and call B the **conclusion**.

Assertion 22 tells us that if you cut the red wire, then the bomb will explode. Thus, it is logically equivalent to Assertion 21, so it can be symbolized as $R \Rightarrow B$.

Assertion 23 is also a conditional assertion that tells us something must be true if some other thing is true. Since the word "if" appears in the second half of the assertion, it might be tempting to symbolize this in the same way as Assertions 21 and 22. That would be a mistake.

The implication $R \Rightarrow B$ says that *if* R were true, *then* B would also be true. It does not say that your cutting the red wire is the *only* way that the bomb could explode. Someone else might cut the wire, or the bomb might be on a timer. The assertion $R \Rightarrow B$ does not say anything about what to expect if R is false. Assertion 23 is different. It says that the only conditions under which the bomb will explode involve your having cut the red wire; i.e., if the bomb explodes, then you must have cut the wire. As such, Assertion 23 should be symbolized as $B \Rightarrow R$.

Remark 2.9. The paraphrased assertion "$\mathcal{A}$ only if $\mathcal{B}$" is logically equivalent to "If $\mathcal{A}$, then $\mathcal{B}$."

"If $\mathcal{A}$, then $\mathcal{B}$" means that if $\mathcal{A}$ is true, then so is $\mathcal{B}$. So we know that if the hypothesis $\mathcal{A}$ is true, but the conclusion $\mathcal{B}$ is false, then the implication "If $\mathcal{A}$, then $\mathcal{B}$" is false. (For example, if you cut the red wire, but the bomb does not explode, then Assertion 21 is obviously false.) What is the truth value of "If $\mathcal{A}$, then $\mathcal{B}$" under other circumstances?

- Suppose, for instance, that you do *not* cut the red wire. Then Assertion 21 is not a lie, whether the bomb explodes or not, because the assertion does not promise anything in this case. Thus, we consider Assertion 21 to be true in this case. In general, if $\mathcal{A}$ is false, then the implication "$\mathcal{A} \Rightarrow \mathcal{B}$" is true. (The truth value of $\mathcal{B}$ does not matter.)
- The only remaining case to consider is when you cut the red wire and the bomb does explode. In this case, Assertion 21 has told the truth. In general, if $\mathcal{A}$ and $\mathcal{B}$ are true, then the implication "$\mathcal{A} \Rightarrow \mathcal{B}$" is true.

> $\mathcal{A} \Rightarrow \mathcal{B}$ is true unless $\mathcal{A}$ is true and $\mathcal{B}$ is false.
> In that case, the implication is false.

We can summarize this with a truth table for "implies."

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$
T	T	T
T	F	F
F	T	T
F	F	T

Remark 2.10. Logic students are sometimes confused by the fact that $\mathcal{A} \Rightarrow \mathcal{B}$ is true whenever $\mathcal{A}$ is false, but it is actually quite natural. For example, suppose a teacher promises, "If you do all of the homework, then you will pass the course." A student who fails to do all of the homework cannot accuse the teacher of a falsehood, whether he passes the course or not.

Also, people often use this principle when speaking sarcastically. An example is the assertion, "If Rudy is the best player on the team, then pigs can fly." We all know that pigs cannot fly, but, logically, the assertion is true as long as Rudy is *not* the best player on the team.

WARNING. The connective "implies" is *not* commutative: you cannot swap the hypothesis and the conclusion without changing the meaning of the assertion, because $\mathcal{A} \Rightarrow \mathcal{B}$ and $\mathcal{B} \Rightarrow \mathcal{A}$ are not logically equivalent.

Let us go back to the example with which we started our discussion of "$\Rightarrow$," in which R is the assertion "You will cut the red wire," and B means "The bomb will explode." There are many different ways of saying $R \Rightarrow B$ in English. Here are some of the ways; all of these mean the same thing!

- If you cut the red wire, then the bomb will explode.
- You cutting the red wire implies that the bomb will explode.
- Whenever you cut the red wire, the bomb will explode.
- The bomb will explode whenever you cut the red wire.
- The bomb exploding is a necessary consequence of you cutting the red wire.
- You cutting the red wire is sufficient to ensure that the bomb will explode.
- You cutting the red wire guarantees that the bomb will explode.
- You cutting the red wire is a stronger condition than the bomb exploding.
- The bomb exploding is a weaker condition than you cutting the red wire.
- You cut the red wire only if the bomb will explode.
- If the bomb does not explode, you must not have cut the red wire.
- Either you will not cut the red wire, or the bomb will explode.

EXERCISES 2.11. Using the given symbolization key, translate each English-language assertion into Propositional Logic.

A: Mister Ace was murdered.

B: The butler did it.

C: The cook did it.

D: The Duchess is lying.

E: Mister Edge was murdered.

F: The murder weapon was a frying pan.

1) If Mister Ace was murdered, then the cook did it.
2) If Mister Edge was murdered, then the cook did not do it.
3) The cook did it only if the Duchess is lying.
4) If the murder weapon was a frying pan, then the culprit must have been the cook.
5) If the murder weapon was not a frying pan, then the culprit was either the cook or the butler.
6) The Duchess is lying, unless it was Mister Edge who was murdered.
7) If Mister Ace was murdered, he was done in with a frying pan.
8) The cook did it, so the butler did not.

EXERCISES 2.12. Give a symbolization key and symbolize the following assertions in Propositional Logic.

1) If Gregor plays first base, then the team will lose.
2) If either Gregor or Evan plays first base, then there will not be a miracle.
3) If neither Gregor nor Evan plays first base, then there will be a miracle.
4) The team will lose unless there is a miracle.
5) If there is a miracle, then Gregor's mom will not bake cookies.

EXERCISES 2.13. For each deduction, write a symbolization key and translate the deduction as well as possible into Propositional Logic.

1) If Dorothy plays the piano in the morning, then Roger wakes up cranky. Dorothy plays piano in the morning unless she is distracted. So if Roger does not wake up cranky, then Dorothy must be distracted.
2) It will either rain or snow on Tuesday. If it rains, Neville will be sad. If it snows, Neville will be cold. Therefore, Neville will either be sad or cold on Tuesday.
3) If Zoog remembered to do his chores, then things are clean but not neat. If he forgot, then things are neat but not clean. Therefore, things are either neat or clean—but not both.

EXERCISES 2.14. Using the given symbolization key, translate each assertion into English.

J: Romeo likes Juliet.

M: Mercutio likes Juliet.

T: Romeo likes Tybalt.

1) $M \Rightarrow J$
2) $J \vee (M \Rightarrow \neg T)$
3) $(T \Rightarrow J)\ \&\ (M \Rightarrow J)$

2B.5. Iff ($\Leftrightarrow$). Consider these assertions:

24. The figure on the board is a triangle only if it has exactly three sides.
25. The figure on the board is a triangle if it has exactly three sides.
26. The figure on the board is a triangle if and only if it has exactly three sides.

Let T mean "The figure is a triangle" and S mean "The figure has exactly three sides."

Assertion 24, for reasons discussed above, can be translated as $T \Rightarrow S$.

Assertion 25 is importantly different. It can be paraphrased as, "If the figure has three sides, then it is a triangle." So it can be translated as $S \Rightarrow T$.

Assertion 26 says two things: that "T is true if S is true" *and* that "T is true only if S is true." The first half is Assertion 25, and the second half is Assertion 24; thus, it can be translated as

$$(S \Rightarrow T)\ \&\ (T \Rightarrow S).$$

However, this "if and only if" comes up so often that it has its own name. Officially, this is called a **biconditional**, and is denoted "$\Leftrightarrow$"; Assertion 26 can be translated as $S \Leftrightarrow T$. Unofficially, the name of this connective is "iff."

Because we could always write $(\mathcal{A} \Rightarrow \mathcal{B})\ \&\ (\mathcal{B} \Rightarrow \mathcal{A})$ instead of $\mathcal{A} \Leftrightarrow \mathcal{B}$, we do not strictly speaking *need* to introduce a new symbol for "iff." Nevertheless, it is commonly accepted as one of the basic logical connectives.

$\mathcal{A} \Leftrightarrow \mathcal{B}$ is true if and only if $\mathcal{A}$ and $\mathcal{B}$ have the same truth value (either both are true or both are false).

This is the truth table for "iff":

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Leftrightarrow \mathcal{B}$
T	T	T
T	F	F
F	T	F
F	F	T

EXERCISES 2.15. Using the given symbolization key, translate each English-language assertion into Propositional Logic.

E_1: Ava is an electrician.

E_2: Harrison is an electrician.

F_1: Ava is a firefighter.

F_2: Harrison is a firefighter.

S_1: Ava is satisfied with her career.

S_2: Harrison is satisfied with his career.

1) If Ava is not an electrician, then neither is Harrison, but if she is, then he is too.

2) Ava is satisfied with her career if and only if Harrison is not satisfied with his.

3) Harrison and Ava are both firefighters if and only if neither of them is an electrician.

EXERCISES 2.16. Using the given symbolization key, translate each assertion into English.

J: Romeo likes Juliet.

M: Mercutio likes Juliet.

T: Romeo likes Tybalt.

Y: Romeo likes Yorick.

1) $T \Leftrightarrow Y$

2) $M \Leftrightarrow (J \vee Y)$

3) $(J \Leftrightarrow M) \,\&\, (T \Rightarrow Y)$

SUMMARY:

- Practice in translating between English and Propositional Logic.
- In mathematics, "or" is inclusive.
- Notation:
  - $\neg$ (not; means "It is not the case that_____")
  - & (and; means "Both _____ and _____")
  - $\vee$ (or; means "Either _____ or _____")
  - $\Rightarrow$ (implies; means "If _____ then _____")
  - $\Leftrightarrow$ (iff; means "_____ if and only if _____")

Chapter 3

Basic Theorems of Propositional Logic

Beyond the obvious facts that he has at some time done manual labor, that he takes snuff, that he is a Freemason, that he has been in China, and that he has done a considerable amount of writing lately, I can deduce nothing else.

Sherlock Holmes, fictional British detective
in *The Red-Headed League*

In this chapter, we will see some fundamental examples of valid deductions. (They will be used as the basis of more sophisticated deductions in later chapters.) As a matter of terminology, any valid deduction can be called a **theorem**.

3A. Calculating the truth-value of an assertion

To put them all in one place, the truth tables for the connectives of Propositional Logic are repeated here:

$\mathcal{A}$	$\neg\mathcal{A}$
T	F
F	T

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A}\&\mathcal{B}$	$\mathcal{A}\vee\mathcal{B}$	$\mathcal{A}\Rightarrow\mathcal{B}$	$\mathcal{A}\Leftrightarrow\mathcal{B}$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Truth tables for the connectives of Propositional Logic.

Every student in mathematics (or computer science) needs to be able to quickly reproduce *all* of these truth tables, without looking them up.

Using these tables, you should be able to calculate the truth-value of any assertion, for any given values of its assertion letters. (In this chapter, we often refer to assertion letters as "**variables**.")

EXAMPLE 3.1. What is the truth value of $(A \vee B) \Rightarrow (B \,\&\, \neg C)$ when A is true, B is false, and C is false?

SOLUTION. We have

$$\begin{aligned}(A \vee B) \Rightarrow (B \,\&\, \neg C) &= (\mathsf{T} \vee \mathsf{F}) \Rightarrow (\mathsf{F} \,\&\, \neg\mathsf{F}) \\ &= \mathsf{T} \Rightarrow (\mathsf{F} \,\&\, \mathsf{T}) \\ &= \mathsf{T} \Rightarrow \mathsf{F} \\ &= \mathsf{F}.\end{aligned}$$

The assertion is false. □

What does this mean in English? Suppose, for example, that we have the symbolization key

A: Bill baked an apple pie,

B: Bill baked a banana pie,

C: Bill baked a cherry pie.

Also suppose Ellen tells us (maybe because she knows what ingredients Bill has):

> If Bill baked either an apple pie or a banana pie,
> then he baked a banana pie, but did not bake a cherry pie.

Now, it turns out that

> Bill baked an apple pie, but did not bake a banana pie, and did not bake a cherry pie.

Then the above calculation shows that *Ellen was wrong*; her assertion is *false*.

EXAMPLE 3.2. Assume A is true, B is false, and C is true. What is the truth-value of

$$(A \vee C) \Rightarrow \neg(A \Rightarrow B)?$$

SOLUTION. We have

$$\begin{aligned}(A \vee C) \Rightarrow \neg(A \Rightarrow B) &= (\mathsf{T} \vee \mathsf{T}) \Rightarrow \neg(\mathsf{T} \Rightarrow \mathsf{F}) \\ &= \mathsf{T} \Rightarrow \neg\mathsf{F} \\ &= \mathsf{T} \Rightarrow \mathsf{T} \\ &= \mathsf{T}.\end{aligned}$$

The assertion is true. □

EXERCISES 3.3. Find the truth-value of the given assertion for the given values of the variables.

1) $(A \vee C) \Rightarrow \neg(A \Rightarrow B)$
   (a) A is true, B is false, and C is false.
   (b) A is false, B is true, and C is false.
2) $\big(P \vee \neg(Q \Rightarrow R)\big) \Rightarrow \big((P \vee Q) \,\&\, R\big)$
   (a) P, Q, and R are all true.
   (b) P is true, Q is false, and R is true.
   (c) P is false, Q is true, and R is false.
   (d) P, Q, and R are all false.
3) $\big((U \,\&\, \neg V) \vee (V \,\&\, \neg W) \vee (W \,\&\, \neg U)\big) \Rightarrow \neg(U \,\&\, V \,\&\, W)$
   (a) U, V, and W are all true.
   (b) U is true, V is true, and W is false.

(c) U is false, V is true, and W is false.

(d) U, V, and W are all false.

4) $(X \vee \neg Y)\ \&\ (X \Rightarrow Y)$

(a) X and Y are both true.

(b) X is true and Y is false.

(c) X is false and Y is true.

(d) X and Y are both false.

3B. Identifying tautologies, contradictions, and contingent sentences

By evaluating an assertion for all possible values of its variables, you can decide whether it is a tautology, a contradiction, or a contingent assertion.

EXAMPLE 3.4. Is the assertion $(H\ \&\ I) \Rightarrow H$ a tautology?

SOLUTION. The variables H and I may each be either true or false, and we will evaluate the assertion for all possible combinations. To make it clear that none of the possibilities have been missed, we proceed systematically: for each value of H, we consider the two possible values for I.

Case 1: Assume H is true.

Subcase 1.1: Assume I is true. We have

$$(H\ \&\ I) \Rightarrow H \quad = \quad (\mathsf{T}\ \&\ \mathsf{T}) \Rightarrow \mathsf{T} \quad = \quad \mathsf{T} \Rightarrow \mathsf{T} \quad = \quad \mathsf{T}.$$

Subcase 1.2: Assume I is false. We have

$$(H\ \&\ I) \Rightarrow H \quad = \quad (\mathsf{T}\ \&\ \mathsf{F}) \Rightarrow \mathsf{T} \quad = \quad \mathsf{F} \Rightarrow \mathsf{T} \quad = \quad \mathsf{T}.$$

Case 2: Assume H is false.

Subcase 2.1: Assume I is true. We have

$$(H\ \&\ I) \Rightarrow H \quad = \quad (\mathsf{T}\ \&\ \mathsf{F}) \Rightarrow \mathsf{T} \quad = \quad \mathsf{F} \Rightarrow \mathsf{T} \quad = \quad \mathsf{T}.$$

Subcase 2.2: Assume I is false. We have

$$(H\ \&\ I) \Rightarrow H \quad = \quad (\mathsf{F}\ \&\ \mathsf{F}) \Rightarrow \mathsf{F} \quad = \quad \mathsf{F} \Rightarrow \mathsf{F} \quad = \quad \mathsf{T}.$$

The assertion is true in all cases, so it is a tautology. □

EXERCISE 3.5 (Law of excluded middle). Verify that

$A \vee \neg A$ is a tautology

by evaluating it for all possible values of the variable.

Remark 3.6.

1) Recall that an assertion is a **tautology** if it must be true as a matter of logic. This means that its truth-value is "true," no matter what truth-values are assigned to its variables.

- To show that an assertion *is* a tautology, we could calculate its truth-value for every possible assignment to its variables. (If the result comes out "true" for every one of the possibilities, then the assertion is a tautology.) Unfortunately, this will be a lot of work if there are many variables.

- It takes a lot less work to show that an assertion is *not* a tautology. This is because it suffices to find a single choice of truth-values for its variables that makes the assertion false. For example, if M and N are true, and P is false, then $\neg M \vee (N \Rightarrow P)$ is false. Therefore, the assertion $\neg M \vee (N \Rightarrow P)$ is not a tautology.

2) Similarly, an assertion of Propositional Logic is a **contradiction** if its truth-value is "false," no matter what truth-values are assigned to its variables. So there is more work involved in showing that an assertion is a contradiction than there is in showing that it is not. For example, if M, N and P are all true, then $\neg M \vee (N \Rightarrow P)$ is true, so the assertion $\neg M \vee (N \Rightarrow P)$ is not a contradiction.

3) An assertion of Propositional Logic is **contingent** if it is neither a tautology nor a contradiction. That is, there is an assignment for which its truth-value is false, and some other assignment for which its truth value is true. For example, the assertion $\neg M \vee (N \Rightarrow P)$ is contingent, because (as we have seen above):

- its truth value is false if M is true, and N and P are false, but
- its truth value is true if M, N and P are all true.

EXERCISES 3.7. Show that each of the following assertions is *not* a tautology.

1) $A \Rightarrow (A \,\&\, B)$
2) $(A \vee B) \Rightarrow A$
3) $(A \Leftrightarrow B) \vee (A \,\&\, \neg B)$
4) $\big(P \,\&\, \neg(Q \,\&\, R)\big) \vee (Q \Rightarrow R)$
5) $\big(P \,\&\, (\neg Q \vee \neg R)\big) \Rightarrow (P \Rightarrow \neg Q)$
6) $\big((P \Rightarrow Q) \,\&\, (Q \Rightarrow R)\big) \Rightarrow (R \Rightarrow P)$
7) $(X \Rightarrow Z) \Rightarrow (Y \Rightarrow Z)$
8) $(X \Leftrightarrow Y) \vee (X \Leftrightarrow Z) \vee (Y \,\&\, Z)$
9) $(\neg X \vee \neg Y \vee \neg Z) \Rightarrow \big((\neg X \vee \neg Y) \,\&\, (\neg Y \vee \neg Z)\big)$

EXERCISES 3.8. Determine whether each of the following assertions is a tautology, a contradiction, or a contingent assertion. (Justify your answer.)

1) $A \Rightarrow A$
2) $C \Rightarrow \neg C$
3) $(A \Leftrightarrow B) \Leftrightarrow \neg(A \Leftrightarrow \neg B)$
4) $(A \Rightarrow B) \vee (B \Rightarrow A)$
5) $(A \,\&\, B) \Rightarrow (B \vee A)$
6) $\neg(A \vee B) \Leftrightarrow (\neg A \,\&\, \neg B)$
7) $\big[(A \,\&\, B) \,\&\, \neg(A \,\&\, B)\big] \,\&\, C$
8) $[(A \,\&\, B) \,\&\, C] \Rightarrow B$
9) $\neg\big[(C \vee A) \vee B\big]$
10) $(C \Rightarrow \neg C) \,\&\, (\neg C \Rightarrow C)$

3C. Logical equivalence

Recall that two assertions are **logically equivalent** if they have the same truth value as a matter of logic. This means that, for every possible assignment of true or false to the variables, the two assertions come out with the same truth-value (either both are true or both are false). Verifying this can take a lot of work.

On the other hand, to show that two assertions are *not* logically equivalent, you should find an assignment to the variables, such that one of the assertions is true and the other is false.

EXAMPLE 3.9. If A is true and B is false, then $A \vee B$ is true, but $A \Rightarrow B$ is false. Therefore, the assertions $A \vee B$ and $A \Rightarrow B$ are *not* logically equivalent.

EXERCISE 3.10. Show that each of the following pairs of sentences are *not* logically equivalent.

1) $A \vee B \vee \neg C$, $(A \vee B)\ \&\ (C \Rightarrow A)$

2) $(P \Rightarrow Q) \vee (Q \Rightarrow P)$, $P \vee Q$

3) $(X\ \&\ Y) \Rightarrow Z$, $X \vee (Y \Rightarrow Z)$

EXAMPLE 3.11. Are the assertions $\neg(A \vee B)$ and $\neg A\ \&\ \neg B$ logically equivalent?

SOLUTION. We consider all the possible values of the variables.

Case 1: Assume A is true.

Subcase 1.1: Assume B is true. We have

$$\neg(A \vee B) \quad = \quad \neg(T \vee T) \quad = \quad \neg T \quad = \quad F$$

and

$$\neg A\ \&\ \neg B \quad = \quad \neg T\ \&\ \neg T \quad = \quad F\ \&\ F \quad = \quad F.$$

Both assertions are false, so they have the same truth value.

Subcase 1.2: Assume B is false. We have

$$\neg(A \vee B) \quad = \quad \neg(T \vee F) \quad = \quad \neg T \quad = \quad F$$

and

$$\neg A\ \&\ \neg B \quad = \quad \neg T\ \&\ \neg F \quad = \quad T\ \&\ F \quad = \quad F.$$

Both assertions are false, so they have the same truth value.

Case 2: Assume A is false.

Subcase 2.1: Assume B is true. We have

$$\neg(A \vee B) \quad = \quad \neg(F \vee T) \quad = \quad \neg T \quad = \quad F$$

and

$$\neg A\ \&\ \neg B \quad = \quad \neg F\ \&\ \neg T \quad = \quad T\ \&\ F \quad = \quad F.$$

Both assertions are false, so they have the same truth value.

Subcase 2.2: Assume B is false. We have

$$\neg(A \vee B) \quad = \quad \neg(F \vee F) \quad = \quad \neg F \quad = \quad T$$

and

$$\neg A\ \&\ \neg B \quad = \quad \neg F\ \&\ \neg F \quad = \quad T\ \&\ T \quad = \quad T.$$

Both assertions are true, so they have the same truth value.

In all cases, the two assertions have the same truth value, so they are logically equivalent. □

EXERCISES 3.12. Determine whether each pair of assertions is logically equivalent (and justify your answer).

1) $A \Rightarrow A$, $A \Leftrightarrow A$

2) $(A \vee \neg B)$, $(A \Rightarrow B)$

3) $A \,\&\, \neg A$, $\neg B \Leftrightarrow B$

4) $\neg(A \,\&\, B)$, $(\neg A \vee \neg B)$

EXERCISES 3.13. Answer each of the questions below and justify your answer.

1) Suppose that $\mathcal{A}$ and $\mathcal{B}$ are logically equivalent. What can you say about $\mathcal{A} \Leftrightarrow \mathcal{B}$?

2) Suppose that $\mathcal{A}$ and $\mathcal{B}$ are *not* logically equivalent. What can you say about $\mathcal{A} \Leftrightarrow \mathcal{B}$?

3) Suppose that $\mathcal{A}$ and $\mathcal{B}$ are logically equivalent. What can you say about $(\mathcal{A} \vee \mathcal{B})$?

4) Suppose that $\mathcal{A}$ and $\mathcal{B}$ are *not* logically equivalent. What can you say about $(\mathcal{A} \vee \mathcal{B})$?

NOTATION 3.14. We will write $\mathcal{A} \equiv \mathcal{B}$ to denote that $\mathcal{A}$ is logically equivalent to $\mathcal{B}$.

Sometimes it is possible to see that two assertions are equivalent, without having to evaluate them for all possible values of the variables.

EXAMPLE 3.15. Explain how you know that

$$\neg(A \vee B) \quad \equiv \quad \neg A \,\&\, \neg B.$$

SOLUTION. Note that the assertion $\neg(A \vee B)$ is true if and only if $A \vee B$ is false, which means that neither A nor B is true. Therefore,

$$\neg(A \vee B) \text{ is true if and only if } A \text{ and } B \text{ are both false.}$$

Also, $\neg A \,\&\, \neg B$ is true if and only if $\neg A$ and $\neg B$ are both true, which means that:

$$\neg A \,\&\, \neg B \text{ is true if and only if } A \text{ and } B \text{ are both false.}$$

So the two assertions $\neg(A \vee B)$ and $\neg A \,\&\, \neg B$ are true in exactly the same situation (namely, when A and B are both false); and they are both false in all other situations. So the two assertions have the same truth value in all situations. Therefore, they are logically equivalent.□

EXERCISES 3.16. Verify each of the following important logical equivalences. For most of these, you should not need to evaluate the assertions for all possible values of the variables.

1) commutativity of &, $\vee$, and $\Leftrightarrow$:

$$\begin{aligned} A \,\&\, B \quad &\equiv \quad B \,\&\, A \\ A \vee B \quad &\equiv \quad B \vee A \\ A \Leftrightarrow B \quad &\equiv \quad B \Leftrightarrow A \end{aligned}$$

2) associativity of & and $\vee$:

$$\begin{aligned} (A \,\&\, B) \,\&\, C \quad &\equiv \quad A \,\&\, (B \,\&\, C) \\ (A \vee B) \vee C \quad &\equiv \quad A \vee (B \vee C) \end{aligned}$$

3) rules of negation ("De Morgan's Laws"):

$$\begin{aligned} \neg\neg A &\equiv A \\ \neg(A \,\&\, B) &\equiv \neg A \vee \neg B \\ \neg(A \vee B) &\equiv \neg A \,\&\, \neg B \\ \neg(A \Rightarrow B) &\equiv A \,\&\, \neg B \\ \neg(A \Leftrightarrow B) &\equiv (A \,\&\, \neg B) \vee (B \,\&\, \neg A) \end{aligned}$$

The rules of negation can be used to simplify the negation of any assertion.

EXAMPLE 3.17. Simplify $\neg\big((A \vee B) \Rightarrow (A \,\&\, \neg C)\big)$.

SOLUTION. We have

$$\begin{aligned} \neg\big((A \vee B) \Rightarrow (A \,\&\, \neg C)\big) &\equiv (A \vee B) \,\&\, \neg(A \,\&\, \neg C) \\ &\equiv (A \vee B) \,\&\, (\neg A \vee \neg\neg C) \\ &\equiv (A \vee B) \,\&\, (\neg A \vee C). \end{aligned}$$ □

Remark 3.18. If $\mathcal{A} \equiv \mathcal{B}$, then $\mathcal{A},\ \therefore \mathcal{B}$ is a theorem. For example, the above example shows that

$$\neg\big((A \vee B) \Rightarrow (A \,\&\, \neg C)\big),\ \therefore (A \vee B) \,\&\, (\neg A \vee C)$$

is a theorem.

EXERCISE 3.19. Use De Morgan's Laws (that is, the rules of negation) to simplify each of the following assertions (until negation is not applied to anything but variables).

1) $\neg\big((A \vee B) \Rightarrow (C \,\&\, D)\big)$
2) $\neg\big((A \Rightarrow B) \vee (C \,\&\, D)\big)$
3) $\neg\Big(A \Rightarrow \big(B \Rightarrow (C \Rightarrow D)\big)\Big)$
4) $\neg\Big(\big((A \Rightarrow B) \Rightarrow C\big) \Rightarrow D\Big)$
5) $\neg\big((P \vee \neg Q) \,\&\, R\big)$
6) $\neg(P \,\&\, Q \,\&\, R \,\&\, S)$
7) $\neg\Big(\big(P \Rightarrow (Q \,\&\, \neg R)\big) \vee (P \,\&\, \neg Q)\Big)$

EXERCISE 3.20. Use De Morgan's Laws to simplify the *negation* of each of these assertions. Express your answers in English.

1) If it is raining, then the bus will not be on time.
2) I am sick, and I am tired.
3) Either the Pope is here, or the Queen and the Russian are both here.
4) If Tom forgot his backpack, then Sam will eat either a pickle or a potato, and either Bob will not have lunch, or Alice will drive to the store.

EXERCISES 3.21. It was mentioned in Chapter 2 that "$\Leftrightarrow$" is not necessary, because $A \Leftrightarrow B$ is just an abbreviation for $(A \Rightarrow B) \,\&\, (B \Rightarrow A)$. Some of the other connectives are also unnecessary.

1) It would be enough to have only "not" and "implies." Show this by writing assertions that are logically equivalent to each of the following, using only parentheses, assertion letters, "¬," and "⇒."

(a) $A \vee B$ (b) $A \,\&\, B$ (c) $A \Leftrightarrow B$

2) As an alternative, show that it would be enough to have only "not" and "or": using only parentheses, assertion letters, "¬," and "∨," write assertions that are logically equivalent to each of the following.

(a) $A \,\&\, B$ (b) $A \Rightarrow B$ (c) $A \Leftrightarrow B$

3) The logical connective "**nand**" (also called the "*Sheffer stroke*") has the following truth table:

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \barwedge \mathcal{B}$
T	T	F
T	F	T
F	T	T
F	F	T

(a) Write an assertion using the connectives of Propositional Logic that is logically equivalent to $A \barwedge B$.

(b) Show that it would suffice to have only "nand," and no other connectives: using only "$\barwedge$" (and parentheses and assertion letters), write assertions that are equivalent to each of the following.

(i) $\neg A$ (iii) $A \vee B$ (v) $A \Leftrightarrow B$

(ii) $A \,\&\, B$ (iv) $A \Rightarrow B$

3D. Converse and contrapositive

The **converse** of an implication $\mathcal{A} \Rightarrow \mathcal{B}$ is the implication $\mathcal{B} \Rightarrow \mathcal{A}$. For example, the converse of "if Bob pays the cashier a dollar, then the server gives Bob an ice cream cone" is "if the server gives Bob an ice cream, then Bob pays the cashier a dollar." It should be clear that these are not saying the same thing. (For example, perhaps Bob has a coupon for a free cone.(This illustrates the fact that the converse of an assertion is usually not logically equivalent to the original assertion. In other words (as was mentioned in section 2B.4), the connective ⇒ is *not* commutative: $A \Rightarrow B$ is *not* logically equivalent to $B \Rightarrow A$.

EXERCISE 3.22. Show that $A \Rightarrow B$ is not logically equivalent to its converse $B \Rightarrow A$, by finding values of the variables A and B for which the two assertions have different truth values.

The **inverse** of an implication $\mathcal{A} \Rightarrow \mathcal{B}$ is the implication $\neg\mathcal{A} \Rightarrow \neg\mathcal{B}$. For example, the inverse of "if Bob pays the cashier a dollar, then the server gives Bob an ice cream cone" is "if Bob does not pay the cashier a dollar, then the server does not give Bob an ice cream cone." It should be clear that these are not saying the same thing (because one assertion is about what happens if Bob pays a dollar, and the other is about the completely different situation in which Bob does not pay a dollar). This illustrates the fact that the inverse of an assertion is usually not logically equivalent to the original assertion: $A \Rightarrow B$ is *not* logically equivalent to $\neg A \Rightarrow \neg B$.

EXERCISE 3.23. Show that $A \Rightarrow B$ is not logically equivalent to its inverse $\neg A \Rightarrow \neg B$, by finding values of the variables A and B for which the two assertions have different truth values.

The **contrapositive** of an implication is the converse of its inverse (or the inverse of its converse, which amounts to the same thing). That is, the contrapositive of $\mathcal{A} \Rightarrow \mathcal{B}$ is the implication $\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$. For example, the contrapositive of "if Bob pays the cashier a dollar, then the server gives Bob an ice cream cone" is "if the server does not give Bob an ice cream cone, then Bob does not pay the cashier a dollar." A bit of thought should convince you that these *are* saying the same thing. This illustrates the following important fact:

Any implication is logically equivalent to its contrapositive.

EXERCISE 3.24. Show that $A \Rightarrow B$ is logically equivalent to its contrapositive $\neg B \Rightarrow \neg A$, by verifying that the two assertions have the same truth value, for all possible values of the variables A and B.

Remark 3.25. The inverse will not be important to us, although the converse and the contrapositive are fundamental. However, it is worth mentioning that the inverse is the contrapositive of the converse, and therefore the inverse and the converse are logically equivalent to each other.

Warning: Implications (that is, those of the form $\mathcal{A} \Rightarrow \mathcal{B}$) are the only assertions that have a converse or a contrapositive. For example, the converse of "I hate cheese" does not exist, because this assertion is not an if-then statement.

EXERCISES 3.26. State (a) the converse and (b) the contrapositive of each implication. (You do not need to show your work.)

1) If the students come to class, then the teacher lectures.

2) If it rains, then I carry my umbrella.

3) I go to school only if it is a weekday.

4) If you give me $5, I can take you to the airport.

5) If the Mighty Ducks are the best hockey team, then pigs can fly.

6) Alberta is a province.

7) You will do well in your math class only if you do all of the homework problem.

3E. Some valid deductions

Recall that a deduction is **valid** if its conclusion is true in all situations where all of its hypotheses are true. This means that the conclusion is true for each and every possible assignment of truth-values to the variables that make all of the hypotheses true.

EXAMPLE 3.27. Show that the following deduction is valid:

Hypotheses:

1. $\neg L \Rightarrow (J \vee L)$
2. $\neg L$

Conclusion: J

SOLUTION. We proceed in two steps.

Step I. We look at all possible combinations of values of the variables, to find out which ones make the hypotheses true. To do this, we consider each of the two possible values (T or F) of the variable J as separate case. In each case, we consider the two possible values of the variable L as subcases.

Case 1. Assume J is true.

Subcase 1.1. Assume L is true. We have

$$\neg L \quad = \quad \neg T \quad = \quad F,$$

so Hypothesis (2) is false.

Subcase 1.2. Assume L is false. We have

$$\neg L \Rightarrow (J \vee L) \quad = \quad \neg F \Rightarrow (T \vee F) \quad = \quad T \Rightarrow T \quad = \quad T$$

and

$$\neg L \quad = \quad \neg F \quad = \quad T,$$

so both hypotheses are true in this case.

Case 2. Assume J is false.

Subcase 2.1. Assume L is true. We have

$$\neg L \quad = \quad \neg T \quad = \quad F,$$

so Hypothesis (2) is false.

Subcase 2.2. Assume L is false. We have

$$\neg L \Rightarrow (J \vee L) \quad = \quad \neg F \Rightarrow (F \vee F) \quad = \quad T \Rightarrow F \quad = \quad F$$

so Hypothesis (1) is false.

Step II. We find the truth value of the conclusion for each assignment of variables that makes all of the hypotheses true. From the work in Step I, we see that the only situation where both hypotheses are true is in Subcase 1.2, where

$$J \text{ is true and } L \text{ is false.}$$

In this situation, the conclusion J is obviously true.

Since the conclusion of the deduction is true in the only situation where both hypotheses are true, the deduction is valid. □

Remark 3.28. Checking all of the possible values of the variables is called **case-by-case analysis**; it can be a lengthy and tedious process. In the future, we will usually try to show that a deduction is valid without having to do so much work. The logician's tools for doing this are the main topic of Chapter 4 and, in particular, Example 4.4 provides a short proof that the above deduction is valid, without having to check all of the cases.

EXERCISES 3.29. Answer each of the questions below and justify your answer.

1) Suppose that $(\mathcal{A} \,\&\, \mathcal{B}) \Rightarrow \mathcal{C}$ is contingent. What can you say about the deduction "$\mathcal{A}$, $\mathcal{B}$, $\therefore \mathcal{C}$"?
2) Suppose that $\mathcal{A}$ is a contradiction. What can you say about the deduction "$\mathcal{A}$, $\mathcal{B}$, $\therefore \mathcal{C}$"?
3) Suppose that $\mathcal{C}$ is a tautology. What can you say about the deduction "$\mathcal{A}$, $\mathcal{B}$, $\therefore \mathcal{C}$"?

Here is an example that we can justify without doing a case-by-case analysis:

EXAMPLE 3.30. Explain how you know that the following deduction is valid.

$$A \vee B, \quad \neg A, \quad \therefore \; B.$$

SOLUTION. Assume we are in a situation in which both hypotheses of the deduction are true. Then, from the first hypothesis, we know that either A is true or B is true. However, from the second hypothesis, we know that A is *not* true. Therefore, it must be B that is true. Hence, the conclusion of the deduction is true. □

EXERCISE 3.31 (Rules of Propositional Logic). It is not difficult to see that each of the following is a valid deduction. For each of them, either give a short explanation of how you know that it is valid, or verify the deduction by evaluating the conclusion for all possible values of the variables that make the hypotheses true.) All of these theorems will be used on a regular basis in the following chapters (and in your later mathematics courses).

1) repeat:

$$A, \therefore A$$

2) &-introduction:

$$A,\ B,\ \therefore A \,\&\, B$$

3) &-elimination:

$$A \,\&\, B,\ \therefore A \qquad\qquad A \,\&\, B,\ \therefore B$$

4) $\vee$-introduction:

$$A,\ \therefore A \vee B \qquad\qquad B,\ \therefore A \vee B$$

5) $\vee$-elimination:

$$A \vee B,\ \neg A,\ \therefore B \qquad\qquad A \vee B,\ \neg B,\ \therefore A$$

6) $\Rightarrow$-elimination ("*modus ponens*"):

$$A \Rightarrow B,\ A,\ \therefore B$$

7) $\Leftrightarrow$-introduction:

$$A \Rightarrow B,\ B \Rightarrow A,\ \therefore A \Leftrightarrow B$$

8) $\Leftrightarrow$-elimination:

$$A \Leftrightarrow B,\ \therefore A \Rightarrow B \qquad\qquad A \Leftrightarrow B,\ \therefore B \Rightarrow A$$

9) proof by cases:

$$A \vee B,\ A \Rightarrow C,\ B \Rightarrow C,\ \therefore C$$

Remark 3.32. A theorem remains valid if we change the names of the variables. For example, $P \vee Q,\ \neg P,\ \therefore Q$ is the same as $\vee$-elimination, but we have replaced A with P and B with Q. (In the language of high-school algebra, we have plugged in P for A, and plugged in Q for B.) Indeed, it should be clear that any theorem remains valid even if we substitute more complicated expressions into the variables.

EXAMPLE 3.33. The theorem

$$(X \vee Y) \Rightarrow (Y \vee Z),\ X \vee Y,\ \therefore Y \vee Z$$

is obtained from "$\Rightarrow$-elimination," by letting $A = (X \vee Y)$ and $B = (Y \vee Z)$.

EXERCISE 3.34. Each of the following is a valid theorem that is obtained from one of the basic theorems of Exercise 3.31, by substituting some expressions into the variables. Identify the theorem it is obtained from, and the expressions that were substituted into each variable.

1) $(A \vee B) \,\&\, (Y \Rightarrow Z),\ \therefore Y \Rightarrow Z$

2) $(A \vee B) \,\&\, (Y \Rightarrow Z),\ \therefore (A \vee B) \,\&\, (Y \Rightarrow Z)$

3) $A \vee B,\ \therefore (A \vee B) \vee (Y \Rightarrow Z)$

4) $(A \vee B), (Y \Rightarrow Z),\ \therefore (A \vee B)\ \&\ (Y \Rightarrow Z)$

EXERCISE 3.35. Each of the following is the English-language version of a valid theorem that is obtained from one of the basic theorems of Exercise 3.31, by substituting some expressions into the variables. Identify the theorem it is obtained from.

1) John went to the store. Therefore, as I already told you, John went to the store.

2) Susie will stop at either the grocery store or the drug store. If she stops at the grocery store, she will buy milk. If she stops at the drug store, she will buy milk. Therefore, I am sure that Susie will buy milk.

3) My opponent in this election is a liar! My opponent in this election is a cheat! Therefore, I say to you that my opponent is a liar and a cheat!

4) If I had $50, I would be able to buy a new coat. Hey, look! I found a $50 bill on the sidewalk! So I will be able to buy a new coat.

3F. Counterexamples

Not all deductions are valid. To show that a particular deduction is *not* valid, you need to show that it is possible for its conclusion to be false at the same time that all of its hypotheses are true. To do this, you should find an assignment to the variables that makes all of the hypotheses true, but makes the conclusion false.

EXAMPLE 3.36. Show that the deduction

$$A \vee B, \quad A \Rightarrow B, \quad \therefore\ A$$

is not valid.

Scratchwork. To make the conclusion false, we let A be false. Then, to make the first hypothesis true, we must let B be true. Fortunately, this also makes the second hypothesis true.

SOLUTION. Let A be false, and let B be true. Then

$$A \vee B \quad = \quad \mathsf{F} \vee \mathsf{T} \quad = \quad \mathsf{T}$$

and

$$A \Rightarrow B \quad = \quad \mathsf{F} \Rightarrow \mathsf{T} \quad = \quad \mathsf{T},$$

so both hypotheses of the deduction are true. However, the conclusion of the deduction (namely, A) is false.

Since we have a situation in which both hypotheses of the deduction are true, but the conclusion of the deduction is false, the deduction is not valid. □

DEFINITION 3.37. Any situation in which all of the hypotheses of a deduction are true, but the conclusion is false, is called a **counterexample** to the deduction.

To show that a deduction is *not* valid, find a counterexample.

EXERCISE 3.38. Show that each of these deductions is invalid, by finding a counterexample.

1) $A \vee B, \therefore A \Rightarrow B.$

2) $P \vee Q,\ \therefore P\ \&\ Q.$

3) $A \Rightarrow (B\ \&\ C),\ \neg A \Rightarrow (B \vee C),\ \therefore C.$

4) $P \Rightarrow Q, \neg P \Rightarrow R, \therefore Q\ \&\ (P \vee R)$

SUMMARY:

- Important definitions:
  - theorem
  - converse
  - contrapositive
- An implication might *not* be equivalent to its converse.
- Every implication is logically equivalent to its contrapositive.
- Expressions can be substituted into the variables of a valid deduction.
- To show that a deduction is *not* valid, find a counterexample.
- Basic theorems of Propositional Logic:
  - law of the excluded middle
  - commutativity of &, $\vee$, and $\Leftrightarrow$
  - associativity of & and $\vee$
  - rules of negation ("De Morgan's Laws")
  - repeat
  - introduction and elimination rules for &, $\vee$, and $\Leftrightarrow$
  - elimination rule for $\Rightarrow$
  - proof by cases

Chapter 4

Two-Column Proofs

. . . if it is a Miracle, any sort of evidence will answer, but if it is a Fact, proof is necessary.

Mark Twain (1835–1910), American author
Letters from the Earth

The aim of a *proof* is to show that a deduction is valid, and it does this by putting together a number of simpler deductions that are already known to be valid. This method has two major benefits over evaluating the conclusion for all possible values of the variables that make the hypotheses true.

- A proof justifies a deduction in a way that can give us an understanding of *why* the deduction is valid, rather than merely verifying that it can be trusted.
- A proof is often much shorter, and easier to verify, than a case-by-case consideration of all possible values of the variables.

For example, if a deduction has 10 assertion letters, and you have to evaluate the conclusion for all possible values of the variables, then the number of different cases you will need to look at is $2^{10} = 1024$. That would take a tremendous amount of work, and, in practice, no one will want to check all of that work to make sure you have not made a mistake. At the same time, there may be a short proof that takes only a few minutes of work to check.

Remark 4.1. Ultimately, our goal is to teach you to write clear and correct proofs, in English, of claims stated in English. But we will start with the simpler situation of proofs written in the language of Propositional Logic. This has several advantages:

- it allows assertions to be written more concisely, because entire English phrases are abbreviated to a single letter,
- it avoids the difficulties caused by the fact that sentences written in English can be ambiguous, and
- it displays the logical structure of a proof in a way that makes it easier to decide whether or not each step in a proof is valid.

After you are familiar with proofs in this simpler setting, you will employ the same principles to write proofs in English.

4A. First example of a two-column proof

Let us begin our exploration of proofs by looking at the following simple deduction.

Hypotheses:

1. $P \Rightarrow (Q \,\&\, R)$
2. P

Conclusion: R

You could verify that this deduction is valid by evaluating the conclusion for all possible values of the variables that make the hypotheses true. That would not be difficult, but let us take a different approach. Namely, we will prove that the deduction is valid by showing that it is a combination of deductions that are already known to be valid. Informally, we could try to convince someone that the deduction is valid by making the following explanation:

> Assume the Hypotheses (1) and (2) are true. Then applying $\Rightarrow$-elimination (with P in the role of A, and $Q \,\&\, R$ in the role of B) establishes that $Q \,\&\, R$ is true. This is an *intermediate conclusion*. It follows logically from the hypotheses, but it is not the conclusion we want. Now, applying &-elimination (with Q in the role of A, and R in the role of B) establishes that R is true. This is the conclusion of the deduction. Thus, we see that if the hypotheses of this deduction are true, then the conclusion is also true. So the deduction is valid.

For emphasis, let us repeat that this explanation allows us to avoid considering all the possible values of the variables; instead, we showed that the deduction is merely a combination of deductions that were already verified.

Remark 4.2. Notice that we are using the fact that the symbolic deductions are true regardless of the symbolization key we use. This is what allows us to talk about using (for example) "$Q \,\&\, R$ in the role of B." Another way of saying this, is that we are introducing a new symbolization key in which we let A stand for P, and let B stand for $Q \,\&\, R$.

Formally, a **proof** is a sequence of assertions. The first assertions of the sequence are assumptions; these are the hypotheses of the deduction. It is required that every assertion later in the sequence is an immediate consequence of earlier assertions. (There are specific rules that determine which assertions are allowed to appear at each point in the proof.) The final assertion of the sequence is the conclusion of the deduction.

In this chapter, we use the format known as "**two-column proofs**" for writing our proofs. As indicated in the tableau below:

- Assertions appear in the left column.
- The reason (or "justification") for including each assertion appears in the right column. (The allowable justifications will be discussed in the later sections of this chapter.)

⟨*assertion*⟩	⟨*justification*⟩

Every assertion in a two-column proof needs to have a justification in the second column.

For clarity, we draw a dark horizontal line to separate the hypotheses from the rest of the proof. (In addition, we will number each row of the proof, for ease of reference, and it is good to make the left border of the figure a dark line.) For example, here is a two-column proof that justifies the deduction above. It starts by listing the hypotheses of the deduction, and ends with the correct conclusion.

1	$P \Rightarrow (Q \,\&\, R)$	hypothesis
2	P	hypothesis
3	$Q \,\&\, R$	$\Rightarrow$-elim (lines 1 and 2)
4	R	&-elim (line 3)

In this example, the assertions were written in the language of Propositional Logic, but sometimes we will write our proofs in English. For example, here is a symbolization key that allows us to translate P, Q, and R into English. For convenience, this same symbolization key will be used in many of the examples in this chapter.

P: The Pope is here.

Q: The Queen is here.

R: The Russian is here.

Now, we can translate the deduction into English:

Hypotheses:

1. If the Pope is here, then the Queen and the Russian are also here.
2. The Pope is here.

Conclusion: The Russian is here.

And we can provide a two-column proof in English:

1	If the Pope is here, then the Queen and the Russian are also here.	hypothesis
2	The Pope is here.	hypothesis
3	The Queen and the Russian are both here.	$\Rightarrow$-elim (lines 1 and 2)
4	The Russian is here.	&-elim (line 3)

Hypotheses:

(1) $P \Rightarrow (Q \,\&\, R)$ If the Pope is here, then the Queen and the Russian are also here.

(2) P The Pope is here.

Conclusion: R Therefore, the Russian is here.

While you are getting accustomed to two-column proofs, it will probably be helpful to see examples in *both* English *and* Propositional Logic. To save space, and make it easier to compare the two, the text will sometimes combine both proofs into one figure, by adding a third column at the right that states the English-language versions of the assertions:

⟨*assertion in Propositional Logic*⟩	⟨*justification*⟩	⟨*English-language version of the assertion*⟩

For example, here is what we get by combining the two proofs above:

1	$P \Rightarrow (Q \,\&\, R)$	hypothesis	If the Pope is here, then the Queen and the Russian are also here.
2	P	hypothesis	The Pope is here.
3	$Q \,\&\, R$	$\Rightarrow$-elim (lines 1 and 2)	The Queen and the Russian are both here.
4	R	&-elim (line 3)	The Russian is here.

The next few sections will explain the justifications that are allowed in a two-column proof.

4B. Hypotheses and theorems in two-column proofs

A two-column proof must start by listing all of the hypotheses of the deduction, and each hypothesis is justified by writing the word **hypothesis** in the second column. (This is the only rule that is allowed above the dark horizontal line, and it is not allowed below the dark horizontal line.) We saw this rule in the above examples of two-column proofs. As a synonym for "hypothesis," one sometimes says "given" or "assumption."

Any deduction that is *already known to be valid* can be used as a justification *if* its hypotheses have been verified earlier in the proof. (And the lines where the hypotheses appear are written in parentheses after the name of the theorem.) For example, the theorems "$\Rightarrow$-elim" and "$\vee$-elim were used in our first examples of two-column proofs. These and several other very useful theorems were given in Chapter 3. You will be expected to be familiar with all of them.

EXAMPLE 4.3. Here is a proof of the deduction

$$P \vee Q, \quad Q \Rightarrow R, \quad \neg P, \quad \therefore R.$$

We provide an English translation by using the symbolization key on page 39.

1	$P \vee Q$	hypothesis	Either Pope is here, or the Queen is here.
2	$Q \Rightarrow R$	hypothesis	If the Queen is here, then the Russian is also here.
3	$\neg P$	hypothesis	The Pope is not here.
4	Q	$\vee$-elim (lines 1 and 3)	The Queen is here.
5	R	$\Rightarrow$-elim (lines 2 and 4)	The Russian is here.

EXAMPLE 4.4. Here is a short proof of the deduction in Example 3.27.

1	$\neg L \Rightarrow (J \vee L)$	hypothesis
2	$\neg L$	hypothesis
3	$J \vee L$	$\Rightarrow$-elim (lines 1 and 2)
4	J	$\vee$-elim (lines 3 and 2)

This proof is much shorter, and easier to check, than the case-by-case analysis of our original solution.

EXERCISES 4.5. Write a two-column proof of each of the following deductions:

1) $P \vee Q,\ \ Q \vee R,\ \ \neg Q,\ \ \therefore\ P \,\&\, R.$

2) $(E \vee G) \vee F,\ \ \neg G \,\&\, \neg F,\ \ \therefore\ E.$

EXERCISE 4.6. Provide a justification (rule and line numbers) for each line of this proof.

1	$W \Rightarrow \neg B$	
2	$A \,\&\, W$	
3	$\neg B \Rightarrow (J \,\&\, K)$	
4	W	
5	$\neg B$	
6	$J \,\&\, K$	
7	K	

EXERCISES 4.7. Write a two-column proof of each of the following deductions. (Write the assertions in English.)

1)

Hypotheses:

The Pope and the Queen are here.

Conclusion: The Queen is here.

2)

Hypotheses:

The Pope is here.

The Russian and the Queen are here.

Conclusion: The Queen and the Pope are here.

3)

Hypotheses:

If the Pope is here, then the Queen is here.

If the Queen is here, then the Russian is here.

The Pope is here.

Conclusion: The Russian is here.

4) Grace is sick.
Frank is sick.
$\therefore$ Either Grace and Frank are both sick, or Ellen is sick.

EXAMPLE 4.8. Many proofs use De Morgan's Laws (in other words, the rules for negation) or the fact that any statement is logically equivalent to its contrapositive. Here is an example.

1	$\neg P \Rightarrow (Q \,\&\, R)$	hypothesis	If the Pope is not here, then the Queen and the Russian are here.
2	$\neg Q \vee \neg R$	hypothesis	Either the Queen is not here, or the Russian is not here.
3	$\neg(Q \,\&\, R) \Rightarrow \neg\neg P$	contrapositive of line 1	If it is not the case that both the Queen and the Russian are here, then it is not the case that the Pope is not here.
4	$(\neg Q \vee \neg R) \Rightarrow P$	De Morgan's Laws applied to line 3	If it is the case either that the Queen is not here, or that the Russian is not here, then the Pope is here.
5	P	$\Rightarrow$-elim (lines 4 and 2)	The Pope is here.

EXERCISE 4.9. Provide a justification (rule and line numbers) for each line of these proofs.

1)

1	$U \Rightarrow V$	
2	$\neg U \Rightarrow V$	
3	$U \vee \neg U$	
4	V	

2)

1	$H \Rightarrow F$	
2	$H \Rightarrow G$	
3	$(F \,\&\, G) \Rightarrow I$	
4	$\neg I$	
5	$\neg I \Rightarrow \neg(F \,\&\, G)$	
6	$\neg(F \,\&\, G)$	
7	$\neg F \vee \neg G$	
8	$\neg F \Rightarrow \neg H$	
9	$\neg G \Rightarrow \neg H$	
10	$\neg H$	

3)

1	$(W \vee X) \Rightarrow (Y \,\&\, Z)$	
2	$\neg Y$	
3	$\neg Y \vee \neg Z$	
4	$\neg(Y \,\&\, Z) \Rightarrow \neg(W \vee X)$	
5	$(\neg Y \vee \neg Z) \Rightarrow (\neg W \,\&\, \neg X)$	
6	$\neg W \,\&\, \neg X$	
7	$\neg X$	

EXERCISES 4.10. Give a two-column proof of each of these deductions.

1) $A \Rightarrow B$, $\neg B$, $\therefore \neg A$

2) $(L \vee M) \Rightarrow (N \,\&\, O)$, M, $\therefore O$

3) Either the Pope is not here, or the Queen is here.
The Pope is here.
$\therefore$ Either the Queen is here, or else the Russian and the Pope are both here.

Remark 4.11. You should also remember that & and $\vee$ are commutative, so, for example,

$$F \Rightarrow \big((E \,\&\, D \,\&\, C \,\&\, B) \vee (A \,\&\, B)\big) \quad \equiv \quad F \Rightarrow \big((A \,\&\, B) \vee (B \,\&\, C \,\&\, D \,\&\, E)\big).$$

4C. Subproofs for ⇒-introduction

Consider this deduction:

	$P \Rightarrow R$	If the Pope is here, then the Russian is here.
$\therefore$	$(P \,\&\, Q) \Rightarrow R$	If the Pope and the Queen are both here, then the Russian is here.

The deduction is a valid one. Intuitively, we can justify it by noting that if $P \,\&\, Q$ is true, then P is certainly true, so the hypothesis implies R is true. Thus, we have verified that $(P \,\&\, Q) \Rightarrow R$. The ⇒-introduction rule will allow us to turn this intuitive justification into an official proof.

We begin the proof by writing down the hypothesis of the deduction and drawing a dark horizontal line, like this:

1	$P \Rightarrow R$	hypothesis	If the Pope is here, then the Russian is here.

The conclusion of the deduction is an assertion about what happens when $P \,\&\, Q$ is true. That is, we want to see what happens if we assume, for the sake of argument, that the assertion $P \,\&\, Q$ is true. To accomplish this, what we will do is start a **subproof**, a proof within the main proof, where we assume that $P \,\&\, Q$ is true. When we start a subproof, we start a new set of double columns, and indent them from the left margin. Then we write in an assumption for the subproof. This can be anything we want. In the case at hand, we want to assume $P \,\&\, Q$. Our proof now looks like this:

1	$P \Rightarrow R$	hypothesis	If the Pope is here, then the Russian is here.
2	$P \,\&\, Q$	assumption	Suppose the Pope and the Queen are both here.

It is important to notice that we are not claiming to have proven $P \,\&\, Q$ (that the Pope and the Queen are here). You can think of the subproof as posing the question: What could we show *if* $P \,\&\, Q$ were true? For one thing, we can derive P. So we do:

1	$P \Rightarrow R$	hypothesis	If the Pope is here, then the Russian is here.
2	$P \,\&\, Q$	assumption	Suppose the Pope and the Queen are both here.
3	P	&-elim (line 2)	The Pope is here.

And now, since the Pope is here, we can derive R, from the hypothesis that $P \Rightarrow R$:

1	$P \Rightarrow R$	hypothesis	If the Pope is here, then the Russian is here.
2	$P \,\&\, Q$	assumption	Suppose the Pope and the Queen are both here.
3	P	&-elim (line 2)	The Pope is here.
4	R	$\Rightarrow$-elim (lines 1 and 3)	The Russian is here.

This has shown that *if* we had $P \,\&\, Q$ as a hypothesis, *then* we could prove R. In effect, we have proven $(P \,\&\, Q) \Rightarrow R$: that if the Pope and the Queen are here, then the Russian is here. In recognition of this, the if-introduction rule ($\Rightarrow$-intro) will allow us to close the subproof and derive $(P \,\&\, Q) \Rightarrow R$ in the main proof. Our final proof looks like this:

1	$P \Rightarrow R$	hypothesis	If the Pope is here, then the Russian is here.
2	$P \,\&\, Q$	assumption	Suppose the Pope and the Queen are both here.
3	P	&-elim (line 2)	The Pope is here.
4	R	$\Rightarrow$-elim (lines 1 and 3)	The Russian is here.
5	$(P \,\&\, Q) \Rightarrow R$	$\Rightarrow$-intro (lines 2–4)	If the Pope and the Queen are both here, then the Russian is here.

Notice that the justification for applying the $\Rightarrow$-intro rule is the entire subproof. Usually that will be more than just three lines.

It may seem as if the ability to assume anything at all in a subproof would lead to chaos: does it allow you to prove any conclusion from any hypotheses? The answer is no, it does not. Consider this proof:

1	P	hypothesis	The Pope is here.
2	Q	assumption	Suppose that the Queen is here.
3	Q	repeat (line 2)	As mentioned previously, the Queen is here.

It may seem as if this is a proof that you can derive any conclusion Q (such as the conclusion that the Queen is here) from any hypothesis P (such as the hypothesis that the Pope is here). When the vertical line for the subproof ends, the subproof is *closed*. In order to complete a proof, you must close all of the subproofs. And you cannot close the subproof and use the repeat rule again on line 4 to derive Q in the main proof. Once you close a subproof, you cannot refer back to individual lines inside it.

You **cannot** use a line from a subproof as a hypothesis for a theorem that is being applied in the main proof. Lines in a subproof stay in the subproof.

In particular, you **cannot** use the repeat theorem to copy a line from a subproof into the main proof.

Closing a subproof is called *discharging* the assumptions of that subproof. So we can put the point this way: You cannot complete a proof until you have discharged all of the assumptions besides the original hypotheses of the deduction.

Of course, it is legitimate to do this:

1	P	hypothesis	The Pope is here.
2	Q	assumption	Suppose that the Queen is here.
3	Q	repeat (line 2)	As mentioned previously, the Queen is here.
4	$Q \Rightarrow Q$	$\Rightarrow$-intro (lines 2 and 3)	If the Queen is here, then the Queen is here.

This should not seem so strange, though. Since $Q \Rightarrow Q$ is a tautology, it follows validly from any hypotheses.

Put in a general form, the $\Rightarrow$-intro rule looks like this:

m	$\mathcal{A}$	assumption (want $\mathcal{B}$)	Suppose that Alberta is big.
	$\vdots$	$\vdots$	$\vdots$
n	$\mathcal{B}$	⟨*whatever reason*⟩	Then BC is big.
	$\mathcal{A} \Rightarrow \mathcal{B}$	$\Rightarrow$-intro (lines m–n)	If Alberta is big, then BC is big.

When we introduce a subproof, it is helpful to make a note of what we want to derive (and add it to the justification). This is so that anyone reading the proof will find it easier to understand why we are doing what we are doing (and also so that we do not forget why we started the subproof if it goes on for five or ten lines). There is no "want" rule. It is a note to ourselves and to the reader; it is not formally part of the proof.

Although it is legal to open a subproof with any assumption you please, there is some strategy involved in picking a useful assumption. Starting a subproof with an arbitrary, wacky assumption would just waste lines of the proof. In order to derive a conditional by using $\Rightarrow$-intro, for instance, you must assume the hypothesis of the if-then statement in a subproof.

Now that we have rules for "implies," we can prove that the following deduction is valid:

$P \Rightarrow Q$ If the Pope is here, then so is the Queen.
$Q \Rightarrow R$ If the Queen is here, then so is the Russian.
$\therefore$ $P \Rightarrow R$ Therefore, if the Pope is here, then so is the Russian.

We begin the proof by writing the two hypotheses as assumptions. Since the main logical operator in the conclusion is $\Rightarrow$, we can expect to use the $\Rightarrow$-introduction rule. For that, we need a subproof—so we write in the hypothesis of the implication as assumption of a subproof:

1	$P \Rightarrow Q$	hypothesis	If the Pope is here, then so is the Queen.
2	$Q \Rightarrow R$	hypothesis	If the Queen is here, then so is the Russian.
3	P	assumption (want R)	Suppose that the Pope is here.

We made P available by assuming it in a subproof, allowing us to apply $\Rightarrow$-elim to line 1. This gives us Q, which allows us to apply $\Rightarrow$-elim to line 2. Having derived R, we close the subproof. By assuming P we were able to prove R, so $\Rightarrow$-elim completes the proof. Here it is written out:

1	$P \Rightarrow Q$	hypothesis	If the Pope is here, then so is the Queen.
2	$Q \Rightarrow R$	hypothesis	If the Queen is here, then so is the Russian.
3	P	assumption (want R)	Suppose that the Pope is here.
4	Q	$\Rightarrow$-elim (lines 1 and 3)	The Queen is here.
5	R	$\Rightarrow$-elim (lines 2 and 4)	The Russian is here.
6	$P \Rightarrow R$	$\Rightarrow$-intro (lines 3–5)	If the Pope is here, then so is the Russian.

EXERCISE 4.12. Provide a justification (rule and line numbers) for each line of these proofs.

1)

1	$L \Leftrightarrow \neg O$	
2	$L \vee \neg O$	
3	L	
4	L	
5	$L \Rightarrow L$	
6	$\neg O \Rightarrow L$	
7	L	

2)

1	$F \Rightarrow \big((G \,\&\, H) \vee I\big)$	
2	$\neg I$	
3	$\neg G$	
4	$\neg G \vee \neg H$	
5	$(\neg G \vee \neg H) \,\&\, \neg I$	
6	$\neg\big((G \,\&\, H) \vee I\big)$	
7	$\neg\big((G \,\&\, H) \vee I\big) \Rightarrow \neg F$	
8	$\neg F$	
9	$\neg G \Rightarrow \neg F$	
10	$\neg\neg F \Rightarrow \neg\neg G$	
11	$F \Rightarrow G$	

3)

1	$\neg C \Rightarrow B \vee C$	
2	$C \vee \neg C$	
3	C	
4	$B \vee C$	
5	$C \Rightarrow (B \vee C)$	
6	$B \vee C$	
7	$A \,\&\, \neg B$	
8	$\neg B$	
9	C	
10	$(A \,\&\, \neg B) \Rightarrow C$	

4)

1	$Z \Rightarrow (C \,\&\, \neg N)$	
2	$\neg Z \Rightarrow (N \,\&\, \neg C)$	
3	$Z \vee \neg Z$	
4	Z	
5	$C \,\&\, \neg N$	
6	C	
7	$N \vee C$	
8	$Z \Rightarrow (N \vee C)$	
9	$\neg Z$	
10	$N \,\&\, \neg C$	
11	N	
12	$N \vee C$	
13	$\neg Z \Rightarrow (N \vee C)$	
14	$N \vee C$	

5)

1	$A \Rightarrow E$	
2	$C \Rightarrow E$	
3	$A \vee C$	
4	E	
5	$(A \vee C) \Rightarrow E$	

EXERCISE 4.13. Provide a two-column proof of the following theorem.

$$A \vee B,\ A \Rightarrow C,\ B \Rightarrow D,\ C \Rightarrow E,\ D \Rightarrow E,\ \therefore E$$

[*Hint:* Use proof by cases from the previous chapter.]

EXERCISES 4.14. Write a two-column proof of each of the following deductions:

1) $Q \Rightarrow (Q \Rightarrow P), \quad \therefore Q \Rightarrow P$

2) $R \Rightarrow \Big(R \Rightarrow \big(R \Rightarrow (R \Rightarrow Q)\big)\Big), \quad \therefore R \Rightarrow (Q \vee P)$

3)

Hypotheses:

The Pope is here if and only if the Queen is here.

The Queen is here if and only if the Russian is here.

Conclusion: The Pope is here if and only if the Russian is here.

4D. Proof by contradiction

> *How often have I said to you that when you have eliminated the impossible, whatever remains,* however improbable, *must be the truth?*
>
> Sherlock Holmes, fictional British detective in *The Sign of the Four*

The usual way to prove that an assertion is false is to show that it cannot be true. We do this by considering what would happen if it were indeed true. That is, we assume, for the sake of argument, that the assertion is true. If, by using logic, we can show that this assumption leads to a contradiction, then we can conclude that the hypothesis was wrong: the assertion we are interested in must be false. This is known as **proof by contradiction**.

EXAMPLE 4.15. Here is an argument in English that shows there is no greatest (i.e., largest) natural number:

> Suppose there is some greatest natural number. Call it n.
>
> That number plus one is also a natural number.
>
> Obviously, $n + 1 > n$.
>
> So there is a natural number greater than n.
>
> This is impossible, since n is assumed to be the greatest natural number.

Conclusion: Our hypothesis cannot be true: there is no greatest natural number.

The ¬-introduction rule allows for deductions like this. If we assume that a particular assertion is true and show that this leads to a contradiction, then we have proven that our assumption is wrong; the assertion must be false, so its negation must be true:

> $\mathcal{A}$: Alberta is big.
>
> $\mathcal{B}$: BC is big.

m	$\mathcal{A}$	assumption (for contradiction)	Suppose that Alberta is big.
	⋮	⋮	⋮
n	$\mathcal{B} \,\&\, \neg\mathcal{B}$	⟨*whatever reason*⟩	Then BC is big and BC is not big.
	$\neg\mathcal{A}$	¬-intro (lines m–n)	Alberta must not be big.

For this rule to apply, the last line of the subproof must be an explicit contradiction of the form $\mathcal{B} \,\&\, \neg\mathcal{B}$: some assertion and its negation. We write "(will lead to a contradiction)" or "(for contradiction)" as a note to ourselves and the reader. It is an explanation of why we started the subproof, and is not formally part of the proof.

EXERCISES 4.16. Provide a justification (rule and line numbers) for each line of these proofs.

1)

1	$P \Rightarrow Q$	
2	$Q \Rightarrow R$	
3	$R \Rightarrow \neg P$	
4	P	
5	Q	
6	R	
7	$\neg P$	
8	$P \,\&\, \neg P$	
9	$\neg P$	

2)

1	$(A \vee B) \Rightarrow \neg B$	
4	B	
5	$A \vee B$	
6	$\neg B$	
7	$B \,\&\, \neg B$	
9	$\neg B$	

3)

1	$Z \Rightarrow (C \,\&\, \neg N)$	
2	$\neg Z \Rightarrow (N \,\&\, \neg C)$	
3	$\neg(N \vee C)$	
4	N	
5	$N \vee C$	
6	$(N \vee C) \,\&\, \neg(N \vee C)$	
7	$\neg N$	
8	C	
9	$N \vee C$	
10	$(N \vee C) \,\&\, \neg(N \vee C)$	
11	$\neg C$	
12	Z	
13	$C \,\&\, \neg N$	
14	C	
15	$C \,\&\, \neg C$	
16	$\neg Z$	
17	$N \,\&\, \neg C$	
18	N	
19	$N \,\&\, \neg N$	
20	$\neg\neg(N \vee C)$	
21	$N \vee C$	

4)

1	$\neg C \Rightarrow B \vee C$	
2	$A \,\&\, \neg B$	
3	$\neg C$	
4	$B \vee C$	
5	B	
6	$\neg B$	
7	$B \,\&\, \neg B$	
8	$\neg\neg C$	
9	C	
10	$(A \,\&\, \neg B) \Rightarrow C$	

5)

1	$(P \vee \neg Q) \Rightarrow \neg R$	
2	$Q \Rightarrow P$	
3	R	
4	Q	
5	P	
6	$P \vee \neg Q$	
7	$\neg R$	
8	$R \,\&\, \neg R$	
9	$\neg Q$	
10	$P \vee \neg Q$	
11	$\neg R$	
12	$R \,\&\, \neg R$	
13	$\neg R$	

EXERCISES 4.17. Give a two-column proof of each of these deductions.

1) $Q \Rightarrow (Q \,\&\, \neg Q)$, $\therefore\ \neg Q$

2) $J \Rightarrow \neg J$, $\therefore\ \neg J$

3) $M \vee (N \Rightarrow M)$, $\therefore\ \neg M \Rightarrow \neg N$

4) *Hypotheses:*

If Sammy is not tired, then she does not need a nap.

Sammy needs a nap.

Conclusion: Sammy is tired.

5) *Hypotheses:*

If Jim is sick, he should stay in bed.

If Jim is not sick, he should go outside to play.

Conclusion: Jim should either stay in bed or go outside to play.

6) *Hypotheses:*

If King will sing, then the Queen will sing.

If the King and the Queen will both sing, then the Prince and the Princess will also sing.

If the King and the Queen and the Prince and the Princess will all sing, then the party will be fun.

Conclusion: If the King will sing, then the party will be fun.

7) *Hypotheses:*

If Alice is here, then Bob is here.

If Bob is here, then Carol is here.

If Carol is here, then Bob is not here.

Conclusion: Alice is not here.

8) *Hypotheses:*

1. If the Pope is here, then either the Queen is here or the Russian is here.
2. If the Queen is here, then the Spaniard is here.
3. If the Russian is here, then the Spaniard is here.

Conclusion: If the Pope is here, then the Spaniard is here.

4E. Proof strategies

There is no simple recipe for doing proofs, and there is no substitute for practice. Here, though, are some rules of thumb and strategies to keep in mind.

- *Work backwards from what you want.* The ultimate goal is to derive the conclusion. Look at the conclusion and ask what the introduction rule is for its main logical operator. This gives you an idea of where you want to be *just before* the last line of the proof. Then you can treat this line as if it were your goal. Ask what you could do to derive this new goal.

  For example: If your conclusion is a conditional $\mathcal{A} \Rightarrow \mathcal{B}$, plan to use the $\Rightarrow$-intro rule. This requires starting a subproof (a separate paragraph) in which you assume $\mathcal{A}$. In the subproof, you want to derive $\mathcal{B}$.

- *Work forwards from what you have.* Look at the hypotheses (and any other assertions that you have derived so far). Think about the elimination rules for the main operators in these assertions. These will tell you what your options are. For example:

- If you have $\mathcal{A} \vee \mathcal{B}$, you should think about using a proof by cases.
- If you have $\mathcal{A} \Rightarrow \mathcal{B}$, you should think about whether you can obtain $\mathcal{A}$ somehow, so that you can apply $\Rightarrow$-elimination.

- *Change what you are looking at.* Replacement rules can often make your life easier; if a proof seems impossible, try out some different substitutions. For example, it is often difficult to prove a disjunction $\mathcal{A} \vee \mathcal{B}$ by using the basic rules; it is often easier to show $\neg\mathcal{A} \Rightarrow \mathcal{B}$, which is a logically equivalent assertion.

  And De Morgan's Laws should become second nature; they can often transform an assertion into a more useful form.
- *Try breaking the proof down into cases.* If it looks like you need an additional hypothesis (P) to prove what you want, try considering two cases: since $P \vee \neg P$ is a tautology ("law of the excluded middle"), it suffices to prove that P and $\neg P$ each yield the desired conclusion.
- *Do not forget proof by contradiction.* If you cannot find a way to show something directly, try assuming its negation, and then look for a contradiction.
- *Repeat as necessary.* After you have made some progress, by either deriving some new assertions or deciding on a new goal that would represent substantial progress, see what the above strategies suggest in your new situation.
- *Persist.* Try different things. If one approach fails, try something else.

EXERCISES 4.18. Give a two-column proof of each of these deductions.

1) $P \Rightarrow Q$, $Q \Rightarrow \neg P$, $\therefore \neg P$
2) $(P \vee Q) \Rightarrow (R \,\&\, S)$, $(R \vee S) \Rightarrow (P \,\&\, Q)$, $\therefore P \Rightarrow Q$
3) $P \Rightarrow Q$, $\neg P \Rightarrow R$, $(Q \vee R) \Rightarrow S$, $\therefore S$
4) $(P \,\&\, \neg Q) \Rightarrow (Q \vee R)$, $\therefore (P \,\&\, \neg Q) \Rightarrow (R \vee S)$
5) $P \Rightarrow (Q \vee R)$, $Q \Rightarrow \neg P$, $R \Rightarrow S$, $\therefore P \Rightarrow S$
6) $(R \vee S) \Rightarrow (P \vee Q)$, $\neg Q$, $\therefore R \Rightarrow P$

4F. What is a proof?

I don't know — a proof is a proof. What kind of a proof? It's a proof. A proof is a proof, and when you have a good proof, it's because it's proven.

Jean Chrétien (b. 1934), Prime Minister of Canada

The goal of a mathematical proof is to provide a completely convincing explanation that a deduction is valid. It needs to be so carefully written that it would hold up in court forever, even against your worst enemy, in any country of the world, and without any further explanation required. Fortunately, the rules of logic are accepted worldwide, so, if applied properly, they create an irrefutable case.

In the previous sections of this chapter, we wrote our proofs in two-column format. We will now start the transition to writing our proofs in English prose; our ideas will be expressed in sentences and paragraphs, using correct grammar, combining words with appropriate mathematical notation. A proof written in prose needs to convey the same information as would be found in a two-column proof, so essentially the same rules and strategies will still apply, but writing in ordinary English provides more freedom, and often leads to shorter proofs that are more reader-friendly.

Remark 4.19. The big advantage of a two-column proof is that the rules are very clear, so it is a good method for beginners who may have difficulty deciding what they are allowed to do. The disadvantage is that

> *"... its confining and verbose format render it of very limited utility to any but the most simple of theorems."*
>
> Eric W. Weisstein (b. 1969), encyclopedist
> *MathWorld–A Wolfram Web Resource*
> http://mathworld.wolfram.com/Two-ColumnProof.html

Just as when using the two-column format, our proofs will be a sequence of assertions that lead from the hypotheses to the desired conclusion. Each assertion must have a logical justification based on assertions that were stated earlier in the proof. Any subproof will form a paragraph of its own within the proof.

Before the proof begins, we always provide a statement of the theorem that will be proved.

- The statement is preceded by the label "Theorem" (or a suitable substitute).
- The statement of the result begins with a list all of the hypotheses. To make it clear that they are assumptions, not conclusions, this list of assertions is introduced by an appropriate word or phrase such as "Assume...," or "Suppose that ...," or "If ...," or "Let ...."
- The statement of the result ends with a statement of the desired conclusion, introduced by an appropriate word or phrase such as "Then ...," or "Therefore, ..."

Following the statement of the result, we begin our proof in a new paragraph.

- The proof is labelled with the single word: "Proof."
- We then proceed to give a series of assertions that logically leads from our hypotheses to the desired conclusion.
- A small square is drawn at the right margin at the end of the proof to signify that the proof is complete.

For example, here is how the chapter's first deduction could be treated:

THEOREM. *Assume:*

a) if the Pope is here, then the Queen and the Russian are both here, and

b) the Pope is here.

Then the Russian is here.

PROOF. From Assumption (b), we know that the Pope is here. Therefore, Assumption (a) tells us that the Queen and the Russian are both here. In particular, the Russian is here. □

Remark 4.20. Note that some of the rules of the two-column format are relaxed for proofs written in prose:

1) We will no longer list all of the hypotheses at the start of our proof. Instead, we refer to the list that is in the statement of the theorem.
2) We will no longer make a practice of numbering all of the assertions in our proofs. However, if there is a particular assertion that will be used repeatedly, we may label it with a number for easy reference.
3) We will usually not cite the basic rules of Propositional Logic by name every time they are used. However, we should be able to justify any assertion with a rule, if called upon to do so.

EXERCISE 4.21. Write a proof of each of these theorems in English prose.

1) *Hypotheses:*
   1. If the Pope is here, then the Queen is here.
   2. If the Queen is here, then the Russian is here.

   Conclusion: If the Pope is here, then the Russian is here.

2) **THEOREM.** *Assume:*

   (a) If Jack and Jill went up the hill, then something will go wrong.

   (b) If Jack went up the hill, then Jill went up the hill.

   (c) Nothing will go wrong.

   Then Jack did not go up the hill.

SUMMARY:

- A "two-column proof" is a tool that we use to learn techniques for writing proofs.
  - The left-hand column contains a sequence of assertions.
  - The right-hand column contains a justification for each assertion.
  - Each row of the proof is numbered (in the left margin) for easy reference.
  - A dark horizontal line is drawn to indicate the end of the hypotheses.
- In addition to the basic theorems of Propositional Logic, we have two rules that use subproofs:
  - $\Rightarrow$-introduction
  - proof by contradiction
- The repeat rule cannot be used to copy a line from a subproof into the main proof.
- Writing proofs takes practice, but there are some strategies that can help.
- Proofs can also be written in English prose, using sentences and paragraphs.

Part II

Sets and First-Order Logic

Chapter 5

Sets, Subsets, and Predicates

A collection or set is a Many that we think of as a One.

"Unter einer Mannigfaltigkeit oder Menge verstehe ich nämlich allgemein jedes Viele, welches sich als Eines denken läßt..."

Georg Cantor (1845–1918), German mathematician
Über unendliche lineare Punktmannigfaltigkeiten, V

5A. Propositional Logic is not enough

Consider the following deduction:

Merlin is a wizard. All wizards wear funny hats.
Therefore, Merlin wears a funny hat.

To symbolize it in Propositional Logic, we define a symbolization key:

W: Merlin is a wizard.

A: All wizards are wearing funny hats.

H: Merlin is wearing a funny hat.

Now we symbolize the deduction:

Hypotheses:

W

A

Conclusion: H

This is *not* valid in Propositional Logic. (If W and A are true, but H is false, then it is obvious that both hypotheses are true, but the conclusion is false.) There is something very wrong here, because this is clearly a valid deduction in English.

The problem is that symbolizing this deduction in Propositional Logic leaves out some of the important structure: The assertion "All wizards are wearing funny hats" is about both wizards and hat-wearing, but Propositional Logic is not able to capture this information. It loses the connection between Merlin's being a wizard and Merlin's wearing a hat. However, the problem is not that we have made a mistake while symbolizing the deduction; it is the best symbolization we can give for this deduction *in Propositional Logic*.

In order to symbolize this deduction properly, we need to use a more powerful logical language. This language is called **First-Order Logic**, and its assertions are built from "predicates" and "quantifiers."

A predicate is an expression like "is wearing a funny hat." This is not an assertion on its own. It is neither true nor false. In order to be true or false, we need to specify something: Who or what is it that is wearing a funny hat?

The details of this will be explained in section 5D, but here is the basic idea: In First-Order Logic, we will represent predicates with capital letters. For instance, we could let H stand for "_____ is wearing a funny hat." However, we will use variables instead of blanks; so "x is wearing a funny hat" is a predicate, and we could represent it as $H(x)$.

The words "all" and "some" are *quantifiers*, and we will have symbols that represent them. For instance, "$\exists$" will mean "There exists some_____, such that." Thus, to say that someone is wearing a funny hat, we can write $\exists x, H(x)$; that is: There exists some x, such that x is wearing a funny hat. Quantifiers will be dealt with in Chapter 7, when First-Order Logic is fully explained.

With predicates and quantifiers, we will be talking about many people (or other things) all at once, instead of one at a time. For example, we may wish to talk about "the people who are wearing hats," or "the mammals that lay eggs." These are examples of *sets*.

5B. Sets and their elements

In mathematics, a **set** is a collection of objects. The objects in the collection are called "**elements**" (or "**members**") of the set. If someone has a particular set in mind, they may wish to tell other people which set it is. One good way to do this is to list its elements. The list needs to be surrounded with curly braces to indicate that it represents a set, rather than some other type of object.

EXAMPLE 5.1.

1) $\{1, 2, 3, 4, 5\}$ is the set of natural numbers from 1 to 5.
2) $\{1, 2, 3, \ldots, 100\}$ is the set of natural numbers from 1 to 100.
3) {British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, New Brunswick, Nova Scotia, Prince Edward Island, Newfoundland} is the set of provinces in Canada.
4) $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ is the set of suits in a standard deck of cards.

Remark 5.2. In everyday life, when you have a bunch of things that you want to keep together, you might look for a box to put them in. (The box itself probably has no value — you are interested only in the stuff that is in the box.) In mathematics, you should put the things into a set, not a box. If you think of a set as being a box of stuff, then the elements of the set are the things you see when you open the box.

EXAMPLE 5.3.

1) If $A = \{1, 2, 3\}$, then the elements of A are the numbers 1, 2, and 3.
2) If $B = \big\{1, \{2, 3\}\big\}$, then the elements of B are the number 1 and the set $\{2, 3\}$. It is important to note that the numbers 2 and 3 are *not* elements of B.
   (a) To understand this, it may help to consider the analogy with boxes: if we open the box B, we will see the number 1 and a box, but we will not see the number 2 or the number 3. We would need to open up the box that is inside of B in order to see those extra numbers. So 2 and 3 are not elements of the set B — they are elements of a set that is an element of B.
   (b) As another illustration of this same phenomenon, suppose we make a list of the teams in a chess tournament. The list might be:
      (i) U of Lethbridge,

(ii) U of Alberta,

(iii) U of Calgary.

And maybe the members of the Lethbridge team are Alice, Bob, and Cindy. Then Alice is *not* on the list of teams; she is a *member* of one of the teams on the list.

NOTATION 5.4. We use

- "$\in$" as an abbreviation for "is an element of," and
- "$\notin$" as an abbreviation for "is *not* an element of."

For example, if $A = \{1, 2, 3, 4, 5\}$, then we have $3 \in A$ and $7 \notin A$, because 3 is an element of A, but 7 is not an element of A.

DEFINITION 5.5. The set with no elements can be denoted { }. (It is like an empty box.) It is called the *empty set*, and it comes up so often that is named by a special symbol: $\emptyset$ denotes the empty set.

Remark 5.6. Because the empty set has no elements,

for all x, we have $x \notin \emptyset$.

EXERCISE 5.7. Fill in the blank with $\in$ or $\notin$.

1) t_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$
2) i_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$
3) m_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$
4) $\{\mathsf{t}\}$_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$
5) $\{\mathsf{i}\}$_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$
6) $\{\mathsf{m}\}$_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$
7) $\{\mathsf{t}, \mathsf{i}\}$_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$
8) $\{\mathsf{m}, \mathsf{e}\}$_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$
9) t_____$\{\mathsf{t}, \{\mathsf{i}\}, \{\mathsf{m}, \mathsf{e}\}\}$
10) i_____$\{\mathsf{t}, \{\mathsf{i}\}, \{\mathsf{m}, \mathsf{e}\}\}$
11) m_____$\{\mathsf{t}, \{\mathsf{i}\}, \{\mathsf{m}, \mathsf{e}\}\}$
12) $\{\mathsf{t}\}$_____$\{\mathsf{t}, \{\mathsf{i}\}, \{\mathsf{m}, \mathsf{e}\}\}$
13) $\{\mathsf{i}\}$_____$\{\mathsf{t}, \{\mathsf{i}\}, \{\mathsf{m}, \mathsf{e}\}\}$
14) $\{\mathsf{m}\}$_____$\{\mathsf{t}, \{\mathsf{i}\}, \{\mathsf{m}, \mathsf{e}\}\}$
15) $\{\mathsf{t}, \mathsf{i}\}$_____$\{\mathsf{t}, \{\mathsf{i}\}, \{\mathsf{m}, \mathsf{e}\}\}$
16) $\{\mathsf{m}, \mathsf{e}\}$_____$\{\mathsf{t}, \{\mathsf{i}\}, \{\mathsf{m}, \mathsf{e}\}\}$
17) $\emptyset$_____$\emptyset$
18) $\emptyset$_____$\{\emptyset\}$
19) $\{\emptyset\}$_____$\emptyset$
20) $\{\emptyset\}$_____$\{\emptyset\}$

We said that a set is a collection of objects, but this needs a bit of elaboration:

1) *A set is **determined by its elements**.* This means that there cannot be two different sets that have exactly the same elements. (Or, in other words, if two sets have the same elements, then the two sets are equal.) For example, suppose:
   (a) H is the set of students who had a perfect score on last week's history quiz,
   (b) M is the set of students who had a perfect score on last week's math quiz.
   (c) Alice and Bob are the only two students who had a perfect score on last week's history quiz, and
   (d) Alice and Bob are also the only two students who had a perfect score on last week's math quiz.

   Then H and M have exactly the same elements, so H and M are just different names for the same set: namely, both represent $\{\mathsf{Alice}, \mathsf{Bob}\}$. So the sets are equal: we have $H = M$.

   Suppose A and B are two sets.
   We have $A = B$ if and only if
   for every x, $\big((x \in A) \Leftrightarrow (x \in B)\big)$.

2) *A set is an **unordered** collection.* This means that listing the elements of a set in a different order does not give a different set. For example, $\{1, 2, 3\}$ and $\{1, 3, 2\}$ are the same set. We write $\{1, 2, 3\} = \{1, 3, 2\}$. Both of them are the set whose elements are 1, 2, and 3.
3) *A set is a collection **without repetition**.* This means that repeating something in the list of elements does not change the set. For example, $\{1, 2, 2, 3, 3\}$ is the same set as $\{1, 2, 3\}$. We write $\{1, 2, 2, 3, 3\} = \{1, 2, 3\}$.

EXERCISES 5.8. Fill in the blank with $=$ or $\neq$.
1) $\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{e}\}$_____$\{\mathsf{t}, \mathsf{m}, \mathsf{i}, \mathsf{e}\}$
2) $\{\mathsf{t}, \mathsf{i}, \mathsf{m}\}$_____$\{\mathsf{t}, \mathsf{m}, \mathsf{i}, \mathsf{e}\}$
3) $\{\mathsf{t}, \mathsf{i}, \mathsf{m}\}$_____$\{\mathsf{t}, \mathsf{m}, \mathsf{i}, \mathsf{m}\}$
4) $\{\mathsf{t}, \mathsf{i}, \mathsf{m}\}$_____$\{\mathsf{t}, \mathsf{m}, \mathsf{i}\}$
5) $\{\mathsf{t}, \mathsf{i}, \mathsf{m}\}$_____$\{\mathsf{t}, \mathsf{i}, \mathsf{m}, \mathsf{i}\}$
6) $\{\mathsf{t}, \mathsf{i}, \mathsf{m}\}$_____$\{\mathsf{t}, \mathsf{t}, \mathsf{t}, \mathsf{i}, \mathsf{i}, \mathsf{m}\}$
7) $\{\mathsf{t}, \mathsf{t}\}$_____$\{\mathsf{t}\}$
8) $\{\mathsf{t}, \mathsf{t}\}$_____$\{\mathsf{i}, \mathsf{i}\}$
9) $\{\mathsf{t}, \mathsf{t}\}$_____$\{\mathsf{t}, \mathsf{i}\}$

EXERCISES 5.9. Provide a 2-column proof of each deduction.
1) $(a \in A) \Rightarrow (a \notin B)$, $(b \in B) \Rightarrow (a \in B)$, $\therefore\ (b \in B) \Rightarrow (a \notin A)$
2) $(p \in X)\ \&\ (q \in X)$, $(p \in X) \Rightarrow \big((q \notin X) \vee (Y = \emptyset)\big)$, $\therefore Y = \emptyset$.

EXERCISES 5.10. Write your proofs in English.
1) Assume:
   (a) If $p \in H$, then either $q \in H$ or $r \in H$.
   (b) $q \notin H$.

   Show that if $r \notin H$, then $p \notin H$.

2) Assume:

(a) If $X \neq \emptyset$, then $a \in Y$.

(b) If $X = \emptyset$, then $b \in Y$.

(c) If either $a \in Y$ or $b \in Y$, then $Y \neq \emptyset$.

Show $Y \neq \emptyset$.

Remark 5.11. Sets are the most fundamental objects in mathematics. Indeed, modern mathematicians consider every object everywhere to be a set, but we will not be quite this extreme. In particular, in addition to sets, we will consider two additional types of objects: numbers and ordered pairs.

- It is assumed that you already have a lot of experience with numbers, and know how to deal with them.
- For any objects x and y, we write (x, y) to denote the **ordered pair** whose first coordinate is x and whose second coordinate is y. It is important to know that the order matters: (x, y) is usually not the same as (y, x). That is why these are called *ordered* pairs. (Notice that sets are not like this: sets are unordered, so $\{x, y\}$ *is* always the same as $\{y, x\}$.)

Functions are another very important class of mathematical objects, but, as will be seen in Chapter 9, we can think of them as being a particular type of set.

NOTATION 5.12. A few particularly important sets of numbers have been given names that every mathematician needs to know:

- $\mathbb{N} = \{0, 1, 2, ...\}$ is the set of *natural numbers*.
  (*Warning:* Some textbooks do not consider 0 to be a natural number.)
- $\mathbb{N}^+ = \{1, 2, ...\}$ is the set of *positive natural numbers*.
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the set of *integers*. A number is an integer if and only if it is either a natural number or the negative of a natural number.
- $\mathbb{Q} = \left\{ \dfrac{p}{q} \;\middle|\; \begin{array}{c} p, q \in \mathbb{Z} \\ q \neq 0 \end{array} \right\}$ is the set of *rational numbers*. (This notation means that a number x is an element of $\mathbb{Q}$ if and only if there exist integers p and q, with $q \neq 0$, such that $x = p/q$ (cf. §5E).) For example, $1/2$, $7/5$, and $-32/9$ are elements of $\mathbb{Q}$.
- $\mathbb{R}$ is the set of all *real numbers*. (That is, the set of all numbers that are either positive or negative or 0. Unless you have learned about "complex numbers" or "imaginary numbers," it is probably the case that all the numbers you know are real numbers.) For example, $\sqrt[3]{n}$ is a real number whenever $n \in \mathbb{Z}$; and $\sqrt{n}$ is a real number whenever $n \in \mathbb{N}$. ("You can't take the square root of a negative number.")

NOTATION 5.13. We use $\#A$ to denote the number of elements in the set A. Thus, for example,

$$\#\{\mathsf{a}, \mathsf{e}, \mathsf{i}, \mathsf{o}, \mathsf{u}\} = 5.$$

Mathematicians call $\#A$ the **cardinality** of A. This seemingly simple notion actually has some complicated implications, and will be discussed in more detail in Chapter 15.

Remark 5.14. You probably already know that some sets are finite and some (such as $\mathbb{N}$) are infinite. We will discuss this in more detail in Chapter 15. For now, we remind you that a set A is **finite** iff the elements of A can be counted (and the answer is some number n); that is, if $\#A = n$, for some $n \in \mathbb{N}$.

EXERCISES 5.15. How many elements are there in each set?

1) $\#\{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}\} =$
2) $\#\{\mathsf{a}, \mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{c}, \mathsf{d}\} =$
3) $\#\big\{\mathsf{a}, \{\mathsf{b}, \mathsf{c}\}\big\} =$
4) $\#\big\{\mathsf{a}, \mathsf{a}, \{\mathsf{b}, \mathsf{c}\}, \{\mathsf{b}, \mathsf{c}, \mathsf{d}\}\big\} =$
5) $\#\emptyset =$

Remark 5.16. It is traditional to use:

- capital letters (such as A, B, C, X, Y, Z) to represent sets, and
- lower-case letters (such as a, b, c, x, y, z) to represent numbers and other objects that are individual elements (or "atoms"), rather than sets.

Furthermore, it is a good idea to maintain a correspondence between the upper-case letters and lower-case letters: when feasible, use a to represent an element of A and b to represent an element of B, for example.

5C. Subsets

Geometry students are taught that every square is a rectangle. Translating this into the terms of set theory, we can say that if

- S is the set of all squares, and
- R is the set of all rectangles,

then every element of the set S is also an element of R. For short, we say that S is a *subset* of R, and we may write $S \subset R$.

DEFINITION 5.17. Suppose A and B are two sets. We say that B is a **subset** of A iff every element of B is an element of A.

When B is a subset of A:

- In symbols, we write $B \subset A$.
- We may say that B is **contained in** A or that A **contains** B.
- We may also write $A \supset B$ (and call A a **superset** of B).

EXAMPLE 5.18.

1) $\{1, 2, 3\}$ is a subset of $\{1, 2, 3, 4\}$, because the elements of $\{1, 2, 3\}$ are 1, 2, and 3, and every one of those numbers is an element of $\{1, 2, 3, 4\}$.
2) $\{1, 3, 5\}$ is *not* a subset of $\{1, 2, 3, 4\}$, because there is an element of $\{1, 3, 5\}$ (namely, 5) that is not an element of $\{1, 2, 3, 4\}$.
3) We have $\mathbb{N}^+ \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Remark 5.19.

1) We write $B \not\subset A$ to denote that B is *not* a subset of A.
2) We have $B \not\subset A$ iff there is at least one element of B that is *not* an element of A.

Remark 5.20.

1) In the language of every-day life, suppose someone gives you a box A that has some stuff in it. You are allowed to take some of the things from the box and put them into a new box B. But you are not allowed to put anything into B if it was not in box A. Then B will be a subset of A.

2) If you decide to take all of the things that were in box A, then box B will end up being exactly the same as A; that is $B = A$. This illustrates the fact that every set is a subset of itself.

For every set A, we have $A \subset A$.

3) If you decide not to take anything at all from box A, then box B will be empty. This illustrates the important fact that the empty set is a subset of every set.

For every set A, we have $\emptyset \subset A$.

DEFINITION 5.21. Suppose A and B are sets. We say B is a **proper subset** of A iff $B \subset A$ *and* $B \neq A$.

Remark 5.22. Many mathematicians use a slightly different notation: they define $A \subset B$ to mean that A is a *proper* subset of B. Then, to say that A is a subset of B, they write $A \subseteq B$.

EXERCISE 5.23. Fill each blank with $\subset$ or $\not\subset$, as appropriate.

1) $\{\mathsf{s}\}$_____$\{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$
2) $\{\mathsf{o}, \mathsf{r}\}$_____$\{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$
3) $\{\mathsf{n}, \mathsf{o}, \mathsf{r}\}$_____$\{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$
4) $\{\mathsf{p}, \mathsf{r}, \mathsf{o}, \mathsf{n}, \mathsf{g}\}$_____$\{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$
5) $\{\mathsf{s}, \mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}\}$_____$\{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$
6) $\emptyset$_____$\{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$
7) $\{\emptyset\}$_____$\{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$
8) $\{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$_____$\emptyset$

It is intuitively clear that a subset of a set cannot have more elements than the original set. That is:

If $B \subset A$, then $\#B \leq \#A$.

We will prove this fact in Chapter 15.

In Chapter 8, we will prove that two sets are equal if and only if they are subsets of each other. This is a basic principle that will be very important in later chapters when we are doing proofs with sets:

To show two sets A and B are equal, prove $A \subset B$ and $B \subset A$.

5D. Predicates

The simplest predicates are things you can say about a single object; they are properties of individuals. For example, "x is a dog" and "x is a *Harry Potter* fan" are both predicates. In First-Order Logic, we symbolize predicates with capital letters A through Z (with or without subscripts). Thus, our symbolization key might include:

$D(x)$: x is a dog.

$H(x)$: x is a *Harry Potter* fan.

Predicates like these are called **one-place** or **unary**, because there is only one variable. Assigning a value to this variable yields an assertion. For example, letting x = "Lassie" in the first predicate yields the assertion "Lassie is a dog." Note that in translating English assertions, the

variable will not always come at the beginning of the assertion: "a piano fell on x" is also a predicate.

Other predicates are about the *relation* between two things. For instance, in algebra, we have the relations "x is equal to y," symbolized as $x = y$, and "x is greater than y," symbolized as $x > y$. These are **two-place** or **binary** predicates, because values need to be assigned to two variables in order to make an assertion. Our symbolization key might include:

$x\ F\ y$: x is a friend of y.

$x\ L\ y$: x is to the left of y.

$x\ M\ y$: x owes money to y.

In general, we can have predicates with as many variables as we need. Predicates with n variables, for some number n, are called n-**place** or n-**ary**. However, in practice, predicates almost always have only one or two variables.

Whenever we have predicates with two (or more) variables, it is important to be careful about the order in which the variables occur. Saying that x is to the left of y is certainly not the same as saying that y is to the left of x! Some special choices of predicates are "symmetric," which means that if the predicate is true with variables in one order, then it is true for the same variables in a different order, but this should *never* be assumed. The order of the variables should always represent exactly what we know. We will give an example of this shortly.

By convention, **constants** (that is, the names of specific objects) are listed at the end of the key. For example, we might write a key that looks like this:

$A(x)$: x is angry.

$H(x)$: x is happy.

$x\ T\ y$: x is at least as tall as y.

$x\ F\ y$: x is at least as friendly as y.

$x\ M\ y$: x is married to y.

d: Donald

g: Gregor

m: Marybeth

We can symbolize assertions that use any combination of these predicates and terms. For example:

1. Donald is angry.
2. If Donald is angry, then so are Gregor and Marybeth.
3. Marybeth is at least as tall and as friendly as Gregor.
4. Donald is shorter than Gregor.
5. Donald is married to Marybeth.
6. Gregor is at least as tall as both Donald and Marybeth.

Assertion 1 is straightforward: $A(d)$.

Assertion 2 can be paraphrased as, "If $A(d)$, then $A(g)$ and $A(m)$." First-Order Logic has all the logical connectives of Propositional Logic, so we translate this as $A(d) \Rightarrow \big(A(g) \& A(m)\big)$.

Assertion 3 can be translated as $(m\ T\ g)\ \&\ (m\ F\ g)$.

Assertion 4 might seem as if it requires a new predicate. If we only needed to symbolize this assertion, we could define a predicate like $x\ S\ y$ to mean "x is shorter than y." However, this would ignore the logical connection between "shorter" and "taller." Considered only as symbols of First-Order Logic, there is no connection between S and T. They might mean anything at

all. Instead of introducing a new predicate, we paraphrase Assertion 4 using predicates already in our key: "It is not the case that Donald is at least as tall as Gregor." We can translate it as $\neg(d\ T\ g)$.

Notice that, as mentioned previously, the order of the variables (or here, the constants) is important: saying $\neg(d\ T\ g)$ (that Donald is shorter than Gregor) is very different from saying $\neg(g\ T\ d)$) (that Gregor is shorter than Donald)!

Assertion 5 can be translated as $d\ M\ m$. Even though in English, if Donald is married to Marybeth, then it is also true that Marybeth is married to Donald, we should *not* translate this as $m\ M\ d$. Getting sloppy with the order of variables (or constants) can lead you to making mistakes in cases where the order really is important.

Assertion 6 says two things: that Gregor is at least as tall as Donald, and that Gregor is at least as tall as Marybeth. Thus, we can translate it as $(g\ T\ d)\ \&\ (g\ T\ m)$.

EXERCISES 5.24. Using the symbolization key given below, give an English version of each assertion.

$x\ O\ y$: x is older than y.

$x\ F\ y$: x is a friend of y.

S: the set of all students.

r: Roger

s: Sam

t: Tess

1) $r\ O\ s$

2) $t\ O\ s$

3) $(r\ F\ t) \Rightarrow (t \in S)$

4) $\big((s \in S)\ \&\ (r \in S)\big) \Rightarrow (s\ F\ r)$

5) $(t \in S) \vee (r\ O\ t)$

6) $(r\ F\ s) \Leftrightarrow (t \notin S)$

EXERCISES 5.25. Using the same symbolization key, write these English assertions using predicates and logical connectives.

1) Tess is older than Roger.

2) Roger is a friend of Sam.

3) If Tess is a student then Tess is a friend of Sam.

4) Either Sam is a student, or Roger is not a student.

5) Roger is a friend of Sam unless Sam is a student.

6) Sam is older than Roger if and only if Roger is a student.

7) If Sam and Roger both are students, then Sam is not a friend of Roger.

EXERCISES 5.26. Using the same symbolization key, write a two-column proof to justify each of the following deductions.

1) $(r \in S) \Rightarrow \big((r\ O\ s) \vee (r \notin S)\big), \quad \therefore\ \big((t \in S)\ \&\ \neg(r\ O\ s)\big) \Rightarrow (r \notin S)$

2) If either Roger is a student, or Tess is *not* a student, then Sam is older than Tess.
If Tess is a student, then Roger is also a student.
$\therefore$ Sam is older than Tess.

5E. Using predicates to specify subsets

Subsets arise in everyday life whenever you want only *part* of something. For example, suppose you are in a kitchen with a lot of plates. If you are washing dishes, then you do not want to be given *all* of the plates, but only the ones that are dirty. In mathematical terms, you do not want the set of all plates, but only want a subset, those that are dirty. That is, if P represents the set of all plates, and D represents the set of all dirty plates, then $D \subset P$.

This type of situation is handled by the following useful notation:

> Suppose A is a set and $P(x)$ is a predicate.
> Then $\{\, a \in A \mid P(a) \,\}$ denotes
> the set of all elements a of A, such that $P(a)$ is true.
> It is a subset of A.

In the example above, you are interested in the subset

$$\{\, p \in P \mid p \text{ is dirty} \,\},$$

because this is the set of plates that are dirty. The notation tells us to look through all of the plates in P, and check each one to see whether it is dirty. If it is, we put it in the subset. If it is not dirty, then we do not put it in the subset.

EXAMPLE 5.27.

1) Suppose $B = \{1, 2, 3, \ldots, 10\}$. Then:
   (a) $\{\, b \in B \mid b \text{ is odd} \,\} = \{1, 3, 5, 7, 9\}$.
   (b) $\{\, b \in B \mid b \text{ is even} \,\} = \{2, 4, 6, 8, 10\}$.
   (c) $\{\, b \in B \mid b \text{ is prime} \,\} = \{2, 3, 5, 7\}$.
   (d) $\{\, b \in B \mid b^2 - 1 \text{ is divisible by } 3 \,\} = \{1, 2, 4, 5, 7, 8, 10\}$.
   (e) $\{\, b \in B \mid (b-5)^2 > 4 \,\} = \{1, 2, 8, 9, 10\}$.
   (f) $\{\, b \in B \mid 3 \leq b \leq 8 \text{ and } b \text{ is even} \,\} = \{4, 6, 8\}$.
2) For any $n \in \mathbb{N}$, we have $\{\, i \in \mathbb{N} \mid 1 \leq i \leq n \,\} = \{1, 2, 3, \ldots, n\}$.

EXERCISE 5.28. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{1, 3, 5, 7, 9\}$. Specify each set by listing its elements.

1) $\{\, a \in A \mid a \text{ is even} \,\} =$
2) $\{\, b \in B \mid b \text{ is even} \,\} =$
3) $\{\, a \in A \mid a \text{ is odd} \,\} =$
4) $\{\, b \in B \mid b \text{ is odd} \,\} =$
5) $\{\, a \in A \mid a < 4 \,\} =$
6) $\{\, b \in B \mid b < 4 \,\} =$
7) $\{\, a \in A \mid (a-3)^2 = 9 \,\} =$
8) $\{\, b \in B \mid (b-3)^2 = 9 \,\} =$
9) $\{\, a \in A \mid a \in B \,\} =$
10) $\{\, b \in B \mid b \in A \,\} =$
11) $\{\, a \in A \mid a \notin B \,\} =$
12) $\{\, b \in B \mid b \notin A \,\} =$
13) $\{\, a \in A \mid 2a \in B \,\} =$

14) $\{\, b \in B \mid 2b \in A \,\} =$

15) $\{\, a \in A \mid a^2 \in B \,\} =$

16) $\{\, a \in A \mid a^2 < 0 \,\} =$

NOTATION 5.29. When talking about sets or using predicates, we usually assume that a "**universe of discourse**" $\mathcal{U}$ has been agreed on. This means that all the elements of all of the sets under discussion are assumed to be members of $\mathcal{U}$. Then

$$\{\, x \mid P(x) \,\}$$

can be used as an abbreviation for $\{\, x \in \mathcal{U} \mid P(x) \,\}$.

The universe of discourse is sometimes assumed to be understood from the context, but it is an important concept, and it is best to specify it so that there is no room for confusion. For example, if we say "Everyone is happy," who is included in this *everyone*? We usually do not mean everyone now alive on the Earth. We certainly do not mean everyone who was ever alive or who will ever live. We mean something more modest: perhaps we mean everyone in the building, or everyone in the class, or maybe we mean everyone in the room.

Specifying a universe of discourse eliminates this ambiguity. The $\mathcal{U}$ is the set of things that we are talking about. So if we want to talk about people in Lethbridge, we define $\mathcal{U}$ to be the set of all people in Lethbridge. We write this at the beginning of our symbolization key, like this:

$\mathcal{U}$: the set of all people in Lethbridge

Everything that follows *ranges over* the universe of discourse. Given this $\mathcal{U}$, "everyone" means "everyone in Lethbridge" and "someone" means "someone in Lethbridge."

Each constant names some member of $\mathcal{U}$, so, if $\mathcal{U}$ is the set of people in Lethbridge, then constants Donald, Gregor, and Marybeth can only be used if these three people are all in Lethbridge. If we want to talk about people in places besides Lethbridge, then we need to specify a different universe of discourse.

EXAMPLE 5.30. If $\mathcal{U}$ is the set of all Canadian provinces, then

$$\begin{aligned}&\{\, x \mid \text{the English name of } x \text{ has three syllables} \,\}\\ &\quad = \{\mathsf{Alberta}, \mathsf{New\ Brunswick}, \mathsf{Newfoundland}\}.\end{aligned}$$

Remark 5.31. There is a very close relationship between sets and unary predicates. In general:

- From any unary predicate $P(x)$, we can define the set
$$\{x \mid P(x)\}.$$
- Conversely, from any set A, we can define a unary predicate $P(x)$ to be "x is a member of A."

Because of this, sets are more-or-less interchangeable with unary predicates. For example, the predicate "x is a dog" can be symbolized in two quite different ways:

- Our symbolization key could state that $D(x)$ means "x is a dog."
- Alternatively, our symbolization key could let D be the set of all dogs. Then "x is a dog" would be translated as "$x \in D$."

In most of mathematics and computer science we make use of sets, rather than unary predicates. We will see that this makes it simpler to translate statements from English into First-Order Logic when quantifiers are involved.

SUMMARY:

- Important definitions:
  - set
  - element, member
  - ordered pair
  - subset, proper subset
  - predicate
- A set is unordered and without repetition.
- $\emptyset$ and A are subsets of A.
- $A = B$ if and only if we have both $A \subset B$ and $B \subset A$.
- For our purposes, predicates usually have only one or two variables.
- If a predicate has two variables, the order of the variables is important.
- Notation:
  - $\{ \quad \}$
  - $\in$, $\notin$
  - $\emptyset$ (empty set)
  - $A \subset B$, $A \not\subset B$, $A \supset B$
  - $\#A$
  - $P(x)$, $x\ Q\ y$ (predicates)
  - $\{\, a \in A \mid P(a) \,\}$
  - $\mathcal{U}$ (universe of discourse)
  - (x, y) (ordered pair)
  - $\mathbb{N}$, $\mathbb{N}^+$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

Chapter 6

Operations on Sets

While I am interested both in economics and in philosophy, the union of my interests in the two fields far exceeds their intersection.

Amartya Sen (b. 1933), Nobel prize-winning economist
Autobiography on nobelprize.org

There are several important ways that a new set can be made from sets that you already have. Any method of doing this is called a **set operation**.

6A. Union and intersection

Two of the most basic operations are *union* and *intersection*. Let us first discuss them in informal terms. Suppose:

- Alice and Bob are going to have a party, and need to decide who should be invited,
- Alice made a list of all the people that she would like to invite, and
- Bob made a list of all the people that he would like to invite.

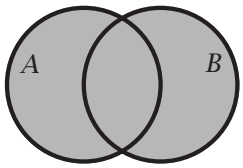
Here are two of the many possible decisions they could make.

1) One solution would be to invite everyone that is on either of the lists. That is, they could begin their invitation list by writing down all of the names on Alice's list, and then add all of the names from Bob's list (or, more precisely, the names from Bob's list that are not already included in Alice's list). This is the *union* of the lists.
2) A much more conservative solution would be to invite only the people that appear on both of the lists. That is, they could go through Alice's list, and cross off everyone that does not appear on Bob's list. (They would get the same result by going through Bob's list, and crossing off everyone that does not appear on Alice's list.) This is the *intersection* of the lists.

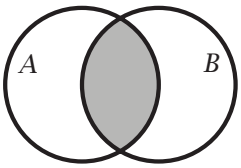
DEFINITION 6.1. Suppose A and B are sets.

1) The **union** of A and B is the set
$$A \cup B = \{\, x \mid x \in A \textbf{ or } x \in B \,\}.$$
2) The **intersection** of A and B is the set
$$A \cap B = \{\, x \mid x \in A \textbf{ and } x \in B \,\}.$$

Remark 6.2. By drawing the sets A and B as overlapping circles, the union and intersection can be represented as follows:



$A \cup B$ is shaded



$A \cap B$ is shaded

Pictures like these are called **Venn diagrams**.

Remark 6.3.

1) In ordinary English, the word "intersection" refers to where two things meet. For example, the intersection of two streets is where the two streets come together. We can think of this area as being part of both streets, so this is consistent with the way the term is used in mathematics.
2) In ordinary English, the word "union" refers to joining things together. For example, a marriage is the union of two people — it joins the two people into a single married couple. This is consistent with the way the term is used in mathematics — we could form the union of Alice's list and Bob's list by gluing Bob's list to the end of Alice's list.

EXAMPLE 6.4.

1) $\{1,3,5,7,9\} \cup \{1,4,7,10\} = \{1,3,4,5,7,9,10\}$
2) $\{1,3,5,7,9\} \cap \{1,4,7,10\} = \{1,7\}$

EXERCISES 6.5. Specify each set by listing its elements.

1) $\{1,2,3,4\} \cup \{3,4,5,6,7\} =$
2) $\{1,2,3,4\} \cap \{3,4,5,6,7\} =$
3) $\{\mathsf{p},\mathsf{r},\mathsf{o},\mathsf{n},\mathsf{g}\} \cap \{\mathsf{h},\mathsf{o},\mathsf{r},\mathsf{n},\mathsf{s}\} =$
4) $\{\mathsf{p},\mathsf{r},\mathsf{o},\mathsf{n},\mathsf{g}\} \cup \{\mathsf{h},\mathsf{o},\mathsf{r},\mathsf{n},\mathsf{s}\} =$
5) $\big(\{1,3,5\} \cup \{2,3,4\}\big) \cap \{2,4,6\} =$
6) $\big(\{1,3,5\} \cap \{2,3,4\}\big) \cup \{2,4,6\} =$

Remark 6.6.

1) It is not difficult to see that $\cup$ and $\cap$ are commutative. That is, for all sets A and B, we have

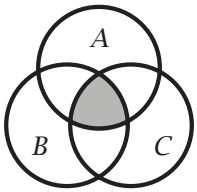
$$A \cup B = B \cup A \quad \text{and} \quad A \cap B = B \cap A.$$

2) It is not difficult to see that $\cup$ and $\cap$ are associative. That is, for all sets A, B, and C, we have

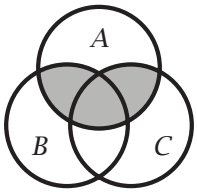
$$(A \cup B) \cup C = A \cup (B \cup C) \quad \text{and} \quad (A \cap B) \cap C = A \cap (B \cap C).$$

So there is no need for parenthesis when writing $A \cup B \cup C$ or $A \cap B \cap C$.

EXAMPLE 6.7. A Venn diagram can include more than two sets. For example, here are Venn diagrams of $A \cap B \cap C$ and $A \cap (B \cup C)$.



$A \cap B \cap C$ is shaded



$A \cap (B \cup C)$ is shaded

EXERCISE 6.8. Draw Venn diagrams of the indicated sets.

1) $A \cup B \cup C$
2) $A \cup (B \cap C)$
3) $(A \cup B) \cap C$
4) $(A \cap C) \cup (B \cap C)$

6B. Set difference and complement

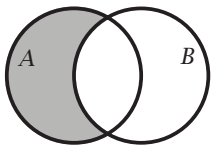
The "set difference" is another fundamental operation. (The "complement" is an important special case.)

EXAMPLE 6.9. If there is a list of people that Alice would like to invite to the party, and also a list of people that Bob refuses to allow to come to the party (the "veto list"), then it would be reasonable to invite the people that are on Alice's list, but not on the veto list. That is, they could start with Alice's list, and remove all of the names that are on the veto list. This is the ⌈set!difference]set difference of Alice's list and the veto list.

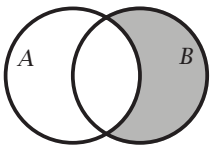
DEFINITION 6.10. Suppose A and B are sets.

1) The **set difference** of A and B is the set
$$A \smallsetminus B = \{\, x \in A \mid x \notin B \,\} = \{\, x \mid (x \in A) \,\&\, (x \notin B) \,\}.$$
(Some authors denote this $A-B$, but that can cause confusion with the usual arithmetic operation of subtraction.)
2) The **complement** of B is the set
$$\overline{B} = \mathcal{U} \smallsetminus B = \{\, x \mid x \notin B \,\},$$
where $\mathcal{U}$ is the universal set, as usual. (As an alternative, the complement is sometimes denoted B^c, instead of $\overline{B}$.)

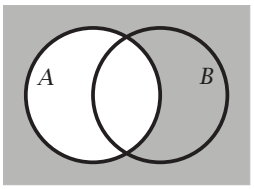
Remark 6.11. Here are Venn diagrams.



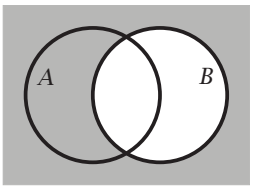
$A \smallsetminus B$ is shaded



$B \smallsetminus A$ is shaded



$\overline{A}$ is shaded



$\overline{B}$ is shaded

EXAMPLE 6.12. Suppose $\mathcal{U} = \mathsf{PEOPLE}$ is the set of all people.

1) $\overline{\mathsf{CHILDREN}} = \mathsf{ADULTS}$, because adults are the people who are not children.

2) $\mathsf{FEMALES} \smallsetminus \mathsf{CHILDREN}$ is the set of all adult women.

EXERCISES 6.13. Assume $\mathcal{U} = \{1, 2, 3, \ldots, 10\}$.
Specify each set by listing its elements.

1) $\{1, 3, 5, 7, 9\} \smallsetminus \{4, 5, 6, 7\} =$

2) $\{4, 5, 6, 7\} \smallsetminus \{1, 3, 5, 7, 9\} =$

3) $\overline{\{1, 3, 5, 7, 9\}} =$

4) $\overline{\{4, 5, 6, 7\}} =$

EXERCISE 6.14. Draw a Venn diagram of each set.

1) $\overline{A \cup B}$

2) $\overline{A \cap B}$

3) $(A \smallsetminus B) \smallsetminus (A \smallsetminus C)$

4) $A \smallsetminus (B \smallsetminus C)$

5) $(A \cup B) \smallsetminus C$

6C. Cartesian product

The Cartesian product is another important set operation. Before introducing it, let us recall the notation for an ordered pair.

NOTATION 6.15. For any objects x and y, mathematicians use (x, y) to denote the **ordered pair** whose first coordinate is x and whose second coordinate is y. We have

$$(x_1, y_1) = (x_2, y_2) \text{ iff } x_1 = x_2 \text{ and } y_1 = y_2.$$

EXAMPLE 6.16. A special case of the Cartesian product is familiar to all algebra students: recall that
(6.17)

$$\mathbb{R}^2 = \{\, (x, y) \mid x \in \mathbb{R},\, y \in \mathbb{R} \,\}$$

is the set of all ordered pairs of real numbers. This is the "coordinate plane" (or "xy-plane") that is used for graphing functions.

The only functions considered in elementary algebra are from $\mathbb{R}$ to $\mathbb{R}$, but this course considers functions from any set A to any set B. Therefore, it is important to generalize the above example by replacing the two symbols $\mathbb{R}$ in the right-hand side of eq. (6.17) with arbitrary sets A and B:

DEFINITION 6.18. For any sets A and B, we let

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

This notation means, for all x, that

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

The set $A \times B$ is called the **Cartesian product** of A and B.

EXAMPLE 6.19.

1) $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

2) $\{1,2,3\} \times \{\mathsf{a},\mathsf{b}\} = \big\{(1,\mathsf{a}),(1,\mathsf{b}),(2,\mathsf{a}),(2,\mathsf{b}),(3,\mathsf{a}),(3,\mathsf{b})\big\}$.

3) $\{\mathsf{a},\mathsf{b}\} \times \{1,2,3\} = \big\{(\mathsf{a},1),(\mathsf{a},2),(\mathsf{a},3),(\mathsf{b},1),(\mathsf{b},2),(\mathsf{b},3)\big\}$.

By comparing (2) and (3), we see that $\times$ is *not* commutative: $A \times B$ is usually *not* equal to $B \times A$.

EXERCISES 6.20. Specify each set by listing its elements.

1) $\{\mathsf{a},\mathsf{i}\} \times \{\mathsf{n},\mathsf{t}\} =$

2) $\{\mathsf{Q},\mathsf{K}\} \times \{\clubsuit,\diamondsuit,\heartsuit,\spadesuit\} =$

3) $\{1,2,3\} \times \{3,4,5\} =$

Remark 6.21. In all of the above examples that involve finite sets, we have

$$\#(A \times B) = \#A \cdot \#B.$$

In other words:

> The cardinality of a Cartesian product is the product of the cardinalities.

The equation is always valid, and will be proved in Theorem 15.19 below. For now, let us now give an informal justification:

Suppose $\#A = m$ and $\#B = n$. Then, by listing the elements of these sets, we may write

$$A = \{a_1, a_2, a_3, \ldots, a_m\} \quad \text{and} \quad B = \{b_1, b_2, b_3, \ldots, b_n\}.$$

The elements of $A \times B$ are:

$$\begin{array}{ccccc}
(a_1,b_1), & (a_1,b_2), & (a_1,b_3), & \cdots & (a_1,b_n), \\
(a_2,b_1), & (a_2,b_2), & (a_2,b_3), & \cdots & (a_2,b_n), \\
(a_3,b_1), & (a_3,b_2), & (a_3,b_3), & \cdots & (a_3,b_n), \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(a_m,b_1), & (a_m,b_2), & (a_m,b_3), & \cdots & (a_m,b_n).
\end{array}$$

In this array,

- each row has exactly n elements, and
- there are m rows,

so the number of elements is the product $mn = \#A \cdot \#B$.

6D. Disjoint sets

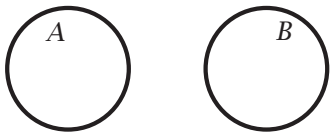
DEFINITION 6.22. Two sets A and B are said to be **disjoint** iff their intersection is empty (that is, $A \cap B = \emptyset$). In other words, they have no elements in common:

$$A \text{ and } B \text{ are disjoint} \quad \Leftrightarrow \quad \begin{array}{c}\text{there does } \textit{not} \text{ exist an } x, \\ \text{such that } \big((x \in A)\ \&\ (x \in B)\big)\end{array}.$$

We may also say that A is **disjoint from** B.

EXAMPLE 6.23.

1) The sets $\{1, 3, 5\}$ and $\{2, 4, 6\}$ are disjoint, because they have no elements in common.
2) The sets $\{1, 3, 5\}$ and $\{2, 3, 4\}$ are *not* disjoint, because 3 is in their intersection.
3) The following Venn diagram illustrates two disjoint sets A and B (they do not overlap):



A and B are disjoint

Remark 6.24. Let us point out some well-known facts that will be formally proved in Chapter 15.

1) If A and B are two disjoint sets, then $\#(A \cup B) = \#A + \#B$.
2) The situation is similar even if there are more than 2 sets: Suppose $A_1, A_2, \ldots, A_n$ are pairwise disjoint sets. (This means that A_i is disjoint from A_j whenever $i \neq j$.) Then
$$\#(A_1 \cup A_2 \cup \cdots \cup A_n) = \#A_1 + \#A_2 + \cdots + \#A_n.$$
3) If A and B are two finite sets that are *not* disjoint, then $\#(A \cup B) < \#A + \#B$.

6E. The power set

EXAMPLE 6.25. It is not difficult to list all of the subsets of $\{a, b, c\}$. One way to do this is to consider the possible number of elements in the subset:

0) A subset with 0 elements has no elements at all. It must be the empty set $\emptyset$.
1) Consider a subset with 1 element. That one element must be one of the elements of $\{a, b, c\}$. That is, the element of the set must be a, b, or c. So the 1-element subsets are $\{a\}$, $\{b\}$, and $\{c\}$.
2) Consider the subsets with 2 elements.
   - If a is one of the elements in the subset, then the other element must be either b or c.
   - If a is not in the subset, then the subset must contain both b and c.

   Hence, the 2-element subsets are $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$.
3) A subset with 3 elements must have all of the elements of $\{a, b, c\}$, so the subset must be $\{a, b, c\}$.

(≥ 4) Because $\{a, b, c\}$ has only 3 elements, we know that no subset can have more than 3 elements.

Thus, the subsets of $\{a, b, c\}$ are
$$\emptyset,\ \{a\}, \{b\}, \{c\},\ \{a, b\}, \{a, c\}, \{b, c\},\ \{a, b, c\}.$$
Counting them, we see that there are exactly 8 subsets.

Remark 6.26. In general, one can show that any set with n elements has exactly 2^n subsets. In the above example, we have $n = 3$, and the number of subsets is $2^3 = 8$.

EXERCISES 6.27.

1) List the subsets of $\{a\}$.

2) List the subsets of $\{a, b\}$.

3) List the subsets of $\{a, b, c, d\}$.

4) List the subsets of $\emptyset$.

We can make a set by putting set braces at the ends of the above list of subsets of $\{a, b, c\}$:

$$\big\{\emptyset,\ \{a\}, \{b\}, \{c\},\ \{b, c\}, \{a, c\}, \{a, b\},\ \{a, b, c\}\big\}.$$

In general, the set of all subsets of a set is called its *power set*:

DEFINITION 6.28. Suppose A is a set. The **power set** of A is the set of all subsets of A. It is denoted $\mathcal{P}(A)$. This means

$$\mathcal{P}(A) = \{\, B \mid B \subset A \,\}.$$

Remark 6.29. From Remark 6.26, we see that if $\#A = n$, then $\#\mathcal{P}(A) = 2^n$. This formula involving "two-to-the-nth-*power*" is the motivation for calling $\mathcal{P}(A)$ the *power* set.

EXERCISES 6.30.

1) Describe each of the following sets by listing its elements.

(a) $\mathcal{P}(\emptyset)$.

(b) $\mathcal{P}\big(\{\mathsf{a}\}\big)$.

(c) $\mathcal{P}\big(\{\mathsf{a}, \mathsf{b}\}\big)$.

(d) $\mathcal{P}\big(\{\mathsf{a}, \mathsf{b}, \mathsf{c}\}\big)$.

(e) $\mathcal{P}\big(\{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}\}\big)$.

2) Which of the following are elements of $\mathcal{P}\big(\{\mathsf{a}, \mathsf{c}, \mathsf{d}\}\big)$?

(a) a (b) $\{\mathsf{a}\}$ (c) $\{\mathsf{a}, \mathsf{b}\}$

3) Suppose A is a set.

(a) Is $\emptyset \in \mathcal{P}(A)$? *Why?*

(b) Is $A \in \mathcal{P}(A)$? *Why?*

4) Does there exist a set A, such that $\mathcal{P}(A) = \emptyset$?

5) Let

- $V_0 = \emptyset$,
- $V_1 = \mathcal{P}(V_0)$,
- $V_2 = \mathcal{P}(V_1) = \mathcal{P}\big(\mathcal{P}(V_0)\big)$,
- and so forth.

In general, $V_n = \mathcal{P}(V_{n-1})$ whenever $n > 0$.

(a) What are the cardinalities of V_0, V_1, V_2, V_3, V_4, and V_5?

(b) Describe V_0, V_1, V_2, and V_3 by listing their elements.

(c) (harder) Describe V_4 by listing its elements.

(d) Is it reasonable to ask someone to list the elements of V_5? *Why?*

SUMMARY:

- Important definitions:
  - union
  - intersection
  - set difference
  - complement
  - disjoint
  - Cartesian product
  - power set
- Venn diagrams are a tool for illustrating set operations.
- $\#\mathcal{P}(A) = 2^{\#A}$
- Notation:
  - $A \cup B$
  - $A \cap B$
  - $A \setminus B$
  - $\overline{A}$
  - $A \times B$
  - $\mathcal{P}(A)$

Chapter 7

First-Order Logic

It was thought for a long time that the theory of sets and mathematical logic were abstract sciences having no practical application. But when electronic computers were invented, it turned out that their programming was based on mathematical logic, and many investigations previously thought to be remote from practical affairs acquired the greatest practical significance (this often happens in the history of science — even at the beginning of the 1930's a book could still be published saying: "Uranium has no practical uses.")

N. Ya. Vilenkin (1920–1991), Russian mathematician
Stories About Sets

7A. Quantifiers

Earlier, we observed that Propositional Logic cannot fully express ideas involving quantity, such as "some" or "all." In this chapter, we will introduce quantifier symbols. Together with predicates and sets, which have already been introduced, this completes the language of First-Order Logic. We will then use this language to translate assertions from English into mathematical notation.

Consider these assertions:

$\mathcal{U}$: The set of all people.

L: The set of all people in Lethbridge.

A: The set of all angry people.

H: The set of all happy people.

$x \; R \; y$: x is richer than y

d: Donald

g: Gregor

m: Marybeth

1. Everyone is happy.
2. Everyone in Lethbridge is happy.
3. Everyone in Lethbridge is richer than Donald.
4. Someone in Lethbridge is angry.

It might be tempting to translate Assertion 1 as $(d \in H) \,\&\, (g \in H) \,\&\, (m \in H)$. Yet this would only say that Donald, Gregor, and Marybeth are happy. We want to say that *everyone* is happy, even if we have not listed them in our symbolization key. In order to do this, we

introduce the "$\forall$" symbol. This is called the **universal quantifier**.

$\forall x$ means "for all x"

A quantifier must always be followed by a variable and a formula that includes that variable. We can translate Assertion 1 as $\forall x, (x \in H)$. Paraphrased in English, this means "For all x, x is happy."

In quantified assertions such as this one, the variable x is serving as a kind of placeholder. The expression $\forall x$ means that you can pick anyone and put them in as x. There is no special reason to use x rather than some other variable. The assertion "$\forall x, (x \in H)$" means exactly the same thing as "$\forall y, (y \in H)$," "$\forall z, (z \in H)$," or "$\forall x_5, (x_5 \in H)$."

To translate Assertion 2, we use a different version of the universal quantifier:

If X is any set, then $\forall x \in X$ means "for all x in X"

Now we can translate Assertion 2 as $\forall \ell \in L, (\ell \in H)$. (It would also be logically correct to write $\forall x \in L, (x \in H)$, but ℓ is a better name for elements of the set L.) Paraphrased in English, our symbolic assertion means "For all ℓ in Lethbridge, ℓ is happy."

Assertion 3 can be paraphrased as, "For all ℓ in Lethbridge, ℓ is richer than Donald." This translates as $\forall \ell \in L, (\ell \; R \; d)$.

To translate Assertion 4, we introduce another new symbol: the **existential quantifier**, $\exists$.

$\exists x$ means "there exists some x, such that"

If X is any set, then $\exists x \in X$ means "there exists some x in X, such that"

We write $\exists \ell \in L, (\ell \in A)$. This means that there exists some ℓ in Lethbridge who is angry. More precisely, it means that there is *at least one* angry person in Lethbridge. Once again, the variable is a kind of placeholder; it would have been logically correct (but poor form) to translate Assertion 4 as $\exists z \in L, (z \in A)$.

EXAMPLE 7.1. Consider this symbolization key.

S: The set of all students.

B: The set of all books.

N: The set of all novels.

$x \; L \; y$: x likes to read y.

Then:

1) $\forall n \in N, (n \in B)$ means "every novel is a book," and

2) $\forall s \in S, \big(\exists b \in B, (s \; L \; b)\big)$ means "every student likes to read some book."

Notice that all of the quantifiers in this example are of the form $\forall x \in X$ or $\exists x \in X$, not $\forall x$ or $\exists x$. That is, all of the variables range over specific sets, rather than being free to range over the entire universe of discourse. Because of this, it is acceptable to omit specifying a universe of discourse. Of course, the universe of discourse (whatever it is) must include at least all students, all books, and all novels.

EXERCISE 7.2. Suppose A and B are sets.
Give your answers in the notation of First-Order Logic (*not English*).

1) What does it mean to say that A is a subset of B?

2) What does it mean to say that A is *not* a subset of B?

7B. Translating to First-Order Logic

We now have all of the pieces of First-Order Logic. Translating assertions (no matter how complicated) from English to mathematical notation will only be a matter of knowing the right way to combine predicates, constants, quantifiers, connectives, and sets. Consider these assertions:

5. Every coin in my pocket is a dime.
6. Some coin on the table is a dime.
7. Not all the coins in my pocket are dimes.
8. None of the coins on the table are dimes.

In providing a symbolization key, we need to specify $\mathcal{U}$. Since we are not talking about anything besides coins, we may let $\mathcal{U}$ be the set of all coins. (It is not necessary to include all coins in $\mathcal{U}$, but, since we are talking about the coins in my pocket and the coins on the table, $\mathcal{U}$ must at least contain all of those coins.) Since we are not talking about any specific coins, we do not need to define any constants. Since we will be explicitly talking about the coins in my pocket and the coins on the table, it will be helpful to have these defined as sets. The symbolization key also needs to say something about dimes; let's do this with a predicate. So we define this key:

$\mathcal{U}$: The set of all coins.
P: The set of all coins in my pocket.
T: The set of all coins on the table.
$D(x)$: x is a dime.

Assertion 5 is most naturally translated with a universal quantifier. It talks about all of the coins in my pocket (that is, the elements of the set P). It means that, for any coin in my pocket, that coin is a dime. So we can translate it as $\forall p \in P, D(p)$.

Assertion 6 says there is some coin on the table, such that the coin is a dime. So we translate it as $\exists t \in T, D(t)$.

Assertion 7 can be paraphrased as, "It is not the case that every coin in my pocket is a dime." So we can translate it as $\neg\big(\forall p \in P, D(p)\big)$. This is simply the negation of Assertion 5.

Assertion 8 can be paraphrased as, "It is not the case that some coin on the table is a dime." This can be translated as $\neg\big(\exists t \in T, D(t)\big)$. It is the negation of Assertion 6.

Remark 7.3. Alternatively, we could have defined a set D, the set of all dimes, instead of the predicate $D(x)$. In this case:

- Assertion 5 would be translated as $\forall p \in P, p \in D$.
- Assertion 6 would be translated as $\exists t \in T, t \in D$.
- Assertion 7 would be translated as $\neg(\forall p \in P, p \in D)$.
- Assertion 8 would be translated as $\neg(\exists t \in T, t \in D)$.

Either approach is perfectly legitimate and the choice is a matter of personal preference: in this example, neither is clearly superior to the other. However, mathematicians tend to use sets, instead of predicates, and we will do the same.

Remark 7.4. If we had defined the predicate $P(x)$ (for "x is in my pocket") instead of the corresponding set P, we would have needed to translate Assertion 5 as $\forall x, \big(P(x) \Rightarrow D(x)\big)$: that is, "for any coin, if it is in my pocket, then it is a dime." Since the assertion is about coins that are both in my pocket *and* that are dimes, it might be tempting to translate it using &. However, the assertion $\forall x, \big(P(x)\ \&\ D(x)\big)$ would mean that everything in $\mathcal{U}$ is both in my

pocket and a dime: All the coins that exist are dimes in my pocket. This is would be a crazy thing to say, and it means something very different than Assertion 5. However, this issue is completely avoided when we use sets. Thus, defining P to be a set, rather than a predicate, is the best approach in this problem (and similarly for T).

We can now translate the deduction from page 59, the one that motivated the need for quantifiers:

Merlin is a wizard. All wizards wear funny hats.
$\therefore$ Merlin wears a funny hat.

$\mathcal{U}$: The set of all people.

W: The set of all wizards.

H: The set of all people who wear a funny hat.

m: Merlin

Translating, we get:

Hypotheses:

$m \in W$

$\forall w \in W, (w \in H)$

Conclusion: $m \in H$

This captures the structure that was left out when we translated the deduction into Propositional Logic, and this is a valid deduction in First-Order Logic. We will be able to prove it rigorously after we have discussed the introduction and elimination rules for $\forall$ (and $\exists$) in Chapter 8.

EXERCISES 7.5. Using the given symbolization key, translate each English-language assertion into First-Order Logic.

$\mathcal{U}$: The set of all animals.

A: The set of all alligators.

R: The set of all reptiles.

Z: The set of all animals who live at the zoo.

M: The set of all monkeys.

$x \heartsuit y$: x loves y.

a: Amos

b: Bouncer

c: Cleo

1) Amos, Bouncer, and Cleo all live at the zoo.

2) Bouncer is a reptile, but not an alligator.

3) If Cleo loves Bouncer, then Bouncer is a monkey.

4) If both Bouncer and Cleo are alligators, then Amos loves them both.

5) Some reptile lives at the zoo.

6) Every alligator is a reptile.

7) Any animal that lives at the zoo is either a monkey or an alligator.

8) There are reptiles which are not alligators.

9) Cleo loves a reptile.

10) Bouncer loves all the monkeys that live at the zoo.
11) All the monkeys that Amos loves love him back.
12) If any animal is an reptile, then Amos is.
13) If any animal is an alligator, then it is a reptile.
14) Every monkey that Cleo loves is also loved by Amos.
15) There is a monkey that loves Bouncer, but sadly Bouncer does not reciprocate this love.

EXERCISES 7.6. Using the given symbolization key, translate each English-language assertion into First-Order Logic.

$\mathcal{U}$: The set of all animals.
D: The set of all dogs.
S: The set of all animals who like samurai movies.
$x\ L\ y$: x is larger than y.
b: Bertie
e: Emerson
f: Fergis

1) Bertie is a dog who likes samurai movies.
2) Bertie, Emerson, and Fergis are all dogs.
3) Emerson is larger than Bertie, and Fergis is larger than Emerson.
4) All dogs like samurai movies.
5) Only dogs like samurai movies.
6) There is a dog that is larger than Emerson.
7) No animal that likes samurai movies is larger than Emerson.
8) Any animal that does not like samurai movies is larger than Bertie.
9) There is an animal that is between Bertie and Emerson in size.
10) There is no dog that is between Bertie and Emerson in size.
11) No dog is larger than itself.

EXERCISES 7.7. For each deduction, write a symbolization key and translate the deduction into First-Order Logic.

1) Nothing on my desk escapes my attention. There is a computer on my desk. Therefore, there is a computer that does not escape my attention.
2) All my dreams are black and white. Old TV shows are in black and white. Therefore, some of my dreams are old TV shows.
3) Neither Holmes nor Watson has been to Australia. A person could see a kangaroo only if they had been to Australia or to a zoo. Although Watson has not seen a kangaroo, Holmes has. Therefore, Holmes has been to a zoo.
4) No one expects the Spanish Inquisition. No one knows the troubles I've seen. Therefore, anyone who expects the Spanish Inquisition knows the troubles I've seen.

5) An antelope is bigger than a bread box. One of the things I am thinking of is no bigger than a bread box, and it is either an antelope or a cantaloupe. Therefore, I am thinking of a cantaloupe.

7C. Multiple quantifiers

EXAMPLE 7.8. Consider the following symbolization key and the assertions that follow it:

$\mathcal{U}$: The set of all people.

$x\ L\ y$: x likes y.

F: The set of all of Karl's friends.

N: The set of all of Imre's neighbours.

i: Imre.

k: Karl.

9. All of Imre's neighbours like all of Karl's friends.
10. At least one of Karl's friends likes at least one of Imre's neighbours.
11. All of Karl's friends like at least one of Imre's neighbours.
12. There is one of Imre's neighbours, who is a friend of Karl and who likes all of Imre's neighbours.

Beginning to translate Assertion 9, we start with all of Imre's neighbours: $\forall n \in N$. Now we would like to say $n\ L\ f$, where f represents every one of Karl's friends. Before we can do this, we need to introduce the variable f, and give it the desired meaning and the appropriate quantifier: $\forall f \in F$. Thus, Assertion 9 can be translated as $\forall n \in N, \big(\forall f \in F, (n\ L\ f)\big)$.

For Assertion 10, we start with at least one of Karl's friends. Another way to say this is that there is some friend of Karl's: $\exists f \in F$. Similarly, we now need to introduce at least one of Imre's neighbours: $\exists n \in N$. The completed translation is $\exists f \in F, \big(\exists n \in N, (f\ L\ n)\big)\big)$.

For Assertion 11, we start with all of Karl's friends: $\forall f \in F$. Now we need at least one of Imre's neighbours: $\exists n \in N$. The completed translation is $\forall f \in F, \big(\exists n \in N, (f\ L\ n)\big)$.

Finally, for Assertion 12, we start with one of Imre's neighbours: $\exists n \in N$. Now we need this person to be a friend of Karl: $n \in F$. For the next part of the sentence, we need all of Imre's neighbours. It is tempting to write $\forall n \in N$, but we have already used the variable n for a particular one of Imre's neighbours, so we cannot use it again here to mean something else. Let's use n' instead: $\forall n' \in N$. We are now ready to translate Assertion 12:

$$\exists n \in N, \big(n \in F\ \&\ \big[\forall n' \in N, (n\ L\ n')\big]\big).$$

(Alternatively, we could have used n_1 and n_2 instead of n and n'.)

When symbolizing assertions with multiple quantifiers, it is best to proceed by small steps. Figure out who is being discussed in the sentence, and what quantifiers are required to introduce these variables. Paraphrase the English assertion so that the logical structure is readily symbolized in First-Order Logic. Then translate bit by bit, replacing the daunting task of translating a long assertion with the simpler task of translating shorter formulas.

WARNING. It is important to put quantifiers in the correct order. For example, consider the following symbolization key and assertions:

$\mathcal{U}$: everything

13. $\forall x, \big(\exists y, (x = y)\big)$
14. $\exists y, \big(\forall x, (x = y)\big)$

They are exactly the same, except for which of $\forall x$ and $\exists y$ is first, and which is second. Assertion 13 is obviously true: "For every thing, there is something that it is equal to." (Namely, every thing is equal to itself.) But Assertion 14 says: "There is some thing (let us call it y), such that everything is equal to y." There is no such y, so this is obviously false.

EXERCISES 7.9. Using the symbolization key from Exercise 7.6, translate each English-language assertion into First-Order Logic.

1) If there is a dog larger than Fergis, then there is a dog larger than Emerson.
2) Every dog is larger than some dog.
3) There is an animal that is smaller than every dog.
4) If there is an animal that is larger than any dog, then that animal does not like samurai movies.
5) For every dog that likes samurai movies, there is a smaller dog that does not like them.
6) Any dog that likes samurai movies is larger than any dog that does not like them.
7) Some animal is larger than all of the dogs that like samurai movies.
8) If there is an animal that likes samurai movies, than all of the dogs are larger than it.

EXERCISES 7.10 (harder). Using the given symbolization key, translate each English-language assertion into First-Order Logic.

$\mathcal{U}$: The set of all people.
D: The set of all ballet dancers.
F: The set of all females.
M: The set of all males.
$x\ C\ y$: x is a child of y.
$x\ S\ y$: x is a sibling of y.
e: Elmer
j: Jane
p: Patrick

1) Everyone who dances ballet is the child of someone who dances ballet.
2) Every man who dances ballet is the child of someone who dances ballet.
3) Everyone who dances ballet has a sister who also dances ballet.
4) Jane is an aunt.
5) Patrick's brothers have no children.

7D. Negations

Recall part of the symbolization key of section 7A:

$\mathcal{U}$: The set of all people.
A: The set of all angry people.
$H(x)$: The set of all happy people.

Consider these further assertions:

15. No one is angry.
16. Not everyone is happy.

Assertion 15 can be paraphrased as, "It is not the case that someone is angry." (In other words, "There does not exist a person who is angry.") This is the negation of the assertion that there exists an angry person, so it can be translated using "not" and "there exists": $\neg\exists x, (x \in A)$.

It is important to notice that Assertion 15 is equivalent to the assertion that "Everyone is nonangry." This assertion can be translated using "for all" and "not": $\forall x, \neg(x \in A)$, or, in other words, $\forall x, (x \notin A)$. In general:

$\neg\exists x, \mathcal{A}$ is logically equivalent to $\forall x, \neg\mathcal{A}$.

This means that the negation of a "$\exists$" assertion is a "$\forall$" assertion.

Assertion 16 says it is not true that everyone is happy. This is the negation of the assertion that everyone is happy, so it can be translated using "not" and "$\forall$": $\neg\forall x, (x \in H)$.

Moreover, saying that not everyone is happy is the same as saying that someone is not happy. This latter assertion translates to $\exists x, (x \notin H)$. In general:

$\neg\forall x, \mathcal{A}$ is logically equivalent to $\exists x, \neg\mathcal{A}$.

This means that the negation of a "$\forall$" assertion is a "$\exists$" assertion.

Just as for "$\forall x$" and "$\exists x$," the bounded quantifiers "$\forall x \in X$" and "$\exists x \in X$" are interchanged under negation:

$\neg\forall x \in X, \mathcal{A}$ is logically equivalent to "$\exists x \in X, \neg\mathcal{A}$.

$\neg\exists x \in X, \mathcal{A}$ is logically equivalent to "$\forall x \in X, \neg\mathcal{A}$.

There is no fundamental difference between this and the previous examples; we have simply replaced $\mathcal{U}$ with the set X.

In summary: if you need to negate an assertion that starts with a quantifier, switch the quantifier to the other one (from $\exists$ to $\forall$ or vice-versa), and then continue, negating the remainder of the assertion.

To perform the additional negations, you will want to remember the following rules from Chapter 3:

De Morgan's Laws

$\neg(A \vee B)$ is logically equivalent to $\neg A \,\&\, \neg B$.

$\neg(A \,\&\, B)$ is logically equivalent to $\neg A \vee \neg B$.

$\neg(A \Rightarrow B)$ is logically equivalent to $A \,\&\, \neg B$.

$\neg\neg A$ is logically equivalent to A.

EXAMPLE 7.11. Let us simplify the assertion

$$(*) \qquad \neg\forall s \in S, \Big(\big((s \in A) \vee (s \in B)\big) \,\&\, \big((s \in C) \Rightarrow (s \neg D)\big)\Big).$$

We bring $\neg$ inside the quantifier, switching from $\forall$ to $\exists$:

$$\exists s \in S, \neg\Big(\big((s \in A) \vee (s \in B)\big) \,\&\, \big((s \in C) \Rightarrow (s \notin D)\big)\Big).$$

Now, we switch & to $\vee$, and apply $\neg$ to each of the two terms:

$$\exists s \in S, \Big(\neg\big((s \in A) \vee (s \in B)\big) \vee \neg\big((s \in C) \Rightarrow (s \notin D)\big)\Big).$$

Next, the connective $\vee$ in the left term is changed to & (and $\neg$ is applied to the subterms), and the rule for negating $\Rightarrow$ is implied to the right term:

$$\exists s \in S, \Big(\big(\neg(s \in A) \,\&\, \neg(s \in B)\big) \vee \big((s \in C) \,\&\, \neg(s \notin D)\big) \Big).$$

Finally, we use the abbreviation $\notin$ in the first three terms, and eliminate the double negative in the final term:

$$\exists s \in S, \Big(\big((s \notin A) \,\&\, (s \notin B)\big) \vee \big((s \notin C) \,\&\, (s \in D)\big) \Big).$$

This final result is logically equivalent to Assertion $(*)$ above.

The same principles apply to negating assertions in English.

EXAMPLE 7.12. Suppose that we want to negate

"Every umbrella either needs a new handle or is not big enough."

We create a symbolization key:

U: The set of all umbrellas.

H: The set of all umbrellas that need a new handle.

B: The set of all umbrellas that are big enough.

Now we can translate the assertion as $\forall u \in U, \big((u \in H) \vee (u \notin B)\big)$. Negating this, we have

$$\neg\forall u \in U, \big((u \in H) \vee (u \notin B)\big).$$

We have just learned that this is equivalent to

$$\exists u \in U, \neg\big((u \in H) \vee (u \notin B)\big),$$

which can be simplified to

$$\exists u \in U, \big((u \notin H) \,\&\, \neg(u \notin B)\big),$$

and finally, eliminating the double negative, this is equivalent to

$$\exists u \in U, \big((u \notin H) \,\&\, (u \in B)\big).$$

Now we translate back to English:

"There is some umbrella that does not need a new handle and is big enough."

Applying these rules systematically will enable you to simplify the negation of any assertion (no matter whether it is expressed in English or in First-Order Logic).

English is more open to interpretation and inexactitude than First-Order Logic. Therefore, when we need to negate an English assertion in this chapter, we translate it into First-Order Logic, perform the negation, and translate back. You will also be expected to do this. Later, in proofs, you may work directly with the English version, although you may find it helpful to keep the First-Order Logic version in mind.

WARNING. Suppose we want to symbolize the assertion "there exists an umbrella." It is tempting to symbolize this simply as $\exists u \in U$. However, this causes a serious problem if you then apply the rules for negation: according to the rules, the negation would be $\forall u \in U$, which does not make sense: its English translation is "for all u in U," which is not a complete sentence. The problem is that $\exists u \in U$ is also not a complete sentence: it means "there exists an umbrella, such that." (In order to form a complete sentence, quantifiers should always be followed by a predicate.) One way to solve this problem is to rephrase the original assertion as: "there exists something that is an umbrella." This translates to $\exists x, (x \in U)$, which is a correct symbolization of the assertion. Its negation simplifies to $\forall x, (x \notin U)$, which means "every thing that exists is not an umbrella."

EXERCISES 7.13. Negate each of the assertions in Exercise 7.5. Express your answer both in the language of First-Order Logic and in English (after simplifying).

EXERCISES 7.14. Negate each of the following assertions of First-Order Logic (and simplify, so that $\neg$ is not applied to anything but predicates or assertion variables).

1) $(L \Rightarrow \neg M)\ \&\ (M \vee N)$

2) $\big((a \in A)\ \&\ (b \in B)\big) \vee (c \in C)$

3) $\forall a \in A, \Big(\big(P(a) \vee Q(a)\big)\ \&\ R(a)\Big)$

4) $\forall a \in A, \Big(T(a) \Rightarrow \exists c \in C, \big(Q(c)\ \&\ (c\ R\ a)\big)\Big)$

5) $\forall x, \Big(A(x)\ \&\ \Big(\exists \ell \in L, \big((x\ B\ \ell) \vee C(\ell)\big)\Big)\Big)$

6) $A \Rightarrow \Big(\big(\exists x \in X, B(x)\big) \vee \big(\forall e \in E, \exists d \in D, (e\ C\ d)\big)\Big)$

7) $\forall a \in A, \exists b \in B, \exists c \in C, \forall d \in D, \Big((a\ K\ b)\ \&\ \big((a\ Z\ c) \vee (b > d)\big)\Big)$

7E. Equality

The equals sign "=" is a part of every symbolization key (even though we do not bother to include it explicitly). It is a binary predicate, and, as you would expect, "$x = y$" means "x is equal to y." This does not mean merely that x and y look very much alike, or that they are indistinguishable, or that they have all of the same properties. Rather, it means that x and y are (different) names for the same object.

Consider this symbolization key and these assertions:

$\mathcal{U}$: The set of all people.

H: The set of people who owe money to Hikaru.

p: Pavel

h: Hikaru

17. No one other than Pavel owes money to Hikaru.

18. Only Pavel owes Hikaru money.

Assertion 17 can be paraphrased as, "There is no one who owes money to Hikaru and is not Pavel." This can be translated as $\neg\exists h \in H, h \neq p$. (We use $x \neq y$ as an abbreviation for $\neg(x = y)$.) Simplifying, this is logically equivalent to $\forall h \in H, h = p$, which can be paraphrased as, "Any person that owes Hikaru must be Pavel."

Assertion 18 can be paraphrased as, "Pavel owes Hikaru *and* any person that owes Hikaru must be Pavel." We have already translated the second conjunct, and the first is straightforward. Assertion 18 becomes $p \in H\ \&\ (\forall h \in H, h = p)$.

EXERCISES 7.15. Using the given symbolization key, translate each English-language assertion into First-Order Logic.

$\mathcal{U}$: The set of all cards in a standard deck.

C: The set of all clubs.

B: The set of all black cards.

D: The set of all deuces.

J: The set of all jacks.

W: The set of all wild cards.

1) There are at least two clubs.

2) There is more than one black jack.

3) There are exactly two black jacks.

4) If there is a deuce of clubs, then it is the only wild card.

5) There are at least three clubs.

7F. Vacuous truth

The difference between the translations of Assertion 17 ("No one other than Pavel owes money to Hikaru") and Assertion 18 ("Only Pavel owes Hikaru money") brings up an interesting point: what if no one owes Hikaru money? Then we have $H = \emptyset$. Certainly, if $H = \emptyset$, then $\exists h \in H, h \neq p$ must be false (because it is impossible to find an element of the empty set), so its negation, $\neg\exists h \in H, h \neq p$, must be true. If our two translations of Assertion 17 really are logically equivalent, as we have claimed, then it must be the case that when $H = \emptyset$, the assertion $\forall h \in H, h = p$ is true.

Why should this be? In fact, you can make any assertion at all about all of the elements of the empty set, and it will be true. Such statements are called **vacuously true**. The point is that there is nothing in the empty set to contradict whatever assertion you care to make about all of the elements. For example, if you say, "All of the people on Mars have purple skin," and there are not any people on Mars, then you have spoken the truth — otherwise, there would have to be an example of a person on Mars whose skin is not purple.

This is related to the concept that "If pigs fly, then cows are green" is a true assertion. As long as no one can produce a flying pig and a cow that is not green to prove the assertion false, it is true by default.

EXERCISES 7.16. Which of the following English assertions are vacuously true (in the real world)?

1) All quintuplets are sickly.

2) All standard playing cards that are numbered fifteen, are green.

3) All prime numbers that are divisible by 12, have 5 digits.

4) All people who have been to the moon are men.

5) All people who do not breathe are dead.

7G. Uniqueness

Saying "there is a *unique* so-and-so" means not only that there is a so-and-so, but also that there is only one of them—there are not two different so-and-so's. For example, to say that "there is a *unique* person who owes Hikaru money" means

some person owes Hikaru *and* no other person owes Hikaru.

This translates to

$$\exists h \in H, \big(\forall y, (y \neq h \Rightarrow y \notin H)\big);$$

or, equivalently,

$$\exists h \in H, \big(\forall y, (y \in H \Rightarrow y = h)\big).$$

Unfortunately, both of these are quite complicated expressions (and are examples of "multiple quantifiers," because they use both $\exists$ and $\forall$). To simplify the situation, mathematicians

introduce a special notation:

"$\exists!\, x$" means "there is a unique x, such that..."

If X is any set, then "$\exists!\, x \in X$" means "there is a unique x in X, such that..."

For example, $\exists!\, h, h \in H$ means exactly the same thing as the complicated expression above.

If we add

R: The set of people who are rich.

to our symbolization key, we can translate "There is a unique rich person who owes Hikaru money." Namely, it translates as:

$$\exists!\, r \in R, (r \in H).$$

Remark 7.17. Unfortunately, there is no nice, compact way of negating assertions involving uniqueness. If we want to say "It is not the case that there is a unique person who owes Hikaru money," we need to say that "Either no one owes Hikaru money, or more than one person owes Hikaru money." This translates to

$$(H = \emptyset) \vee \big(\exists h_1 \in H, (\exists h_2 \in H, h_2 \neq h_1)\big).$$

Although it is important to know how to negate assertions involving uniqueness, we will not expect you to be able to do so at this point. The example above should give you an idea of how to proceed, if you do come across a situation where you want to negate such a sentence.

EXERCISES 7.18. Using the given symbolization key, translate each English-language assertion into First-Order Logic.

$\mathcal{U}$: The set of all creatures.

H: The set of all horses.

P: The set of all Pegasuses.

W: The set of all creatures with wings.

B: The set of all creatures in Farmer Brown's field.

1) There is a unique winged creature in Farmer Brown's field.

2) If every Pegasus has wings, then there is a unique horse in Farmer Brown's field.

3) If there is a horse in Farmer Brown's field, then there is a unique winged horse.

7H. Bound variables

Recall that an assertion is a statement that is either true or false. For example, consider the following symbolization key:

$\mathcal{U}$: The set of all students.

$M(x)$: x is taking a math class.

a: Anna

- $M(a)$ is an assertion. Either Anna is taking a math class, or she is not.
- $M(x)$ is *not* an assertion. The letter x is a variable, not any particular object. (We call x a **free variable**.) If we plug in a particular value for x (such as a), then we will have an assertion. However, until some value is plugged in for x, we cannot say whether the expression is true or false. So the expression is not an assertion if the variable remains free.

- $\exists x, M(x)$ and $\forall x, M(x)$ are assertions. The letter x is a variable in both of these expressions, but it is no longer free, because it is acted on by the quantifier. (We call x a **bound variable**.)

An important principle of First-Order Logic is that, in an assertion, each variable must be bound by some quantifier:

Assertions cannot have free variables.

EXERCISES 7.19. Suppose that p is a constant, but all other lower-case letters represent variables. For each of the following, (a) does it have a free variable? (b) is it an assertion?

1) $\forall x \in X, (x \; L \; y)$
2) $(p \in S) \;\&\; \exists y \in Y, (y \; T \; p)$
3) $\forall v \in V, \big(\exists! \, y \in Y, \big[\big((v \; R \; p) \;\&\; (y \; R \; v)\big) \Rightarrow (z = p)\big]\big)$
4) $y \in Y \;\&\; \big(\forall x \in X, T(x)\big)$
5) $(p \; L \; p) \Rightarrow \exists x, (x \; L \; p)$
6) $\forall x \in X, (x \; L \; x)$

7I. Counterexamples in First-Order Logic

EXAMPLE 7.20. Show that the following deduction is not valid:

$$\exists x, (x \in A), \qquad \therefore \;\; \forall x, (x \in A).$$

Scratchwork. To get the idea of what is going on, it may be helpful to translate the deduction into English. For example, we could use the symbolization key

$\mathcal{U}$: things on the kitchen table

A: apples on the kitchen table.

In this setting, the deduction becomes:

There is an apple on the kitchen table. $\quad\therefore$ Everything on the kitchen table is an apple.

This deduction is obviously not valid: it is easy to imagine a situation in which one thing on the kitchen table is an apple, but something else on the kitchen table is not an apple.

To find the official solution, we will do something analogous, but using the notation of First-Order Logic, instead of talking about apples and tabletops:

In order to construct a counterexample, we want the hypothesis of the deduction to be true and the conclusion to be false.

- To make the hypothesis $\exists x, (x \in A)$ true, we need something to be an element of A. For example, we could let $1 \in A$.
- To make the the conclusion $\forall x, (x \in A)$ false, we want its negation to be true: we want $\exists x, (x \notin A)$ to be true. For example, we could arrange that $2 \notin A$.

To satisfy the above two conditions, we let $A = \{1\}$. Since 1 and 2 are the only elements mentioned in the discussion, we can let $\mathcal{U} = \{1, 2\}$. This results in the counterexample we were hoping to find.

SOLUTION. We provide a counterexample. Let

$$\mathcal{U} = \{1, 2\} \text{ and } A = \{1\}.$$

Then:

$1 \in A$ is true, so $\exists x, (x \in A)$ is true, so the hypothesis is true,

but

$2 \notin A$, so $\forall x, (x \in A)$ is false, so the conclusion is false.

Since we have a situation in which the hypothesis is true, but the conclusion is false, the deduction is not valid. □

EXAMPLE 7.21. Show that the following deduction is not valid:

Hypotheses:

1. $\forall x, \big((x \in A) \vee (x \in B)\big)$
2. $A \neq \emptyset$
3. $B \neq \emptyset$

Conclusion: $\exists x, \big((x \in A)\ \&\ (x \in B)\big)$.

Scratchwork. In order to construct a counterexample, we want all of the hypothesis of the deduction to be true and the *negation* of the conclusion to be true. The negation of the conclusion is

$$\forall x, \big((x \notin A) \vee (x \notin B)\big),$$

which is logically equivalent to

$$\forall x, \big((x \in A) \Rightarrow (x \notin B)\big). \tag{7.22}$$

Now:

- To make Hypothesis 2 true, we may let $1 \in A$.
- To make Hypothesis 3 true, we must put something in the set B. However, it is important to note that (7.22) tells us $1 \notin B$, so we must put something else into B. For example, we may let $2 \in B$.
- Now, after A and B have been constructed, we can make Hypothesis 1 true by letting $\mathcal{U} = A \cup B$.

To satisfy all three of the above conditions, we may let $A = \{1\}$, $B = \{2\}$, and $\mathcal{U} = A \cup B = \{1, 2\}$.

SOLUTION. We provide a counterexample. Let

$$\mathcal{U} = \{1, 2\}, \quad A = \{1\}, \quad \text{and} \quad B = \{2\}.$$

Then:

1) We have
   - $1 \in A$ is true, so $(1 \in A) \vee (1 \in B)$ is true, and
   - $2 \in B$ is true, so $(2 \in A) \vee (2 \in B)$ is true.

   Since 1 and 2 are the only elements of $\mathcal{U}$, this implies, for every x, that $(x \in A) \vee (x \in B)$ is true. So Hypothesis 1 is true.

2) $1 \in A$, so $A \neq \emptyset$. Hence, Hypothesis 2 is true.

3) $2 \in B$, so $B \neq \emptyset$. Hence, Hypothesis 3 is true.

However:

- $1 \notin B$, so $(1 \in A)\ \&\ (1 \in B)$ is false, and
- $2 \notin A$, so $(2 \in A)\ \&\ (2 \in B)$ is false.

Since 1 and 2 are the only elements of $\mathcal{U}$, this implies there is no x for which the assertion $(x \in A) \,\&\, (x \in B)$ is true. Hence, the assertion $\exists x, \big((x \in A) \,\&\, (x \in B)\big)$ is false; in other words, the conclusion of the deduction is false. Since we have a situation in which the hypothesis is true, but the conclusion is false, the deduction is not valid. □

EXERCISES 7.23. Explain how you know that each of the following deductions is not valid.

1) $\exists x, (x \in A),\ \exists x, (x \in B),\ \therefore\ \exists x, \big((x \in A) \,\&\, (x \in B)\big)$

2) $\forall a \in A, \exists b \in B, (a \neq b),\ A \neq \emptyset,\ \therefore\ \forall b \in B, \exists a \in A, (a \neq b).$

3) $A \neq B,\ \therefore\ A \cup B \neq A.$

4) $\forall x \in A, (x \notin B),\ \forall x \in B, (x \notin A),\ \therefore\ A \neq B.$

SUMMARY:

- Practice in translating between English and First-Order Logic.
- The order of the quantifiers is important, and can change the meaning of an assertion.
- Rules for negating quantifiers:
  - the negation of a "∀" assertion is a "∃" assertion;
  - the negation of a "∃" assertion is a "∀" assertion;
- The symbol = is part of any symbolization key.
- Any assertion about all elements of $\emptyset$ is true.
- Any variable in an assertion must be bound by a quantifier.
- To show a deduction is *not* valid, find a counterexample.
- Notation:
  - $\forall x$ (universal quantifier; means "For all x")
  - $\forall x \in X$ (universal quantifier; means "For all x in X")
  - $\exists x$ (existential quantifier; means "There exists some x, such that…")
  - $\exists x \in X$ (existential quantifier; means "There exists some x in X, such that…")
  - $\exists!\, x$ (means "There is a unique x, such that…")
  - $\exists!\, x \in X$ (means "There is a unique x in X, such that…")
  - $=, \neq$

Chapter 8

Quantifier Proofs

The grand aim of all science is to cover the greatest number of empirical facts by logical deduction from the smallest number of hypotheses or axioms.
Albert Einstein (1879–1955), Nobel prize-winning physicist
in *Life* magazine

This chapter explains the introduction and elimination rules for the quantifiers $\exists$ and $\forall$. Proofs in First-Order Logic can use both of these rules, plus all of the rules of Propositional Logic, such as De Morgan's Laws, the basic theorems (including introduction and elimination rules), and any theorems that have been previously proved.

8A. The introduction and elimination rules for quantifiers

As you know, there are two quantifiers ($\exists$ and $\forall$). Each of these has an introduction rule and an elimination rule, so there are 4 rules to present in this section.

8A.1. $\exists$-introduction. We need to know how to prove a conclusion of the form $\exists x \in X, \ldots$. For example, in a murder mystery, perhaps Inspector Thinkright gathers the suspects in a room and tells them, "Someone in this room has red hair." That is a $\exists$-statement. (With an appropriate symbolization key, in which P is the set of all of the the people in the room, and $R(x)$ is the predicate "x has red hair," it is the assertion $\exists p \in P, R(p)$.) How would the Inspector convince a skeptic that the claim is true? The easiest way would be to exhibit an explicit example of a person in the room who has red hair. For example, if Jim is in the room, and he has red hair, the Inspector might say,

> "Look, Jim is sitting right there by the door, and now, when I take off his wig, you can see for yourself that he has red hair. So I am right that someone in this room has red hair."

In general, the most straightforward way to prove $\exists p \in P, R(p)$ is true is to find a specific example of a p that makes $R(p)$ true. That is the essence of the $\exists$-intro rule.

Here is a principle to remember:

> The proof of an assertion that begins
> "there exists $x \in X$, such that..."
> will usually be based on the statement "Let $x =$ $\square$,"
> where the box is filled with an appropriate element of X.

Remark 8.1. Most mathematicians are not familiar with the terminology of introduction rules and elimination rules. Instead of saying this is the $\exists$-introduction rule, they would call it "proof by constructing an example," or "giving an explicit example," or other words to the same effect.

Here are some proofs that use ∃-introduction, but we cannot do very much with only one quantifier rule — the examples will be more interesting when we have more rules to work with.

EXAMPLE 8.2. Prove there is a natural number n, such that $n^2 = 64$.

PROOF. Let $n = 8 \in \mathbb{N}$. Then $n^2 = 8^2 = 64$. □

EXAMPLE 8.3. Prove there is a real number c, such that $5c^2 - 5c + 1 < 0$.

PROOF. Let $c = 1/2 \in \mathbb{R}$. Then

$$5c^2 - 5c + 1 = 5\left(\frac{1}{2}\right)^2 - 5\left(\frac{1}{2}\right) + 1 = \frac{5}{4} - \frac{5}{2} + 1 = -\frac{1}{4} < 0,$$

as desired. □

EXAMPLE 8.4. Let $N = \{1, 3, 5, 7\}$. Prove there is some $n \in N$, such that $n^3 - 11n^2 + 31n \neq 21$.

PROOF. Let $n = 5 \in N$. Then

$$n^3 - 11n^2 + 31n = 5^3 - 11(5^2) + 31(5) = 125 - 11(25) + 155 = 125 - 275 + 155 = 5 \neq 21.$$ □

EXERCISES 8.5.

1) Prove there is a real number r, such that $2r^2 + 9r + 4 = 0$.
2) Prove there exist natural numbers m and n, such that $m^2 = n^3 + 1 > 1$.
[*Hint:* Try *small* values of m and n.]

8A.2. ∃-elimination. Perhaps Inspector Thinkright knows that one of the men lit a match at midnight, but does not know who it was. The Inspector might say,

> "We know that one of the men lit a match at midnight. Let us call this mysterious gentleman 'Mr. X.' Because right-handed matches are not allowed on the island, we know that Mr. X is left handed. Hence, Mr. X is not a butler, because all of the butlers in this town are right handed. . . ."

and so on, and so on, telling us more and more about Mr. X, based only on the assumption that he (or she) lit a match at midnight.

The situation in mathematical proofs is similar. Suppose we know there exists an element of the set A. Then it would be helpful to have a name for this mysterious element, so that we can talk about it. But a mathematician would not call the element "Mr. X": if it is an element of the set A, then he or she would probably call it a (or a_1 if there are going to be other elements of A to talk about). In general, the idea of the ∃-elimination rule is:

> If $\exists x \in X, P(x)$ is known to be true, then we may let x be an element of X, such that $P(x)$ is true.

In the remainder of the proof, we may assume only two things about x: that $x \in X$, and that $P(x)$ is true.

EXAMPLE 8.6. Show that if there exists $a \in \mathbb{R}$, such that $a^3 + a + 1 = 0$, then there exists $b \in \mathbb{R}$, such that $b^3 + b - 1 = 0$.

PROOF. Assume there exists $a \in \mathbb{R}$, such that $a^3 + a + 1 = 0$. Let $b = -a$. Then

$$\begin{aligned} b^3 + b - 1 &= (-a)^3 + (-a) - 1 \\ &= (-a)^3 + (-a) - 1 \\ &= -a^3 - a - 1 \\ &= -(a^3 + a + 1) \\ &= -f(a) \\ &= -0 \\ &= 0, \end{aligned}$$

as desired. □

8A.3. ∀-elimination. Perhaps Inspector Thinkright knows that Jeeves is a butler in the town, and that all of the butlers in the town are right handed. Well, then it is obvious to the Inspector that Jeeves is right handed. This is an example of ∀-elimination: if you know something is true about every element of a set, then it is true about any particular element of the set that you are interested in.

If $\forall x \in X, P(x)$ is true, and $a \in X$, then $P(a)$ is true.

EXAMPLE 8.7. Suppose

- $C \subset \mathbb{R}$, and
- $\forall x \in \mathbb{R}, \big((x^2 = 9) \Rightarrow (x \in C)\big)$.

Show $\exists c \in \mathbb{R}, c \in C$.

PROOF. Let $c = 3 \in \mathbb{R}$. Then $c^2 = 3^2 = 9$, and, because $c \in \mathbb{R}$, we know

$$(c^2 = 9) \Rightarrow (c \in C).$$

Therefore $c \in C$. □

Here is a simple proof that combines all three of the quantifier rules that have been discussed so far: ∃-elim, ∀-elim, and ∃-intro.

EXAMPLE 8.8. Assume $A \neq \emptyset$ and $A \subset B$. Prove $\exists b, (b \in B)$.

PROOF. Because A is not the empty set, we know it has at least one element; that is, we have $\exists x, (x \in A)$. Hence, we may let a be some element of A. Now, let $b = a$. Because $A \subset B$, we know that every element of A is an element of B. In particular, since $b = a \in A$, this means that $b \in B$. So $\exists b, (b \in B)$. □

WARNING. When applying ∀-elimination, the variable does not need to be called "x," (it could be y or z or any other variable), and the constant does not need to be called "a" (it could be any element of X). However, if the variable occurs more than once in the formula, it is important to replace *all* of its occurrences with a. For example, if $a \in X$, then, from $\forall x \in X, \big(A(x) \Rightarrow B(x)\big)$, we can conclude $A(a) \Rightarrow B(a)$, but *not* $A(a) \Rightarrow B(x)$ or $A(x) \Rightarrow B(a)$.

EXERCISES 8.9. Use the symbolization key

$\mathcal{U}$: The set of all U of L students.

$x\ L\ y$: x likes y.

b: Bobby

c: Cindy

Assume

$$\forall x, \Big(\big(\exists y, (x \ L \ y) \big) \Rightarrow \forall z, (z \ L \ x) \Big)$$

and

$$b \ L \ c.$$

For each of the following assertions:

a) translate it into First-Order Logic, and

b) provide a proof in First-Order Logic.

1) Bobby likes some student at the U of L.
2) Some student at the U of L likes Bobby.
3) Bobby likes himself.
4) Some student at the U of L likes himself or herself.
5) If there is a student at the U of L whom Cindy likes, then there is a student at the U of L who likes Cindy.
6) If there is a student at the U of L who likes Bobby, then there is a student at the U of L whom Bobby likes.

8A.4. $\forall$-introduction. If Inspector Thinkright needs to verify that all of the butlers in town have seen the aurora borealis, he would probably get a list of all the butlers, and check them one-by-one. That is a valid approach, but it could be very time-consuming if the list is very long. In mathematics, such one-by-one checking is often not just time-consuming, but impossible. For example, the set $\mathbb{N}$ is infinite, so, if we wish to show $\forall n \in \mathbb{N}, (2n \text{ is even})$, then we would never finish if we tried to go through all of the natural numbers one-by-one; we need to deal with many numbers at once.

Consider the following simple deduction:

Hypotheses:

Every butler in town got up before 6am today.

Everyone who got up before 6am today, saw the aurora.

Conclusion: Every butler in town saw the aurora.

This is clearly a valid deduction in English. Let us translate it into First-Order Logic to analyze how we were able to reach a conclusion about all of the butlers, without checking each of them individually. Here is a symbolization key:

B: The set of all of the butlers in town.

P: The set of all people.

$U(x)$: x got up before 6am today.

$S(x)$: x saw the aurora.

We can now translate our English deduction, as follows:

Hypotheses:

$\forall b \in B, U(b)$.

$\forall p \in P, \big(U(p) \Rightarrow S(p) \big)$.

Conclusion: $\forall b \in B, S(b)$.

How do we justify the conclusion? Well, suppose for a moment that we start to check every butler in town, and that j represents Jimmy, who is one of the butlers in town. Then our first hypothesis allows us to conclude $U(j)$. Since Jimmy is a person, our second hypothesis allows us to conclude that $U(j) \Rightarrow S(j)$. Then, using $\Rightarrow$-elimination, we conclude $S(j)$. But there was nothing special about our choice of Jimmy. All that we know about him, is that he is a butler in the town. So we could use exactly the same argument to deduce $S(b)$ for any butler b in the town.

This is how we justify a $\forall$-introduction. If we can prove that the desired conclusion is true for an *arbitrary* element of a set, when we assume *nothing* about the element except that it belongs to the set, then the conclusion must be true for every element of the set.

We write the above deduction as follows:

THEOREM 8.10. *Assume that every butler in town got up before 6am today. Also assume that everyone who got up before 6am today, saw the aurora. Then every butler in town saw the aurora.*

PROOF. Let b represent an arbitrary butler in town. Then, since all of the butlers got up before 6am, we know that b got up before 6am. By hypothesis, this implies that b saw the aurora. Since b is an arbitrary butler in town, we conclude that every butler in town saw the aurora. □

This reasoning leads to the $\forall$-introduction rule: in order to prove that *every* element of a set X has a certain property, it suffices to show that an *arbitrary* element of X has the desired property. For example, if we wish to prove $\forall b \in B, P(b)$, then our proof should start with the sentence "Let b be an arbitrary element of B." (However, this can be abbreviated to: "Given $b \in B$, ...") After this, our task will be to prove that $P(b)$ is true, without assuming anything about b other than it is an element of B.

> The proof of an assertion that begins "for all $x \in X$,"
> will usually begin with "Let x be an arbitrary element of X"
> or, for short, "Given $x \in X$,").

WARNING. It is important not to assume anything about x other than that it is an element of X. If you choose x to be a particular element of X that has some special property, then your deduction will not be valid for *all* elements of the set.

EXAMPLE 8.11. Suppose we would like to justify the following deduction:

> All of the butlers in town dislike Jimmy, and Jimmy is a butler in town.
> Therefore, all of the butlers in town dislike themselves.

Then it suffices to show, for an arbitrary butler b, that b dislikes b. We might try the following proof:

PROOF ATTEMPT. Let b be Jimmy, who is a butler in town. Then, since all of butlers in town dislike Jimmy, we know that b dislikes Jimmy. Since Jimmy $= b$, this means b dislikes b, as desired. So every butler in town dislikes himself. □

This proof is certainly *not* valid, however. Letting $b =$ Jimmy does not make b an *arbitrary* butler; rather, it makes b a very special butler — the one that everybody dislikes. In this case, conclusions that are true about b are not necessarily true about the other butlers.

Another point that should be emphasized is that an *arbitrary* member of a set is not the same as a *random* member of a set. If we want to prove that all of the butlers have seen the aurora, it is not enough to choose a butler at random, ask if he saw the aurora and draw a

conclusion about all of the butlers based on that single answer. It is only if we can determine through logical deduction that *no matter which* butler we choose, that person saw the aurora, that we can conclude that all of the butlers saw the aurora.

In Chapter 5, we claimed that two sets are equal if and only if each is a subset of the other. With ∀-introduction, we can now prove this important fact.

THEOREM 8.12. *Suppose A and B are sets.*
We have $A = B$ if and only if $A \subset B$ and $B \subset A$.

PROOF. ($\Rightarrow$) Assume $A = B$. Every set is a subset of itself (see Remark 5.20), so we have

$$A = B \subset B \quad \text{and} \quad B = A \subset A,$$

as desired.

($\Leftarrow$) Assume $A \subset B$ and $B \subset A$. We wish to show $A = B$; in other words, we wish to show

$$\forall x, (x \in A \Leftrightarrow x \in B).$$

Let x be arbitrary.

($\Rightarrow$) Suppose $x \in A$. Since $A \subset B$, this implies $x \in B$.

($\Leftarrow$) Suppose $x \in B$. Since $B \subset A$, this implies $x \in A$.

Therefore, $x \in A \Leftrightarrow x \in B$.

Since x is arbitrary, this implies $\forall x, (x \in A \Leftrightarrow x \in B)$, as desired. □

EXERCISES 8.13. Using the given symbolization key, translate each theorem from First-Order Logic into English, and provide a proof. (Note that you do not need to know what "coprime" or "perfect" means. Also, although the deductions are valid, some of them may have a conclusion that is false, because some of the hypotheses are not true.)

$\mathcal{U}$: $\mathbb{N}$

$E(x)$: x is even.

$x \; C \; y$: x is coprime to y.

$P(x)$: x is perfect.

1) $\forall x, \forall y, (x \; C \; y), \therefore \exists x, (x \; C \; x)$.

2) $\forall x, \forall y, \big((x \; C \; y) \Rightarrow (y \; C \; x)\big), \therefore \forall x, \forall y, \big((x \; C \; y) \Leftrightarrow (y \; C \; x)\big)$.

3) $\big(\forall x, (x \; C \; x)\big) \Rightarrow \big(\exists x, \exists y, (x \; C \; y)\big)$

4) $\forall y, \exists x, \big(E(y) \Rightarrow E(x)\big)$

5) $P(2) \Rightarrow \forall x, \big(E(x) \Leftrightarrow E(2)\big), E(2), \neg E(1), \therefore \neg P(2)$.

EXERCISE 8.14. Which of the 4 quantifier rules does each deduction illustrate?

1) Everyone who ate in the cafeteria yesterday is sick today. Oh, no! Susie ate in the cafeteria — she must be sick!!
2) Susie ate in the cafeteria yesterday, so I'm sure that *somebody* ate in the cafeteria yesterday.
3) Without knowing which of the athletes it was, I figured out that he or she must have eaten in the cafeteria yesterday. The only way that can be true is if every athlete ate in the cafeteria yesterday.
4) Our food reporter says that some woman knocked over a big box of lima beans while she was eating in the cafeteria yesterday. Whoever she is, let's call her "Ms. Clumsy." So this morning's headline can be "Ms. Clumsy spilled the beans!"

8A.5. Proof strategies revisited. The strategies you used to find proofs in Propositional Logic are the same approaches that you should use in First-Order Logic: working backwards, working forwards, changing what you are looking at, breaking the proof into cases, and proof by contradiction are all important. The introduction and elimination rules for quantifiers just add some new options when you are working forwards or working backwards. In particular:

- If you have $\exists x, \mathcal{A}(x)$, you will probably use $\exists$-elimination: assume $\mathcal{A}(c)$ for some letter c that is not already in use, and then derive a conclusion that does not contain c.
- If the desired conclusion is $\forall x \in X, \mathcal{A}(x)$, then your proof will almost certainly be based on $\forall$-introduction, so the first words of your proof will usually be "Given $x \in X$, . . . ".
- If you have $\forall x, \mathcal{A}(x)$, and it might be helpful to know $\mathcal{A}(c)$ (for some constant c), then you could use $\forall$-elimination.

8B. Some proofs about sets

Students of mathematics are expected to be able to *prove* assertions about unions and intersections. Before giving some examples of this, we should say a few words about how definitions are used in proofs.

> Any term that has been defined may be interchanged with its definition at any point in a proof.

EXAMPLE 8.15. Suppose, for the sake of argument, that we agree to

define a dog as an animal with a tail, that barks.

Then if the assertion "Matt is a dog" appears in a proof, we can say, "By definition (of dog), Matt is an animal with a tail, that barks." The &-elimination rule then justifies any of the assertions, "Matt is an animal," "Matt has a tail," and "Matt barks." Likewise, if the assertion "A coyote is an animal with a tail, that barks" appears in a proof, we are justified in asserting, "By definition (of dog), a coyote is a dog." While you might quarrel with this assertion, the fault lies in the definition that we have chosen, not in our logic. It is not acceptable to use any "facts" that you may believe you know about dogs, unless they are included in the definition, or can be deduced from given definitions and hypotheses. In this example, we cannot assert "By definition (of dog), Matt has a long tongue," because that was not part of our definition.

That example was rather silly, but here is an example that is more realistic:

EXAMPLE 8.16. The notation $A \subset B$ has been defined to mean $\forall a \in A, (a \in B)$. Therefore, if we know, say, that $X \subset Y$, then we can conclude $\forall x \in X, (x \in Y)$. Conversely, if we know $\forall h \in H, (h \in M)$, then we can conclude that $H \subset M$.

Now, here are some examples that show the quantifier introduction and elimination rules in action.

EXAMPLE 8.17. Suppose A and B are sets (and $\mathcal{U}$ is the universal set, as usual). Then

1) $A \cap B \subset A$,

2) $A \subset A \cup B$, and

3) $A \cap \mathcal{U} = A$.

PROOF. (1) We wish to show that every element of $A \cap B$ is an element of A. Given $x \in A \cap B$, we know, from the definition of $A \cap B$, that $x \in A$ and $x \in B$. In particular, $x \in A$, as desired.

(2) We wish to show that every element of A is an element of $A \cup B$. Given $x \in A$, it is obviously true that either $x \in A$ or $x \in B$ (since, in fact, we know $x \in A$). Therefore $x \in A \cup B$, as desired.

(3) From (1), we know that $A \cap \mathcal{U} \subset A$, so it suffices to show that $A \subset A \cap \mathcal{U}$. Given $a \in A$, we obviously have $a \in A$. Furthermore, since the universal set $\mathcal{U}$ contains every element that is under consideration, we also have $a \in \mathcal{U}$. Hence $a \in A \cap \mathcal{U}$, as desired. □

EXERCISES 8.18. Suppose A, B, and C are sets (and $\mathcal{U}$ is the universal set, as usual).

1) Show that if $A \subset B$ and $B \subset C$, then $A \subset C$.
2) Show $A \cap B \subset A \cup B$. [*Hint:* Use Example 8.17 for a very short proof.]
3) Show that if $A \subset B$, then $A \cap B = A$.
4) Show if $A \subset B$, then $A \cup B = B$.
5) Show that if $B \subset C$, then $A \cap B \subset A \cap C$.
6) Show that if $A \subset C$ and $B \subset C$, then $A \cup B \subset C$.
7) Show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
8) Show $A \setminus B = A \setminus (A \cap B)$.
9) Let $X = A \cap B$, and show $A \cup B = (A \setminus X) \cup (B \setminus X) \cup X$.
10) Show that if $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$, then either $A \subset B$ or $B \subset A$. [*Hint:* Prove the contrapositive. Choose $a \in A$ and $b \in B$, such that $a \notin B$ and $b \notin A$. Then $\{a, b\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.]

EXERCISES 8.19. Suppose A and B are sets.

1) Show $A \setminus B = A \cap \overline{B}$.
2) Show $A = (A \setminus B) \cup (A \cap B)$.
3) Prove De Morgan's Laws:
   (a) $\overline{\overline{A}} = A$.
   (b) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
   (c) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
4) Show that if $\overline{A} = \overline{B}$, then $A = B$.
   [*Hint:* Follows immediately from one of De Morgan's Laws.]

EXERCISES 8.20. Suppose A, B, and C are sets.

1) Show that A is disjoint from B if and only if $A \subset \overline{B}$.
2) Show $A \setminus B$ is disjoint from B.
3) Show that if A is disjoint from B, and C is a subset of B, then A is disjoint from C.
4) Show that $A \setminus B$ is disjoint from $A \cap B$.
5) Show that A is disjoint from $B \cup C$ iff A is disjoint from both B and C.

EXERCISES 8.21.
1) Show $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$.
2) Show the three sets $A \setminus B$, $B \setminus A$, and $A \cap B$ are all disjoint from each other.

Here are some examples of proofs involving Cartesian products.

EXAMPLE 8.22. If A and B are nonempty sets, and $A \times B = B \times A$, then $A = B$.

PROOF. Assume A and B are nonempty sets, such that $A \times B = B \times A$. It suffices to show $A \subset B$ and $B \subset A$. By symmetry, we need only show $A \subset B$.

Given $a_0 \in A$. Since B is nonempty, there exists some $b_0 \in B$. Then

$$(a_0, b_0) \in A \times B = B \times A = \{\, (b, a) \mid b \in B, a \in A \,\},$$

so there exist $b \in B$ and $a \in A$, such that $(a_0, b_0) = (b, a)$. Therefore, $a_0 = b$ (and $b_0 = a$, but we do not need that fact). Hence $a_0 = b \in B$. □

EXAMPLE 8.23. If B is disjoint from C, then $A \times B$ is disjoint from $A \times C$.

PROOF. We prove the contrapositive: Assume $A \times B$ is *not* disjoint from $A \times C$, and we will show B is *not* disjoint from C.

By assumption, the intersection of $A \times B$ and $A \times C$ is not empty, so we may choose some

$$x \in (A \times B) \cap (A \times C).$$

Then:

- Since $x \in A \times B$, there exist $a_1 \in A$ and $b \in B$, such that $x = (a_1, b)$.
- Since $x \in A \times C$, there exist $a_2 \in A$ and $c \in C$, such that $x = (a_2, c)$.

Hence $(a_1, b) = x = (a_2, c)$, so $b = c$. Now $b \in B$ and $b = c \in C$, so $b \in B \cap C$. Therefore $B \cap C \neq \emptyset$, so, as desired, B and C are *not* disjoint. □

WARNING. In the proof above, the single variable x was used to represent an ordered pair (a, b). There is nothing wrong with this: a variable can represent anything at all. However, this can be a source of confusion.

EXERCISES 8.24.

1) Suppose A, B, and C are sets.
   (a) Show that if $B \subset C$, then $A \times B \subset A \times C$.
   (b) Show that if $A \times B = A \times C$, and $A \neq \emptyset$, then $B = C$.

2) Suppose A is a set.
   (a) Show $A \times \emptyset = \emptyset$.
   (b) Show $A \times A = \emptyset$ if and only if $A = \emptyset$.

3) Show that $\times$ distributes over $\cup$. That is, for all sets A, B, and C, we have
   (a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$, and
   (b) $(B \cup C) \times A = (B \times A) \cup (C \times A)$.

4) Show that $\times$ distributes over $\cap$. That is, for all sets A, B, and C, we have
   (a) $A \times (B \cap C) = (A \times B) \cap (A \times C)$, and
   (b) $(B \cap C) \times A = (B \times A) \cap (C \times A)$.

We have been discussing proofs in this chapter, but you should keep in mind that counterexamples are also an important part of logic:

To show that a deduction is valid, provide a proof.
To show that a deduction is *not* valid, provide a counterexample.

EXERCISES 8.25. Determine whether each of the following deductions is valid, and justify your answer by giving a proof or a counterexample.

1) $\exists u \in U, (u \notin V), \ \therefore \ \forall u \in U, (u \notin V)$.

2) $\forall x, \big((x \in S) \Rightarrow (1 \in T)\big), \quad S \neq \emptyset, \quad \therefore \ 1 \in T$.

3) $\forall a \in A, (a \in B), \quad \forall b \in B, (b \in C), \quad \therefore \ \forall a \in A, (a \in C)$.

4) $D \cup E \neq \emptyset, \quad D \subset F, \quad \therefore \ D \cap F \neq \emptyset$.

5) $\forall a_1 \in A, \forall a_2 \in A, \big((a_1 \ R \ a_2) \vee (a_2 \ R \ a_1)\big), \quad 2 \in A, \quad \therefore \ 2 \ R \ 2$.

6) $(M \neq \emptyset) \Rightarrow (N \neq \emptyset), \quad N = \emptyset, \quad \therefore \ \forall x, (x \notin M)$.

7) $\exists x, \big((x \in P) \ \& \ (x \notin Q)\big), \quad \therefore \ \forall x, \big((x \in P) \Rightarrow (x \notin Q)\big)$.

8) $\forall x \in X, \exists y \in Y, (x \ R \ y), \quad \therefore \ \exists y \in Y, \forall x \in X, (x \ R \ y)$

9) $\exists y, \forall x, (x \ R \ y), \quad \therefore \ \forall x, \exists y, (x \ R \ y)$

8C. Theorems, Propositions, Corollaries, and Lemmas

Mathematicians use a number of different names for assertions that can be proved. Sometimes they are called theorems, but other names are also used. In addition to "theorem," the names most commonly used are "lemma," "proposition," and "corollary." There are no hard-and-fast rules for which name to use when, but here are some guidelines.

- A **theorem** is generally a result that the author believes to be important. A theorem may be given a special name, for ease of reference. Often, important theorems are named after the mathematician who first proved them, for example "Hall's Theorem." Sometimes theorems are given names that relate to their content or importance, for example "the Fundamental Theorem of Calculus."
- A **proposition** is a minor theorem. In text books, mathematicians employ the term "proposition" to refer to some result that they do not think is sufficiently important to be called a theorem.
- A **corollary** is a result that can be proved very easily from some other result.
- A **lemma** is generally a minor result that is being used as a stepping stone for proving a more significant result (a theorem, usually). Mathematicians will separate a lemma from the main proof of a theorem either because the proof is long and complicated and needs to be broken down into smaller steps, or because it is a step that needs to be performed repeatedly. It is much easier and clearer to refer to a lemma multiple times, than to either include the reasoning repeatedly, or refer back to an earlier portion of a single long proof.

  Like "theorem," "lemma" is a word that was originally Greek, although it was also adopted into Latin. Although the English plural "lemmas" is quite acceptable, some mathematicians prefer the original plural form of the word, "lemmata."

The results in this chapter have all been called "theorems," but this should not be taken as an indication of their importance. Now that we have introduced this terminology, all of these results should have been called "propositions." In each case, the result was being proven to demonstrate a proof technique, rather than for any value in the statement of the result itself.

SUMMARY:

- Rules for quantifiers were introduced. For each quantifier ($\forall$ and $\exists$) there are introduction and elimination rules.
- The use of definitions in a proof was explained.
- Theorems, lemmas, propositions, and corollaries are all names used for assertions that are being, or have been, proved. Each term is used differently; these differences were discussed.

Part III

Functions

Chapter 9

Functions

It is the pervading law of all things ... that form ever follows function. This is the law.

Louis Sullivan (1856–1924), American architect
The tall office building artistically considered

9A. Informal introduction to functions

You have seen many examples of functions in your previous math classes. Most of these were probably given by formulas (such as $f(x) = x^3$), but functions can also be given in other ways. The key property of a function is that it accepts inputs, and provides a corresponding output value for each possible input.

EXAMPLE 9.1. For the function $f(x) = x^3$, the input x can be any real number. Plugging a value for x into the formula yields an output value, which is also a real number. For example, using $x = 2$ as the input yields the output value $f(2) = 2^3 = 8$.

DEFINITION 9.2 (unofficial). Suppose f is any function.

1) The set of allowable inputs of f is called the **domain** of f.
2) If A is the domain of f, and B is any set that contains all of the possible outputs of f, then we say that f is a **function from** A **to** B. In the case of the function $f(x) = x^3$, we may take A and B to both be the set of real numbers; thus, f is a function from $\mathbb{R}$ to $\mathbb{R}$.

EXAMPLE 9.3. $g(x) = 1/x$ is *not* a function from $\mathbb{R}$ to $\mathbb{R}$. This is because 0 is an element of $\mathbb{R}$, but the formula does not define a value for $g(0)$. Thus, 0 cannot be in the domain of g. To correct this problem, one could say that g is a function from the set $\{ x \in \mathbb{R} \mid x \neq 0 \}$ of *nonzero* real numbers, to $\mathbb{R}$.

Intuitively, a function from A to B can be thought of being any process that accepts inputs from the set A, and assigns an element of the set B to each of these inputs. The process need not be given by a formula. Indeed, most of the functions that arise in science or in everyday life are not given by any formula.

EXAMPLE 9.4.

1) Each point on the surface of the earth has a particular temperature right now, and the temperature (in degrees centigrade) is a real number. Thus, temperature defines a function temp from the surface of the earth to $\mathbb{R}$: $\mathsf{temp}(x)$ is the temperature at the point x.

2) The items in a grocery store each have a particular price, which is a certain number of cents, so price can be thought of as a function from the set of items for sale to the set $\mathbb{N}$ of all natural numbers: $\mathsf{price}(x)$ is the price of item x (in cents).

3) If we let People be the set of all people (alive or dead), then mother is a function from People to People. For example,

$$\mathsf{mother}(\text{Prince Charles}) = \text{Queen Elizabeth}.$$

(To avoid ambiguity, we need to say that, by "mother," we mean "biological mother.")

4) In contrast, grandmother is *not* a function from People to People. This is because people have not just one grandmother, but two (a maternal grandmother and a paternal grandmother). For example, if we say that Prince Charles wrote a poem for his grandmother, we do not know whether he wrote the poem for the Queen Mother, or for his other grandmother. A function is not ever allowed to have such an ambiguity. (In technical terms, grandmother is a "relation," not a function. This will be explained in section 18A.)

Functions are often given by a *table* of values.

EXAMPLE 9.5. The list of prices in a store is an example of this:

item	price (in cents)
apple	65
banana	83
cherry	7
donut	99
eggs	155

In this example:

- The domain of price is $\{\mathsf{apple}, \mathsf{banana}, \mathsf{cherry}, \mathsf{donut}, \mathsf{eggs}\}$.
- $\mathsf{price}(\mathsf{banana}) = 83$.
- $\mathsf{price}(\mathsf{guava})$ does not exist, because guava is not in the domain of the function.

Instead of making a table, mathematicians prefer to represent each row of the table by an ordered pair. For example, the first row of the table is apple | 65. This has apple on the left and 65 on the right, so we represent it by the ordered pair $(\mathsf{apple}, 65)$, which has apple on the left and 65 on the right. The second row is represented by $(\mathsf{banana}, 83)$. Continuing in this way yields a total of 5 ordered pairs (one for each row). To keep them gathered together, a mathematician puts them into a set. Thus, instead of writing a table, a mathematician would represent this function as:

$$\big\{\, (\mathsf{apple}, 65), (\mathsf{banana}, 83), (\mathsf{cherry}, 7), (\mathsf{donut}, 99), (\mathsf{eggs}, 155) \,\big\}.$$

The set of ordered pairs contains exactly the same information as a table of values, but the set is a more convenient form for mathematical manipulations.

EXERCISE 9.6. Here is a function f given by a table of values.

x	$f(x)$
1	7
2	3
3	2
4	4
5	9

1) What is the domain of f?

2) What is $f(3)$?

3) Represent f as a set of ordered pairs.

4) Find a formula to represent f.
[*Hint:* There is a formula of the form $f(x) = ax^2 + bx + c$.]

EXAMPLE 9.7. Not every table of values represents a function. For example, suppose we have the following price list, which is a slight change from Example 9.5:

item	price (in cents)
apple	65
banana	83
cherry	7
donut	99
banana	155

There is a problem here, because there are two possible prices for a banana, depending on which line of the table is looked at. (So you might pick up a banana, expecting to pay 83 cents, and end up having the cashier charge you $1.55.) This is not allowed in a function: each input must have exactly one output, not a number of different possible outputs. Thus, if a table represents a function, and an item appears in the left side of more than one row, then all of those rows must have the same output listed on the right side.

Remark 9.8. A 2-column table represents a function from A to B if and only if:

1) every value that appears in the left column of the table is an element of A,

2) every value that appears in the right column of the table is an element of B,

3) every element of A appears in the left side of the table, and

4) no two rows of the table have the same left side, but different right sides.

EXERCISE 9.9. Let

- $A = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}\}$, and
- $B = \{1, 3, 5, 7, 9, 11\}$.

Which of the following sets of ordered pairs represent functions from A to B?

1) $\{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 5), (\mathsf{d}, 7), (\mathsf{e}, 9)\}$

2) $\{(\mathsf{a}, 1), (\mathsf{b}, 2), (\mathsf{c}, 3), (\mathsf{d}, 4), (\mathsf{e}, 5)\}$

3) $\{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 5), (\mathsf{d}, 3), (\mathsf{e}, 1)\}$

4) $\{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 5), (\mathsf{d}, 7), (\mathsf{e}, 9), (\mathsf{a}, 11)\}$

5) $\{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 5), (\mathsf{e}, 7)\}$

6) $\{(\mathsf{a}, 1), (\mathsf{b}, 1), (\mathsf{c}, 1), (\mathsf{d}, 1), (\mathsf{e}, 1)\}$

7) $\{(\mathsf{a}, \mathsf{a}), (\mathsf{b}, \mathsf{a}), (\mathsf{c}, \mathsf{a}), (\mathsf{d}, \mathsf{a}), (\mathsf{e}, \mathsf{a})\}$

8) $\{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 5), (\mathsf{d}, 5), (\mathsf{e}, 3), (\mathsf{a}, 1)\}$

9) $\{(1, \mathsf{a}), (3, \mathsf{a}), (5, \mathsf{a}), (7, \mathsf{a}), (9, \mathsf{a}), (11, \mathsf{a})\}$

10) $\{(\mathsf{c}, 1), (\mathsf{b}, 3), (\mathsf{e}, 5), (\mathsf{a}, 7), (\mathsf{d}, 9)\}$

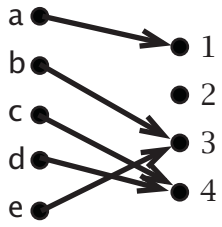
Remark 9.10. It is sometimes helpful to represent a function $f\colon A \to B$ by drawing an **arrow diagram**:

- a dot is drawn for each element of A and each element of B, and
- an arrow is drawn from a to $f(a)$, for each $a \in A$.

For example, suppose

- $A = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}, \mathsf{f}\}$,
- $B = \{1, 2, 3, 4\}$, and
- $f = \{(\mathsf{a}, 1), (\mathsf{b}, 3), (\mathsf{c}, 4), (\mathsf{d}, 4), (\mathsf{e}, 3)\}$.

Then the following picture is an arrow diagram of f:



Notice that:

1) There is exactly one arrow coming out of each element of A. This is true for the arrow diagram of any function.
2) There can be any number of arrows coming into each element of B (perhaps none, perhaps one, or perhaps many). The elements of B that do have arrows into them are precisely the elements of the range of f. In this example, the range of f is $\{1, 3, 4\}$.

9B. Official definition

The preceding section provided some intuition about how and why functions are represented as sets of ordered pairs, but it was not intended to be taken too literally. Here are the official definitions.

DEFINITION 9.11. Suppose A and B are sets.

1) A set f is a **function from** A **to** B if
   (a) each element of f is an ordered pair (a, b), such that $a \in A$ and $b \in B$, and
   (b) for each $a \in A$, there is a *unique* $b \in B$, such that $(a, b) \in f$.
2) If f is a function from A to B, then
   - A is called the **domain** of f, and
   - B is the **codomain** of f.
3) We write "$f\colon A \to B$" to denote that f is a function from A to B.

EXERCISE 9.12. We can express the definition of a function in First-Order Logic:

1) Translate the assertion of Defn. 9.11(1a) into First-Order Logic.
2) Translate the assertion of Defn. 9.11(1b) into First-Order Logic.

NOTATION 9.13. Suppose $f\colon A \to B$.

1) For $a \in A$, it is convenient to have a name for the element b of B, such that $(a, b) \in f$. The name we use is $f(a)$:

$$f(a) = b \text{ if and only if } (a, b) \in f.$$

2) Each element a of A provides us with an element $f(a)$ of B. The **range** of f is the set that collects together all of these elements $f(a)$. That is,

$$b \text{ is in the range of } f \text{ iff there is some } a \in A, \text{ such that } b = f(a).$$

The range can be denoted $\{ f(a) \mid a \in A \}$.

EXAMPLE 9.14. Suppose that the function f is defined by $f(x) = x^2$, on the domain $\{0, 1, 2, 4\}$. Then

1) to represent f as a set of ordered pairs, each element of the domain must appear exactly once as a first coordinate, with the corresponding output given in the second coordinate. Since there are four elements in the domain, there will be four ordered pairs: $\{(0, 0), (1, 1), (2, 4), (4, 16)\}$;
2) to give a table for f, we include one row for every element of the domain. The table will be:

n	$f(n)$
0	0
1	1
2	4
4	16

3) if we are asked what is $f(3)$, the answer is that $f(3)$ is *undefined*, because 3 is not in the domain of f. Even though we know that $3^2 = 9$, the formula we gave for f only applies to elements that are in the domain of f! It is not true that $f(3) = 9$;
4) the range of f is the set of possible outputs: in this case, $\{0, 1, 4, 16\}$;
5) if we are asked what is $f(2)$, the answer is $f(2) = 4$;
6) is f a function from $\{n \in \mathbb{N} \mid n \leq 4\}$ to $\{0, 1, 4, 16\}$? The answer is no, because the first set is $\{0, 1, 2, 3, 4\}$, which includes the value 3, but 3 is not in the domain of f.
7) is f a function from $\{0, 1, 2, 4\}$ to $\{n \in \mathbb{N} \mid n \leq 16\}$? The answer is yes; even though the second set has many values that are not in the range, it is a possible codomain for f. A codomain can be any set that contains all of the elements of the range.

EXERCISES 9.15.

1) The following table describes a certain function g.

n	$g(n)$
2	7
4	9
6	11
8	13
10	15

   (a) What is the domain of g?
   (b) What is the range of g?
   (c) What is $g(6)$?
   (d) What is $g(7)$?
   (e) Represent g as a set of ordered pairs.
   (f) Draw an arrow diagram to represent g.
   (g) Write down a formula that describes g. (Express $g(n)$ in terms of n.)

2) Suppose
   - f is a function whose domain is $\{0, 2, 4, 6\}$, and

- $f(x) = 4x - 5$, for every x in the domain.

Describe the function in each of the following ways:

(a) Make a table.

(b) Use ordered pairs.

(c) Draw an arrow diagram involving two sets.

3) Which of the following sets of ordered pairs are functions from $\{\mathsf{x}, \mathsf{y}, \mathsf{z}\}$ to $\{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}\}$?

- If it is such a function, then what is its range?
- If it is not such a function, then explain why not.

(a) $\{(\mathsf{y}, \mathsf{a}), (\mathsf{x}, \mathsf{b}), (\mathsf{y}, \mathsf{c})\}$

(b) $\{(\mathsf{y}, \mathsf{a}), (\mathsf{x}, \mathsf{b}), (\mathsf{z}, \mathsf{c})\}$

(c) $\{(\mathsf{y}, \mathsf{a}), (\mathsf{x}, \mathsf{c}), (\mathsf{z}, \mathsf{a})\}$

4) Which of the following are functions from $\{1, 2, 3\}$ to $\{\mathsf{w}, \mathsf{h}, \mathsf{o}\}$? (If it is not such a function, then explain why not.)

(a) $\{(1, \mathsf{w}), (1, \mathsf{h}), (1, \mathsf{o})\}$

(b) $\{(1, \mathsf{h}), (2, \mathsf{h}), (3, \mathsf{h})\}$

(c) $\{(1, \mathsf{h}), (2, \mathsf{o}), (3, \mathsf{w})\}$

(d) $\{(\mathsf{w}, 1), (\mathsf{h}, 2), (\mathsf{o}, 3)\}$

5) For the given sets A and B:

(i) Find all of the functions from A to B.
(Write each function as a set of ordered pairs.)
[*Hint:* You may assume, without proof, that if A has exactly m elements, and B has exactly n elements, then the number of functions from A to B is n^m. (Do you see why?)]

(ii) Find the range of each function.

(a) $A = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$, $B = \{\mathsf{d}\}$

(b) $A = \{\mathsf{a}, \mathsf{b}\}$, $B = \{\mathsf{c}, \mathsf{d}\}$

(c) $A = \{\mathsf{a}\}$, $B = \{\mathsf{b}, \mathsf{c}, \mathsf{d}\}$

(d) $A = \{\mathsf{a}, \mathsf{b}\}$, $B = \{\mathsf{c}, \mathsf{d}, \mathsf{e}\}$

SUMMARY:

- A function accepts inputs, and provides a single output for each input.
- Some ways of representing functions are:
  - a formula;
  - a table;
  - a set of ordered pairs;
  - an arrow diagram.
- Important definitions:
  - function
  - domain
  - codomain, range
- Notation:
  - $f\colon A \to B$
  - $f(a)$
  - $\{\, f(a) \mid a \in A \,\}$

Chapter 10

One-to-One Functions

To think logically the logically thinkable — that is the mathematician's aim.
Cassius Jackson Keyser (1862–1947), American mathematician
The Human Worth of Rigorous Thinking

We begin this chapter with an example.

EXAMPLE 10.1.

1) Suppose Inspector Thinkright knows two facts:
   (a) Alice is the thief's wife, and
   (b) Alice is Bob's wife.

   Then the Inspector can arrest Bob for theft, because a woman cannot be the wife of more than one man.
2) On the other hand, suppose the Inspector knows:
   (a) Alice is the forger's mother, and
   (b) Alice is Charlie's mother.

   Then the Inspector does not know enough to be sure who the forger is, because it could be some other child of Alice.

This example illustrates a fundamental difference between the wife function and the mother function: two different people can have the same mother, but only one person can have any particular person as their wife. (For example, if Bud and Charlie have the same wife, then "Bud" must be a nickname for Charlie.) In mathematical terms, this important property of the wife function is expressed by saying that the wife function is "one-to-one."

The notion is formalized in the following definition:

DEFINITION 10.2. Suppose $f\colon A \to B$. We say f is **one-to-one** iff, for all $a_1, a_2 \in A$, such that $f(a_1) = f(a_2)$, we have $a_1 = a_2$.

EXERCISE 10.3. Suppose $f\colon A \to B$. Translate the assertion that f is one-to-one into First-Order Logic.

Remark 10.4. If you have an arrow diagram of a function, then it is easy to tell whether or not the function is one-to-one. For example:

1) The function f of Figure 10.1(a) on page 118 is *not* one-to-one. This is because the arrow from b and the arrow from c go to the same place, so $f(\mathsf{b}) = f(\mathsf{c})$. In general, if arrows from two different elements of the domain go to the same element of the range, then the function is not one-to-one.

2) The function g of Figure 10.1(b) is one-to-one. This is because the arrows from two different elements of the domain never go to the same element of the range. In short, there is only *one* element of the domain that goes *to* any *one* element of the range. (This is the reason for the terminology "one-to-one." A function is "two-to-one" if there are two elements of the domain mapping to each element of the range, as is true of the function h in Figure 10.1(c).)

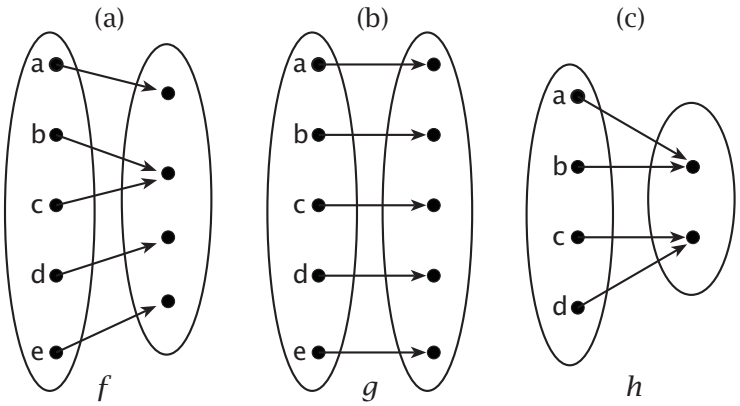


Figure 10.1. Arrow diagrams of three functions f, g, and h.

EXAMPLE 10.5. Without giving official proofs, let us determine which of the following functions are one-to-one.

1) $f\colon \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x + 1$.

This is one-to-one. For any real numbers x and y, $f(x) = f(y)$ means that $x+1 = y+1$. Subtracting 1 from both sides of the equation, we conclude that $x = y$ whenever $f(x) = f(y)$.

2) $g\colon \mathbb{R} \to \mathbb{R}$, defined by $g(x) = |x|$.

This is not one-to-one. We demonstrate this by finding two distinct real numbers whose image is the same:

$$g(1) = |1| = 1 = |-1| = g(-1),$$

but $1 \neq -1$. This shows that g is *not* one-to-one.

3) $f\colon \{1,2,3\} \to \{\mathsf{a},\mathsf{b},\mathsf{c}\}$ defined by $f = \{(1,b),(2,a),(3,a)\}$.

This is not one-to-one. We demonstrate this by finding two distinct values in $\{1,2,3\}$ whose image is the same:

$$f(2) = a = f(3),$$

but $2 \neq 3$. This shows that f is *not* one-to-one.

4) $h\colon \mathbb{N} \to \mathbb{N}$, defined by $h(x) = |x|$.

This is one-to-one. Since all natural numbers are nonnegative, we have $|x| = x$ for every natural number x. So if $h(x) = h(y)$, then

$$x = |x| = h(x) = h(y) = |y| = y,$$

making $x = y$.

These examples demonstrate the general pattern of how we prove whether or not a function is one-to-one. To prove that a function $f\colon A \to B$ *is* one-to-one, we need to demonstrate that for *every* $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$ then we must have $a_1 = a_2$. To prove that a function $f\colon A \to B$ is *not* one-to-one, we need only find a single pair of values $a_1, a_2 \in A$, for which $f(a_1) = f(a_2)$ but $a_1 \neq a_2$.

EXERCISES 10.6. *Explain why your answers are correct.*

1) Each formula defines a function from $\mathbb{R}$ to $\mathbb{R}$. Which of the functions are one-to-one?
   (a) $f(x) = 1$.
   (b) $g(x) = x$.
   (c) $h(x) = x^2$.
   (d) $i(x) = 3x + 2$.
   (e) $j(x) = 1/\big(|x| + 1\big)$.
2) Each of the following sets of ordered pairs is a function from $\{1, 2, 3, 4\}$ to $\{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}\}$. Which are one-to-one?
   (a) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{d}), (4, \mathsf{e})\}$
   (b) $g = \{(1, \mathsf{c}), (2, \mathsf{d}), (3, \mathsf{d}), (4, \mathsf{e})\}$
   (c) $h = \{(1, \mathsf{e}), (2, \mathsf{d}), (3, \mathsf{c}), (4, \mathsf{b})\}$
   (d) $i = \{(1, \mathsf{e}), (2, \mathsf{e}), (3, \mathsf{e}), (4, \mathsf{e})\}$
   (e) $j = \{(1, \mathsf{a}), (2, \mathsf{c}), (3, \mathsf{e}), (4, \mathsf{c})\}$
   (f) $k = \{(1, \mathsf{a}), (2, \mathsf{c}), (3, \mathsf{e}), (4, \mathsf{d})\}$

The fact that the wife function is one-to-one can be restated as the fact that two different people cannot have the same wife. In general, a function is one-to-one iff two different elements of the domain always map to two different elements of the range:

(10.7) A function $f\colon A \to B$ is one-to-one if and only if
$$\forall a_1, a_2 \in A, \big(a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)\big).$$

The notation $\forall a_1, a_2 \in A$ is short for $\forall a_1 \in A, \forall a_2 \in A$.

The assertion in this box can be justified with a proof. The implication $\Rightarrow$ is proved in the following theorem; the other direction is an exercise.

THEOREM 10.8. *If a function $f\colon A \to B$ is one-to-one, then*
$$\forall a_1, a_2 \in A, \big(a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)\big).$$

PROOF. Let $f\colon A \to B$ be one-to-one. Given $a_1, a_2 \in A$, we know, from the definition of one-to-one, that
$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$
So the contrapositive of this implication is also true. That is,
$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2).$$

EXERCISES 10.9.

1) Prove that if (10.7) holds, then f is one-to-one. (Assume $f\colon A \to B$.)
2) Give a proof to justify the following theorem: Suppose
   - $f\colon A \to B$,

- f is one-to-one,
- $g\colon B \to C$,
- g is one-to-one,
- $a_1, a_2 \in A$,
- $b_1, b_2 \in B$,
- $f(a_1) = b_1$,
- $f(a_2) = b_2$, and
- $g(b_1) = g(b_2)$.

Then $a_1 = a_2$.

We can also now provide formal proofs that particular functions are, or are not, one-to-one. Here is an example of a proof that a function is one-to-one.

PROPOSITION 10.10. *Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x/2 + 1$. Then f is one-to-one.*

Scratchwork. By definition, we wish to show $\forall a, b \in \mathbb{R}, \big(f(a) = f(b) \Rightarrow a = b\big)$. Thus, the proof will use $\forall$-introduction: the first words in the proof will be "Given $a, b \in \mathbb{R}$" (or other words to that effect). Then, because we wish to show $f(a) = f(b) \Rightarrow a = b$, we will assume $f(a) = f(b)$, and the proof will be complete as soon as we can prove $a = b$.

PROOF. Let $a, b \in \mathbb{R}$ be arbitrary. Suppose that $f(a) = f(b)$. This means that $a/2+1 = b/2+1$, by the definition of f. Subtracting 1 from both sides, we see that $a/2 = b/2$. Multiplying both sides by 2, we conclude that $a = b$. □

In some cases, when a function is not one-to-one, it is easy to find examples of distinct elements whose images are equal. In other cases, such examples may be hard to find. When we do not know whether or not a particular function is one-to-one, it may help to try proving that it *is* one-to-one. If the proof works, great! – we are done. If the proof fails, the manner in which it fails may help us find an example to show that the function is not one-to-one. Here is an example of this technique.

EXAMPLE 10.11. Let $f\colon \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = (n-1)^2$. Is f one-to-one?

Scratchwork. Let us try to prove that f is one-to-one, and see what happens. To do this, we start with arbitrary elements $m, n \in \mathbb{N}$, and suppose that $f(m) = f(n)$. By the definition of f, this means that $(m-1)^2 = (n-1)^2$. Two numbers have the same square, if and only if they are equal in absolute value, so we can conclude that $m - 1 = \pm(n-1)$. If $m - 1 = +(n-1)$ then adding 1 to each side, we get $m = n$, completing the proof. But if $m - 1 = -(n-1) = -n + 1$, then adding 1 to each side, we get $m = -n + 2$. Since $m, n \in \mathbb{N}$, it is not hard to see that if $n \geq 3$, then $-n + 2 \leq -3 + 2 = -1$, so $-n + 2$ is not a natural number, and these cases cannot arise. But if n is 0, 1, or 2, then $-n + 2$ is 2, 1, or 0 (respectively), all of which are natural numbers. If $n = 1$ then $m = -n + 2 = 1 = n$, so this case is not a problem. But if $m = 2$ and $n = 0$, then $(m-1)^2 = 1^2 = (-1)^2 = (n-1)^2$, so $f(m) = f(n)$ even though $m \neq n$. (We could also choose $m = 0$ and $n = 2$.) This is the example that shows that f is *not* one-to-one.

SOLUTION. f is *not* one-to-one.

To prove this, let $m = 0$ and $n = 2$. Then

$$f(m) = f(0) = (0-1)^2 = 1$$

and

$$f(n) = f(2) = (2-1)^2 = 1,$$

so $f(m) = f(n)$. On the other hand, we also have $m = 0 \neq 2 = n$, so $m \neq n$. Since $f(m) = f(n)$ and $m \neq n$, we know that f is not one-to-one. □

EXERCISES 10.12. For each function, either prove that it is one-to-one, or prove that it is not.

1) $f\colon \mathbb{Q} \to \mathbb{Q}$ defined by $f(x) = 3x/5 - 2$.

2) $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$.

3) $g\colon \mathbb{R} \to \mathbb{R}$ defined by $g(x) = |(x + 1)/2|$.

Remark 10.13 (alternative terminology). Many mathematicians use the word "*injective*," rather than "one-to-one." (This comes from French.) Also, a function that is one-to-one can be called an *injection*.

SUMMARY:

- Important definitions:
  - one-to-one
- Notation:
  - $\forall a_1, a_2 \in A$ means $\forall a_1 \in A, \forall a_2 \in A$.

Chapter 11

Onto Functions

There are two ways to do great mathematics. The first way is to be smarter than everybody else. The second way is to be stupider than everybody else – but persistent.

Rauol Bott (1923–2005), Harvard mathematician

11A. Concept and definition

In an arrow diagram of a function $f\colon A \to B$, the definition of a function requires that there is exactly one arrow out of each element of A, but it says nothing about the number of arrows into each element of B. There may be elements of B with lots of arrows into them (unless the function is one-to-one), and there may be other elements of B that have no arrows into them. The function is called "onto" if all of the elements of B are hit by arrows; none are missed.

EXAMPLE 11.1. Figure 11.1 shows arrow diagrams of various functions, some onto and some not.

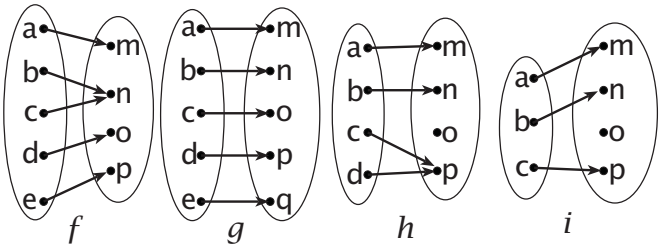


Figure 11.1. Function f is onto, but not one-to-one.
Function g is both one-to-one and onto.
Function h is neither one-to-one nor onto.
Function i is one-to-one, but not onto.

EXAMPLE 11.2. Not every woman is a mother. This means that if you draw an arrow from each person to his or her mother, there will be some women who have no arrows into them. So the function

$$\text{mother}\colon \text{People} \to \text{Women}$$

is *not* onto.

The following official definition of "onto" formalizes the ideas described above.

DEFINITION 11.3. Suppose $f\colon A \to B$. We say f is **onto** if, for all $b \in B$, there is some $a \in A$, such that $f(a) = b$.

EXERCISES 11.4. Suppose $f\colon A \to B$. Translate each of the following assertions into First-Order Logic:

1) f is onto.

2) f is *not* onto. (Simplify your answer, so $\neg$ is applied only to predicates.)

EXAMPLE 11.5. Without giving formal proofs, let us determine which of the following functions are onto.

1) $f\colon \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x + 1$.
   This is onto. For any real number y, $f(x) = y$ means that $x + 1 = y$. Subtracting 1 from both sides of the equation, we conclude that for any real number y, if $x = y - 1$, then $f(x) = y$.

2) $g\colon \mathbb{R} \to \mathbb{R}$, defined by $g(x) = |x|$.
   This is not onto. We demonstrate this by finding a real number that is not mapped onto. The number -1 is one such: we can never have $|x| = -1$ for any real number x. This shows that g is *not* onto.

3) $f\colon \{1, 2, 3\} \to \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$ defined by $f = \{(1, b), (2, a), (3, a)\}$.
   This is not onto. We need only notice that c never appears as an image of this function. This shows that f is *not* onto.

4) $h\colon \mathbb{N} \to \mathbb{N}$, defined by $h(x) = |x|$.
   This is onto. Since all natural numbers are nonnegative, we have $h(x) = |x| = x$ for every natural number x. So if $x = y$, then $|x| = x = y$, making $h(x) = y$.

11B. How to prove that a function is onto

Let us see how to prove that a function $f\colon A \to B$ is onto. By definition, we wish to show:

$$\text{for all } b \in B, \text{ there is some } a \in A, \text{ such that } f(a) = b.$$

In other words: "$\forall b \in B, \exists a \in A, \big(f(a) = b\big)$."

The first quantifier is $\forall$; we are required to prove something about every element of B. Hence, we use $\forall$-introduction, so our proof should start with the sentence "Let b be an arbitrary element of B." (However, this can be abbreviated to: "Given $b \in B$, ...") After this, our task will be to prove "$\exists a \in A, \big(f(a) = b\big)$."

At this point, the quantifier that concerns us is $\exists$; we are required to prove that some element of A has a certain property. The tool to use for this is $\exists$-introduction: we find (or "construct") an appropriate element of A, and then verify that it does what it is supposed to. Thus, the next step in the proof is "Let a = ???" (where ??? needs to be replaced with an appropriate expression). Then all that remains is to verify that the value we assigned to a does the job it is required to do: calculate that $f(a)$ is indeed equal to b.

So here what a typical "onto" proof looks like:

$$\text{Given } b \in B, \text{ let } a = \boxed{}. \text{ Then } f(a) = \cdots = b.$$

An appropriate value for a needs to be put in the box (probably a formula that depends on b), and the dots need to be filled in with a calculation that shows the value of $f(a)$ is b. (Also, of course, some of the letters will need to be changed if the name of the function is not f, or if the sets are not called A and B.)

EXAMPLE 11.6. Define $g\colon \mathbb{R} \to \mathbb{R}$ by $g(x) = 5x - 2$. Show g is onto.

Scratchwork. We wish to show $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, \big(g(x) = y\big)$. By $\forall$-introduction, the first sentence of the proof is easy: "Given $y \in \mathbb{R}$." Then we need to find a value of x that makes $g(x) = y$. The appropriate value of x is probably not obvious, so we need to do some scratchwork. We postulate the desired equation $g(x) = y$ and use algebra to solve it:

$$\begin{aligned} g(x) &= y \\ 5x - 2 &= y \\ 5x &= y + 2 \\ x &= \frac{y+2}{5} \end{aligned}$$

This scratchwork is necessary background, but it is not to be included in the actual proof.

PROOF. Given $y \in \mathbb{R}$, let $x = (y+2)/5 \in \mathbb{R}$. Then

$$g(x) = 5x - 2 = 5\left(\frac{y+2}{5}\right) - 2 = (y+2) - 2 = y.$$

Remark 11.7. Some "onto" proofs are a bit more complicated than what is described above, because it may not be possible to go directly from "Given $b \in B$" to "let $a = \boxed{}$." Sometimes it is necessary to insert calculations (or other explanations) between "given b" and "let a." Some good examples of this will be seen in Exercise 14.8.

Remark 11.8 (alternative terminology). Some mathematicians use the word "*surjective*," rather than "onto." (Like "injective" in place of "one-to-one," this comes from French.) Also, a function that is onto can be called a *surjection*.

EXERCISES 11.9.

1) Each formula defines a function from $\mathbb{R}$ to $\mathbb{R}$. Which of the functions are onto? *Prove that your answers are correct.*
   (a) $a(x) = 1$.
   (b) $b(x) = x$.
   (c) $c(x) = x^2$.
   (d) $d(x) = 3x + 2$.
   (e) $e(x) = 1/\big(|x| + 1\big)$.
   (f) $f(x) = 4x - 6$.
   (g) $g(x) = \sqrt[3]{x+5} - 5$.
2) Each of the following sets of ordered pairs is a function from $\{1,2,3,4,5\}$ to $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$. Which of the functions are onto? *Briefly justify your answers.*
   (a) $a = \{(1,\clubsuit), (2,\diamondsuit), (3,\heartsuit), (4,\spadesuit), (5,\clubsuit)\}$
   (b) $b = \{(1,\clubsuit), (2,\heartsuit), (3,\clubsuit), (4,\heartsuit), (5,\clubsuit)\}$
   (c) $c = \{(1,\heartsuit), (2,\heartsuit), (3,\heartsuit), (4,\heartsuit), (5,\heartsuit)\}$
   (d) $d = \{(1,\diamondsuit), (2,\spadesuit), (3,\heartsuit), (4,\spadesuit), (5,\clubsuit)\}$
   (e) $e = \{(1,\clubsuit), (2,\spadesuit), (3,\heartsuit), (4,\spadesuit), (5,\clubsuit)\}$
3) Suppose $f\colon A \to B$. Show that f is onto if and only if the range of f is B.

EXERCISE 11.10. Define functions f and g from $\mathbb{R}$ to $\mathbb{R}$ by:

$$f(x) = \begin{cases} 1/x & \text{if } x > 0 \\ x+1 & \text{if } x \leq 0 \end{cases}$$

and

$$g(x) = \begin{cases} 1/x & \text{if } x > 0 \\ x-1 & \text{if } x \leq 0. \end{cases}$$

Show:

1) f is onto;

2) g is not onto;

3) f is not one-to-one; and

4) g is one-to-one.

11C. Image and pre-image

DEFINITION 11.11. Suppose $f\colon A \to B$.

1) For any subset A_1 of A, the **image** of A_1 under f is

$$f(A_1) = \left\{ f(a) \;\middle|\; a \in A_1 \right\}.$$

It is a subset of B.

2) For any subset B_1 of B, the **pre-image** (or **inverse image**) of B_1 under f is

$$f^{-1}(B_1) = \left\{ a \in A \;\middle|\; f(a) \in B_1 \right\}.$$

It is a subset of A. When $B_1 = \{b\}$ has only one element, we usually write $f^{-1}(b)$, instead of $f^{-1}\big(\{b\}\big)$.

EXAMPLE 11.12.

1) For the function $\mathsf{mother}\colon \mathsf{PEOPLE} \to \mathsf{WOMEN}$, $\mathsf{mother}^{-1}(m)$ is the set of all children of m.

2) For the function $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$:

(a) We have $f^{-1}(4) = \{2, -2\}$, because 2 and -2 are all of the square roots of 4.

(b) We have $f^{-1}\big([-4, 4]\big) = [-2, 2]$, because $-4 \leq x^2 \leq 4$ iff $-2 \leq x \leq 2$.

WARNING. The fact that we write $f^{-1}(B_1)$ does not imply that f^{-1} is a function. This is simply a notation that refers to the set we have defined.

Here are examples of proofs involving inverse images:

EXAMPLE 11.13. Suppose $f\colon A \to B$ and $B_1 \subset B$.

1) We have $f\big(f^{-1}(B_1)\big) \subset B_1$.

2) If f is onto, then $f\big(f^{-1}(B_1)\big) = B_1$.

PROOF. (1) Let $b \in f\big(f^{-1}(B_1)\big)$. By definition, we have

$$f\big(f^{-1}(B_1)\big) = \left\{ f(a) \;\middle|\; a \in f^{-1}(B_1) \right\},$$

so we must have $b = f(a_1)$, for some $a_1 \in f^{-1}(B_1)$. From the definition of $f^{-1}(B_1)$, we know that $f(a_1) \in B_1$. Therefore $b = f(a_1) \in B_1$. Since b is an arbitrary element of $f\big(f^{-1}(B_1)\big)$, this implies that $f\big(f^{-1}(B_1)\big) \subset B_1$, as desired.

(2) Assume f is onto. We know, from (1), that $f\big(f^{-1}(B_1)\big) \subset B_1$, so it suffices to show that $B_1 \subset f\big(f^{-1}(B_1)\big)$.

Let $b \in B_1$ be arbitrary. Because f is onto, we know there exists $a_1 \in A$, such that $f(a_1) = b$. Then $f(a_1) = b \in B_1$, so $a_1 \in f^{-1}(B_1)$. Therefore

$$f(a_1) \in \big\{\, f(a) \;\big|\; a \in f^{-1}(B_1) \,\big\} = f\big(f^{-1}(B_1)\big).$$

Since $f(a_1) = b$, we conclude that $b \in f\big(f^{-1}(B_1)\big)$. □

EXERCISES 11.14. Suppose that $f\colon A \to B$, that $A_1 \subset A$, and that $B_1 \subset B$.

1) Show that if $A_2 \subset A_1$, then $f(A_2) \subset f(A_1)$.

2) Show that if $B_2 \subset B_1$, then $f^{-1}(B_2) \subset f^{-1}(B_1)$.

3) Show $A_1 \subset f^{-1}\big(f(A_1)\big)$.

4) Show that if f is one-to-one, then $A_1 = f^{-1}\big(f(A_1)\big)$.

5) Show $f\Big(f^{-1}\big(f(A_1)\big)\Big) = f(A_1)$.

SUMMARY:

- Important definitions:
  - onto
  - image, pre-image
- Notation:
  - $f(A_1)$, $f^{-1}(B_1)$

Chapter 12

Bijections

> *"How dreadful!" cried Lord Henry. "I can stand brute force, but brute reason is quite unbearable. There is something unfair about its use. It is hitting below the intellect."*
>
> Oscar Wilde (1854–1900), Irish author
> *The Picture of Dorian Gray*

The best functions are both one-to-one *and* onto. These are called "bijections" or "one-to-one correspondences."

DEFINITION 12.1. A function is a **bijection** if and only if it is both one-to-one and onto.

Remark 12.2. You may recall that a one-to-one function may be called an "injection," and an onto function may be called a "surjection." The term "bijection" comes from having both of these properties.

EXAMPLE 12.3. Consider a hypothetical country Married, in which

- everyone is married (to only one person — there is no polygamy!), and
- every marriage is between a man and a woman (there are no same-sex marriages).

Let

- Men be the set of men in the country, and
- Women be the set of women in the country.

Then wife: Men → Women is a bijection:

- Two different men cannot have the same wife, so we know that wife is one-to-one.
- Every woman is the wife of some man (because everyone is married), so wife is also onto.

Similarly, the function husband: Women → Men is also a bijection.

Remark 12.4. In the country Married described above, it is clear that the number of men is exactly equal to the number of women. (If there were more men than women, then not every man could have a wife; if there were more women than men, then not every women could have a husband.) This is an example of the following important principle that will be discussed in the later chapters on "cardinality": *If there is a **bijection** from A to B, then the two sets A and B must have exactly the same number of elements.* Finding a bijection is the most common way to show two sets have the same number of elements.

Remark 12.5. Showing that a function is a bijection requires two things: showing that the function is one-to-one, and showing that the function is onto. So a proof that a function is a bijection will (usually) have two parts:

1) Show that the function is one-to-one.

2) Show that the function is onto.

The two parts can come in either order: it is perfectly acceptable to first prove that the function is onto, and then prove that it is one-to-one.

EXAMPLE 12.6. *Define $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = 5x - 7$. Then f is a bijection.*

PROOF. It suffices to show that f is both one-to-one and onto.

(one-to-one) Given $x_1, x_2 \in \mathbb{R}$, such that $f(x_1) = f(x_2)$, we have

$$x_1 = \frac{(5x_1 - 7) + 7}{5} = \frac{f(x_1) + 7}{5} = \frac{f(x_2) + 7}{5} = \frac{(5x_2 - 7) + 7}{5} = x_2.$$

So f is one-to-one.

(onto) Given $y \in \mathbb{R}$, let $x = (y + 7)/5$. Then

$$f(x) = 5x - 7 = 5\left(\frac{y + 7}{5}\right) - 7 = (y + 7) - 7 = y.$$

So f is onto.

Since f is both one-to-one and onto, we conclude that f is a bijection. □

EXERCISE 12.7. Each formula defines a function from $\mathbb{R}$ to $\mathbb{R}$. Show that the function is a bijection.

1) $a(x) = 5x + 2$

2) $b(x) = 2x - 5$

3) $c(x) = 12x - 15$

4) $d(x) = -15x - 12$

5) $e(x) = x^3$

6) $f(x) = \sqrt[3]{x - 4}$

EXERCISE 12.8. Each formula defines a function from $\mathbb{R}$ to $\mathbb{R}$. Which of the functions are bijections? *Show that your answers are correct.*

1) $a(x) = 1$.

2) $b(x) = x$.

3) $c(x) = x^2$.

4) $d(x) = 3x + 2$.

5) $e(x) = 1/\big(|x| + 1\big)$.

6) $f(x) = 4x - 6$.

7) $g(x) = \sqrt[3]{x} - 5$.

8) $h(x) = \sqrt{x^2 + 1}$

EXERCISE 12.9. Let $a, b \in \mathbb{R}$, and define $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = ax + b$.

1) Show that if $a \neq 0$, then f is a bijection.

2) Show that if $a = 0$, then f is *not* a bijection.

EXERCISE 12.10. Suppose $f\colon A \to B$ and $g\colon B \to C$.

1) Show that if f and g are bijections, then $g \circ f$ is a bijection.

2) Show that if f and $g \circ f$ are bijections, then g is a bijection.

3) Show that if g and $g \circ f$ are bijections, then f is a bijection.

EXERCISE 12.11. Suppose

- $f\colon A \to B$,
- $g\colon B \to A$,
- $(g \circ f)(a) = a$, for every $a \in A$, and
- $(f \circ g)(b) = b$, for every $b \in B$.

Show that f is a bijection.

EXERCISE 12.12. Suppose $f\colon A \to B$. Show f is a bijection if and only if, for each $b \in B$, there is a *unique* $a \in A$, such that $f(a) = b$. In other words, f is a bijection if and only if

$$\forall b \in B, \exists!\, a \in A, \big(f(a) = b\big).$$

EXERCISES 12.13. 1) Define $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(m,n) = m^2 + n$.

(a) Show that f is onto.

(b) Show that f is *not* one-to-one.

2) Define $g\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $g(m,n) = (m+n, m-n)$.

(a) Show that g is *not* onto.

(b) Show that g is one-to-one.

Remark 12.14. Officially, $\times$ is *not* associative, because

$$(A \times B) \times C = \{\, \big((a,b),c\big) \mid a \in A, b \in B, c \in C \,\}$$

and

$$A \times (B \times C) = \{\, \big(a,(b,c)\big) \mid a \in A, b \in B, c \in C \,\}.$$

are (usually) not the same sets: an element of $(A \times B) \times C$ must have an ordered pair (a,b) as its first coordinate, whereas an element of $A \times (B \times C)$ can have any element of A as its first coordinate.

EXERCISE 12.15. Suppose A, B, and C are sets. Define

$$f\colon (A \times B) \times C \to A \times (B \times C) \quad \text{by} \quad f\big((a,b),c\big) = \big(a,(b,c)\big).$$

Show that f is a bijection.

Remark 12.16. One can define the Cartesian product of more than two sets. For example,

$$A \times B \times C = \{\, (a,b,c) \mid a \in A, b \in B, c \in C \,\}.$$

Although $A \times B \times C$ is not the same as $(A \times B) \times C$ or $A \times (B \times C)$, the difference between them can often be ignored in practice.

SUMMARY:

- Important definitions:
  - bijection

Chapter 13

Inverse Functions

Backwards poets write inverse.

Author unknown

All students of mathematics have experience with solving an equation for x. Inverse functions are a special case of this.

EXAMPLE 13.1. In Example 12.6, it was shown that $f(x) = 5x - 7$ is a bijection. A quick look at the proof reveals that the formula

$$\frac{y+7}{5}$$

plays a key role (sometimes with y replaced by $f(x_1)$ or $f(x_2)$). The reason this formula is so important is that (solving for x) we have

$$y = 5x - 7 \qquad \Leftrightarrow \qquad x = \frac{y+7}{5}.$$

In order to see this as an "inverse function," we translate into the language of functions, by letting $g\colon \mathbb{R} \to \mathbb{R}$ be defined by $g(y) = (y+7)/5$. Then the above assertion can be restated as:

(13.2)
$$y = f(x) \qquad \Leftrightarrow \qquad x = g(y).$$

This tells us that g does exactly the opposite of what f does: if f takes x to y, then g takes y to x. We will say that g is the "inverse" of f.

The following exercise provides a restatement of (13.2) that will be used in the official definition of inverse functions.

EXERCISE 13.3. Suppose $f\colon X \to Y$ and $g\colon Y \to X$. Show that if

$$\forall x \in X, \forall y \in Y, \big(y = f(x) \Leftrightarrow x = g(y)\big),$$

then

a) $f\big(g(y)\big) = y$ for all $y \in Y$, and

b) $g\big(f(x)\big) = x$ for all $x \in X$.

DEFINITION 13.4. Suppose

- $f\colon X \to Y$, and
- $g\colon Y \to X$,

We say that g is the **inverse** of f if and only if:

a) $f\big(g(y)\big) = y$ for all $y \in Y$, and

b) $g\big(f(x)\big) = x$ for all $x \in X$.

NOTATION 13.5. The inverse of f is denoted f^{-1}.

EXAMPLE 13.6. Because

- the husband of the wife of any married man is the man himself, i.e.,

$$\mathsf{husband}\big(\mathsf{wife}(y)\big) = y,$$

and

- the wife of the husband of any married woman is the woman herself, i.e.,

$$\mathsf{wife}\big(\mathsf{husband}(x)\big) = x,$$

the wife function is the inverse of the husband function. That is, $\mathsf{husband}^{-1} = \mathsf{wife}$.

EXERCISES 13.7. In each case, verify that g is the inverse of f.

1) $f\colon \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = 9x - 6$ and
   $g\colon \mathbb{R} \to \mathbb{R}$ is defined by $g(x) = (x + 6)/9$.
2) $f\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $f(x) = x^2$ and
   $g\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $g(x) = \sqrt{x}$.
3) $f\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $f(x) = 1/x$ and
   $g\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $g(x) = 1/x$.
4) $f\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $f(x) = \sqrt{x+1} - 1$ and
   $g\colon \mathbb{R}^+ \to \mathbb{R}^+$ is defined by $g(x) = x^2 + 2x$.

Most functions do *not* have an inverse. In fact, only bijections have an inverse:

THEOREM 13.8. *Suppose $f\colon X \to Y$. If f has an inverse $f^{-1}\colon Y \to X$, then f is a bijection.*

PROOF. Assume there is a function $f^{-1}\colon Y \to X$ that is an inverse of f. Then

1) $f\big(f^{-1}(y)\big) = y$ for all $y \in Y$, and
2) $f^{-1}\big(f(x)\big) = x$ for all $x \in X$.

We wish to show that f is a bijection. This is left as an exercise for the reader. [*Hint:* This is very similar to many of the previous proofs that functions are bijections, but with the equation $x = f^{-1}(y)$ in place of an explicit formula for x.] □

EXERCISES 13.9.

1) Prove that the inverse of a bijection is a bijection.
2) Prove the converse of Exercise 13.3.
3) Show that the inverse of a function is *unique*: if g_1 and g_2 are inverses of f, then $g_1 = g_2$. (This is why we speak of *the* inverse of f, rather than *an* inverse of f.)

Remark 13.10. If f is a function that has an inverse, then it is easy to find f^{-1} as a set of ordered pairs. Namely,

$$f^{-1} = \{\, (y, x) \mid (x, y) \in f \,\}.$$

This is simply a restatement of the fact that

$$y = f(x) \Leftrightarrow x = f^{-1}(y).$$

EXERCISE 13.11. Prove the converse of Theorem 13.8.
[*Hint:* Find f^{-1} as a set of ordered pairs.]

NOTATION 13.12. For any set A, define the **identity map** $I_A\colon A \to A$ by $I_A(a) = a$ for every $a \in A$.

EXERCISES 13.13.

1) Suppose $f\colon A \to B$ and $g\colon B \to C$ are bijections. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
2) Suppose $f\colon X \to Y$ and $g\colon Y \to X$. Show that g is the inverse of f if and only if
$$f \circ g = I_Y \quad \text{and} \quad g \circ f = I_X.$$
3) Suppose $f\colon X \to Y$ is a bijection. Show that the inverse of f^{-1} is f. That is, $(f^{-1})^{-1} = f$.

WARNING. We have already introduced f^{-1} as notation for pre-images, even when f^{-1} was not a function (that is, even when f was not a bijection). Be aware that this notation is used in both contexts.

SUMMARY:

- Important definitions:
  - inverse function
  - identity map
- A function f has an inverse iff f is a bijection.
- Notation:
  - f^{-1}
  - $I_A\colon A \to A$

Chapter 14

Composition of Functions

Nothing goes by luck in composition. It allows of no tricks.
Henry David Thoreau (1817–1862), American author

The term "composition" is a name that mathematicians use for an idea that comes up fairly often in everyday life.

EXAMPLE 14.1.

1) The father of the mother of a person is the grandfather the person. (To be precise, it is the *maternal* grandfather of the person — and his or her other grandfather is *paternal*.) To express the relationship in a mathematical formula, we can write:

$$\forall x, \Big(\mathsf{grandfather}(x) = \mathsf{father}\big(\mathsf{mother}(x)\big)\Big).$$

A mathematician abbreviates this formula by writing

$$\mathsf{grandfather} = \mathsf{father} \circ \mathsf{mother}$$

and says that the (maternal) grandfather function is the *composition* of father and mother.

2) The brother of the mother of a person is an uncle of the person, so uncle is the composition of brother and mother:

$$\forall x, \Big(\mathsf{uncle}(x) = \mathsf{brother}\big(\mathsf{mother}(x)\big)\Big),$$

or, more briefly,

$$\mathsf{uncle} = \mathsf{brother} \circ \mathsf{mother}.$$

(For the sake of this example, let us ignore the issue that uncle and brother are not functions.)

3) The daughter of a child is a granddaughter, so granddaughter is a composition of daughter and child:

$$\mathsf{granddaughter} = \mathsf{daughter} \circ \mathsf{child}.$$

EXERCISES 14.2. State the usual name for each composition. (Ignore the fact that sister, daughter, and many of the other relations are not functions.)

1) husband ∘ sister

2) husband ∘ mother

3) husband ∘ wife
4) husband ∘ daughter
5) mother ∘ sister
6) daughter ∘ sister
7) parent ∘ parent
8) child ∘ child
9) parent ∘ parent ∘ parent
10) child ∘ brother ∘ parent

DEFINITION 14.3. Suppose $f\colon A \to B$ and $g\colon B \to C$. The **composition** $g \circ f$ of g and f is the function from A to C defined by

$$(g \circ f)(a) = g\big(f(a)\big) \text{ for all } a \in A.$$

EXAMPLE 14.4. Define $f\colon \mathbb{R} \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = 3x$ and $g(x) = x^2$. Then $g \circ f$ and $f \circ g$ are functions from $\mathbb{R}$ to $\mathbb{R}$. For all $x \in \mathbb{R}$, we have

$$(g \circ f)(x) = g\big(f(x)\big) = g(3x) = (3x)^2 = 9x^2$$

and

$$(f \circ g)(x) = f\big(g(x)\big) = f(x^2) = 3(x^2) = 3x^2.$$

Notice that (in this example) $f \circ g \neq g \circ f$, so *composition is not commutative.*

WARNING. To calculate the value of the function $g \circ f$ at the point a, do *not* begin by calculating $g(a)$. Instead, you need to calculate $f(a)$. Then plug that value into the function g.

EXAMPLE 14.5. Figure 14.1 provides an arrow diagram to illustrate the composition $g \circ f$.

- Starting from any point of A, follow the arrow (for the function f that starts there to arrive at some point of B.
- Then follow the arrow (for the function g) that starts there to arrive at a point of C.

For example, the f-arrow from a leads to m and the g-arrow from m leads to u. So $(g \circ f)(a) = u$.

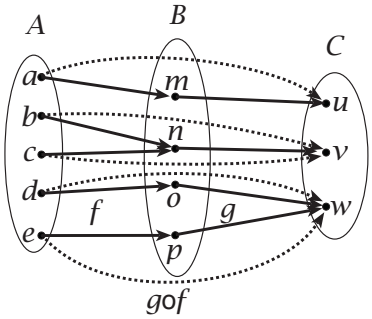


Figure 14.1. Arrows for the composition $g \circ f$ are dotted.

Notice that even though g appears on the left in the expression $g \circ f$, the arrow diagram for g appears on the right in the figure. This is an unfortunate consequence of the way that we calculate $g\big(f(x)\big)$ — see the warning above.

EXERCISE 14.6. The definition of $g \circ f$ requires that the domain of g is equal to the codomain of f. (They are both called B in the definition, so they are required to be equal.) *Why?*

EXERCISES 14.7.

1) The formulas define functions f and g from $\mathbb{R}$ to $\mathbb{R}$. Find formulas for $(f \circ g)(x)$ and $(g \circ f)(x)$.
   (a) $f(x) = 3x + 1$ and $g(x) = x^2 + 2$
   (b) $f(x) = 3x + 1$ and $g(x) = (x - 1)/3$
   (c) $f(x) = ax + b$ and $g(x) = cx + d$ (where $a, b, c, d \in \mathbb{R}$)
   (d) $f(x) = |x|$ and $g(x) = x^2$
   (e) $f(x) = |x|$ and $g(x) = -x$

2) Let $A = \{1, 2, 3, 4\}$, $B = \{\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}\}$, and $C = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$. The sets of ordered pairs in each part are functions $f\colon A \to B$ and $g\colon B \to C$. Represent $g \circ f$ as a set of ordered pairs.
   (a) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{c}), (4, \mathsf{d})\}$,
   $g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \diamondsuit), (\mathsf{c}, \heartsuit), (\mathsf{d}, \spadesuit)\}$
   (b) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{c}), (4, \mathsf{d})\}$,
   $g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \clubsuit), (\mathsf{c}, \clubsuit), (\mathsf{d}, \clubsuit)\}$
   (c) $f = \{(1, \mathsf{b}), (2, \mathsf{c}), (3, \mathsf{d}), (4, \mathsf{a})\}$,
   $g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \spadesuit), (\mathsf{c}, \heartsuit), (\mathsf{d}, \diamondsuit)\}$
   (d) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{c}), (4, \mathsf{d})\}$,
   $g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \clubsuit), (\mathsf{c}, \heartsuit), (\mathsf{d}, \spadesuit)\}$
   (e) $f = \{(1, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{a}), (4, \mathsf{b})\}$,
   $g = \{(\mathsf{a}, \clubsuit), (\mathsf{b}, \clubsuit), (\mathsf{c}, \heartsuit), (\mathsf{d}, \spadesuit)\}$

3) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if
$$(g \circ f)(a) = a, \text{ for every } a \in A,$$
then f is one-to-one.

EXERCISES 14.8.

1) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if f and g are one-to-one, then $g \circ f$ is one-to-one.
2) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if f and g are onto, then $g \circ f$ is onto.
3) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if $g \circ f$ is one-to-one, then f is one-to-one.
4) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if $g \circ f$ is onto, then g is onto.
5) Give an example of functions $f\colon A \to B$ and $g\colon B \to C$, such that $g \circ f$ is onto, but f is *not* onto. [*Hint:* Let $A = B = \mathbb{R}$, $C = [0, \infty)$, $f(x) = x^2$, and $g(x) = x^2$.]
6) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if $g \circ f$ is onto, and g is one-to-one, then f is onto.
7) Suppose $f\colon A \to B$ and $g\colon B \to C$. Show that if $g \circ f$ is one-to-one, and the range of f is B, then g is one-to-one.
8) Define $f\colon [0, \infty) \to \mathbb{R}$ by $f(x) = x$ and $g\colon \mathbb{R} \to \mathbb{R}$ by $g(x) = |x|$. Show that $g \circ f$ is one-to-one, but g is *not* one-to-one.

9) Suppose f and g are functions from A to A. If $f(a) = a$ for every $a \in A$, then what are $f \circ g$ and $g \circ f$?

10) (*harder*) Suppose $f\colon A \to B$ and $g\colon B \to C$. Write a definition of $g \circ f$ purely in terms of sets of ordered pairs. That is, find a predicate $P(x, y)$, such that

$$g \circ f = \{\, (a, c) \in A \times C \mid P(a, c) \,\}.$$

The predicate cannot use the notation $f(x)$ or $g(x)$. Instead, it should refer to the ordered pairs that are elements of f and g.

SUMMARY:

- Important definitions:
  - ∘ composition of functions
- Notation:
  - ∘ composition $(g \circ f)(x) = g\big(f(x)\big)$

Part IV

Other Fundamental Concepts

Chapter 15

Cardinality

God created infinity, and man, unable to understand infinity, had to invent finite sets.

Gian-Carlo Rota (1932–1999), MIT mathematician
Combinatorics essay

15A. Definition and basic properties

Informally, the *cardinality* of a set is the number of elements that it contains. For example, the cardinality of $\{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$ is 3. Children learn to verify this by counting: 1 (for a), 2 (for b), 3 (for c). Mathematicians say the same thing in a more sophisticated way: if we define a function $f\colon \{\mathsf{a}, \mathsf{b}, \mathsf{c}\} \to \{1, 2, 3\}$ by

$$f(\mathsf{a}) = 1,\ f(\mathsf{b}) = 2,\ f(\mathsf{c}) = 3,$$

then f is a bijection. In general, if a set A has n elements, then counting the elements one by one defines a bijection from A to $\{1, 2, 3, \ldots, n\}$. This observation leads to the following official definition.

DEFINITION 15.1.

1) Let A be a set and n be a natural number. We say that the **cardinality** of A is n (and write $\#A = n$) iff there is a bijection from A to $\{1, 2, 3, \ldots, n\}$.
2) A set A is **finite** iff there is some $n \in \mathbb{N}$, such that $\#A = n$.
3) A set A is **infinite** iff it is *not* finite.

Remark 15.2. Many mathematicians use the notation $|A|$ instead of $\#A$.

EXERCISES 15.3. What is the cardinality of each set?
(*You do* not *need to show your work or justify your answers.*)

1) $\#\{1, 2, 3, 4\} =$
2) $\#\{\mathsf{a}, \mathsf{e}, \mathsf{i}, \mathsf{o}, \mathsf{u}\} =$
3) $\#\{\mathsf{a}, \mathsf{l}, \mathsf{b}, \mathsf{e}, \mathsf{r}, \mathsf{t}, \mathsf{a}\} =$
4) $\#\emptyset =$
5) $\#\{\emptyset\} =$
6) $\#\big\{k \in \{1, 2, \ldots, 10\} \;\big|\; k \neq 7\big\} =$

EXAMPLE 15.4. $\mathbb{N}$ is infinite (see Exercise 15.26(2)).

EXERCISES 15.5. Suppose A is a finite set.

1) Show $\#\{1, 2, 3, \ldots, n\} = n$, for every $n \in \mathbb{N}$.
2) For $n \in \mathbb{N}$, show $\#A = n$ iff there is a bijection from $\{1, 2, 3, \ldots, n\}$ to A. [*Hint:* Use Exercise 13.9(1).]
3) Show $\#A = 0$ if and only if $A = \emptyset$.

EXERCISES 15.6. Suppose A and B are finite sets, and $m, n \in \mathbb{N}$.

1) Show that if $m \leq n$, then there exists a one-to-one function $f\colon \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$.
2) Show that if $\#A \leq \#B$, then there exists a one-to-one function $f\colon A \to B$. [*Hint:* Use the preceding exercise.]
3) Assume $n > 0$. Show that if $m \geq n$, then there exists an onto function $f\colon \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$.
4) Assume A and B are nonempty. Show that if $\#A \geq \#B$, then there exists an onto function $f\colon A \to B$. [*Hint:* Use the preceding exercise.]

The converses of the exercises in (15.6) are true, and important. They will be discussed in section 15B.

It is often possible to show that two sets have the same cardinality, without knowing how many elements they have.

EXAMPLE 15.7. In the society Married of Example 12.3, it is clear that there must be exactly the same number of men and women. (If there were more women than men, then either some woman would be unmarried, or more than one woman would have to be married to the same man. Similarly, if there were more men than women.) This is true, even though we have no idea how many women or men there are in the society. All we know is that however many women there are is exactly the same as the number of men.

This observation is formalized in the following proposition.

PROPOSITION 15.8. *Suppose A and B are finite sets. Then $\#A = \#B$ if and only if there is a bijection from A to B.*

PROOF. ($\Rightarrow$) Let n be the cardinality of A. Then, by definition, there is a bijection $f\colon A \to \{1, 2, \ldots, n\}$. By assumption, n is also the cardinality of B, so there is a bijection $g\colon B \to \{1, 2, \ldots, n\}$. The inverse of a bijection is a bijection (see Exercise 13.9(1)), and the composition of bijections is a bijection (see Exercise 12.10(1)), so $g^{-1} \circ f$ is a bijection from A to B.

($\Leftarrow$) We leave this as an exercise. □

EXERCISE 15.9. Prove Proposition 15.8($\Leftarrow$). [*Hint:* Use Exercise 12.10(1).]

EXERCISES 15.10. Assume B is a finite set.

1) Show that if $\#A_1 = \#A_2$, then $\#(A_1 \times B) = \#(A_2 \times B)$. [*Hint:* If $f\colon A_1 \to A_2$ is a bijection, define $g\colon A_1 \times B \to A_2 \times B$ by $g(a_1, b) = \big(f(a_1), b\big)$.]
2) Show that if $\{a_0\}$ is any set with only one element, then $\#\big(\{a_0\} \times B\big) = \#B$. [*Hint:* Define $f\colon B \to \{a_0\} \times B$ by $f(b) = (a_0, b)$, and show f is a bijection.]

EXERCISE 15.11. Suppose $f\colon A \to B$ is one-to-one, and $X \subset A$. Show $\#f(X) = \#X$.

EXAMPLE 15.12. In elementary school, we learn that if Alice has m apples and Bob has n apples, then the sum $m+n$ is the total number of apples that the two of them have. However, this simple example assumes that Alice and Bob are not sharing any of the apples; the set of Alice's apples must be *disjoint* from the set of Bob's apples.

The following result generalizes this example.

PROPOSITION 15.13. *If A and B are disjoint finite sets, then*

$$\#(A \cup B) = \#A + \#B.$$

PROOF. Let $m = \#A$ and $n = \#B$. Then there exist bijections

$$f\colon \{1, 2, \ldots, m\} \to A \quad \text{and} \quad g\colon \{1, 2, \ldots, n\} \to B.$$

Define a function $h\colon \{1, 2, \ldots, m+n\} \to (A \cup B)$ by

$$h(k) = \begin{cases} f(k) & \text{if } k \leq m \\ g(k-m) & \text{if } k > m \end{cases}$$

(Notice that if $k \in \{1, 2, \ldots, m+n\}$, and $k > m$, then $m+1 \leq k \leq m+n$, so $1 \leq k-m \leq n$; therefore, $k-m$ is in the domain of g, so the expression $g(k-m)$ makes sense.)

To complete the proof, it suffices to show that h is a bijection; thus, we we need only show that h is one-to-one and onto.

(onto) Given $y \in A \cup B$, we have either $y \in A$ or $y \in B$, and we consider these two possibilities as separate cases.

1) Suppose $y \in A$. Since f is onto, there is some $k \in \{1, 2, \ldots, m\}$ with $f(k) = y$. Then, because $k \leq m$, we have
$$h(k) = f(k) = y.$$

2) Suppose $y \in B$. Since g is onto, there is some $k \in \{1, 2, \ldots, n\}$ with $g(k) = y$. Then $k+m \in \{1, 2, \ldots, m+n\}$ and $k+m > m$, so
$$h(k+m) = g\big((k+m)-m\big) = g(k) = y.$$

Since y is an arbitrary element of $A \cup B$, we conclude that h is onto.

(one-to-one) We leave this as an exercise. □

EXERCISE 15.14. Show that the function h defined in the proof of Proposition 15.13 is one-to-one.

EXERCISE 15.15. Show that if $A \subset B$ and A and B are finite, then $\#A \leq \#B$. [*Hint:* $\#B = \#A + \#(B \smallsetminus A) \geq \#A$.]

The following more general formula applies to the union of any number of sets, not just two. See Exercise 16.17 for the proof.

DEFINITION 15.16. Sets $A_1, A_2, \ldots, A_n$ are **pairwise-disjoint** iff A_i is disjoint from A_j whenever $i \neq j$.

PROPOSITION 15.17. *If $A_1, A_2, \ldots, A_n$ are pairwise-disjoint finite sets, then*

$$\#(A_1 \cup A_2 \cup \cdots \cup A_n) = \#A_1 + \#A_2 + \cdots + \#A_n.$$

It was pointed out in Remark 6.21 that if A and B are finite sets, then $\#(A \times B) = \#A \cdot \#B$. We can prove this quite easily, after using Proposition 15.17 to solve the following exercise:

EXERCISE 15.18. Show that if $A_1, A_2, \ldots, A_m$ are pairwise-disjoint finite sets, and $A = A_1 \cup \cdots \cup A_m$, then

$$\#(A \times B) = \#(A_1 \times B) + \#(A_2 \times B) + \cdots + \#(A_m \times B).$$

[*Hint:* The sets $A_i \times B$ are pairwise-disjoint, and their union is $A \times B$.]

THEOREM 15.19. *For any finite sets A and B, we have*

$$\#(A \times B) = \#A \cdot \#B.$$

PROOF. Let $m = \#A$. Then there is no harm in assuming $A = \{1, 2, \ldots, m\}$ (see Exercise 15.10(1)). Therefore

$$A = \{1\} \cup \{2\} \cup \cdots \cup \{m\},$$

and the sets $\{1\}, \{2\}, \cdots, \{m\}$ are pairwise-disjoint, so

$$\begin{aligned} \#(A \times B) &= \#\big(\{1\} \times B\big) + \#\big(\{2\} \times B\big) + \cdots + \#\big(\{m\} \times B\big) && \text{(Exercise 15.18)} \\ &= \#B + \#B + \cdots + \#B \qquad (m \text{ summands}) && \text{(Exercise 15.10(2))} \\ &= m \cdot \#B \\ &= \#A \cdot \#B. \end{aligned}$$

□

15B. The Pigeonhole Principle

If a mail carrier has m letters to distribute among n mailboxes (or "pigeonholes"), and $m > n$, then it seems clear that at least one of the mailboxes will have to get more than one letter. This important observation is known as the "Pigeonhole Principle." See Exercise 16.18 for its proof.

PROPOSITION 15.20 (Pigeonhole Principle). *Let B and $A_1, A_2, \ldots, A_n$ be finite sets. If*

$$B \subset A_1 \cup A_2 \cup \ldots \cup A_n,$$

and $n < \#B$, then $\#A_i \geq 2$, for some i.

Here are a few of the many applications of the Pigeonhole Principle. In these real-world examples, our explanations will be a bit informal.

EXAMPLE 15.21. Bob's sock drawer has many, many socks in it, and they come in 4 colours. Unfortunately, the light in his room has burned out, so he cannot see anything. How many socks should he grab from the drawer, so that he can be sure at least two of them are of the same colour.

SOLUTION. Bob should grab 5 (or more) socks.

To see this, note, first, that taking 4 socks may not be enough: If Bob grabs only 4 socks, it is possible that he has one sock of each of the 4 different colours. Then he would not have two socks of the same colour.

Now suppose Bob grabs (at least) 5 socks. He can sort them into 4 piles, by colour. Since $5 > 4$, one of the piles must have more than one sock. So there are (at least) 2 socks of the same colour. □

EXAMPLE 15.22. If you pick 50 numbers from 1 to 98, then it is guaranteed that two of them will add up to exactly 99.

SOLUTION. The numbers from 1 to 98 can be divided into 49 pigeonholes:

$$\{1, 98\},\ \{2, 97\},\ \{3, 96\},\ \ldots,\ \{49, 50\}.$$

(So two different numbers x and y are in the same pigeonhole iff $x+y = 99$.) Since $50 > 49$, two of the numbers we chose must be in the same pigeonhole. Then the sum of these two numbers is exactly 99. □

EXAMPLE 15.23. If you pick 5 points on the surface of a (spherical) orange, then there is always a way to cut the orange exactly in half, such that at least 4 of your points are in the same half. (We assume any point that is exactly on the cut is considered to belong to both halves.)

SOLUTION. Any two of the points will lie on a great circle of the sphere, so we can cut the orange so that 2 of the points are exactly on the cut. The other 3 points are distributed in some way among the two halves of the orange. By the Pigeonhole Principle, at least two of those three points are in the same half. Then that half contains the 2 points on the cut, plus these additional 2 points, for a total of (at least) 4 of the points you picked. □

EXERCISES 15.24.

1) It is known that:

   - No one has more than 300,000 hairs on their head.
   - More than a million people live in Calgary.

   Show that there are two people in Calgary who have exactly the same number of hairs on their heads.

2) Show that if you put 5 points into an equilateral triangle of side length 2 cm, then there are two of the points that are no more than 1 cm apart.
   [*Hint:* Divide the triangle into 4 equilateral triangle of side length 1 cm.]

In addition to the above real-world examples, the Pigeonhole Principle has important applications in theoretical mathematics.

COROLLARY 15.25. *Suppose A and B are finite sets, with $\#A = m$ and $\#B = n$.*

1) If there exists a one-to-one function $f\colon A \to B$, then $m \leq n$.

2) If there exists an onto function $f\colon A \to B$, then $m \geq n$.

PROOF. (1) Suppose $f\colon A \to B$ is onto, and $m > n$. There is no harm in assuming $B = \{1, 2, \ldots, n\}$, and then we may let

$$A_i = f^{-1}(i)$$

for $i = 1, 2, \ldots, n$. For any $a \in A$, we have $a \in f^{-1}\big(f(a)\big) = A_{f(a)}$, so $a \in A_1 \cup A_2 \cup \cdots \cup A_n$. Since a is an arbitrary element of A, this implies $A \subset A_1 \cup A_2 \cup \ldots \cup A_n$. Because $\#A = m > n$, we conclude that $\#A_i \geq 2$ for some i. This means $\#f^{-1}(i) > 1$, which contradicts the fact that f is one-to-one.

(2) Suppose $f\colon A \to B$ is onto, and $m < n$. There is no harm in assuming $A = \{1, 2, \ldots, m\}$, and then we may let

$$B_i = \{f(i)\}$$

for $i = 1, 2, \ldots, m$. Since f is onto, we know, for any $b \in B$, there is some $i \in A$, such that $f(i) = b$. This means $b \in B_i$; hence, $b \in B_1 \cup B_2 \cup \cdots \cup B_m$. Since b is an arbitrary element of B, this implies $B \subset B_1 \cup B_2 \cup \ldots \cup B_m$. Because $\#B = n > m$, we conclude that $\#B_i \geq 2$ for some i. This contradicts the fact that $\#B_i = 1$ (because $B_i = \{f(i)\}$ has only one element. □

EXERCISES 15.26.

1) Show that $\#A$ is well-defined. That is, if $\#A = m$ and $\#A = n$, for some $m, n \in \mathbb{N}$, then $m = n$. [*Hint:* Apply Corollary 15.25 with $B = A$.]

2) Show $\mathbb{N}$ is infinite. [*Hint:* Proof by contradiction. Apply Thm. 15.25(1).]

15C. Cardinality of a union

The cardinality of $A \cup B$ is not $\#A + \#B$, unless A and B are disjoint. Here is a formula that works in general:

PROPOSITION 15.27. *For any finite sets A and B, we have*

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

PROOF. From Exercise 8.21, we know that $A \smallsetminus B$, $B \smallsetminus A$, and $A \cap B$ are pairwise-disjoint, and that their union is $A \cup B$, so

$$\#(A \smallsetminus B) + \#(B \smallsetminus A) + \#(A \cap B) = \#\big((A \smallsetminus B) \cup (B \smallsetminus A) \cup (A \cap B)\big) = A \cup B.$$

Also, we have

$$\begin{aligned} \#A &= \#\big((A \smallsetminus B) \cup (A \cap B)\big) && \text{(Exercise 8.19(2))} \\ &= \#(A \smallsetminus B) + \#(A \cap B) && \text{(Exercise 8.20(4)).} \end{aligned}$$

Similarly, we have

$$\#B = \#(B \smallsetminus A) + \#(A \cap B).$$

Therefore

$$\begin{aligned} \#A + \#B - \#(A \cap B) &= \big(\#(A \smallsetminus B) + \#(A \cap B)\big) + \big(\#(B \smallsetminus A) + \#(A \cap B)\big) - \#(A \cap B) \\ &= \#(A \smallsetminus B) + \#(B \smallsetminus A) + \#(A \cap B) \\ &= \#(A \cup B). \end{aligned}$$

□

EXAMPLE 15.28. Let $A = \{\mathsf{p}, \mathsf{r}, \mathsf{o}, \mathsf{n}, \mathsf{g}\}$ and $B = \{\mathsf{h}, \mathsf{o}, \mathsf{r}, \mathsf{n}, \mathsf{s}\}$. Then

$$\#A = 5,\ \#B = 5, \text{ and } \#(A \cap B) = \#\{\mathsf{r}, \mathsf{o}, \mathsf{n}\} = 3,$$

so Proposition 15.27 tells us that

$$\#(A \cup B) = \#A + \#B - \#(A \cap B) = 5 + 5 - 3 = 7.$$

This is correct, since

$$\#(A \cup B) = \#\{\mathsf{p}, \mathsf{r}, \mathsf{o}, \mathsf{n}, \mathsf{g}, \mathsf{h}, \mathsf{s}\} = 7.$$

EXAMPLE 15.29. Every one of the 4000 students at Modern U owns either a cell phone or an iPod (or both). Surveys show that:

- 3500 students own a cell phone, and
- 1000 students own an iPod.

How many students own *both* a cell phone and an iPod?

SOLUTION. Let

- S be the set of all students at Modern U,
- C be the set of students who own a cell phone, and
- I be the set of students who own an iPod.

Then, by assumption,

$$\#S = 4000,$$
$$\#C = 3500,$$
$$\#I = 1000.$$

Since every student owns either a cell phone or an iPod, we have $S = C \cup I$. Therefore, Proposition 15.27 tells us that

$$\#S = \#(C \cup I) = \#C + \#I - \#(C \cap I),$$

so

$$\#(C \cap I) = \#C + \#I - \#S = 3500 + 1000 - 4000 = 500.$$

Hence, there are exactly 500 students who own both a cell phone and an iPod. □

EXERCISES 15.30.

1) Assume $\#U = 15$, $\#V = 12$, and $\#(U \cap V) = 4$. Find $\#(U \cup V)$.
2) Assume $\#R = 13$, $\#S = 17$, and $\#(R \cup S) = 25$. Find $\#(R \cap S)$.
3) Assume $\#J = 300$, $\#(J \cup L) = 500$, and $\#(J \cap L) = 150$. Find $\#L$.
4) At a small university, there are 90 students that are taking either Calculus *or* Linear Algebra (or both). If the Calculus class has 70 students, and the Linear Algebra class has 35 students, then how many students are taking both Calculus *and* Linear Algebra?
5) (*harder*) Suppose A, B, and C are finite sets. Show

$$\begin{aligned}\#(A \cup B \cup C) = \#A + \#B + \#C \\ - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) \\ + \#(A \cap B \cap C).\end{aligned}$$

[*Hint:* We have formulas for $\#\big((A \cup B) \cup C\big)$ and $\#(A \cup B)$. The equality $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ provides another useful formula.]

The following exercises are examples of another type of application of the formula for the cardinality of a union.

EXERCISES 15.31.

1) Suppose A and B are subsets of a finite set C. Show that if $\#A + \#B > \#C$, then $A \cap B \neq \emptyset$. [*Hint:* Use Proposition 15.27 to show that $\#(A \cap B) \neq 0$.]
2) Show that if A is a set of at least 600 natural numbers that are less than 1000, then two of the numbers in A differ by exactly 100. [*Hint:* Let $B = \{\, a + 100 \mid a \in A \,\}$, and use the preceding exercise to show that $A \cap B \neq \emptyset$.]

15D. Hotel Infinity and the cardinality of infinite sets

The above discussion of cardinality included the following important fact that appeared in Proposition 15.8:

> Two finite sets A and B have the same cardinality if and only if there is a bijection from A to B.

Extending this property to all sets (not just the finite ones) is the *definition* of cardinality for infinite sets:

DEFINITION 15.32. Two sets A and B have the **same cardinality** if there exists a bijection from A to B.

Two main ideas will be developed in the remainder of this chapter:

1) Many sets have the same cardinality as $\mathbb{N}^+$. These are the smallest infinite sets, and they are said to be **countably** infinite.
2) Not all sets are countably infinite: some sets are more infinite than others! These sets are said to be **uncountable**.

Let us begin with an informal discussion of some of the ideas that are involved in countability, rather than looking at the official definition right away. First, a simple example involving finite sets.

EXAMPLE 15.33. Suppose a hotel has n rooms, numbered $1, 2, 3, \ldots, n$.

1) If A is a tour group of n people $a_1, a_2, \ldots, a_n$, then the hotel clerk will obviously have no trouble assigning each of them a room: a_i can be put in room i. There will be no empty rooms left.
2) On the other hand, if, in addition to this tour group, there is another person b who wants a room, then the situation is hopeless. There is no way to give each of these $n+1$ people a room, without making two of them share a room. In general:

   If there are more guests than hotel rooms, then not everyone can have a room.

   This is a restatement of the Pigeonhole Principle (15.20).

EXAMPLE 15.34 (Hotel Infinity). Now consider a hotel with a countably infinite number of rooms, numbered $1, 2, 3, \ldots$. (There is one room for each $i \in \mathbb{N}^+$.)

1) If A is a tour group of n people $a_1, a_2, \ldots, a_n$, then the hotel clerk will obviously have no trouble giving each of them a room: a_i can be put in room i. There will be lots of empty rooms left over.
2) Even if A is countably infinite, rather than finite, with people $a_1, a_2, \ldots$, the hotel clerk can accommodate all of them, by putting a_i in room i. There will be no empty rooms left.
3) Now suppose that, in addition to this tour group, there is another person b who also wants a room. The hotel clerk can handle this situation quite easily, by putting
   - b into room 1, and
   - a_i in room $i+1$.

   Everyone will have his or her own room.
4) The same idea works, even if, instead of just one person, there is a whole group B of n people $b_1, b_2, \ldots, b_n$ that want rooms. The clerk can put
   - b_i in room i, and
   - a_i in room $i+n$.
5) It may seem that there would be a problem if the second group B consists of infinitely many people $b_1, b_2, b_3, \ldots$, but a clever hotel clerk can accommodate even this situation. Note that there are infinitely many odd-numbered rooms, so all of A can be put in those rooms, and there are also infinitely many even-numbered rooms, so all of B can be put in there. More precisely, the clerk can put
   - a_i in room $2i-1$, and

- b_i in room $2i$.

6) Even if there are several of these countably infinite tour groups, not just 2 of them, they can all be accommodated. Namely, if there are n tour groups $A_1, A_2, A_3, \ldots, A_n$, then note that there are infinitely many numbers that are congruent to k modulo n, so all of A_k can be put in those rooms. More precisely, let $a_{k,1}, a_{k,2}, a_{k,3}, \ldots$ be a list of the people in A_k. Then the clerk can put

- $a_{k,i}$ in room $k + in$.

EXERCISES 15.35.

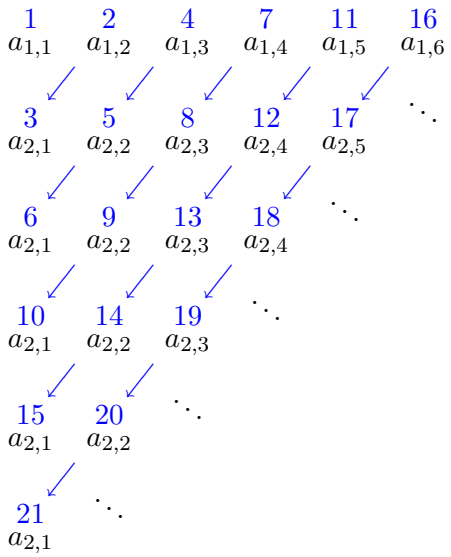
(a) Show that the clerk has not put two guests in the same room. That is, show, for all $k_1, k_2 \in \{1, 2, \ldots, n\}$ and $i_1, i_2 \in \mathbb{N}^+$, such that $k_1 + i_1 n = k_2 + i_2 n$, we have $k_1 = k_2$ and $i_1 = i_2$.

(b) The clerk has left some rooms empty, which is wasteful. (For example, it is not difficult to see that no guest has been put in room 1.) Modify the clerk's formula to obtain a method that does not leave any empty rooms (and, of course, does not put two guests in the same room.)

7) Going further, even if there were infinitely many infinite tour groups $A_1, A_2, \ldots$, they could all be accommodated. (We assume that each tour group is countably infinite, and that the number of groups is countably infinite.) To see this, start by considering an infinitely large table (or matrix) that lists the elements of A_k in the kth row:

$$\begin{array}{lccccccc}
A_1: & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & \cdots \\
A_2: & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & \cdots \\
A_3: & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & \cdots \\
A_4: & a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & \cdots \\
A_5: & a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

We can assign rooms $1, 2, 3, \ldots$ to the entries of this table as indicated in the following figure:



The numbering:

- Begins with 1 in the top left corner.
- Then places 2 at the top of the second column and moves diagonally (down and to the left) to place 3.
- Then places 4 at the top of the third column, and moves diagonally (down and to the left) to place 5 and 6.
- Then places the next number (namely, 7) at the first open spot in the top row (namely, at the top of the fourth column), and moves diagonally (down and to the left) to place the following numbers (namely, 8, 9, and 10), until a number (namely, 10) is placed in the first column.
- The procedure then moves to the first open spot in the top row, and repeats infinitely.

No entries of the table are omitted from the numbering, and no room numbers are repeated, so each guest has his or her own room.

Remark 15.36. In Eg. 15.34(7), It can be shown that guest $a_{k,i}$ is given room

$$\frac{(k+i-1)(k+i-2)}{2}+k,$$

but we have no need for this formula.

It might seem that Hotel Infinity could accommodate every set of tourists, but that is not the case. For example, we will see later in the chapter that if all of the real numbers want rooms at the hotel, then some of them will have to share. In other words, the set $\mathbb{R}$ of real numbers is *uncountable*.

15E. Countable sets

For use in proving theorems, the ideas encountered in the discussion of Hotel Infinity need to be stated more formally. Let us begin with the definitions that form the foundation of the subject.

DEFINITION 15.37. Suppose A and B are sets.

1) A and B **have the same cardinality** iff there is a bijection from A to B.
2) A is **countably infinite** iff it has the same cardinality as $\mathbb{N}^+$.
3) A is **countable** iff either A is finite or A is countably infinite.
4) A is **uncountable** iff A is *not* countable.

Remark 15.38.

1) In the terminology of the preceding section, a set is countable if and only if all of its elements can be given rooms in Hotel Infinity (see Exercise 15.41(3)).
2) If you are told to show that A is countably infinite, directly from the definition, then you should find a bijection from A to $\mathbb{N}^+$. However, because it is so well known that the inverse of a bijection is a bijection, it is acceptable to find a bijection from $\mathbb{N}^+$ to A, instead.

Remark 15.39. One can (and should!) think of countable sets as the sets whose elements can be listed in a sequence. The sequence may have only finitely many terms, or may continue forever:

1) A set A is finite iff its elements can be listed in a sequence $a_1, a_2, \ldots, a_n$, for some n.
2) If the elements of A can be listed in an infinite sequence $a_1, a_2, a_3, \ldots$, then we may define a bijection $f\colon \mathbb{N}^+ \to A$ by $f(i) = a_i$. Therefore, A is countably infinite.

3) Conversely, if A is countably infinite, then there is a bijection $f\colon \mathbb{N}^+ \to A$, so letting $a_i = f(i)$ yields an infinite sequence $a_1, a_2, a_3, \ldots$ that lists the elements of A.

The following fundamental result shows that the smallest infinite sets are the countable ones:

THEOREM 15.40.

1) Every infinite set contains a countably infinite subset.

2) Every subset of a countable set is countable.

PROOF. (1) Given an infinite set A, it suffices to construct an infinite sequence $a_1, a_2, a_2, \ldots$ of distinct elements of A, for then $\{a_1, a_2, a_3, \ldots\}$ is a countably infinite subset of A.

1) Since A is infinite, it is certainly not empty, so it has some elements. Let a_1 be any of these elements of A.

2) Since A is infinite, we know that a_1 is not its only element. Let a_2 be any element of A other than a_1. Then a_1 and a_2 are distinct elements of A.

3) Since A is infinite, we know that a_1 and a_2 are not its only elements. Let a_3 be any element of A other than a_1 and a_2. Then a_1, a_2, and a_3 are distinct elements of A.

$\vdots$

(i) Since A is infinite, we know that $a_1, a_2, a_3, \ldots, a_{i-1}$ are not its only elements. Let a_i be any element of A other than $a_1, a_2, a_3, \ldots, a_{i-1}$. Then the elements $a_1, a_2, a_3, \ldots, a_i$ are distinct.

$\vdots$

Continuing this inductive process yields the desired infinite sequence $a_1, a_2, a_3, \ldots$ of distinct elements of A.

(2) Given a subset M of a countable set A, we wish to show that M is countable. We may assume M is infinite, for otherwise it is obviously countable. So we wish to show there is a sequence $m_1, m_2, m_3, \ldots$ that lists all the elements of M.

To simplify the notation, let us first consider the case where $A = \mathbb{N}^+$.

Case 1. Assume $A = \mathbb{N}^+$. Let

1) m_1 be the smallest element of M,

2) m_2 be the smallest element of $M \smallsetminus \{m_1\}$,

3) m_3 be the smallest element of $M \smallsetminus \{m_1, m_2\}$,

4) m_4 be the smallest element of $M \smallsetminus \{m_1, m_2, m_3\}$,

$\vdots$

(i) m_i be the smallest element of $M \smallsetminus \{m_1, m_2, \ldots, m_{i-1}\}$.
(In other words, m_i is the smallest element of M that is not in $\{m_1, m_2, \ldots, m_{i-1}\}$.)

$\vdots$

It suffices to show that every element k of M appears in the sequence $m_1, m_2, m_3, \ldots$. To obtain this desired conclusion, notice, for each $i \in \mathbb{N}^+$, that $m_{i+1} > m_i$. Using this, it is easy to show (by induction) that $m_i \geq i$ for every $i \in \mathbb{N}^+$. In particular,

$$m_{k+1} \geq k + 1 > k.$$

Since, by definition, m_{k+1} is the *smallest* element of M that is not in $\{m_1, m_2, \ldots, m_k\}$, we conclude that $k \in \{m_1, m_2, \ldots, m_k\}$. So k is one of the terms in the sequence, as desired.

Case 2. The general case. This is left as an exercise. □

EXERCISES 15.41.

1) Complete Case 2 in the proof of Theorem 15.40.
[*Hint:* If M is infinite, then A must be infinite (why?). List the elements of A in a sequence $a_1, a_2, a_3, \ldots$, and apply the argument of Case 1.]

2) Suppose that $f\colon A \to B$, that f is one-to-one, and that B is countable. Show that A is countable.
[*Hint:* If f is not onto, you will want to use the fact that every subset of a countable set is countable.]

3) Show that a set A is countable if and only if there exists a one-to-one function $f\colon A \to \mathbb{N}^+$.

Remark 15.42. Mathematicians think of countable sets as being small — even though they may be infinite, they are almost like finite sets. Consider the following basic properties of finite sets:

1) Any subset of a finite set is finite.
2) The union of two finite sets is fiinite.
3) More generally, the union of finitely many finite sets is finite.
4) If you have two finite sets, then you can make only finitely many ordered pairs from them. (That is, the Cartesian product of two finite sets is finite.)
5) If you have only finitely many darts to throw, then you can hit only finitely many things with them. That is, if $f\colon A \to B$, and A is finite, then the image $f(A)$ is finite.

All of the above assertions remain true when the word "finite" is replaced with "countable." The first assertion was established in Thm. 15.40(2); the others are contained in the following important theorem:

THEOREM 15.43.

1) A countable union of countable sets is countable.
2) The cartesian product of two countable sets is countable.
3) The image of a countable set is countable.

Remark 15.44. Here are more precise statements of the assertions of Theorem 15.43:

1) If $A_1, A_2, A_3, \ldots$ is any sequence of countable sets, then the union
$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots$$
is countable. Also, if $A_1, A_2, A_3, \ldots, A_n$ is any finite sequence of countable sets, then the union
$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n$$
is countable.
2) If A and B are any countable sets, then $A \times B$ is countable.
3) If $f\colon A \to B$, and A is countable, then $f(A)$ is countable.

PROOF OF THEOREM 15.43. (2) Given countable sets A and B, we wish to show that $A \times B$ is countable. Subsets of a countable set are countable, so there is no harm in assuming that A and B are infinite (because replacing A and B with infinite supersets will make the cartesian product larger). Let

- $a_1, a_2, a_3, \ldots$ be a list of the elements of A, and

- $b_1, b_2, b_3, \ldots$ be a list of the elements of B,

Then the elements of $A \times B$ are listed in the following table (or matrix):

$$\begin{array}{cccccc}
(a_1,b_1) & (a_1,b_2) & (a_1,b_3) & (a_1,b_4) & (a_1,b_5) & \cdots \\
(a_2,b_1) & (a_2,b_2) & (a_2,b_3) & (a_2,b_4) & (a_2,b_5) & \cdots \\
(a_3,b_1) & (a_3,b_2) & (a_3,b_3) & (a_3,b_4) & (a_3,b_5) & \cdots \\
(a_4,b_1) & (a_4,b_2) & (a_4,b_3) & (a_4,b_4) & (a_4,b_5) & \cdots \\
(a_5,b_1) & (a_5,b_2) & (a_5,b_3) & (a_5,b_4) & (a_5,b_5) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

The numbering method of Eg. 15.34(7) defines a bijection from $A \times B$ to $\mathbb{N}^+$. So $A \times B$ is countable.

(3) Suppose $f\colon A \to B$, and A is countable. By replacing B with $f(B)$, we may assume f is onto; then we wish to show that B is countable.

By Exercise 15.41(2), it suffices to define a one-to-one function $g\colon B \to A$. The function f is onto, so, for each $b \in B$, there is some $a \in A$, such that $f(a) = b$; thus, for each $b \in B$, we may choose $g(b)$ to be an element of A such that

$$f\big(g(b)\big) = b.$$

Then $g\colon B \to A$, and all that remains is to show that g is one-to-one. Given $b_1, b_2 \in B$, such that $g(b_1) = g(b_2)$, we have $f\big(g(b_1)\big) = b_1$ and $f\big(g(b_2)\big) = b_2$. Therefore

$$b_1 = f\big(g(b_1)\big) = f\big(g(b_2)\big) = b_2.$$

So g is one-to-one, as desired.

(1) Given either an infinite sequence $A_1, A_2, A_3, \ldots$ of countable sets, or a finite sequence $A_1, A_2, A_3, \ldots, A_n$ of countable sets, we wish to show that the the union of the sets is countable. Subsets of a countable set are countable, so there is no harm in assuming:

- the sequence is infinite (because adding additional terms to the sequence will make the union larger), and
- each of the sets is infinite (because replacing A_i with an infinite superset will make the union larger).

Now, the numbering method of Eg. 15.34(7) shows there is an onto function $g\colon \mathbb{N}^+ \to \bigcup_{i=1}^{\infty} A_i$. So, from (3), we conclude that $\bigcup_{i=1}^{\infty} A_i$ is countable. □

The theorems of this section make it easy to show that many sets are countable. Here are a few important examples:

EXERCISE 15.45. Show that each of the following sets is countable.

1) $\mathbb{N}^+$.
2) $\mathbb{N}$. [*Hint:* $\mathbb{N} = \mathbb{N}^+ \cup \{0\}$.]
3) $\mathbb{Z}$. [*Hint:* Let $\mathbb{Z}^- = \{\, n \in \mathbb{Z} \mid n < 0 \,\}$, so $\mathbb{Z} = \mathbb{N} \cup \mathbb{Z}^-$. The set $\mathbb{Z}^-$ is the image of $\mathbb{N}^+$ under a function.]
4) $\mathbb{Q}$. [*Hint:* Let $\mathbb{Z}^\times$ be the set of nonzero integers, so $\mathbb{Q}$ is the image of $\mathbb{Z} \times \mathbb{Z}^\times$ under the function $f(a,b) = a/b$.]

Remark 15.46. It is very important to remember that $\mathbb{Q}$ is countable. Since $\mathbb{N}$ and $\mathbb{Z}$ are subsets of $\mathbb{Q}$, this implies that $\mathbb{N}$ and $\mathbb{Z}$ are also countable.

EXERCISES 15.47.

1) Suppose A is countably infinite, and $b \notin A$. Show, directly from the definition, that $A \cup \{b\}$ is countably infinite.
2) Suppose A is countably infinite, and $a \in A$. Show, directly from the definition, that $A \smallsetminus \{a\}$ is countably infinite.
3) Suppose A and B are countably infinite and disjoint. Show, directly from the definition, that $A \cup B$ is countably infinite.
4) Suppose
   - A_1 is disjoint from B_1,
   - A_2 is disjoint from B_2,
   - $A_1 \approx A_2$, and
   - $B_1 \approx B_2$.

   Show that $(A_1 \cup B_1) \approx (A_2 \cup B_2)$.
5) Suppose A is infinite. Show there is a *proper* subset B of A, such that $A \approx B$. [*Hint:* Combine Thm. 15.40(1) with items 2 and 4.]

15F. Uncountable sets

The preceding section showed that many sets (including $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$) are countable. But we will now see that some sets are *not* countable.

15F.1. The reals are uncountable. Here is perhaps the most important example of an uncountable set:

THEOREM 15.48. *The set $\mathbb{R}$ of real numbers is uncountable.*

If $\mathbb{R}$ were countable, then all of its subsets, including the interval $[0, 1)$, would be countable. Thus, in order to establish Theorem 15.48, it suffices to prove the following result:

THEOREM 15.49. *The interval $[0, 1)$ is uncountable.*

PROOF BY CONTRADICTION. Suppose $[0, 1)$ is countable. (This will lead to a contradiction.) This means there is a list $x_1, x_2, x_3, \ldots$ of all the numbers in $[0, 1)$. To obtain a contradiction, we will use a method called the *Cantor Diagonalization Argument*. It was discovered by the mathematician Georg Cantor in the 19th century.

Each number in $[0, 1)$ can be written as a decimal of the form $0.d_1d_2d_3\ldots$, where each d_k is a digit (0, 1, 2, 3, 4, 5, 6, 7, 8, or 9). In particular, we can write each x_i in this form:

$$x_i = 0.x_{i,1}x_{i,2}x_{i,3}x_{i,4}x_{i,5}\ldots$$

Then we can make a list of all of these decimals (omitting the leading 0 in each one):

$$\begin{aligned}
x_1 &= .x_{1,1}x_{1,2}x_{1,3}x_{1,4}x_{1,5}\ldots \\
x_2 &= .x_{2,1}x_{2,2}x_{2,3}x_{2,4}x_{2,5}\ldots \\
x_3 &= .x_{3,1}x_{3,2}x_{3,3}x_{3,4}x_{3,5}\ldots \\
x_4 &= .x_{4,1}x_{4,2}x_{4,3}x_{4,4}x_{4,5}\ldots \\
x_5 &= .x_{5,1}x_{5,2}x_{5,3}x_{5,4}x_{5,5}\ldots \\
&\vdots \qquad\qquad\qquad \vdots
\end{aligned}$$

The right-hand side can be thought of as any array of digits, and the diagonal entries of this array form a sequence $x_{1,1}, x_{2,2}, x_{3,3}, \ldots$. Make a new sequence $d_1, d_2, d_3, \ldots$ of digits, by letting

$$d_i = \begin{cases} 1 & \text{if } x_{i,i} \neq 1 \\ 5 & \text{if } x_{i,i} = 1, \end{cases}$$

and then let

$$d = 0.d_1d_2d_3\ldots \in [0,1).$$

For each i, it is clear from the definition of d_i that $d_i \neq x_{i,i}$; that is, the ith digit of d is different from the ith digit of x_i. Therefore, for each i, we have $d \neq x_i$.* So d is an element of $[0,1)$ that is not in the list $x_1, x_2, x_3, \ldots$. This contradicts the fact that $x_1, x_2, x_3, \ldots$ is a list of *all* the numbers in $[0,1)$. □

EXERCISES 15.50.

1) Show that the interval $(0,1)$ is uncountable.
[*Hint:* $[0,1) = (0,1) \cup \{0\}$ is uncountable.]

2) Suppose $a, b \in \mathbb{R}$. Show that if $a < b$, then the interval (a,b) has the same cardinality as $(0,1)$.
[*Hint:* Define $f\colon (0,1) \to (a,b)$ by $f(x) = a + (b-a)x$.]

3) Suppose $a \in \mathbb{R}$. Show that the interval (a,∞) has the same cardinality as $(0,1)$.
[*Hint:* Define $f\colon (0,1) \to (a,\infty)$ by $f(x) = (1/x) + a - 1$.]

4) Decide which of the following sets are countable, and which are uncountable. (*You do not need to justify your answers.*)
   (a) $[3, 3.1]$.
   (b) $\{1, 2, 3, \ldots, 1000\}$.
   (c) $\mathbb{Z} \times \mathbb{Z}$.
   (d) $\mathbb{Z} \times \mathbb{Q}$.
   (e) $\mathbb{Z} \times \mathbb{R}$.
   (f) $\mathbb{R} \setminus \mathbb{Q}$.
   (g) $\{\, (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \,\}$.
   (h) $\{\, (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = -1 \,\}$.

15F.2. The cardinality of power sets. If A is a finite set, then the set $\mathcal{P}(A)$ of all subsets of A is also finite. (Indeed, $\#\mathcal{P}(A) = 2^{\#A}$.) However, this assertion does *not* remain true when the word "finite" is replaced with "countable":

EXERCISE 15.51. Show that $\mathcal{P}(\mathbb{N}^+)$ is uncountable.
[*Hint:* For any $f\colon \mathbb{N}^+ \to \mathcal{P}(\mathbb{N}^+)$, the set $\{\, i \in \mathbb{N}^+ \mid i \notin f(i) \,\}$ is not in the image of f.]

For every set A, not just the countable ones, the same argument shows that the cardinality of $\mathcal{P}(A)$ is greater than the cardinality of A. Thus, there is no "largest" infinite set. For every set, there is always some set that has *much* larger cardinality.

EXERCISE 15.52. Show, for every set A, that there does not exist an onto function $f\colon A \to \mathcal{P}(A)$.
[*Hint:* The set $\{\, a \in A \mid a \notin f(a) \,\}$ is not in the image of f.]

15F.3. Examples of irrational numbers. Since $\mathbb{Q}$ is countable, but $\mathbb{R}$ is uncountable, there must be many, many real numbers that are not rational. Such numbers are said to be **irrational**. After proving a lemma, we give a simple example of an irrational number.

LEMMA 15.53. *Suppose $n \in \mathbb{Z}$. Show that if $2 \mid n^2$, then $2 \mid n$.*

*The digits of d are only 1's and 5's, so it is not a problem that numbers ending $000\ldots$ can also be expressed as a different decimal that ends $999\ldots$.

PROOF. We prove the contrapositive: assume $2 \nmid n$, and we wish to show that $2 \nmid n^2$. By the Division Algorithm (17.20), there exist $q, r \in \mathbb{Z}$, such that $n = 2q + r$, and $r \in \{0, 1\}$. Since $2 \nmid n$, we know $r \neq 0$; hence $r = 1$. Thus, $n = 2q + 1$. Therefore

$$n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 2(2q^2 + 2q) + 1 \equiv 1 \not\equiv 0 \pmod 2,$$

so $2 \nmid n^2$, as desired. □

PROPOSITION 15.54. *$\sqrt{2}$ is irrational.*

PROOF BY CONTRADICTION. Suppose $\sqrt{2}$ is rational. (This will lead to a contradiction.) By definition, this means $\sqrt{2} = a/b$ for some $a, b \in \mathbb{Z}$, with $b \neq 0$. By reducing to lowest terms, we may assume that a and b have no common factors. In particular,

it is not the case that both a and b are even.

We have

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

so $a^2 = 2b^2$ is even. Then Lemma 15.53 tells us that

a is even,

so we have $a = 2k$, for some $k \in \mathbb{Z}$. Then

$$2b^2 = a^2 = (2k)^2 = 4k^2,$$

so $b^2 = 2k^2$ is even. Then Lemma 15.53 tells us that

b is even.

We have now shown that a and b are even, but this contradicts the fact, mentioned above, that it is not the case that both a and b are even. □

EXERCISES 15.55.

1) For $n \in \mathbb{Z}$, show that if $3 \nmid n$, then $n^2 \equiv 1 \pmod 3$.

2) Show that $\sqrt{3}$ is irrational.

3) Is $\sqrt{4}$ irrational?

SUMMARY:

- Important definitions:
  - cardinality
  - finite, infinite
  - countable, countably infinite
  - uncountable
  - irrational
- A and B have the same cardinality iff there is a bijection from A to B.
- Pigeonhole Principle
- For finite sets A and B, we have $\#(A \times B) = \#A \cdot \#B$.
- A formula was given for the cardinality of $A \cup B$.
- Some properties of countable sets were studied. In particular:
  - a countable union of countable sets is countable; and
  - the cartesian product of two countable sets is countable.
- $\mathbb{N}, \mathbb{Z}$, and $\mathbb{Q}$ are countable; $\mathbb{R}$ is uncountable.
- $\mathcal{P}(A)$ has larger cardinality than A, for any set A.
- Notation:
  - $\#A$

Chapter 16

Proof by Induction

An idea which can be used once is a trick. If it can be used more than once it becomes a method.

George Pólya (1887–1985) and Gábor Szegő (1895–1985), Hungarian mathematicians
Problems and Theorems in Analysis

In this chapter, we introduce a special kind of proof, called **proof by induction**, that is often used to prove assertions about natural numbers. This topic requires an understanding of sets and predicates (which were introduced in Chapter 5), but not the full theory of First-Order Logic.

You are familiar with many of the properties of natural numbers, such as:

- the commutative laws: $x + y = y + x$ and $xy = yx$,
- the associative laws: $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$, and
- the distributive laws: $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.

These properties are also true for rational numbers, and for real numbers.

In this chapter, we discuss a very useful property of $\mathbb{N}$ that is not true of $\mathbb{Q}$ or $\mathbb{R}$.

16A. The Principle of Mathematical Induction

REMINDER 16.1. To say that $P(n)$ is a **predicate** of natural numbers, means that, for each natural number n, we have an assertion $P(n)$ that is either true or false. Some examples of predicates are:

$P_{\text{odd}}(n)$: n is odd;
$P_{\text{big}}(n)$: $n > 1000$;
$P_{\text{square}}(n)$: $\exists k \in \mathbb{N}, (n = k^2)$;
$P_{\text{prime}}(n)$: n is a prime number.

AXIOM 16.2 (Mathematical Induction). *Suppose $P(n)$ is a predicate of natural numbers. If*

(i) *$P(1)$ is true, and*

(ii) *for every $k \geq 2$, $\big(P(k-1) \Rightarrow P(k)\big)$,*

then $P(n)$ is true for all $n \in \mathbb{N}^+$.

TERMINOLOGY 16.3.

- In a proof using Mathematical Induction, establishing (i) is called the **base case**, and establishing (ii) is the **induction step**.

- In the induction step, we are proving $P(k-1) \Rightarrow P(k)$, so we assume that $P(k-1)$ is true (and establish $P(k)$). This assumption $P(k-1)$ is called the **induction hypothesis**.

Remark 16.4. Although we cannot *prove* Axiom 16.2, we can give it an informal justification that may convince you to accept it as a valid property of $\mathbb{N}$: Let n be an arbitrary element of $\mathbb{N}^+$.

- From (i), we know $P(1)$ is true.
- From (ii), we know $P(2-1) \Rightarrow P(2)$ is true.
  Since $P(2-1) = P(1)$ is true, we conclude, by $\Rightarrow$-elimination, that $P(2)$ is true.
- From (ii), we know $P(3-1) \Rightarrow P(3)$ is true.
  Since $P(3-1) = P(2)$ is true, we conclude, by $\Rightarrow$-elimination, that $P(3)$ is true.
- From (ii), we know $P(4-1) \Rightarrow P(4)$ is true.
  Since $P(4-1) = P(3)$ is true, we conclude, by $\Rightarrow$-elimination, that $P(4)$ is true.

  $\vdots$
- From (ii), we know $P(n-1) \Rightarrow P(n)$ is true.
  Since $P(n-1)$ is true, we conclude, by $\Rightarrow$-elimination, that $P(n)$ is true.

Since n is an arbitrary element of $\mathbb{N}^+$, we conclude that $P(n)$ is true for all $n \in \mathbb{N}^+$.

Here is an example of how mathematical induction can be used.

PROPOSITION 16.5. *For any natural number n, we have*

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

PROOF BY INDUCTION. Define

$$P(n)\colon 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

(i) *Base case.* For $n = 1$, we have

$$1 + 2 + 3 + \cdots + n = 1 \quad \text{and} \quad \frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1.$$

Since these are equal, $P(1)$ is true.

(ii) *Induction step.* Assume $P(k-1)$ is true. This means that

$$1 + 2 + 3 + \cdots + (k-1) = \frac{(k-1)\big((k-1)+1\big)}{2}.$$

Hence

$$\begin{aligned}
&1+2+3+\cdots+(k-1)+k \\
&\quad=\big(1+2+3+\cdots+(k-1)\big)+k \\
&\quad=\frac{(k-1)\big((k-1)+1\big)}{2}+k && \text{(induction hypothesis)} \\
&\quad=\frac{(k-1)k}{2}+k \\
&\quad=k\left(\frac{k-1}{2}+1\right) \\
&\quad=k\left(\frac{k+1}{2}\right) \\
&\quad=\frac{k(k+1)}{2},
\end{aligned}$$

so $P(k)$ is true.

Therefore, by the Principle of Mathematical Induction, we have

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

for every natural number n. □

Remark 16.6. A proof by induction is often used to show that two functions $f(n)$ and $g(n)$ are equal. (Proposition 16.5 is an example of this, with $f(n) = 1+2+3+\cdots+n$ and $g(n) = n(n+1)/2$.) The base case, verifying that $f(1) = g(1)$ is usually easy. On the other hand, it is usually not immediately obvious how to do the induction step, so it is a good idea to start by doing some scratch work:

- Write down the desired equality $f(k) \stackrel{?}{=} g(k)$.
- Then use algebraic simplifications, together with the induction hypothesis $f(k-1) = g(k-1)$, to arrive at a true statement.

A proof can then be obtained by rewriting these algebraic steps in a logical order (preferably, as a "one-line proof" – a string of equalities that starts with $f(k)$ and ends with $g(k)$).

For example, Figure 16.1 shows the scratch work that led to the above proof of Proposition 16.5. In this case, the algebraic manipulations are fairly simple, but some problems are considerably more difficult.

EXERCISES 16.7. Prove each formula by Mathematical Induction.

1) $2+4+6+8+\cdots+2n = n(n+1)$.

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

3) $2+7+12+17+\cdots+(5n-3) = \dfrac{n(5n-1)}{2}$.

NOTATION 16.8. It is often necessary to add up a long list of numbers (as in the above exercises), so it is convenient to have a good notation for this: if $a_1, a_2, \ldots, a_n$ is any sequence of numbers, then the sum $a_1 + a_2 + \cdots + a_n$ can be denoted by

$$\sum_{k=1}^{n} a_k.$$

$$1+2+3+\cdots+k \stackrel{?}{=} \frac{k(k+1)}{2}$$

$$\big(1+2+3+\cdots+(k-1)\big)+k \stackrel{?}{=} \frac{k(k+1)}{2}$$

$$\frac{(k-1)\big((k-1)+1\big)}{2}+k \stackrel{?}{=} \frac{k(k+1)}{2} \qquad \begin{pmatrix}\text{induction}\\ \text{hypothesis}\end{pmatrix}$$

$$\frac{(k-1)k}{2}+k \stackrel{?}{=} \frac{k(k+1)}{2}$$

$$\left(\frac{(k-1)}{2}+1\right)k \stackrel{?}{=} \frac{k(k+1)}{2}$$

$$\left(\frac{(k+1)}{2}\right)k \stackrel{?}{=} \frac{k(k+1)}{2} \qquad \checkmark$$

Figure 16.1. Scratch work for the proof of Proposition 16.5.

(The symbol $\sum$ is a capital sigma, the Greek version of the letter S — it stands for "sum".)

EXAMPLE 16.9. Let $a_1, a_2, \ldots, a_n$ be a sequence of numbers. Then:

1) $\displaystyle\sum_{k=1}^{1} a_k = a_1, \quad \sum_{k=1}^{2} a_k = a_1 + a_2, \quad \text{and} \quad \sum_{k=1}^{3} a_k = a_1 + a_2 + a_3.$

2) $\displaystyle\sum_{k=1}^{1} k = 1, \quad \sum_{k=1}^{2} k = 1+2 = 3, \quad \sum_{k=1}^{3} k = 1+2+3 = 6.$

3) $\displaystyle\sum_{k=1}^{n} k = 1+2+3+\cdots+n.$

4) For any $n \in \mathbb{N}^+$, we have $\displaystyle\sum_{k=1}^{n} a_k = \left(\sum_{k=1}^{n-1} a_k\right) + a_n.$

EXERCISES 16.10.

1) In Exercise 16.7, the left-hand side of each formula is a sum. Write each of these sums in $\sum$-notation.

2) Show that 16.9(1) and 16.9(4) imply $\displaystyle\sum_{k=1}^{0} a_k = 0.$

Remark 16.11. In the Induction Step, we wish to prove

$$\forall k \geq 2, \big(P(k-1) \Rightarrow P(k)\big).$$

Since k is a bound ("dummy") variable in this assertion, there is no harm in replacing it with a different letter: for example, if you prefer, it is perfectly acceptable to prove, say,

$$\forall i \geq 2, \big(P(i-1) \Rightarrow P(i)\big), \quad \text{or} \quad \forall n \geq 2, \big(P(n-1) \Rightarrow P(n)\big).$$

This is important to keep in mind when the variable k is already being used for something else.

EXAMPLE 16.12. Show that

$$\sum_{k=1}^{n}(2k-5) = n^2 - 4n.$$

PROOF BY INDUCTION. Define $P(n)$ to be the assertion

$$\sum_{k=1}^{n}(2k-5) = n^2 - 4n.$$

(i) *Base case.* For $n = 1$, we have

$$\sum_{k=1}^{n}(2k-5) = \sum_{k=1}^{1}(2k-5) = 2(1) - 5 = -3 = 1^2 - 4(1) = n^2 - 4n.$$

So $P(1)$ is true.

(ii) *Induction step.* Assume $n \geq 2$ and $P(n-1)$ is true. This means that

$$\sum_{k=1}^{n-1}(2k-5) = (n-1)^2 - 4(n-1).$$

Hence

$$\begin{aligned}
\sum_{k=1}^{n}(2k-5) &= \left(\sum_{k=1}^{n-1}(2k-5)\right) + (2n-5) \\
&= \big((n-1)^2 - 4(n-1)\big) + (2n-5) && \text{(Induction Hypothesis)} \\
&= \big((n^2 - 2n + 1) - 4n + 4\big) + (2n-5) \\
&= n^2 - 4n,
\end{aligned}$$

so $P(n)$ is true.

Therefore, by the Principle of Mathematical Induction, we conclude that $P(n)$ is true for every $n \in \mathbb{N}^+$. □

EXERCISES 16.13. Prove each formula by Mathematical Induction.

1) $\displaystyle\sum_{k=1}^{n}(6k+7) = 3n^2 + 10n.$

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

3) $\displaystyle\sum_{k=0}^{n} ar^k = a\frac{r^{n+1} - 1}{r - 1}.$

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

5) (harder) $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2.$

16B. Proofs about sets

Here is a basic fact that may seem to be obvious, but that would be difficult or impossible to prove without using induction.

THEOREM 16.14. *Every subset of any finite set is finite.*

PROOF. Define $P(n)$ to be the assertion

$$\text{If } A \text{ is any set with } \#A = n, \text{ then every subset of } A \text{ is finite.}$$

(i) *Base case.* Assume $n = 0$, and let B be any subset of A. Now $\#A = n = 0$, so $A = \emptyset$. Since the only subset of the empty set is the empty set, we have $B = \emptyset$. Hence $\#B = 0$, so B is finite.

(ii) *Induction step.* Assume $n \geq 1$, and that $P(n-1)$ is true, and let B be any subset of A. We may assume B is a proper subset of A. (Otherwise, we have $B = A$, so $\#B = \#A = n$, which means that B is finite.) Thus, there exists $a \in A$, such that $a \notin B$. Let $A' = A \smallsetminus \{a\}$. Then $\#A' = n - 1$ and $B \subset A'$. So the induction hypothesis tells us that B is finite. □

DEFINITION 16.15. Suppose $A_1, A_2, \ldots, A_n$ are sets. Then

$$\bigcup_{i=1}^{n} A_i = \big\{\, x \mid \exists i \in \{1, 2, \ldots, n\}, x \in A_i \,\big\}.$$

EXERCISE 16.16. Suppose $A_1, A_2, \ldots, A_n$ are sets.

1) Show $\bigcup_{i=1}^{1} A_i = A_1$.

2) If $n > 1$, show $\bigcup_{i=1}^{n} A_i = \left(\bigcup_{i=1}^{n-1} A_i\right) \cup A_n$.

3) Show $\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$.

EXERCISE 16.17. Suppose the sets $A_1, A_2, \ldots, A_n$ are pairwise-disjoint. Show:

1) The sets $A_1, A_2, \ldots, A_{n-1}$ are pairwise-disjoint, if $n > 1$.

2) A_n is disjoint from $A_1 \cup A_2 \cup \cdots \cup A_{n-1}$, if $n > 1$.

3) $\#(A_1 \cup A_2 \cup \cdots \cup A_n) = \#A_1 + \#A_2 + \cdots + \#A_n$.

EXERCISES 16.18. 1) Suppose $A_1, A_2, \ldots, A_n$ are finite sets. Show

$$\#(A_1 \cup A_2 \cup \cdots \cup A_n) \leq \#A_1 + \#A_2 + \cdots + \#A_n.$$

[*Hint:* The induction step uses Proposition 15.27.]

2) Prove the Pigeonhole Principle (15.20). [*Hint:* If $\#(A_1 \cup A_2 \cup \cdots \cup A_n) > n$, then the preceding exercise implies $\#A_i \geq 2$, for some i.]

EXERCISE 16.19. Explain what is wrong with the following "proof" that all horses have the same colour.

Attempt at a proof by induction. Define

$$P(n)\text{: In every set of } n \text{ horses, all of the horses have the same colour.}$$

(i) *Base case.* For $n = 1$, let H be any set of n horses. Since $n = 1$, there is only one horse in H, so it is obvious that all of the horses in H have the same colour.

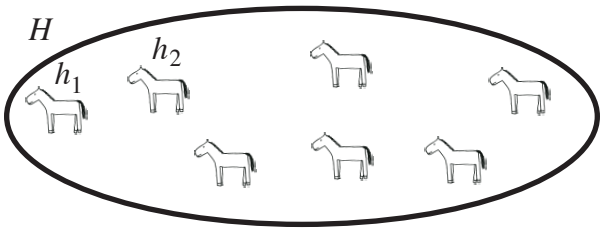
(ii) *Induction step.* Assume $n > 1$, and let H be any set of n horses. Remove one horse h_1 from H to form a set H_1 of $n - 1$ horses. By the induction hypothesis, we know that

(16.20) all of the horses in H_1 have the same colour.

Now, remove some other horse h_2 from H to form a different set H_2 of $n-1$ horses. By applying the induction hypothesis again, we know that

(16.21) all of the horses in H_2 have the same colour.

Now, since H_1 and H_2 each contain all but one of the elements of H, they have an intersection. (Namely, all of the horses other than h_1 and h_2 are in both H_1 and H_2.)



Therefore, we may choose some horse h that is in both H_1 and H_2. Then, from (16.21) and (16.21), we see that all of the horses in H_1 have the same colour as h, and so do all of the horses in H_2. So all of the horses in $H_1 \cup H_2$ have the same colour (namely, the colour of horse h). Since it is clear that $H = H_1 \cup H_2$ (because H_1 contains every horse except h_1, which is in H_2), we conclude that all of the horses in H have the same colour.

By the Principle of Mathematical Induction, we conclude that, in every (finite) set of horses, all of the horses have the same colour. □

If you wish to prove that $P(k)$ is true for every natural number k, then the Principle of Induction can be applied with k in the role of n. This is called "inducting on k." Similarly, any other letter can be used in place of n.

EXAMPLE 16.22. Show, for all $k \in \mathbb{N}^+$, that

$$\sum_{i=1}^{k}(3i^2 - 3i + 1) = k^3.$$

PROOF BY INDUCTION. Define $P(k)$ to be the assertion

$$\sum_{i=1}^{k}(3i^2 - 3i + 1) = k^3.$$

(i) *Base case.* For $k = 1$, we have

$$\sum_{i=1}^{k}(3i^2 - 3i + 1) = \sum_{i=1}^{1}(3i^2 - 3i + 1) = 3(1)^2 - 3(1) + 1 = 1 = 1^3 = k^3.$$

So $P(1)$ is true.

(ii) *Induction step.* Assume $k \geq 2$ and $P(k-1)$ is true. This means that

$$\sum_{i=1}^{k-1}(3i^2 - 3i + 1) = (k-1)^3.$$

Hence

$$\begin{aligned}\sum_{i=1}^{k}(3i^2-3i+1) &= \left(\sum_{i=1}^{k-1}(3i^2-3i+1)\right)+(3k^2-3k+1)\\ &= (k-1)^3+(3k^2-3k+1) && \text{(Induction Hypothesis)}\\ &= (k^3-3k^2+3k-1)+(3k^2-3k+1)\\ &= k^3,\end{aligned}$$

so $P(k)$ is true.

By the Principle of Mathematical Induction, we conclude that $P(k)$ is true for all $k \in \mathbb{N}^+$.□

WARNING. Mathematical induction is a method that is used extensively by mathematicians and computer scientists. However, other scientists (and also philosophers) use the word "induction" to refer to a quite different method of reasoning: scientific induction (or inductive reasoning) is the process of deriving a general rule from specific examples. (It is the opposite of deductive reasoning, where specific conclusions are derived from general rules.) For example, a scientist might measure the length and the width of very many rectangles, and compare with the areas of the rectangles. He or she would find that the area always came out to be the product of the length with the width. The scientist would then conclude (by inductive reasoning) that the area of every rectangle is the product of its length and its width. However, this does *not* constitute a *mathematical proof* of the formula for the area of a rectangle.

16C. Other versions of Induction

It is sometimes difficult to apply the Principle of Mathematical Induction in the form we have stated in Axiom 16.2. The following exercise provides some alternative versions that are more useful in some of those situations.

EXERCISES 16.23. (*harder*) Suppose $P(n)$ is a predicate of natural numbers.

1) (Strong induction) Show that if

   (i) $P(1)$ is true, and

   (ii) for every $n \geq 2$,
   $$\Big(\big(\text{for every } k \in \{1,2,\ldots,n-1\}, P(k)\big) \Rightarrow P(n)\Big),$$

   then $P(n)$ is true for all $n \in \mathbb{N}^+$.

2) (Generalized induction) Let $m \in \mathbb{N}^+$. Show that if

   (i) $P(m)$ is true, and

   (ii) for every $n > m$, $\big(P(n-1) \Rightarrow P(n)\big)$,

   then $P(n)$ is true for all $n \geq m$.

3) (Strong induction with multiple base cases) Let $m \in \mathbb{N}^+$. Show that if

   (i) $P(k)$ is true for all $k \in \{1,2,\ldots,m\}$, and

   (ii) for every $n > m$,
   $$\Big(\big(\text{for every } k \in \{1,2,\ldots,n-1\}, P(k)\big) \Rightarrow P(n)\Big),$$

   then $P(n)$ is true for all $n \in \mathbb{N}^+$.

4) Show that if

   (i) $P(1)$ is true, and

(ii) for every $k \in \mathbb{N}^+$, $P(k) \Rightarrow P(k+1)$,

then $P(n)$ is true for all $n \in \mathbb{N}^+$.

Remark 16.24. There are many other versions of induction. For example, if you wish to prove that $P(n)$ is true for all $n \in \mathbb{N}$ (rather than only for all $n \in \mathbb{N}^+$), then

i) your base case would be to prove $P(0)$, and

ii) your induction step would be to prove $P(n-1) \Rightarrow P(n)$, for all $n \geq 1$.

EXERCISES 16.25. The **Fibonacci sequence** (F_n) is defined by:

- $F_1 = 1$,
- $F_2 = 1$, and
- $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$.

(For example, $F_3 = F_{3-1} + F_{3-2} = F_2 + F_1 = 1 + 1 = 2$.) The first few terms of the sequence are:

$$1, 1, 2, 3, 5, 8, 13, \ldots$$

(Each term is the sum of the two preceding terms.)

Prove each assertion by induction. (You may want to use one of the alternative versions presented in Exercise 16.23.)

1) $F_{n+4} + F_n = 3F_{n+2}$.

2) $\sum_{k=1}^{n} F_k = F_{n+2} - F_2$.

3) $\sum_{k=1}^{n} F_k^2 = F_n F_{n+1}$.

4) $F_{n-1}F_{n+1} = F_n^2 + (-1)^n$, for all $n \geq 2$.

5) $F_n = \dfrac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$, for all $n \in \mathbb{N}^+$.

Here is a standard piece of advice:

SUGGESTION 16.26. *Whenever you need to prove a statement with an n in it, induction is a method that deserves consideration.*

Induction is not only for proving equalities:

EXAMPLE 16.27. Use induction to prove that $F_n < 2^n$, for every $n \in \mathbb{N}^+$.

PROOF BY INDUCTION. More precisely, we use strong induction with 2 bases cases. Define

$$P(n) : F_n < 2^n.$$

(i) *Base cases.* We have

$$F_1 = 1 < 2 = 2^1,$$

and

$$F_2 = 1 < 4 = 2^2,$$

so $P(1)$ and $P(2)$ are true.

(ii) *Induction step.* Assume $n \geq 3$, and that $P(n-1)$ and $P(n-2)$ are true. We have

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &< 2^{n-1} + 2^{n-2} && \text{(Induction Hypotheses)} \\ &< 2^{n-1} + 2^{n-1} \\ &= 2^n, \end{aligned}$$

so $P(n)$ is true.

By the Principle of Mathematical Induction (in the form of strong induction with multiple base cases), we conclude that $P(n)$ is true for all $n \in \mathbb{N}^+$. □

EXERCISES 16.28. 1) Use induction to prove, for every $n \geq 2$, that $3^n > 2^n + 2n$.

2) Prove $(1+x)^n \geq 1 + nx$ for all $x \in \mathbb{R}^+$ and all $n \in \mathbb{N}$.

The induction axiom (16.2) can be phrased in terms of sets, rather than properties:

EXERCISE 16.29. Suppose $S \subset \mathbb{N}^+$. Show that if

i) $1 \in S$, and

ii) for every $n \in S$, $\big(n+1 \in S\big)$,

then $S = \mathbb{N}^+$. [*Hint:* Because $S \subset \mathbb{N}^+$, it suffices to show $\mathbb{N}^+ \subset S$ (in other words, that every element of $\mathbb{N}^+$ is in S).]

SUMMARY:

- Important definitions:
  - Proof by induction
  - base case, induction step
  - induction hypothesis
- Proof by induction is a special kind of proof that allows us to prove facts about all positive natural numbers.
- There are several alternate forms of induction, including strong induction, generalized induction, and strong induction with multiple base cases.
- Notation:
  - $\sum_{k=1}^{n} a_k$ is the sum $a_1 + a_2 + \cdots + a_n$.
  - F_n is the nth term of the Fibonacci sequence.

Chapter 17

Divisibility and Congruence

He who can properly define and divide is to be considered a god.
Plato (428–348 B.C.), Greek philosopher

In this chapter, we will get some practice with proving properties of integers.

17A. Divisibility

Every math student knows that some numbers are even and some numbers are odd; some numbers are divisible by 3, and some are not; etc. Let us introduce a notation that makes it easy to talk about whether or not one number b is divisible by some other number a:

DEFINITION 17.1. Suppose $a, b \in \mathbb{Z}$. We say a is a **divisor** of b (and write "$a \mid b$") iff there exists $k \in \mathbb{Z}$, such that $ak = b$. (Since multiplication is commutative and equality is symmetric, this equation can also be written as $b = ka$.)

NOTATION 17.2. $a \nmid b$ is an abbreviation for "a does *not* divide b."

Remark 17.3. When a is a divisor of b, we may also say:

1) a **divides** b, or
2) b is a **multiple** of a, or
3) b is **divisible** by a.

EXAMPLE 17.4.

1) We have $5 \mid 30$, because $5 \cdot 6 = 30$, and $6 \in \mathbb{Z}$.
2) We have $5 \nmid 27$, because there is no integer k, such that $5k = 27$.

EXERCISE 17.5. Fill each blank with $\mid$ or $\nmid$, as appropriate.

1) 3_____18
2) 4_____18
3) 5_____18
4) 6_____18
5) 18_____6
6) -6_____6

The following definition is perhaps the best known example of divisibility.

DEFINITION 17.6. An integer n is:

- **even** iff $2 \mid n$;
- **odd** iff $2 \nmid n$.

Here are some examples of proofs involving divisibility. We will assume the well-known fact that the sum, difference, and product of integers are integers; that is, for all $k_1, k_2 \in \mathbb{Z}$, we know that $k_1 + k_2 \in \mathbb{Z}$, $k_1 - k_2 \in \mathbb{Z}$, and $k_1 k_2 \in \mathbb{Z}$. Also, the negative of any integer is an integer; that is, for all $k \in \mathbb{Z}$, we have $-k \in \mathbb{Z}$.

Our first result is a generalization of the well-known fact that the sum of two even numbers is even.

PROPOSITION 17.7. *Suppose $a, b_1, b_2 \in \mathbb{Z}$. If $a \mid b_1$ and $a \mid b_2$, then $a \mid (b_1 + b_2)$.*

PROOF. Since, by assumption, a is a divisor of both b_1 and b_2, there exist $k_1, k_2 \in \mathbb{Z}$, such that $ak_1 = b_1$ and $ak_2 = b_2$. Let $k = k_1 + k_2$. Then $k \in \mathbb{Z}$ and

$$ak = a(k_1 + k_2) = ak_1 + ak_2 = b_1 + b_2,$$

so a is a divisor of $b_1 + b_2$, as desired. □

PROPOSITION 17.8. *Suppose $a, b \in \mathbb{Z}$. We have $a \mid b$ iff $a \mid -b$.*

PROOF. ($\Rightarrow$) By assumption, there is some $k \in \mathbb{Z}$, such that $ak = b$. Then $-k \in \mathbb{Z}$, and we have $a(-k) = -ak = -b$, Therefore, a divides $-b$.

($\Leftarrow$) Assume $a \mid -b$. From the preceding paragraph, we conclude that $a \mid -(-b) = b$, as desired. □

EXERCISES 17.9. Assume $a, a', b, b' \in \mathbb{Z}$.

1) Show that if $a \mid b$ and $a \mid b'$, then $a \mid b - b'$.
2) Show that $a \mid b$ iff $-a \mid b$.
3) Show $1 \mid b$.
4) Show $a \mid 0$.
5) Show that if $0 \mid b$, then $b = 0$.
6) Show that if $a \mid b$, then $a \mid bb'$.
7) Show that if $a \mid b$ and $a' \mid b'$, then $aa' \mid bb'$.

PROPOSITION 17.10. *Suppose $a, b_1, b_2 \in \mathbb{Z}$. If $a \mid b_1$ and $a \nmid b_2$, then $a \nmid (b_1 + b_2)$.*

PROOF. Assume $a \mid b_1$ and $a \nmid b_2$.

Suppose $a \mid (b_1 + b_2)$. (This will lead to a contradiction.) Then a is a divisor of both $b_1 + b_2$ and (by assumption) b_1. So Exercise 17.9(1) tells us

$$a \mid \big((b_1 + b_2) - b_1\big) = b_2.$$

This contradicts the assumption that $a \nmid b_2$.

Because it leads to a contradiction, our hypothesis that $a \mid (b_1 + b_2)$ must be false. This means $a \nmid (b_1 + b_2)$. □

It is well known that 1 and -1 are the only integers whose reciprocal is also an integer. In the language of divisibility, this can be restated as the following useful fact:

For any integer n, we have $n \mid 1$ iff $n = \pm 1$.

EXERCISES 17.11.

1) Show that $\mid$ is reflexive: for all $a \in \mathbb{Z}$, we have $a \mid a$.
2) Show that $\mid$ is transitive: for all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

3) Show that $|$ is *not* symmetric: *disprove* the assertion that, for all $a, b \in \mathbb{Z}$, we have $a \mid b$ iff $b \mid a$.

EXERCISES 17.12. Prove or disprove each assertion.

1) For all $a, b_1, b_2 \in \mathbb{Z}$, if $a \nmid b_1$ and $a \nmid b_2$, then $a \nmid (b_1 + b_2)$.
2) For all $a, b_1, b_2 \in \mathbb{Z}$, if $a \nmid b_1$ and $a \nmid b_2$, then $a \nmid b_1 b_2$.
3) For all $a, b, c \in \mathbb{Z}$, if $a \nmid b$ and $b \nmid c$, then $a \nmid c$.
4) For all $a, b \in \mathbb{Z}$, if $a \nmid b$, then $a \nmid -b$.

17B. Congruence modulo n

DEFINITION 17.13. Suppose $a, b, n \in \mathbb{Z}$. We say a is **congruent to** b **modulo** n iff $a - b$ is divisible by n. The notation for this is:

$$a \equiv b \pmod{n}.$$

EXAMPLE 17.14.

1) We have $22 \equiv 0 \pmod 2$, because $22 - 0 = 22 = 11 \times 2$ is a multiple of 2. (More generally, for $a \in \mathbb{Z}$, one can show that $a \equiv 0 \pmod 2$ iff a is even.)
2) We have $15 \equiv 1 \pmod 2$, because $15 - 1 = 14 = 7 \times 2$ is a multiple of 2. (More generally, for $a \in \mathbb{Z}$, one can show that $a \equiv 1 \pmod 2$ iff a is odd.)
3) We have $28 \equiv 13 \pmod 5$, because $28 - 13 = 15 = 3 \times 5$ is a multiple of 5.
4) For any $a, n \in \mathbb{Z}$, it is not difficult to see that $a \equiv 0 \pmod n$ iff a is a multiple of n.

EXERCISES 17.15. Fill each blank with $\equiv$ or $\not\equiv$, as appropriate.

1) $14 \_\_\_\_ 5 \pmod 2$
2) $14 \_\_\_\_ 5 \pmod 3$
3) $14 \_\_\_\_ 5 \pmod 4$
4) $14 \_\_\_\_ 32 \pmod 2$
5) $14 \_\_\_\_ 32 \pmod 3$
6) $14 \_\_\_\_ 32 \pmod 4$

EXERCISES 17.16. Let $n \in \mathbb{Z}$.

1) Show that congruence modulo n is reflexive: for all $a \in \mathbb{Z}$, we have
$$a \equiv a \pmod{n}.$$
2) Show that congruence modulo n is symmetric: for all $a, b \in \mathbb{Z}$, we have
$$a \equiv b \pmod{n} \text{ iff } b \equiv a \pmod{n}.$$
3) Show that congruence modulo n is transitive: for all $a, b, c \in \mathbb{Z}$,
$$\text{if } a \equiv b \pmod{n} \text{ and } b \equiv c \pmod{n}, \text{ then } a \equiv c \pmod{n}.$$

EXERCISES 17.17. Assume $a_1 \equiv a_2 \pmod n$ and $b_1 \equiv b_2 \pmod n$. Show:

1) $a_1 + b_1 \equiv a_2 + b_2 \pmod n$.
2) $a_1 - b_1 \equiv a_2 - b_2 \pmod n$.
3) $a_1 b_1 \equiv a_2 b_2 \pmod n$. [*Hint:* $a_1 b_1 - b_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$.]

EXAMPLE 17.18. Suppose $a, b, n \in \mathbb{Z}$, with $a \equiv b \pmod n$. Show $a^k \equiv b^k \pmod n$, for all $k \in \mathbb{N}$.

PROOF. We induct on k. Define

$$P(k)\colon a^k \equiv b^k \pmod{n}.$$

(i) *Base case.* Since $a^1 = a$ and $b^1 = b$, the hypothesis $a \equiv b \pmod{n}$ tells us that

$$a^1 \equiv b^1 \pmod{n},$$

so $P(1)$ is true.

(ii) *Induction step.* Assume $P(k-1)$ is true. This means that

$$a^{k-1} \equiv b^{k-1} \pmod{n}.$$

By assumption, we also have

$$a \equiv b \pmod{n}.$$

Exercise 17.17(3) tells us that the product of congruent quantities is congruent, so we can multiply the above congruences, to conclude that

$$(a^{k-1})(a) \equiv (b^{k-1})(b) \pmod{n}.$$

In other words,

$$a^k \equiv b^k \pmod{n},$$

so $P(k)$ is true.

Therefore, by the Principle of Mathematical Induction, $P(k)$ is true for every natural number k. □

EXERCISES 17.19. Recall that the Fibonacci sequence $\{F_n\}$ was defined in Exercise 16.25.

1) Show F_{3k} is even, for all $k \in \mathbb{N}^+$.

2) Show F_{4k} is divisible by 3, for all $k \in \mathbb{N}^+$.

Children are taught that if a number a is divided by a number n, then there may be a remainder, but the remainder is always smaller than n. That idea is said more precisely in the following theorem:

THEOREM 17.20. *Suppose $a, n \in \mathbb{Z}$, and $n \neq 0$. Then there exist unique integers q and r in $\mathbb{Z}$, such that:*

1) $a = qn + r$, and

2) $0 \leq r < |n|$.

DEFINITION 17.21. In the situation of Theorem 17.20, the number r is called the **remainder** when a is divided by r.

The following exercise reveals the close relationship between congruence and remainders.

EXERCISE 17.22. Suppose $a, b, n \in \mathbb{Z}$ (and $n \neq 0$).

1) Let r be the remainder when a is divided by n.
Show $a \equiv r \pmod{n}$.

2) Show that $a \equiv b \pmod{n}$ iff a and b have the same remainder when divided by n.

Remark 17.23. From the general statements in parts (1) and (2) of Example 17.14, we see that every integer is congruent to either 0 or 1 modulo 2.

$$\boxed{\begin{array}{c} n \text{ is even iff } n \equiv 0 \pmod 2. \\ n \text{ is odd iff } n \equiv 1 \pmod 2. \end{array}}$$

Exercise 17.22(1) generalizes this to congruence modulo numbers other than 2: if $n \in \mathbb{N}^+$, then every integer is congruent (modulo n) to some number in $\{0, 1, 2, \ldots, n-1\}$.

EXAMPLE 17.24. Let us show that if n is odd, then $9n+6$ is also odd. To see this, note that:

- $9 \equiv 1 \pmod 2$, because $3 = 4(2) + 1$,
- $n \equiv 1 \pmod 2$, because n is odd, and
- $6 \equiv 0 \pmod 2$, because $6 = 3(2) + 0$.

Therefore, using Exercise 17.17, we have

$$9n + 6 \equiv (1)(1) + 0 \equiv 1 \pmod 2.$$

The same method can be applied in the following exercises:

EXERCISES 17.25. Let $n \in \mathbb{Z}$.

1) Show $6n + 3$ is odd.

2) Show that if n is even, then $5n + 3$ is odd.

3) Show that if n is odd, then $5n + 3$ is even.

PROPOSITION 17.26. *Let $n \in \mathbb{Z}$. Then $n^2 + n$ is even.*

PROOF. From Remark 17.23, we know that n is congruent to either 0 or 1 modulo 2. We consider these two possibilities as separate cases.

Case 1. Assume $n \equiv 0 \pmod 2$. By the assumption of this case, we have $n = 2q$, for some $q \in \mathbb{Z}$. Therefore

$$n^2 + n = (2q)^2 + 2q = 4q^2 + 2q = 2(2q^2 + q)$$

is divisible by 2.

Case 2. Assume $n \equiv 1 \pmod 2$. By the assumption of this case, we have $n = 2q + 1$, for some $q \in \mathbb{Z}$. Therefore

$$n^2 + n = (2q+1)^2 + (2q+1) = (4q^2 + 4q + 1) + (2q + 1) = 4q^2 + 6q + 2 = 2(2q^2 + 3q + 1)$$

is divisible by 2. □

EXERCISES 17.27. Let $n \in \mathbb{Z}$.

1) Show that if n is even, then $n^2 \equiv 0 \pmod 4$. [*Hint:* We have $n = 2q$, for some $q \in \mathbb{Z}$.]

2) Show that if n is odd, then $n^2 \equiv 1 \pmod 8$. [*Hint:* We have $n = 2q + 1$, for some $q \in \mathbb{Z}$.]

SUMMARY:

- Important definitions:
  - divisor, multiple
  - congruent modulo n
  - remainder
- Examples of proofs using divisibility.
- Congruence (mod n) is reflexive, symmetric, and transitive
- Notation:
  - $a \mid b$, $a \nmid b$
  - $a \equiv b \pmod{n}$

Chapter 18

Equivalence Relations

Mathematicians are like Frenchmen; when you say something to them, they translate it into their own language, and it immediately becomes something completely different.

Johann Wolfgang von Goethe (1749–1832), German writer
Maximen und Reflexionen #1279

18A. Binary relations

Recall that, by definition, any function $f\colon A \to B$ is a set of ordered pairs. More precisely, each element of f is an ordered pair (a, b), such that $a \in A$ and $b \in B$. Therefore, every element of f is an element of $A \times B$, so f is a subset of $A \times B$.

Every function from A to B is a subset of $A \times B$.

EXAMPLE 18.1. The function mother: PEOPLE $\to$ PEOPLE is represented by the set

$$\{\, (p, m) \in \text{PEOPLE} \times \text{PEOPLE} \mid m \text{ is the mother of } p \,\}.$$

Many other relationships can also be represented by subsets of PEOPLE $\times$ PEOPLE, even though they are not functions. For example, son is not a function, because some people have more than one son (or because some people have no sons at all). However, we can represent this relation by the set

$$\{\, (p, s) \in \text{PEOPLE} \times \text{PEOPLE} \mid s \text{ is a son of } p \,\}.$$

In fact, any relationship that you can define between two people (or, to say this in the official language of logic, any binary predicate on the set PEOPLE) can be represented by an subset of PEOPLE $\times$ PEOPLE. A few examples of possible relationships are:

- x is a sister of y
- x knew y in high school
- x is taller than y
- x and y are in the same math class
- etc.

In recognition of this, mathematicians simply *define* a relation to be a set of ordered pairs; that is, a relation is any subset of $A \times B$. Unlike the case of functions, there are no restrictions — every subset is a relation.

DEFINITION 18.2. Suppose A and B are sets.

1) Any subset of $A \times B$ is called a **relation from A to B**.

2) For the special case where $A = B$, any subset of $A \times A$ is called a **binary relation** on A.

We will mostly be concerned with binary relations, not relations from some set A to some other set B.

EXAMPLE 18.3. Some examples of binary relations on PEOPLE are: brother, sister, aunt, uncle, mother, father, grandfather, cousin, etc.

DEFINITION 18.4. We can draw a picture to represent any given binary relation on any given set A:

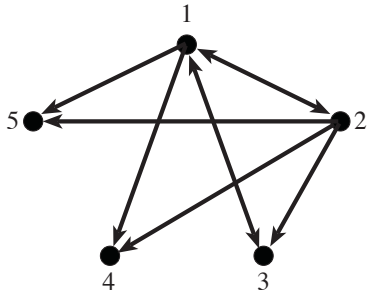
- Draw a dot for each element of A.
- For $a, b \in A$, draw an arrow from a to b if and only if (a, b) is an element of the relation.

The resulting picture is called a **digraph**. (The word is pronounced "DIE-graff" — it is short for "directed graph." We will see more on digraphs in Chapter 19.)

EXAMPLE 18.5. Let $A = \{1, 2, 3, 4, 5\}$. We can define a binary relation R on A by letting

$$R = \{\, (x, y) \mid x^2 + y < 10 \,\}.$$

This binary relation is represented by the following digraph:



For example, note that $(x, 4) \in R$ iff $x \in \{1, 2\}$, and the digraph has arrows from 1 to 4 and from 2 to 4.

EXERCISE 18.6. Let B be the set consisting of you, your siblings, your parents and your grandparents. Draw a digraph that represents each of the following binary relations on B.

1) The relation "has ever had the same last name as."

2) The relation "is a child of."

3) The relation "has ever been married to."

EXAMPLE 18.7. This book (like other mathematics textbooks) deals mainly with relations on sets of mathematical objects. Here are a few well-known examples:

1) The less-than relation "$<$" is a binary relation on $\mathbb{R}$.
That is, for any real numbers x and y, the assertion $x < y$ is either true or false.

2) The equality relation "$=$" is a binary relation on the entire universe of discourse $\mathcal{U}$.

3) The subset relation "$\subset$" is a binary relation on the collection of all sets in $\mathcal{U}$.

4) The relation "x is disjoint from y" is also a binary relation on the collection of all sets in $\mathcal{U}$.

NOTATION 18.8. Suppose R is a binary relation on a set A. For $a_1, a_2 \in A$:

1) To signify that $(a_1, a_2) \in R$, we may write $a_1 \; R \; a_2$.

2) To signify that $(a_1, a_2) \notin R$, we may write $a_1 \not R \; a_2$.

There are three basic properties that any given binary relation may or may not have:

DEFINITION 18.9. Suppose R is a binary relation on a set A.

1) We say that R is **reflexive** iff

$$\forall a \in A, (a \; R \; a).$$

2) We say that R is **symmetric** iff

$$\forall a, b \in A, \big((a \; R \; b) \Rightarrow (b \; R \; a)\big).$$

3) We say that R is **transitive** iff

$$\forall a, b, c \in A, \Big(\big((a \; R \; b) \; \& \; (b \; R \; c)\big) \Rightarrow (a \; R \; c)\Big).$$

EXAMPLE 18.10.

1) "$=$" is reflexive, symmetric, and transitive.

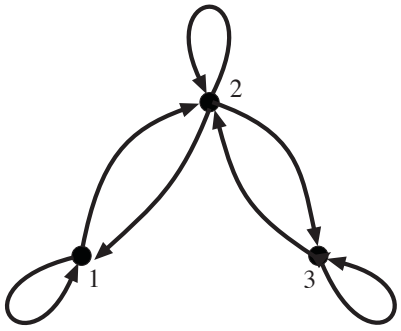
2) "$<$" is transitive, but neither reflexive nor symmetric.

3) "$\subset$" is transitive and reflexive, but not symmetric.

EXAMPLE 18.11. Consider the relation

$$R = \{(1,1), (2,2), (3,3), (1,2), (2,1), (2,3), (3,2)\}$$

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



1) R is reflexive, because $1 \; R \; 1$, $2 \; R \; 2$, and $3 \; R \; 3$.

2) R is symmetric, because, for each $(a, b) \in R$, the reversal (b, a) is also in R.

3) R is *not* transitive, because $1 \; R \; 2$ and $2 \; R \; 3$, but $1 \not R \; 3$.

EXERCISE 18.12. Find binary relations on $\{1, 2, 3\}$ that are:

1) symmetric, but neither reflexive nor transitive.

2) reflexive, but neither symmetric nor transitive.

3) transitive and symmetric, but not reflexive.

4) neither reflexive, nor symmetric, nor transitive.

(*Express each relation as a set of ordered pairs, draw the corresponding digraph, and briefly justify your answers.*)

18B. Definition and basic properties of equivalence relations

People often need to sort through a collection of objects, putting similar objects together in a group.

EXAMPLE 18.13. When making an inventory of the animals in a zoo, we may wish to count the number of antelopes, the number of baboons, the number of cheetahs, and so forth. In this case, all of the animals of the same species might be grouped together. Mathematically speaking, we would define a binary relation S on the set of animals in the zoo by

$$x \; S \; y \quad \text{iff} \quad x \text{ and } y \text{ are in the same species.}$$

When x and y are placed in the same group (that is, when $x \; S \; y$ in the above example), we may say that x is "equivalent" to y. This means that x and y are exactly the same in all respects that are of interest to us. (In the above example, we are interested only in the species of an animal, not its weight, or its age, or anything else.) We call the corresponding binary relation an "equivalence relation." Thus, the binary relation S in the above example is an equivalence relation.

EXAMPLE 18.14. Here are additional examples:

1) If we are interested only in first names, we could define an equivalence relation N on the set of all people by

$$x \; N \; y \text{ iff } x \text{ has the same first name as } y.$$

2) For any $n \in \mathbb{N}^+$, Exercise 17.16 tells us that congruence modulo n is reflexive, symmetric, and transitive, so it is an equivalence relation on $\mathbb{Z}$.

Remark 18.15. Suppose $\sim$ is an equivalence relation. (That is, we have $x \sim y$ iff x and y are exactly the same in all respects that are of interest to us.) Then we would expect:

1) $\sim$ is reflexive (x is the same as x),

2) $\sim$ is symmetric (if x is the same as y, then y is the same as x), and

3) $\sim$ is transitive (if x is the same as y, and y is the same as z, then x is the same as z).

This motivates the following definition:

DEFINITION 18.16. An **equivalence relation** on a set A is a binary relation on A that is reflexive, symmetric, and transitive.

Remark 18.17. Instead of representing an equivalence relation by a letter, it is traditional to use the symbol $\sim$ (or sometimes $\equiv$ or $\cong$).

EXAMPLE 18.18. Define a binary relation $\sim$ on $\mathbb{R}$ by $x \sim y$ iff $x^2 = y^2$. Then $\sim$ is an equivalence relation.

PROOF. We wish to show that $\sim$ is reflexive, symmetric, and transitive.

(reflexive) Given $x \in \mathbb{R}$, we have $x^2 = x^2$, so $x \sim x$.

(symmetric) Given $x, y \in \mathbb{R}$, such that $x \sim y$, we have $x^2 = y^2$. Since equality is symmetric, this implies $y^2 = x^2$, so $y \sim x$.

(transitive) Given $x, y, z \in \mathbb{R}$, such that $x \sim y$ and $y \sim z$, we have $x^2 = y^2$ and $y^2 = z^2$. Therefore $x^2 = y^2 = z^2$, so $x^2 = z^2$. Hence $x \sim z$. □

EXAMPLE 18.19. For any $n \in \mathbb{Z}$, we know that congruence modulo n is reflexive, symmetric, and transitive (see Exercise 17.16). Therefore, congruence modulo n is an equivalence relation.

EXAMPLE 18.20. Define a binary relation $\sim$ on $\mathbb{N}\times\mathbb{N}$ by $(a_1, b_1) \sim (a_2, b_2)$ iff $a_1+b_2 = a_2+b_1$. Then $\sim$ is an equivalence relation.

PROOF. We wish to show that $\sim$ is reflexive, symmetric, and transitive.

(reflexive) Given $(a, b) \in \mathbb{N} \times \mathbb{N}$, we have $a + b = a + b$, so $(a, b) \sim (a, b)$.

(symmetric) Given $(a_1, b_1), (a_2, b_2) \in \mathbb{N} \times \mathbb{N}$, such that $(a_1, b_1) \sim (a_2, b_2)$, we have $a_1 + b_2 = a_2 + b_1$. Since equality is symmetric, this implies $a_2 + b_1 = a_1 + b_2$, so $(a_2, b_2) \sim (a_1, b_1)$.

(transitive) Given $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{N}\times\mathbb{N}$, such that $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$, we have

(18.21)
$$a_1 + b_2 = a_2 + b_1 \text{ and } a_2 + b_3 = a_3 + b_2.$$

Therefore

$$\begin{aligned}(a_1 + b_3) + (a_2 + b_2) &= (a_1 + b_2) + (a_2 + b_3) && \text{(rearrange terms)}\\ &= (a_2 + b_1) + (a_3 + b_2) && \text{(18.21)}\\ &= (a_3 + b_1) + (a_2 + b_2) && \text{(rearrange terms).}\end{aligned}$$

Subtracting $a_2 + b_2$ from both sides of the equation, we conclude that $a_1 + b_3 = a_3 + b_1$, so $(a_1, b_1) \sim (a_3, b_3)$. □

EXERCISES 18.22. Show that each of these binary relations is an equivalence relation.

1) A binary relation $\sim$ on $\mathbb{R}$ is defined by $x \sim y$ iff $x^2 - 3x = y^2 - 3y$.
2) A binary relation $\sim$ on $\mathbb{R}$ is defined by $x \sim y$ iff $x - y \in \mathbb{Z}$. [*Hint:* You may assume (without proof) that the negative of any integer is an integer, and that the sum of any two integers is an integer. For transitivity, notice that $x - z = (x - y) + (y - z)$.]
3) A binary relation $\sim$ on $\mathbb{N}^+ \times \mathbb{N}^+$ is defined by $(a_1, b_1) \sim (a_2, b_2)$ iff $a_1b_2 = a_2b_1$. [*Hint:* Similar to the proof in Example 18.20, but with multiplication in place of addition.]

EXERCISE 18.23. Define a binary relation $\approx$ on the collection of all sets by

$$A \approx B \quad \text{iff} \quad A \text{ and } B \text{ have the same cardinality.}$$

1) Show that $\approx$ is an equivalence relation.
2) What is the equivalence class of $\mathbb{N}^+$?

Any time we have a function, we also get an equivalence relation on its domain.

EXAMPLE 18.24.

1) Every animal has only one species, so Species is a function that is defined on the set of all animals. The equivalence relation S of Example 18.13 can be characterized by
$$x \; S \; y \quad \text{iff} \quad \mathsf{Species}(x) = \mathsf{Species}(y).$$
2) If we assume that every person has a first name, then FirstName is a function on the set of all people. The equivalence relation N of Eg. 18.14(1) can be characterized by
$$x \; N \; y \quad \text{iff} \quad \mathsf{FirstName}(x) = \mathsf{FirstName}(y).$$

The following result generalizes this idea to all functions.

PROPOSITION 18.25. *Suppose $f\colon A \to B$. If we define a binary relation $\sim$ on A by*

$$a_1 \sim a_2 \quad \textit{iff} \quad f(a_1) = f(a_2),$$

then $\sim$ is an equivalence relation.

EXERCISE 18.26. Prove Proposition 18.25.

18C. Equivalence classes

If we are interested in first names (as in Eg. 18.14(1)), then we may also be interested in the set of all people who have the same first name as you. This is called your "equivalence class."

DEFINITION 18.27. Suppose $\sim$ is an equivalence relation on a set A. For each $a \in A$, the **equivalence class** of a is the following subset of A:

$$[a] = \{\, a' \in A \mid a' \sim a \,\}.$$

EXAMPLE 18.28. For the equivalence relation N described in Eg. 18.14(1), we have

$$[\mathsf{Alice\ Cooper}] = \{\, x \in \mathsf{People} \mid \mathsf{FirstName}(x) = \mathsf{FirstName}(\mathsf{Alice\ Cooper}) \,\}.$$

In other words, [Alice Cooper] is the set of all people whose first name is Alice.

WARNING. The notation $[a]$ does not tell us which equivalence relation is being used. This can be confusing if more than one equivalence relation is under consideration.

EXAMPLE 18.29. Suppose $A = \{1, 2, 3, 4, 5\}$ and

$$R = \left\{ \begin{matrix} (1,1), (1,3), (1,4), (2,2), (2,5), (3,1), (3,3), \\ (3,4), (4,1), (4,3), (4,4), (5,2), (5,5) \end{matrix} \right\}.$$

One can verify that R is an equivalence relation on A. The equivalence classes are:

$$[1] = \{1, 3, 4\}, \qquad [2] = \{2, 5\}, \qquad [3] = \{1, 3, 4\}$$

$$[4] = \{1, 3, 4\}, \qquad [5] = \{2, 5\}.$$

EXERCISES 18.30. *You do not need to show your work.*

1) Let $B = \{1, 2, 3, 4, 5\}$ and

$$S = \left\{ \begin{matrix} (1,1), (1,4), (2,2), (2,3), (3.2), \\ (3,3), (4,1), (4,4), (5,5) \end{matrix} \right\}.$$

Assume (without proof) that S is an equivalence relation on B. Find the equivalence class of each element of B.

2) Let $C = \{1, 2, 3, 4, 5\}$ and define T by

$$x\ T\ y \text{ iff } x + y \text{ is even.}$$

Assume (without proof) that T is an equivalence relation on C. Find the equivalence class of each element of C.

The following theorem presents some very important properties of equivalence classes:

THEOREM 18.31. *Suppose $\sim$ is an equivalence relation on a set A. Then:*

1) For all $a \in A$, we have $a \in [a]$.

2) For all $a \in A$, we have $[a] \neq \emptyset$.

3) The union of the equivalence classes is all of A. That is, we have $A = \bigcup_{a \in A} [a]$, where

$$\bigcup_{a \in A} [a] = \{\, x \mid \exists a \in A, (x \in [a]) \,\}.$$

4) For any $a_1, a_2 \in A$, such that $a_1 \sim a_2$, we have $[a_1] = [a_2]$.

5) For any $a_1, a_2 \in A$, such that $a_1 \not\sim a_2$, we have $[a_1] \cap [a_2] = \emptyset$.

EXERCISE 18.32. Prove Theorem 18.31.
[*Hint:* Use the fact that $\sim$ is reflexive, symmetric and transitive.]

Remark 18.33. Suppose $\sim$ is an equivalence relation on a set A. The above theorem implies that any two equivalence classes are either equal or disjoint; that is, either they have exactly the same elements, or they have no elements in common.

PROOF. Given two equivalence classes $[a_1]$ and $[a_2]$ that are not disjoint, we wish to show $[a_1] = [a_2]$. Since the equivalence classes are not disjoint, their intersection is nonempty, thus, there is some $a \in [a_1] \cap [a_2]$. Hence, $a \in [a_1]$ and $a \in [a_2]$. By definition of the equivalence classes, this means $a \sim a_1$ and $a \sim a_2$. Hence, Thm. 18.31(4) tells us that $[a] = [a_1]$ and $[a] = [a_2]$. Therefore $[a_1] = [a] = [a_2]$, as desired. □

18D. Modular arithmetic

Suppose, as usual, that $\sim$ is an equivalence relation on a set A. Writing $a \sim b$ means that a is "equivalent" to b. In this case, we may want to think of a as being *equal* to b. But that would not be right, because a and b are (probably) two different things. However, we have the following fundamental property of equivalence classes:

$$a \sim b \quad \text{iff} \quad [a] = [b].$$

Thus, by putting square brackets around a and b, we can turn mere equivalence into true equality. That is what makes equivalence classes so important. A good example is provided by congruence modulo n.

18D.1. The integers modulo 3. For any $n \in \mathbb{Z}$, we know that congruence modulo n is an equivalence relation (see Exercise 17.16). As an example, let us consider the case where $n = 3$. To emphasize the fact that $n = 3$, we will include a subscript $_3$ in the notation for an equivalence class: we write $[k]_3$, instead of $[k]$.

We all know that when an integer is divided by 3, the remainder must be either 0, 1, or 2, so Exercise 17.22(1) tells us that every integer is congruent (modulo 3) to either 0, 1, or 2. Thus,

- for every $k \in \mathbb{Z}$, the equivalence class $[k]_3$ must be either $[0]_3$, $[1]_3$, or $[2]_3$.

On the other hand, it is easy to check that no two of 0, 1, and 2 are congruent (modulo 3), so

- $[0]_3$, $[1]_3$, and $[2]_3$ are three distinct equivalence classes.

Thus, we see that there are exactly three equivalence classes, namely, $[0]_3$, $[1]_3$, and $[2]_3$. The set of these equivalence classes is called the **integers modulo** 3. It is denoted $\mathbb{Z}_3$.

NOTATION 18.34. The notation $[k]_3$ (or even just $[k]$) is rather cumbersome. For convenience, we may write $\overline{k}$ for the equivalence class of k. Thus,

$$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}.$$

DEFINITION 18.35. We can do arithmetic (add, subtract, and multiply) on these equivalence classes, just as we do for ordinary integers. This is called **arithmetic modulo** 3. The rules are:

- $[a]_3 + [b]_3 = [a+b]_3$ (or $\overline{a} + \overline{b} = \overline{a+b}$),
- $[a]_3 - [b]_3 = [a-b]_3$ (or $\overline{a} - \overline{b} = \overline{a-b}$), and
- $[a]_3 \times [b]_3 = [ab]_3$ (or $\overline{a} \times \overline{b} = \overline{ab}$).

(Actually, we should write $+_3$, $-_3$, and $\times_3$, to indicate that the arithmetic is being done modulo 3, but we will usually not bother.)

EXAMPLE 18.36. We have $[1]_3 + [2]_3 = [1+2]_3 = [3]_3$. However, since $3 \equiv 0 \pmod 3$, we have $[3]_3 = [0]_3$, so the above equation can also be written as $[1]_3 + [2]_3 = [0]_3$. Equivalently, $\overline{1} + \overline{2} = \overline{0}$.

This is an example of the following general principle:

If r is the remainder when $a+b$ is divided by 3, then $\overline{a} +_3 \overline{b} = \overline{r}$.

EXAMPLE 18.37. Here is a table that shows the results of addition modulo 3:

$+_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

EXERCISES 18.38. Make a table that shows the results of:

1) subtraction modulo 3.
2) multiplication modulo 3.

(*Write each of the entries of your table as either $\overline{0}$, $\overline{1}$, or $\overline{2}$.*)

18D.2. The integers modulo n. The preceding discussion can be generalized to apply with any integer n in place of 3. This results in **modular arithmetic**.

DEFINITION 18.39. Fix some nonzero natural number $n \in \mathbb{N}^+$.

1) For any integer k, we use $[k]_n$ to denote the equivalence class of k under congruence modulo n. When n is clear from the context, we may write $\overline{k}$, instead of $[k]_n$.
2) The set of these equivalence classes is called the **integers modulo** n. It is denoted $\mathbb{Z}_n$.
3) Addition, subtraction, and multiplication modulo n are defined by:
   - $\overline{a} +_n \overline{b} = \overline{a+b}$,
   - $\overline{a} -_n \overline{b} = \overline{a-b}$, and
   - $\overline{a} \times_n \overline{b} = \overline{ab}$.

   (When n is clear from the context, we usually write $+$, $-$, and $\times$, rather than $+_n$, $-_n$, and $\times_n$.)

Note that $\#\mathbb{Z}_n = n$. More precisely:

PROPOSITION 18.40. *For any $n \in \mathbb{N}^+$, we have*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

and $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ are all distinct.

EXERCISES 18.41.

1) Make tables that show the results of:
   (a) addition modulo 4.
   (b) subtraction modulo 5.
   (c) multiplication modulo 6.
2) Find $x, y \in \mathbb{Z}_{12}$, such that $x \neq \overline{0}$ and $y \neq \overline{0}$, but $xy = \overline{0}$.

18E. Functions need to be well defined

The discussion of modular arithmetic ignored a very important point: the operations of addition, subtraction, and multiplication need to be **well-defined**. That is, if $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$, then we need to know that

1) $\overline{a_1} +_n \overline{b_1} = \overline{a_2} +_n \overline{b_2}$,
2) $\overline{a_1} -_n \overline{b_1} = \overline{a_2} -_n \overline{b_2}$, and
3) $\overline{a_1} \times_n \overline{b_1} = \overline{a_2} \times_n \overline{b_2}$.

Fortunately, these statements are all true. Indeed, they follow easily from Exercise 17.17:

1) Since $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$, we have $a_1 \equiv a_2 \pmod{n}$ and $b_1 \pmod{b)_2} \pmod{n}$, so Exercise 17.17(1) tells us that $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$. Therefore $\overline{a_1 + b_1} = \overline{a_2 + b_2}$, as desired.

The proofs for $-_n$ and $\times_n$ are similar.

EXAMPLE 18.42. One might try to define an exponentiation operation by:

$$\overline{a} \wedge_n \overline{b} = \overline{a^b} \quad \text{for } \overline{a}, \overline{b} \in \mathbb{Z}_n.$$

Unfortunately, this does not work, because $\wedge_n$ is not well defined:

EXERCISE 18.43. Find $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, such that $[a_1]_3 = [a_2]_3$ and $[b_1]_3 = [b_2]_3$, but $\left[a_1^{b_1}\right]_3 \neq \left[a_2^{b_2}\right]_3$.

EXERCISES 18.44. Assume $m, n \in \mathbb{N}^+$.

1) Show that if $n > 2$, then absolute value does *not* provide a well-defined function from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. That is, show there exist $a, b \in \mathbb{Z}$, such that $[a]_n = [b]_n$, but $\big[|a|\big]_n \neq \big[|b|\big]_n$.
2) Show that if $m \mid n$, then there is a well-defined function
$$f\colon \mathbb{Z}_n \to \mathbb{Z}_m, \text{ given by } f\big([a]_n\big) = [a]_m.$$
3) Show that if we try to define a function $g\colon \mathbb{Z}_3 \to \mathbb{Z}_2$ by $g\big([a]_3\big) = [a]_2$, then the result is *not* well defined.

18F. Partitions

It often happens that someone divides up a set into several disjoint subsets. This is called a "partition" of the set.

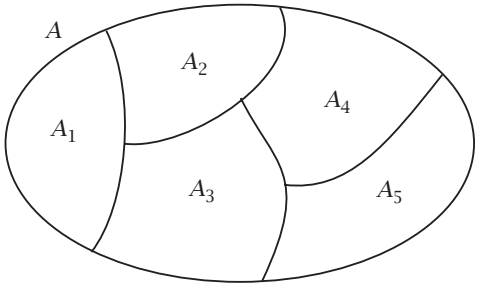


Figure 18.1. A partition of A into subsets $A_1, \ldots, A_5$. (Each element of A is in one and only one of the subsets.)

EXAMPLE 18.45. Mary is leaving for university, and does not want her childhood toys any more, so she will divide them up among her younger siblings: Alice, Bob, and Cindy. Let

- T be the set of all of Mary's toys, and
- A, B, and C be the set of toys that she will give to Alice, to Bob, and to Cindy, respectively.

Then A, B, and C are subsets of T, and they should be chosen so that:

1) the union of A, B and C is T (that is, $A \cup B \cup C = T$), so all of the toys are given away, and
2) the sets A, B, and C are pairwise disjoint (that is, $A \cap B = \emptyset$, $A \cap C = \emptyset$, and $B \cap C = \emptyset$), so there will not be any confusion about who is the new owner of each toy.

Thus, we see that Mary should partition T into three disjoint subsets.

DEFINITION 18.46. A **partition** of a set A is a collection of nonempty subsets of A, such that each element of A is in exactly one of the subsets. In other words:

1) the union of the subsets in the collection is all of A, and
2) the subsets in the collection are pairwise disjoint.

EXAMPLE 18.47. In Example 18.45, the collection $\{A, B, C\}$ is a partition of T.*

EXAMPLE 18.48. In Example 18.29, the equivalence classes are $\{1, 3, 4\}$ and $\{2, 5\}$. Since $1, 2, 3, 4, 5$ each belong to exactly one of these sets, we see that the set

$$\big\{\{1, 3, 4\}, \{2, 5\}\big\}$$

of equivalence classes is a partition of $\{1, 2, 3, 4, 5\}$.

The following result is an immediate consequence of Theorem 18.31. It says that equivalence classes always provide a partition.

COROLLARY 18.49. *Suppose $\sim$ is an equivalence relation on a set A. Then*

$$\{\, [a] \mid a \in A \,\}$$

is a partition of A.

PROOF. From parts (2), (3), and (5) of Theorem 18.31, we know that the equivalence classes are nonempty, that their union is A, and that they are pairwise disjoint. □

*Actually, this may not be correct, because, for a partition, we require the sets A, B, and C to be nonempty, but it is possible that one (or more) of Mary's siblings will not be given any toys.

Remark 18.50. Corollary 18.49 tells us that every equivalence relation gives us a partition. Conversely, the following proposition shows that any partition comes from an equivalence relation. Thus, equivalence relations and partitions are just two different ways of looking at the same thing.

PROPOSITION 18.51. *Suppose $\mathcal{P}$ is a partition of a set A. Define a binary relation $\sim$ on A by*

$$a \sim b \quad \textit{iff} \quad \exists C \in \mathcal{P}, (a \in C \textit{ and } b \in C).$$

Then:

1) $\sim$ is an equivalence relation on A, and

2) the set of equivalence classes is the partition $\mathcal{P}$.

Recall that $\mathbb{Z}_n$ replaces integers a and b that are congruent modulo n with objects $\overline{a}$ and $\overline{b}$ that are exactly equal to each other. This was achieved by letting $\mathbb{Z}_n$ be the set of all equivalence classes. The set $\mathbb{Z}_n$ applies only to congruence modulo n, but the same thing can be done for any equivalence relation:

DEFINITION 18.52. Suppose $\sim$ is an equivalence relation on a set A. The set of all equivalence classes is called A **modulo** $\sim$. It is denoted $A/\sim$.

EXAMPLE 18.53. Suppose we define an equivalence relation $\sim$ on $\mathbb{Z}$ by $a \sim b$ iff $a \equiv b \pmod{n}$. Then $\mathbb{Z}/\sim$ is simply another name for $\mathbb{Z}_n$.

SUMMARY:

- Important definitions:
  - relation, binary relation
  - reflexive, symmetric, transitive
  - equivalence relation
  - equivalence class
  - modular arithmetic
  - integers modulo n
  - well-defined
  - partition
- Modular arithmetic is an important example of the use of equivalence classes.
- Functions must be well-defined.
- Every binary relation can be drawn as a digraph.
- Every partition gives rise to an equivalence relation, and vice versa.
- Notation:
  - $\sim$, $\cong$, or $\equiv$ are used for equivalence relations
  - $[a]$, or $\overline{a}$
  - $\mathbb{Z}_n$

Part V

Topics

Chapter 19

Elementary Graph Theory

If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.

John von Neumann (1903–1957), Hungarian-American mathematician

19A. Basic definitions

In its simplest form, a *road map* consists of

- some towns, represented by dots, and
- some roads, represented by lines (or curved lines) that connect some of the dots.

Here is an example:

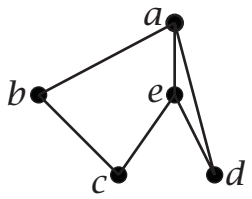


Figure 19.1. A road map.

The same picture could represent some other kind of network, rather than a road map, or it could even represent information of a very different type. For example:

- perhaps the dots represent individual computers in a lab, and a line between two dots indicates that the two computers are joined by an ethernet cable, or
- perhaps the dots represent airports, and a line between two dots indicates that there is a direct flight between the two airports, or
- perhaps the dots represent different species of animals, and a line joining the two dots indicates that they are competitors — there is some food that they both like to eat.

In mathematics and science, such a picture is called a *graph* (or *network*), rather than a road map. Also, instead of speaking of towns and roads (or dots and lines), we speak of *vertices* and *edges*. (The singular of vertices is *vertex*.)

This leads to the following definition.

DEFINITION 19.1.

1) A **graph** G consists of a set V of vertices and a set E of edges.
   - Each **vertex** of the graph is drawn as a dot.
   - Each **edge** of the graph is drawn as a line (or curved line) that connects two of the dots.
2) V is called the **vertex set** of G, and E is called the **edge set** of G.
3) Two vertices are said to be **adjacent** if they are joined by an edge. We may also say that they are **neighbours** of each other.
4) The number of neighbours of a vertex is its **valence**.
5) An edge is said to be **incident** with the two vertices that it connects.

Remark 19.2 (Alternative terminology). Some mathematicians use the term "degree" in place of "valence," for the number of neighbours of a particular vertex. However, as the term "degree" has other common mathematical meanings, the term "valence" has less potential for confusion.

ASSUMPTION 19.3. We always assume:

1) Graphs have at least one vertex; that is, $V \neq \emptyset$.
2) Graphs have only finitely many vertices, and finitely many edges; that is, the sets V and E are required to be finite.

We are most interested in a special kind of graph, called a *simple graph*. In such a graph, the following assumptions hold:

ASSUMPTION 19.4. In a **simple** graph:

1) We do not allow more than one edge to join the same two dots. Thus, you can specify a particular edge simply by naming the two vertices that it connects:

   if u and v are adjacent vertices,
   then uv denotes the edge that connects them.

2) Also, an edge must connect two *different* vertices: it is not allowed to connect an edge with itself (forming a loop).

Figure 19.2. Configurations like these are *not* allowed in a simple graph.

If we specify an edge of a graph
by naming the two vertices that it connects,
then you may assume that the graph involved is simple.

Remark 19.5. Suppose G is a simple graph.

1) Since the order in which we list the vertices does not affect the edge, the edge uv could also be referred to as the edge vu: edges are *not* ordered pairs. It is standard, but not obligatory, to list the vertices in alphabetical order when referring to an edge, if the vertices are labelled by letters.
2) The valence of any vertex v is equal to the number of edges that are incident with v.

EXAMPLE 19.6. Consider the graph drawn in Figure 19.1.

- $V = \{a, b, c, d, e\}$;
- $E = \{ab, ad, ae, bc, ce, de\}$;
- The neighbours of a are b, d, and e, because those are the vertices that are joined directly to a by an edge. (That is, they are the vertices that are adjacent to a.) Since a has 3 neighbours, the valence of a is 3.

EXERCISE 19.7. Find the neighbours and the valence of each vertex of the graph in Figure 19.1. (The answers for vertex a are given in the preceding example.)

Remark 19.8. It is often necessary to have some edges cross other edges when they are drawn (as in the following picture). Such crossings should not be thought of as intersections of the corresponding edges. If edges represent roads, then these crossings are interpreted as underpasses or overpasses, not as intersections.

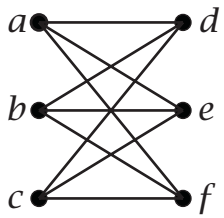


Figure 19.3. This graph cannot be drawn without crossing edges.

DEFINITION 19.9. Any simple graph G has a **complementary** simple graph G^c. We may also call G^c the **complement** of G.

- The vertices of G^c are the same as the vertices of G, but
- two vertices are adjacent in G^c if and only if they are *not* adjacent in G.

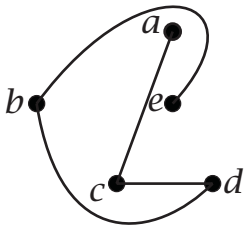


Figure 19.4. This is the complement of the graph in Figure 19.1. For example, b is adjacent to a and c in the original graph; it is adjacent to d and e (the other vertices) in this graph.

Remark 19.10. For a graph G with edge set E, the edges of the complementary graph G^c are precisely the elements of $\overline{E}$, where the universe is the set of all possible edges on the vertices of G. So the terminology we have used is consistent.

Remark 19.11 (optional). Our definitions of the terms *graph* and *simple graph* are sufficient for our purposes, but mathematicians like to be more precise. Although we have no need for it, the reader may be interested to see the following official definition:

> A **simple graph** is an ordered pair (V, E) of sets, such that:
> - V is a nonempty, finite set, and
> - each element of E is a 2-element subset of V.

This definition is the result of two considerations:

1) A graph has both a vertex set V and an edge set E (and it is important not to get confused which one is which). To keep track of these two sets, a mathematician puts them into an ordered pair (V, E).
2) An edge uv is determined by its endpoints u and v, and it does not matter whether we write u first, and then v, or write v first, and then u. That is exactly how the 2-element set $\{u, v\}$ acts, so mathematicians require uv to actually be equal to $\{u, v\}$.

EXERCISES 19.12.

1) For the graphs in (a) Figure 19.3, (b) Figure 19.4 and (c) Example 19.13 below:
   (i) Find the valence of each vertex.
   (ii) List all the neighbours of vertex c.
   (iii) Count the number of vertices of odd valence.
   (iv) Draw the complementary graph.
2) In each part of this problem:
   (i) Draw the graph with the given vertices and given edges (and no others).
   (ii) Find the valence of each vertex.
   (iii) Draw the complementary graph.
   (a) Vertices: a, b, c, d, and e.
   Edges: ab, ad, bd, be, cd, ce, and de.
   (b) Vertices: a, b, c, d, and e.
   Edges: ab, bc, bd, and be.
   (c) Vertices: a, b, c, d, and e.
   Edges: bd, be, cd, and ce.
   (d) Vertices: x, y, z, and w.
   Edges: xy, xw, yz, and zw.
3) Let G be a simple graph with n vertices. Show that:
   (a) The valence of every vertex is $\leq n - 1$. [*Hint:* No vertex is adjacent to itself.]
   (b) If G has a vertex of valence 0, and $n \geq 2$, then G does *not* have a vertex of valence $n-1$. [*Hint:* Can a vertex of valence $n-1$ be adjacent to a vertex of valence 0?]
4) (a) What is the smallest possible valence of a vertex in a simple graph with 10 vertices?
   (b) What is the largest possible valence of a vertex in a simple graph with 10 vertices?
5) Suppose v is a vertex in a simple graph with 18 vertices. What can you say about the valence of v in the complementary graph?

6) Suppose v is a vertex in a simple graph with an odd number of vertices. If the valence of v is odd, then what can you say about the valence of v in the complementary graph?

7) Create a graph G whose vertices are the numbers $\{1, 2, \ldots, n\}$, with an edge between x and y if and only if $x \neq y$ and $x \mid y$ or $y \mid x$. (See Definition 17.1 for the notation used here.) What vertices have valence 1?

8) (*harder*) Let G be a simple graph with at least 2 vertices. Show there are two different vertices of G that have the same valence.

19B. Isomorphic graphs

It is important to realize that the same graph can usually be drawn in many different ways; all that matters is that the correct vertices are connected by edges, not where the vertices are drawn on the paper, or whether the edges are drawn straight or curved. For example, here are two other ways to draw the graph of Figure 19.4:

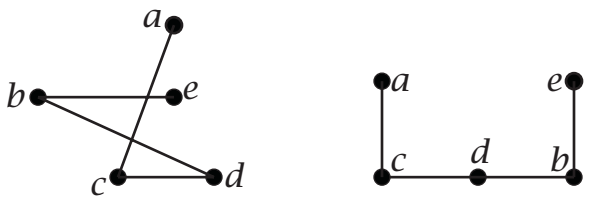
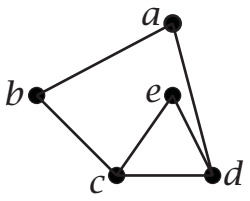
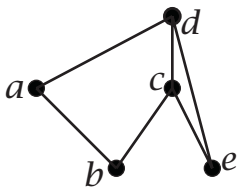


Figure 19.5. Two more drawings of the graph in Figure 19.4. In all three pictures, the edges are ac, cd, db, and be.

EXAMPLE 19.13. The following graph is *not* the same as the graph in Figure 19.1, because the vertices a and e are adjacent in one of them, but not in the other.



However, this graph can be represented by the same picture as Figure 19.1 (ignoring the labels on the dots that represent the vertices), as we see from the following drawing of it. (Verify that, in both drawings, the edges are ab, ad, bc, cd, ce, and de.)



Two graphs that can be represented by the same picture (like the graph in Figure 19.1 and the graph in the above example) are said to be **isomorphic**. This implies that they have the same structure. (The only real difference between them is that the vertices in the two graphs may have been given different names.)

EXERCISES 19.14.

1) Figure 19.6 shows some graphs (A), (B), ..., (I). (Each of them has 4 vertices.) Which of them are isomorphic to which others?

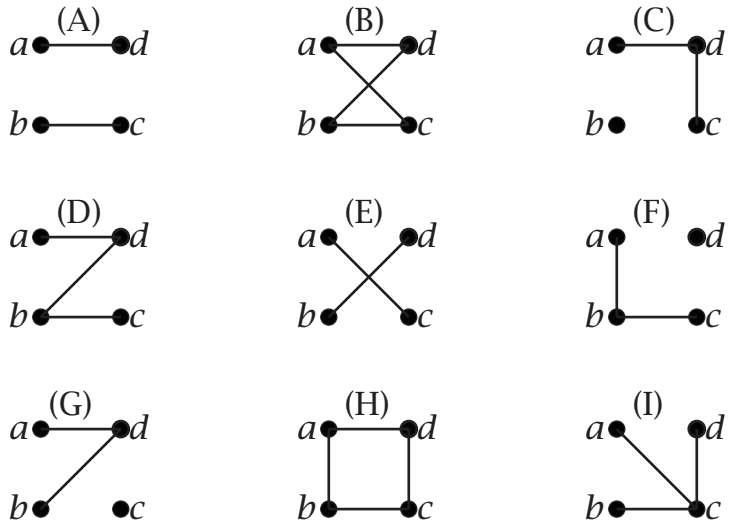


Figure 19.6. Some graphs with 4 vertices.

2) Find a simple graph with 4 vertices that is isomorphic to its complementary graph.

19C. Digraphs

Sometimes a road map or other network has properties that cannot be captured in a graph. An important example of such a property is one-way connections: in a road map, one-way roads; communication nodes that can only receive; wires along which current can only flow in one direction, etc. To allow us to model these situations, we introduce **directed graphs**, which we call "digraphs," for short. Most definitions and basic properties of digraphs are similar to those of graphs, with minor adjustments to take into account the directions on the edges.

DEFINITION 19.15.

1) A **digraph** D consists of a set V of vertices and a set A of arcs.
   - Each vertex of the graph is drawn as a dot.
   - Each arc of the graph is drawn as an arrow (or curved arrow) from one dot to another.
2) V is called the **vertex set** of D, and A is called the **arc set** of D.
3) If there is an arc from u to v, then u is called an **in-neighbour** of v, and v is an **out-neighbour** of u.
4) The number of in-neighbours of a vertex is its **in-valence**; the number of out-neighbours is its **out-valence**.
5) Any pair of oppositely directed arcs (one from u to v and the other from v to u) is called a **digon**.

Remark 19.16. An arc from u to v is often denoted by $\overrightarrow{uv}$. Unlike edges, $\overrightarrow{vu}$ is not the same as $\overrightarrow{uv}$; these arcs have opposite directions!

As for graphs, there are simple digraphs, which do not allow loops, or more than one arc *in the same direction* between two vertices. (Digons are allowed in simple digraphs.) In a simple digraph, the out-valence of any vertex v is equal to the number of arcs that begin at v; similarly, the in-valence of v is equal to the number of arcs that end at v.

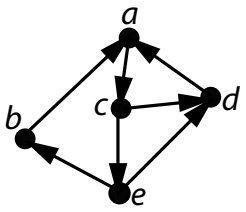


Figure 19.7. A simple directed graph.

EXAMPLE 19.17. Consider the simple digraph drawn in Figure 19.7.

- $V = \{a, b, c, d, e\}$;
- $A = \left\{\overrightarrow{ac}, \overrightarrow{ba}, \overrightarrow{cd}, \overrightarrow{ce}, \overrightarrow{da}, \overrightarrow{eb}, \overrightarrow{ed}\right\}$;
- The only out-neighbour of a is c; the in-neighbours of a are b and d. Thus, the in-valence of a is 2 and the out-valence is 1.

EXERCISE 19.18. Find the in- and out-neighbours and the in- and out-valence of each vertex of the digraph in Figure 19.7. (The answers for vertex a are given in the preceding example.)

The concepts of complement (of a simple digraph) and isomorphism can be extended to digraphs, by adapting the definitions that were given for graphs.

EXERCISES 19.19.

1) In each case:

   (i) Draw the digraph with the given vertices and given arcs (and no others).

   (ii) Find the in-valence and out-valence of each vertex.

   (iii) Draw the complementary digraph.

   (a) Vertices: a, b, c, d, and e.
   Arcs: $\overrightarrow{ab}$, $\overrightarrow{ba}$, $\overrightarrow{bc}$, $\overrightarrow{bd}$, $\overrightarrow{ce}$, $\overrightarrow{ca}$, $\overrightarrow{da}$, and $\overrightarrow{de}$.

   (b) Vertices: a, b, c, d, and e.
   Arcs: $\overrightarrow{ab}$, $\overrightarrow{ac}$, $\overrightarrow{ad}$, $\overrightarrow{ae}$, $\overrightarrow{db}$, and $\overrightarrow{de}$.

   (c) Vertices: a, b, c, d, and e.
   Arcs: $\overrightarrow{bd}$, $\overrightarrow{eb}$, $\overrightarrow{cd}$, $\overrightarrow{ce}$, and $\overrightarrow{da}$.

   (d) Vertices: x, y, z, and w.
   Arcs: $\overrightarrow{xy}$, $\overrightarrow{xw}$, $\overrightarrow{yw}$, $\overrightarrow{zy}$, and $\overrightarrow{zw}$.

2) In each part, draw a simple digraph with 6 vertices that has the specified number of vertices of each out-valence. You may choose the in-valences, as long as the other conditions are met.

   (a) 6 vertices of out-valence 0.

   (b) 6 vertices of out-valence 1.

   (c) 6 vertices of out-valence 2.

(d) 6 vertices of out-valence 3.

(e) 6 vertices of out-valence 4.

(f) 6 vertices of out-valence 5.

(g) 6 vertices of out-valence 6.

(h) 3 vertices of out-valence 3, 2 vertices of out-valence 2, and 1 vertex of out-valence 1.

(i) 3 vertices of out-valence 1, 2 vertices of out-valence 2, and 1 vertex of out-valence 4.

(j) 3 vertices of out-valence 3, and 3 vertices of out-valence 2.

3) Find a simple digraph with 4 vertices that is isomorphic to its complementary digraph.

4) (a) What is the smallest possible out-valence of a vertex in a simple digraph with 10 vertices?

(b) What is the largest possible out-valence of a vertex in a simple digraph with 10 vertices?

19D. Sum of the valences

We will see that the following observation about digraphs has some important consequences for graphs.

LEMMA 19.20. *The number of arcs of any simple digraph is exactly the same as the sum of the in-valences of the vertices of the digraph, which is the same as the sum of the out-valences of the vertices of the digraph.*

PROOF. Let A be the set of arcs of a simple digraph D, so $\#A$ is the number of arcs of D. Also, for convenience, let $v_1, v_2, \ldots, v_n$ be a list of the vertices of D.

For each vertex u_i of D, let A_i be the set of arcs of D that begin at u_i; that is, the arcs $\overrightarrow{u_i v}$, where v is an out-neighbour of u_i. So

(19.21)
$$\#A_i \text{ is the out-valence of } v_i.$$

Note that:

- Every arc of D is of the form $\overrightarrow{u_i u_j}$, for some vertex u_i (and some u_j), so every arc belongs to some A_i. Thus, the union of the sets $A_1, A_2, \ldots, A_n$ is all of A.
- Also, any arc has only one starting vertex u_i, so it cannot belong to two different sets A_i and A_j. Thus, the sets $A_1, A_2, \ldots, A_n$ are pairwise disjoint.

Therefore, applying Proposition 15.17, we conclude that

$$\#A = \#A_1 + \#A_2 + \cdots + \#A_n.$$

Comparing with (19.21), we see that this means $\#A$ is equal to the sum of the out-valences of the vertices.

A similar proof applies to the in-valences; we leave that as an exercise. □

THEOREM 19.22. *The number of edges of any simple graph is exactly one-half of the sum of the valences of the vertices of the graph.*

PROOF. Given a simple graph G, construct a digraph D with the same vertex set V, by replacing each edge of G with 2 oppositely directed arcs with the same endpoints (a digon).

- Since each edge of G has been replaced by 2 arcs, it is clear that the number of arcs of D is exactly twice the number of edges of G.

- By construction, the out-neighbours of any vertex in D are exactly the same as the neighbours of that vertex in G. Thus, the out-valence of any vertex in D is equal to the valence of that vertex in G.

From the lemma, we conclude that the sum of the valences of the vertices of G is exactly twice the number of edges of G. Dividing by 2 yields the desired conclusion. □

This has the following two interesting consequences that are not at all obvious:

COROLLARY 19.23. *The sum of the valences of the vertices of any simple graph is an even number.*

PROOF. Let s be the sum of the valences of the vertices of a simple graph G. Then the theorem tells us that $\frac{1}{2}s$ is the number of edges of G, which is an integer. This means that $\frac{1}{2}s$ is an integer; in other words, s is divisible by 2, so s is even. □

If you know that the sum of an odd number of odd numbers is odd (and that adding an even number to an odd number results in an odd number), then you can see why the following corollary is a consequence of the preceding one.

COROLLARY 19.24. *Any simple graph has an even number of vertices of odd valence.*

EXAMPLE 19.25. As a consequence of this corollary, notice that if every vertex of a simple graph has valence 3, then the graph must have an even number of vertices.

EXERCISES 19.26.

1) For $n = 4$, $n = 6$, and $n = 8$, draw a graph with n vertices, such that every vertex has valence 3.
2) A large number of people were at a party, and each of them shook hands with a certain number of other people. Harold claims that he kept careful track of the events, and found that exactly 55 people shook hands an odd number of times. How do you know that Harold must have made a mistake?

EXERCISE 19.27. Prove that, if G is a simple graph on n vertices in which every vertex has at most 6 neighbours, then the number of edges in G is at most $3n$.

EXERCISE 19.28. In each part, draw a simple graph with 6 vertices that has the specified number of vertices of each valence, or explain why it is not possible.

1) 6 vertices of valence 0.
2) 6 vertices of valence 1.
3) 6 vertices of valence 2.
4) 6 vertices of valence 3.
5) 6 vertices of valence 4.
6) 6 vertices of valence 5.
7) 6 vertices of valence 6.
8) 1 vertex of valence 1, 2 vertices of valence 2, and 3 vertices of valence 3.
9) 3 vertices of valence 1, 2 vertices of valence 2, and 1 vertex of valence 3.
10) 3 vertices of valence 1, and 3 vertices of valence 3.
11) 3 vertices of valence 2, and 3 vertices of valence 3.

EXAMPLE 19.29. For any given collection of vertices, there are two obvious (simple) graphs that can always be drawn:

1) The **empty graph** has no edges.

2) In the **complete graph**, every vertex is adjacent to all of the other vertices.

These two graphs are complementary to each other.

Remark 19.30. Suppose G is a complete graph with n vertices.

1) If v is any vertex of G, then all of the other vertices of G are neighbours of v. Therefore, the valence of each vertex of G is $n - 1$.

2) Combining Theorem 19.22 with the preceding determination of the valences, we calculate that the number of edges of G is $n(n-1)/2$.

No simple graph with n vertices can have more edges than the complete graph, so we conclude that the number of edges in a simple graph with n vertices is never more than $n(n-1)/2$.

EXERCISE 19.31.

1) What is the smallest possible number of edges in a simple graph with 10 vertices?

2) What is the largest possible number of edges in a simple graph with 10 vertices?

EXERCISE 19.32. Draw a simple graph with exactly 12 edges, using as few vertices as possible.

EXERCISE 19.33. A certain simple graph with 25 vertices has 250 edges. How many edges does its complement have?

EXERCISE 19.34. Let G be a simple graph on n vertices, and suppose that G is isomorphic to its complement. Prove that we must have $n \equiv 0 \pmod 4$ or $n \equiv 1 \pmod 4$. [*Hint:* Consider how many edges G must have.]

SUMMARY:

- Important definitions:
  - graph, simple graph
  - digraph, simple digraph
  - vertices, edges, arcs, digons
  - adjacent, neighbours, valence, incident, in-neighbours, out-neighbours, in-valence, out-valence
  - complement
  - empty graph, complete graph
  - isomorphic
- The number of edges in a simple graph is half the sum of the valences of the vertices.
- Every simple graph has an even number of vertices of odd valence.
- Notation:
  - for graphs: V, E, uv
  - for digraphs: V, A, $\overrightarrow{uv}$

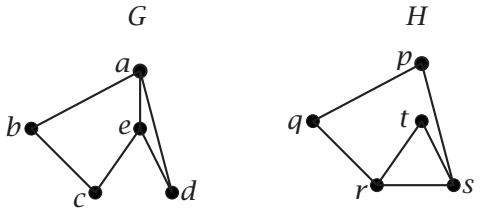
Chapter 20

Isomorphisms

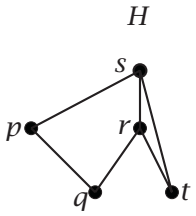
One cannot really argue with a mathematical theorem.
Stephen Hawking (b. 1942), British physicist
A Brief History of Time

20A. Definition and examples

In Chapter 19, we said that two graphs are **isomorphic** if they can be represented by the same picture (ignoring the labels on the dots that represent the vertices). For example, although the following two graphs G and H look different, they are actually isomorphic.



This is because H can be represented by the following picture, which looks just like G:



Now that we are using the same picture for both graphs, the vertices of G can be matched up with the vertices of H, by pairing each vertex of G with the vertex of H that appears in the same place in the drawing:

vertex of G	vertex of H
a	s
b	p
c	q
d	t
e	r

This yields a bijection from the set of vertices of G to the set of vertices of H. Furthermore, one can easily verify that if two vertices of G are adjacent, then the corresponding two vertices of H are adjacent (and vice-versa). This observation is the basis of the following official definition of "isomorphic."

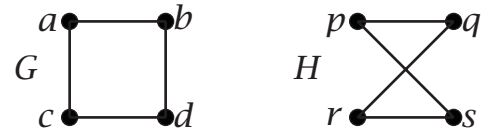
NOTATION 20.1. Suppose v and w are vertices in a graph G. For convenience, let us write $v \overset{G}{\text{---}} w$ to denote that v and w are adjacent.

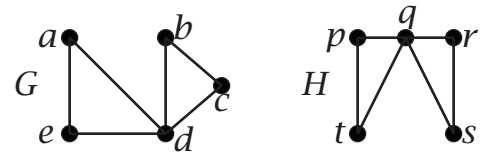
DEFINITION 20.2. Suppose G and H are graphs, with vertex sets V and W, respectively.

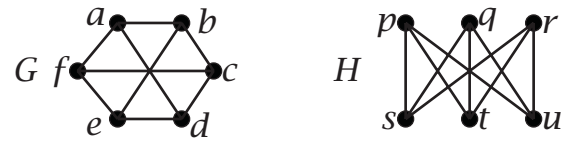
1) A function $\varphi\colon V \to W$ is an **isomorphism from G to H** if and only if
   (a) φ is a bijection, and
   (b) for all $v_1, v_2 \in V$, we have
   $$v_1 \overset{G}{\text{---}} v_2 \text{ iff } \varphi(v_1) \overset{H}{\text{---}} \varphi(v_2).$$
2) G and H are **isomorphic** if and only if there exists an isomorphism from G to H. In this case, we may also say that G **is isomorphic to** H.

NOTATION 20.3. We write $G \cong H$ to denote that G is isomorphic to H.

EXERCISE 20.4. For each pair of graphs G and H, find an isomorphism φ from G to H. (Write φ as a set of ordered pairs.)

1)


2)


3)


EXERCISES 20.5. Draw all nonisomorphic simple graphs on n vertices with the following properties:

1) $n = 4$, and the graphs have 3 edges.
2) $n = 5$, and the vertices have valences 1, 2, 2, 2, and 3.
3) $n = 6$, and the vertices have valences 1, 1, 1, 2, 2, and 3.

20B. Proofs that isomorphisms preserve graph-theoretic properties

Since isomorphic graphs can be drawn with the same picture, it should be the case that whatever you say about the picture of one of the graphs is also be true about this other. Here are some examples of how to prove precise assertions of this type by using the definition of isomorphism:

PROPOSITION 20.6. *Let G and H be graphs, such that G is isomorphic to H. If H is a complete graph, then G is a complete graph.*

PROOF. Assume H is a complete graph. We wish to show that G is a complete graph. In other words, we wish to show that every vertex in G is adjacent to all of the other vertices in G.

Given two vertices v_1 and v_2 of G, such that $v_1 \neq v_2$, it suffices to show that $v_1 \overset{G}{\text{---}} v_2$. Let V be the vertex set of G, and let W be the vertex set of H. Since G and H are isomorphic, there is an isomorphism φ from G to H. Then $\varphi\colon V \to W$, so

$$\varphi(v_1), \varphi(v_2) \in W.$$

Since φ is an isomorphism, it is one-to-one, so we have $\varphi(v_1) \neq \varphi(v_2)$. Hence, $\varphi(v_1)$ and $\varphi(v_2)$ are two distinct vertices of H. Since H is complete, this implies that $\varphi(v_1) \overset{H}{\text{---}} \varphi(v_2)$. Since φ is an isomorphism, we conclude that $v_1 \overset{G}{\text{---}} v_2$, as desired. □

PROPOSITION 20.7. *Suppose G and H are simple graphs, φ is an isomorphism from G to H, and u is a vertex of G. Let N be the set of neighbours of u in G. Then $\varphi(N)$ is the set of neighbours of $\varphi(u)$ in H.*

PROOF. We wish to show, for every vertex w of H, that

$$w \in \varphi(N) \quad \Leftrightarrow \quad w \text{ is a neighbour of } \varphi(u).$$

To this end, let w be an arbitrary vertex of H.

($\Rightarrow$) Assume $w \in \varphi(N)$. This means there is some $v \in N$, such that $w = \varphi(v)$. Now, since $v \in N$, we know v is a neighbour of u, so $u \overset{G}{\text{---}} v$. Because φ is an isomorphism, this implies $\varphi(u) \overset{H}{\text{---}} \varphi(v) = w$. So w is a neighbour of $\varphi(u)$.

($\Leftarrow$) Assume w is a neighbour of $\varphi(u)$. This means $\varphi(u) \overset{H}{\text{---}} w$. Since φ, being an isomorphism, is onto, there is some vertex v of G, such that $w = \varphi(v)$. Hence $\varphi(u) \overset{H}{\text{---}} w = \varphi(v)$. Since φ is an isomorphism, we conclude that $u \overset{G}{\text{---}} v$. So v is a neighbour of u, which means $v \in N$. Therefore

$$w = \varphi(v) \in \varphi(N).$$

COROLLARY 20.8. *Let G and H be simple graphs, such that G is isomorphic to H, and let k be any natural number. If G has a vertex of valence k, then H has a vertex of valence k.*

PROOF. Assume G has a vertex u of valence k. This means that u has exactly k neighbours in G, so $\#N = k$, where N is the set of neighbours of u. Since φ is one-to-one, Exercise 15.11 tells us that

(20.9)
$$\#\,\varphi(N) = \#N.$$

Moreover, Proposition 20.7 tells us that $\varphi(N)$ is the set of neighbours of $\varphi(u)$ in H. Hence, Equation (20.9) tells us that the number of neighbours of $\varphi(u)$ in H is equal to the number of neighbours of u in G, which is k. So $\varphi(u)$ is a vertex of valence k in H. □

The following symmetry property of isomorphisms is very important.

EXERCISES 20.10 ("isomorphism is symmetric"). Assume that G and H are graphs.

1) Show that if φ is an isomorphism from G to H, then φ^{-1} is an isomorphism from H to G.
2) Show that if G is isomorphic to H, then H is isomorphic to G.

The symmetry is important because it allows us to turn "if–then" statements into "if and only iff" statements. For example, Proposition 20.6, and Corollary 20.8 are stated as "if–then," but they imply the corresponding "if and only if" statements.

COROLLARY 20.11. *Let G and H be graphs, such that G is isomorphic to H. Then G is a complete graph if and only if H is a complete graph.*

PROOF. ($\Leftarrow$) This is the assertion of Proposition 20.6.

($\Rightarrow$) Since isomorphism is symmetric, we know that if G is isomorphic to H, then H is isomorphic to G. Thus, we can apply Proposition 20.6 with G and H interchanged. (That is, we replace G with H and replace H with G. See Remark 20.12 if this is confusing.) We thereby conclude that if G is complete, then H is complete. This is what we wanted. □

Remark 20.12. To avoid confusion, let us rewrite the proof of Corollary 20.11($\Rightarrow$) in more detail. It is helpful to introduce some notation: for any graphs X and Y, such that X is isomorphic to Y, Proposition 20.6 tells us that

(20.13)

$$\text{if } Y \text{ is complete, then } X \text{ is complete.}$$

For example, letting $X = G$ and $Y = H$, we know, by assumption, that G is isomorphic to H, so:

$$\text{if } H \text{ is complete, then } G \text{ is complete.}$$

That is simply the conclusion of Proposition 20.6. It is more interesting to interchange the two graphs:

$$\text{Let } X = H \text{ and } Y = G.$$

By assumption, $Y = G$ is isomorphic to $H = X$. Because isomorphism is symmetric, this implies X is isomorphic to Y. So (20.13) tells us that if Y is complete, then X is complete; i.e., if G is complete, then H is complete. This is the *converse* of the conclusion of Proposition 20.6.

The argument that G and H can be interchanged (as described more fully in the preceding remark) is usually condensed to "by symmetry," as in the following examples. The crucial point is that, although it is assumed that G is isomorphic to H, this is the same as assuming that H is isomorphic to G, so the two graphs are interchangeable.

COROLLARY 20.14. *Let G and H be simple graphs, such that G is isomorphic to H, and let k be any natural number. Then G has a vertex of valence k if and only if H has a vertex of valence k.*

PROOF. By symmetry, it suffices to show that if G has a vertex of valence k, then H has a vertex of valence k. This is precisely the conclusion of Corollary 20.8. □

One of the fundamental problems in graph theory is to colour the vertices of a graph, in such a way that adjacent vertices have different colours:

DEFINITION 20.15. Let G be a graph with vertex set V. For any $k \in \mathbb{N}^+$, a k-**colouring** of G is a function $f\colon V \to \{1, 2, 3, \ldots, k\}$, such that, for all $u, v \in V$,

$$\text{if } u \overset{G}{\text{---}} v, \text{ then } f(u) \neq f(v).$$

PROPOSITION 20.16. *Let G and H be simple graphs, such that G is isomorphic to H, and let k be any natural number. Then G has a k-colouring if and only if G has a k-colouring.*

PROOF. By symmetry, it suffices to show that if H has a k-colouring, then G has a k-colouring. Let V and W be the vertex sets of G and H, respectively, and assume H has a k-colouring $f\colon W \to \{1, 2, 3, \ldots, k\}$. Since G is isomorphic to H, there is an isomorphism φ from G to H.

We claim that the composition $f \circ \varphi$ of f with φ is a k-colouring of G. To see this, let u and v be arbitrary vertices of G, such that $u \overset{G}{\text{---}} v$. Since φ is an isomorphism, we know $\varphi(u) \overset{H}{\text{---}} \varphi(v)$. Because f is a k-colouring of H, this implies $f\big(\varphi(u)\big) \neq f\big(\varphi(v)\big)$. In other

words, $(f \circ \varphi)(u) \neq (f \circ \varphi)(v)$. Since u and v are arbitrary adjacent vertices in G, we conclude that $f \circ \varphi$ is a k-colouring of G. □

EXERCISES 20.17. Let G and H be simple graphs, such that G is isomorphic to H.

1) Show that G and H have the same number of vertices.
2) Show that G is an empty graph if and only if H is an empty graph.
3) Show that G has more than one vertex of valence 3 if and only if H has more than one vertex of valence 3.
4) Show that all of the vertices of valence 3 in G are adjacent to each other if and only if all of the vertices of valence 3 in H are adjacent to each other.
5) A **triangle** in G consists of three distinct vertices u, v, w of G, such that each of these vertices is adjacent to the other two. Show that G has a triangle if and only if H has a triangle.

We already know that isomorphism is symmetric. Here are two additional properties:

EXERCISES 20.18. These exercises show that isomorphism is an equivalence relation on the set of all graphs.

1) Show that isomorphism is "reflexive." This means G is isomorphic to G, for any simple graph G.
2) Show that isomorphism is "transitive." This means that if G is isomorphic to H, and H is isomorphic to K, then G is isomorphic to K, for any simple graphs G, H, and K.

EXERCISE 20.19. Using the equivalence relation "isomorphic" on graphs, answer the following questions and justify your answers.

1) How many equivalence classes are there of simple graphs on 4 vertices?
2) How many equivalence classes are there of simple graphs on 5 vertices, where the vertices must have valences 1, 2, 2, 2, and 3?
3) How many equivalence classes are there of simple graphs on 6 vertices, where the vertices must have valences 1, 1, 1, 2, 2, and 3?

SUMMARY:

- Important definitions:
  - isomorphism from G to H
  - isomorphic graphs
- Suppose G is isomorphic to H. Then G is $\square$ iff H is $\square$. (Any "graph-theoretic property" can go in the box.)
- The inverse of an isomorphism is an isomorphism.
- If G is isomorphic to H, then H is isomorphic to G.

Index of Definitions